On the Expressiveness and Semantics of Information Flow Types (Technical appendix)

Vineet Rajani and Deepak Garg

MPI-SWS

December 6, 2019

Contents

1 Fine-grained IFC enforcement (FG)

1.1 FG type system

Syntax, types, constraints:

Expressions	e	$::=$	$x \mid \lambda x.e \mid e\ e \mid (e,e) \mid \mathsf{fst}(e) \mid \mathsf{snd}(e) \mid \mathsf{inl}(e) \mid \mathsf{inr}(e) \mid \mathsf{case}(e, x.e, x.e) \mid \mathsf{new}\ e \mid !e \mid e := e \mid \Lambda e \mid e\ [] \mid \nu\ e \mid e\ \bullet$
Labels	ℓ, pc	$::=$	$l \mid \alpha \mid \ell \sqcup \ell \mid \ell \sqcap \ell$
(Labeled) Types	τ	$::=$	A^ℓ
Unlabeled types	A	$::=$	$\mathsf{b} \mid \tau \xrightarrow{\ell_e} \tau \mid \tau \times \tau \mid \tau + \tau \mid \mathsf{ref}\ \tau \mid \mathsf{unit} \mid \forall \alpha.(\ell_e, \tau) \mid c \stackrel{\ell_e}{\Rightarrow} \tau$
Constraints	c	$::=$	$\ell \sqsubseteq \ell \mid (c, c)$

Lemma 1.1 (FG: Reflexivity of subtyping)**.** *The following hold:*

1. *For all* Σ, Ψ, τ*:* $\Sigma; \Psi \vdash \tau <: \tau$
2. *For all* Σ, Ψ, A*:* $\Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}$

Proof. Proof by simultaneous induction on τ and A.

Proof of statement (1)

Let $\tau = \mathsf{A}^\ell$. Then, we have:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}}\ \text{IH(2)} \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell}{\Sigma; \Psi \vdash \mathsf{A}^\ell <: \mathsf{A}^\ell}\ \text{FGsub-label}$$

Proof of statement (2)

We proceed by cases on A.

1. $\mathsf{A} = \mathsf{b}$:

$$\dfrac{}{\Sigma; \Psi \vdash \mathsf{b} <: \mathsf{b}}\ \text{FGsub-base}$$

2. $\mathsf{A} = \mathsf{ref}\ \tau$:

$$\dfrac{}{\Sigma; \Psi \vdash \mathsf{ref}\ \tau <: \mathsf{ref}\ \tau}\ \text{FGsub-ref}$$

3. $\mathsf{A} = \tau_1 \times \tau_2$:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\ \text{IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\ \text{IH(1) on } \tau_2}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1 \times \tau_2}$$

4. $\mathsf{A} = \tau_1 + \tau_2$:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\ \text{IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\ \text{IH(1) on } \tau_2}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1 + \tau_2}$$

Type system: $\boxed{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau}$

$$\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash_{pc} x : \tau}\ \text{FG-var} \qquad \frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{\ell_e} e : \tau_2}{\Sigma; \Psi; \Gamma \vdash_{pc} \lambda x.e : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\perp}}\ \text{FG-lam}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 \searrow \ell \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1\ e_2 : \tau_2}\ \text{FG-app}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : \tau_1 \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_2}{\Sigma; \Psi; \Gamma \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^{\perp}}\ \text{FG-prod}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^{\ell} \qquad \Sigma; \Psi \vdash \tau_1 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{fst}(e) : \tau_1}\ \text{FG-fst} \qquad \frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau_1}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inl}(e) : (\tau_1 + \tau_2)^{\perp}}\ \text{FG-inl}$$

$$\frac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 + \tau_2)^{\ell} \\ \Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_1 : \tau \qquad \Sigma; \Psi; \Gamma, y : \tau_2 \vdash_{pc \sqcup \ell} e_2 : \tau \qquad \Sigma; \Psi \vdash \tau \searrow \ell\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{case}(e, x.e_1, y.e_2) : \tau}\ \text{FG-case}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc'} e : \tau' \qquad \Sigma; \Psi \vdash pc \sqsubseteq pc' \qquad \Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau}\ \text{FG-sub}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau \qquad \Sigma; \Psi \vdash \tau \searrow pc}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{new}\ e : (\mathsf{ref}\ \tau)^{\perp}}\ \text{FG-ref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\mathsf{ref}\ \tau)^{\ell} \qquad \Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \tau' \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} !e : \tau'}\ \text{FG-deref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\mathsf{ref}\ \tau)^{\ell} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau \qquad \Sigma; \Psi \vdash \tau \searrow (pc \sqcup \ell)}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 := e_2 : \mathsf{unit}}\ \text{FG-assign}$$

$$\frac{}{\Sigma; \Psi; \Gamma \vdash_{pc} () : \mathsf{unit}^{\perp}}\ \text{FG-unitI} \qquad \frac{\Sigma, \alpha; \Psi; \Gamma \vdash_{\ell_e} e : \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} \Lambda e : (\forall \alpha.(\ell_e, \tau))^{\perp}}\ \text{FG-FI}$$

$$\frac{\begin{array}{c}\qquad\qquad\qquad \Sigma; \Psi; \Gamma \vdash_{pc} e : (\forall \alpha.(\ell_e, \tau))^{\ell} \\ FV(\ell') \subseteq \Sigma \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e[\ell'/\alpha] \qquad \Sigma; \Psi \vdash \tau[\ell'/\alpha] \searrow \ell\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} e\ [] : \tau[\ell'/\alpha]}\ \text{FG-FE}$$

$$\frac{\Sigma; \Psi, c; \Gamma \vdash_{\ell_e} e : \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} \nu\ e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\perp}}\ \text{FG-CI}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell} \qquad \Sigma; \Psi \vdash c \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e \qquad \Sigma; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e \bullet : \tau}\ \text{FG-CE}$$

Figure 1: Type system for FG

$$\frac{\Sigma;\Psi \vdash \ell \sqsubseteq \ell' \qquad \Sigma;\Psi \vdash \mathsf{A} <: \mathsf{A}'}{\Sigma;\Psi \vdash \mathsf{A}^{\ell} <: \mathsf{A}'^{\ell'}}\text{ FGsub-label} \qquad \frac{}{\Sigma;\Psi \vdash \mathsf{b} <: \mathsf{b}}\text{ FGsub-base}$$

$$\frac{}{\Sigma;\Psi \vdash \mathsf{ref}\ \tau <: \mathsf{ref}\ \tau}\text{ FGsub-ref} \qquad \frac{\Sigma;\Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma;\Psi \vdash \tau_2 <: \tau_2'}{\Sigma;\Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}\text{ FGsub-prod}$$

$$\frac{\Sigma;\Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma;\Psi \vdash \tau_2 <: \tau_2'}{\Sigma;\Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'}\text{ FGsub-sum}$$

$$\frac{\Sigma;\Psi \vdash \tau_1' <: \tau_1 \qquad \Sigma;\Psi \vdash \tau_2 <: \tau_2' \qquad \Sigma;\Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma;\Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'}\text{ FGsub-arrow}$$

$$\frac{}{\Sigma;\Psi \vdash \mathsf{unit} <: \mathsf{unit}}\text{ FGsub-unit} \qquad \frac{\Sigma,\alpha;\Psi \vdash \tau_1 <: \tau_2 \qquad \Sigma,\alpha;\Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma;\Psi \vdash \forall\alpha.(\ell_e,\tau_1) <: \forall\alpha.(\ell_e',\tau_2)}\text{ FGsub-forall}$$

$$\frac{\Sigma;\Psi \vdash c_2 \implies c_1 \qquad \Sigma;\Psi,c_2 \vdash \tau_1 <: \tau_2 \qquad \Sigma;\Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma;\Psi \vdash c_1 \overset{\ell_e}{\Rightarrow} \tau_1 <: c_2 \overset{\ell_e'}{\Rightarrow} \tau_2}\text{ FGsub-constraint}$$

Figure 2: FG subtyping

$$\frac{\Sigma;\Psi \vdash \mathsf{A}\ WF \qquad \mathrm{FV}(\ell) \in \Sigma}{\Sigma;\Psi \vdash \mathsf{A}^{\ell}\ WF}\text{ FG-wff-label} \qquad \frac{}{\Sigma;\Psi \vdash \mathsf{b}\ WF}\text{ FG-wff-base}$$

$$\frac{}{\Sigma;\Psi \vdash \mathsf{unit}\ WF}\text{ FG-wff-unit} \qquad \frac{\Sigma;\Psi \vdash \tau_1\ WF \qquad \Sigma;\Psi \vdash \tau_2\ WF \qquad \mathrm{FV}(\ell_e) \in \Sigma}{\Sigma;\Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2\ WF}\text{ FG-wff-arrow}$$

$$\frac{\Sigma;\Psi \vdash \tau_1\ WF \qquad \Sigma;\Psi \vdash \tau_2\ WF}{\Sigma;\Psi \vdash \tau_1 \times \tau_2\ WF}\text{ FG-wff-prod} \qquad \frac{\Sigma;\Psi \vdash \tau_1\ WF \qquad \Sigma;\Psi \vdash \tau_2\ WF}{\Sigma;\Psi \vdash \tau_1 + \tau_2\ WF}\text{ FG-wff-sum}$$

$$\frac{\mathrm{FV}(\tau) = \emptyset}{\Sigma;\Psi \vdash (\mathsf{ref}\ \tau)\ WF}\text{ FG-wff-ref} \qquad \frac{\Sigma,\alpha;\Psi \vdash \tau\ WF \qquad \mathrm{FV}(\ell_e) \in \Sigma \cup \{\alpha\}}{\Sigma;\Psi \vdash (\forall\alpha.(\ell_e,\tau))\ WF}\text{ FG-wff-forall}$$

$$\frac{\Sigma;\Psi \vdash \tau\ WF \qquad \mathrm{FV}(c) \in \Sigma \qquad \mathrm{FV}(\ell_e) \in \Sigma}{\Sigma;\Psi \vdash (c \overset{\ell_e}{\Rightarrow} \tau))\ WF}\text{ FG-wff-constraint}$$

Figure 3: Well-formedness relation for FG

5. $\mathsf{A} = \tau_1 \overset{\ell_e}{\to} \tau_2$:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\text{ IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash \tau_2 <: \tau_2}\text{ IH(2) on } \tau_2 \qquad \dfrac{}{\Sigma; \Psi \vdash \ell_e \sqsubseteq \ell_e}}{\Sigma; \Psi \vdash \tau_1 \overset{\ell_e}{\to} \tau_2 <: \tau_1 \overset{\ell_e}{\to} \tau_2}$$

6. $\mathsf{A} = \mathsf{unit}$:

$$\dfrac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}}$$

7. $\mathsf{A} = \forall \alpha.\tau_i$:

$$\dfrac{\dfrac{}{\Sigma, \alpha; \Psi \vdash \tau_i <: \tau_i}\text{ IH(1) on } \tau_i}{\Sigma; \Psi \vdash \forall \alpha.\tau_i <: \forall \alpha.\tau_i}$$

8. $\mathsf{A} = c \Rightarrow \tau_i$:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash c \implies c} \qquad \dfrac{}{\Sigma; \Psi, c \vdash \tau_i <: \tau_i}\text{ IH(1) on } \tau_i}{\Sigma; \Psi \vdash c \Rightarrow \tau <: c \Rightarrow \tau_i}$$

□

1.2 FG semantics

Judgement: $(H, e) \Downarrow_i (H', v)$

The semantics are described in Figure 4

1.3 Model for FG

$W : ((Loc \mapsto Type) \times (Loc \mapsto Type) \times (Loc \leftrightarrow Loc))$

Definition 1.2 (FG: θ_2 extends θ_1)**.** $\theta_1 \sqsubseteq \theta_2 \triangleq$
$\forall a \in \theta_1.\theta_1(a) = \tau \implies \theta_2(a) = \tau$

Definition 1.3 (FG: W_2 extends W_1)**.** $W_1 \sqsubseteq W_2 \triangleq$

1. $\forall i \in \{1, 2\}.\ W_1.\theta_i \sqsubseteq W_2.\theta_i$
2. $\forall p \in (W_1.\hat{\beta}).p \in (W_2.\hat{\beta})$

$$\frac{(H, e_1) \Downarrow_i (H', \lambda x.e_i) \qquad (H', e_2) \Downarrow_j (H'', v_2) \qquad (H'', e_i[v_2/x]) \Downarrow_k (H''', v_3)}{(H, e_1\ e_2) \Downarrow_{i+j+k+1} (H''', v_3)} \text{ fg-app}$$

$$\frac{(H, e_1) \Downarrow_i (H', v_1) \qquad (H', e_2) \Downarrow_j (H'', v_2)}{(H, (e_1, e_2)) \Downarrow_{i+j+1} (H'', (v_1, v_2))} \text{ fg-prod} \qquad \frac{(H, e) \Downarrow_i (H', (v_1, v_2))}{(H, \mathsf{fst}(e)) \Downarrow_{i+1} (H', v_1)} \text{ fg-fst}$$

$$\frac{(H, e) \Downarrow_i (H', (v_1, v_2))}{(H, \mathsf{snd}(e)) \Downarrow_{i+1} (H', v_2)} \text{ fg-snd} \qquad \frac{(H, e) \Downarrow_i (H', v)}{(H, \mathsf{inl}(e)) \Downarrow_{i+1} (H', \mathsf{inl}(v))} \text{ fg-inl}$$

$$\frac{(H, e) \Downarrow_i (H', v)}{(H, \mathsf{inr}(e)) \Downarrow_{i+1} (H', \mathsf{inr}(v))} \text{ fg-inr} \qquad \frac{(H, e) \Downarrow_i (H', \mathsf{inl}\ v) \qquad (H', e_1[v/x]) \Downarrow_j (H'', v_1)}{(H, \mathsf{case}(e, x.e_1, y.e_2)) \Downarrow_{i+j+1} (H'', v_1)} \text{ fg-case1}$$

$$\frac{(H, e) \Downarrow_i (H', \mathsf{inr}\ v) \qquad (H', e_2[v/x]) \Downarrow_j (H'', v_2)}{(H, \mathsf{case}(e, x.e_1, y.e_2)) \Downarrow_{i+j+1} (H'', v_2)} \text{ fg-case2}$$

$$\frac{(H, e) \Downarrow_i (H', \Lambda\ e_i) \qquad (H', e_i) \Downarrow_j (H'', v)}{(H, e[]) \Downarrow_{i+j+1} (H'', v)} \text{ fg-FE}$$

$$\frac{(H, e) \Downarrow_i (H', \nu\ e_i) \qquad (H', e_i) \Downarrow_j (H'', v)}{(H, e\bullet) \Downarrow_{i+j+1} (H'', v)} \text{ fg-CE}$$

$$\frac{(H, e) \Downarrow_i (H', v) \qquad a \notin dom(H)}{(H, \mathsf{new}\ (e)) \Downarrow_{i+1} (H'[a \mapsto v], a)} \text{ fg-ref} \qquad \frac{(H, e) \Downarrow_i (H', a)}{(H, !e) \Downarrow_{i+1} (H', H(a))} \text{ fg-deref}$$

$$\frac{(H, e_1) \Downarrow_i (H', a) \qquad (H', e_2) \Downarrow_j (H'', v)}{(H, e_1 := e_2) \Downarrow_{i+j+1} (H''[a \mapsto v], ())} \text{ fg-assign} \qquad \frac{e \in \{x, \lambda y.-, \Lambda -, \nu -\}}{(H, e) \Downarrow_0 (H, e)} \text{ fg-val}$$

Figure 4: FG semantics

Definition 1.4 (FG: Binary value relation).

$$
\begin{array}{lll}
\lceil \mathsf{b} \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, v_1, v_2) \mid v_1 = v_2 \wedge \{v_1, v_2\} \in [\![\mathsf{b}]\!]\} \\
\lceil \mathsf{unit} \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, (), ()) \mid () \in [\![\mathsf{b}]\!]\} \\
\lceil \tau_1 \times \tau_2 \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, (v_1, v_2), (v_1', v_2')) \mid (W, n, v_1, v_1') \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \wedge (W, n, v_2, v_2') \in \lceil \tau_2 \rceil_V^{\mathcal{A}}\} \\
\lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, \mathsf{inl}\ v, \mathsf{inl}\ v') \mid (W, n, v, v') \in \lceil \tau_1 \rceil_V^{\mathcal{A}}\} \cup \\
& & \{(W, n, \mathsf{inr}\ v, \mathsf{inr}\ v') \mid (W, n, v, v') \in \lceil \tau_2 \rceil_V^{\mathcal{A}}\} \\
\lceil \tau_1 \xrightarrow{\ell_e} \tau_2 \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, \lambda x.e_1, \lambda x.e_2) \mid \\
& & \forall W' \sqsupseteq W, j < n, v_1, v_2. \\
& & ((W', j, v_1, v_2) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \implies (W', j, e_1[v_1/x], e_2[v_2/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}}) \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_1, j, v_c. \\
& & ((\theta_l, j, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, j, e_1[v_c/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e}) \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_2, j, v_c. \\
& & ((\theta_l, j, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, j, e_2[v_c/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e})\} \\
\lceil \forall \alpha.(\ell_e, \tau) \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, \Lambda e_1, \Lambda e_2) \mid \\
& & \forall W' \sqsupseteq W, n' < n, \ell' \in \mathcal{L}. \\
& & ((W', n', e_1, e_2) \in \lceil \tau[\ell'/\alpha] \rceil_E^{\mathcal{A}}) \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_1, j, \ell'' \in \mathcal{L}.((\theta_l, j, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\ell_e[\ell''/\alpha]}) \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_2, j, \ell'' \in \mathcal{L}.((\theta_l, j, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\ell_e[\ell''/\alpha]})\} \\
\lceil c \overset{\ell_e}{\Rightarrow} \tau \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, \nu e_1, \nu e_2) \mid \\
& & \forall W' \sqsupseteq W, n' < n. \\
& & \mathcal{L} \models c \implies (W', n', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}} \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c \implies (\theta_l, j, e_1) \in \lfloor \tau \rfloor_E^{\ell_e} \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c \implies (\theta_l, j, e_2) \in \lfloor \tau \rfloor_E^{\ell_e}\} \\
\lceil \mathsf{ref}\ \tau \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, a_1, a_2) \mid \\
& & (a_1, a_2) \in W.\hat{\beta} \wedge W.\theta_1(a_1) = W.\theta_2(a_2) = \tau\}
\end{array}
$$

$$
\lceil \mathsf{A}^{\ell'} \rceil_V^{\mathcal{A}} \triangleq \begin{cases} \{(W, n, v_1, v_2) \mid (W, n, v_1, v_2) \in \lceil \mathsf{A} \rceil_V^{\mathcal{A}}\} & \ell' \sqsubseteq \mathcal{A} \\ \{(W, n, v_1, v_2) \mid \forall i \in \{1, 2\}.\forall m.(W(n).\theta_i, m, v_i) \in \lfloor \mathsf{A} \rfloor_V\} & \ell' \not\sqsubseteq \mathcal{A} \end{cases}
$$

Definition 1.5 (FG: Binary expression relation).

$$
\begin{array}{lll}
\lceil \tau \rceil_E^{\mathcal{A}} & \triangleq & \{(W, n, e_1, e_2) \mid \\
& & \forall H_1, H_2, j < n.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \\
& & (H_1, e_1) \Downarrow_j (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2') \implies \\
& & \exists W' \sqsupseteq W.(n - j, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - j, v_1', v_2') \in \lceil \tau \rceil_V^{\mathcal{A}}\}
\end{array}
$$

Definition 1.6 (FG: Unary value relation).

$$
\begin{array}{lll}
\lfloor \mathsf{b} \rfloor_V & \triangleq & \{(\theta, m, v) \mid v \in [\![\mathsf{b}]\!]\} \\
\lfloor \mathsf{unit} \rfloor_V & \triangleq & \{(\theta, m, v \mid v \in [\![\mathsf{unit}]\!]\} \\
\lfloor \tau_1 \times \tau_2 \rfloor_V & \triangleq & \{(\theta, m, (v_1, v_2)) \mid (\theta, m, v_1) \in \lfloor \tau_1 \rfloor_V \wedge (\theta, m, v_2) \in \lfloor \tau_2 \rfloor_V\} \\
\lfloor \tau_1 + \tau_2 \rfloor_V & \triangleq & \{(\theta, m, \mathsf{inl}\ v) \mid (\theta, m, v) \in \lfloor \tau_1 \rfloor_V\} \cup \{(\theta, m, \mathsf{inr}\ v) \mid (\theta, m, v) \in \lfloor \tau_2 \rfloor_V\} \\
\lfloor \tau_1 \xrightarrow{\ell_e} \tau_2 \rfloor_V & \triangleq & \{(\theta, m, \lambda x.e) \mid \forall \theta'.\theta \sqsubseteq \theta' \wedge \forall j < m.\forall v.(\theta', j, v) \in \lfloor \tau_1 \rfloor_V \implies \\
& & (\theta', j, e[v/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e}\} \\
\lfloor \forall \alpha.(\ell_e, \tau) \rfloor_V & \triangleq & \{(\theta, m, \Lambda e) \mid \forall \theta'.\theta \sqsubseteq \theta'.\forall m' < m.\forall \ell' \in \mathcal{L}.(\theta', m', e) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\ell_e[\ell'/\alpha]}\} \\
\lfloor c \overset{\ell_e}{\Rightarrow} \tau) \rfloor_V & \triangleq & \{(\theta, m, \nu e) \mid \forall \theta'.\theta \sqsubseteq \theta'.\forall m' < m.\mathcal{L} \models c \implies (\theta', m', e) \in \lfloor \tau \rfloor_E^{\ell_e}\} \\
\lfloor \mathsf{ref}\ \tau \rfloor_V & \triangleq & \{(\theta, m, a) \mid \theta(a) = \tau\}
\end{array}
$$

$$\lfloor \mathsf{A}^{\ell'} \rfloor_V \triangleq \lfloor \mathsf{A} \rfloor_V$$

Definition 1.7 (FG: Unary expression relation).

$$\begin{array}{rcl}\lfloor \tau \rfloor_E^{pc} & \triangleq & \{(\theta, n, e) \mid \forall H.(n, H) \rhd \theta \wedge \forall j < n.(H, e) \Downarrow_j (H', v') \implies \\ & & \exists \theta'.\theta \sqsubseteq \theta' \wedge (n - j, H') \rhd \theta' \wedge (\theta', n - j, v') \in \lfloor \tau \rfloor_V \wedge \\ & & (\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge \\ & & (\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc)\}\end{array}$$

Definition 1.8 (FG: Unary heap well formedness).

$$(n, H) \rhd \theta \quad \triangleq \quad dom(\theta) \subseteq dom(H) \wedge \forall a \in dom(\theta).(\theta, n - 1, H(a)) \in \lfloor \theta(a) \rfloor_V$$

Definition 1.9 (FG: Binary heap well formedness).

$$\begin{array}{rcl}(n, H_1, H_2) \overset{\mathcal{A}}{\rhd} W & \triangleq & dom(W.\theta_1) \subseteq dom(H_1) \wedge dom(W.\theta_2) \subseteq dom(H_2) \wedge \\ & & (W.\hat{\beta}) \subseteq (dom(W.\theta_1) \times dom(W.\theta_2)) \wedge \\ & & \forall (a_1, a_2) \in (W.\hat{\beta}).(W.\theta_1(a_1) = W.\theta_2(a_2) \wedge \\ & & (W, n - 1, H_1(a_1), H_2(a_2)) \in \lceil W.\theta_1(a_1) \rceil_V^{\mathcal{A}}) \wedge \\ & & \forall i \in \{1, 2\}.\forall m.\forall a_i \in dom(W.\theta_i).(W.\theta_i, m, H_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V\end{array}$$

Definition 1.10 (FG: Label substitution). $\sigma : Lvar \mapsto Label$

Definition 1.11 (FG: Value substitution to value pairs). $\gamma : Var \mapsto (Val, Val)$

Definition 1.12 (FG: Value substitution to values). $\delta : Var \mapsto Val$

Definition 1.13 (FG: Unary interpretation of Γ).

$$\lfloor \Gamma \rfloor_V \quad \triangleq \quad \{(\theta, n, \delta) \mid dom(\Gamma) \subseteq dom(\delta) \wedge \forall x \in dom(\Gamma).(\theta, n, \delta(x)) \in \lfloor \Gamma(x) \rfloor_V\}$$

Definition 1.14 (FG: Binary interpretation of Γ).

$$\lceil \Gamma \rceil_V^{\mathcal{A}} \quad \triangleq \quad \{(W, n, \gamma) \mid dom(\Gamma) \subseteq dom(\gamma) \wedge \forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}\}$$

1.4 Soundness proof for FG

Lemma 1.15 (FG: Binary value relation subsumes unary value relation). $\forall W, v_1, v_2, \mathcal{A}, n.$ *The following holds:*

1. $\forall \mathsf{A}.$

   $(W, n, v_1, v_2) \in \lceil \mathsf{A} \rceil_V^{\mathcal{A}} \implies \forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, v_i) \in \lfloor \mathsf{A} \rfloor_V$

2. $\forall \tau.$

   $(W, n, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}} \implies \forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, v_i) \in \lfloor \tau \rfloor_V$

Proof. Proof by simultaneous induction on A and τ

Proof of statement (1)

We analyze the various cases of A in the last step:

1. Case b:

   From Definition 1.6

2. Case $\tau_1 \times \tau_2$:

   Given: $(W, n, (v_{i1}, v_{i2}), (v_{j1}, v_{j2})) \in \lceil \tau_1 \times \tau_2 \rceil_V^{\mathcal{A}}$

   To prove:

   $\forall m.\ (W.\theta_1, m, (v_{i1}, v_{i2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$ (P01)

   and

   $\forall m.\ (W.\theta_2, m, (v_{j1}, v_{j2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$ (P02)

   From Definition 1.4 we know that we are given

   $(W, n, v_{i1}, v_{j1}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \wedge (W, n, v_{i2}, v_{j2}) \in \lceil \tau_2 \rceil_V^{\mathcal{A}}$ (P1)

   IH1a: $\forall m_1.\ (W.\theta_1, m_1, v_{i1}) \in \lfloor \tau_1 \rfloor_V$ and

   IH1b: $\forall m_1.\ (W.\theta_2, m_1, v_{j1}) \in \lfloor \tau_1 \rfloor_V$

   IH2a: $\forall m_2.\ (W.\theta_1, m_2, v_{i2}) \in \lfloor \tau_2 \rfloor_V$ and

   IH2b: $\forall m_2.\ (W.\theta_2, m_2, v_{j2}) \in \lfloor \tau_2 \rfloor_V$

   From (P01) we know that given some m we need to prove

   $(W.\theta_1, m, (v_{i1}, v_{i2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

   Similarly from (P02) we know that given some m we need to prove

   $(W.\theta_2, m, (v_{j1}, v_{j2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

   We instantiate IH1a and IH2a with the given m from (P01) to get

   $(W.\theta_1, m, v_{i1}) \in \lfloor \tau_1 \rfloor_V$ and $(W.\theta_1, m, v_{i2}) \in \lfloor \tau_2 \rfloor_V$

   Then from Definition 1.6, we get

   $(W.\theta_1, m, (v_{i1}, v_{i2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

   Similarly we instantiate IH1b and IH2b with the given m from (P02) to get

   $(W.\theta_2, m, v_{j1}) \in \lfloor \tau_1 \rfloor_V$ and $(W.\theta_2, m, v_{j2}) \in \lfloor \tau_2 \rfloor_V$

   Then from Definition 1.6, we get

   $(W.\theta_2, m, (v_{j1}, v_{j2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

3. Case $\tau_1 + \tau_2$:

   2 cases arise:

   (a) $v_1 = \mathsf{inl}(v_{i1})$ and $v_2 = \mathsf{inl}(v_{j1})$

      Given: $(W, n, \mathsf{inl}(v_{i1}), \mathsf{inl}(v_{j1})) \in \lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}}$

      To prove:

      $\forall m.\ (W.\theta_1, m, \mathsf{inl}(v_{i1})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$ (S01)

      and

      $\forall m.\ (W.\theta_2, m, \mathsf{inl}(v_{i2})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$ (S02)

      From Definition 1.4 we know that we are given

      $(W, n, v_{i1}, v_{j1}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$ (S0)

      IH1: $\forall m_1.\ (W.\theta_1, m_1, v_{i1}) \in \lfloor \tau_1 \rfloor_V$ and

IH2: $\forall m_2.\ (W.\theta_2, m_2, v_{j1}) \in \lfloor \tau_1 \rfloor_V$

From (S01) we know that given some m and we are required to prove:
$(W.\theta_1, m, \mathsf{inl}(v_{i1})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$
Also from (S02) we know that given some m and we are required to prove:
$(W.\theta_2, m, \mathsf{inl}(v_{i2})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$

We instantiate IH1 with m from (S01) to get
$(W.\theta_1, m, v_{i1}) \in \lfloor \tau_1 \rfloor_V$
Therefore from Definition 1.6, we get
$(W.\theta_1, m, \mathsf{inl}(v_{i1})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$

We instantiate IH2 with m from (S02) to get
$(W.\theta_2, m, v_{j1}) \in \lfloor \tau_1 \rfloor_V$
Therefore from Definition 1.6, we get
$(W.\theta_2, m, \mathsf{inl}(v_{j1})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$

(b) $v_1 = \mathsf{inr}(v_{i2})$ and $v_2 = \mathsf{inr}(v_{j2})$
Symmetric case as (a)

4. Case $\tau_1 \xrightarrow{\ell_e} \tau_2$:

Given: $(W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil \tau_1 \xrightarrow{\ell_e} \tau_2 \rceil_V^{\mathcal{A}}$
This means from Definition 1.4 we know that

$$\forall W' \sqsupseteq W, j < n, v_1, v_2.((W', j, v_1, v_2) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \implies (W', j, e_1[v_1/x], e_2[v_2/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}})$$
$$\wedge\ \forall \theta_l \sqsupseteq W.\theta_1, i, v_c.((\theta_l, i, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, i, e_1[v_c/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e})$$
$$\wedge\ \forall \theta_l \sqsupseteq W.\theta_2, k, v_c.((\theta_l, k, v_2) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, k, e_2[v_c/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e}) \qquad \text{(L0)}$$

To prove:

(a) $\forall m.\ (W.\theta_1, m, \lambda x.e_1) \in \lfloor \tau_1 \xrightarrow{\ell_e} \tau_2 \rfloor_V$:
This means from Definition 1.6 we need to prove:
$\forall \theta'. W.\theta_1 \sqsubseteq \theta' \wedge \forall j < m. \forall v.(\theta', j, v) \in \lfloor \tau_1 \rfloor_V \implies (\theta', j, e_1[v/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e}$
This further means that we have some θ', j and v s.t
$W.\theta_1 \sqsubseteq \theta' \wedge j < m \wedge (\theta', j, v) \in \lfloor \tau_1 \rfloor_V$
And we need to prove: $(\theta', j, e_1[v/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e}$

Instantiating θ_l, i and v_c in the second conjunct of L0 with θ', j and v respectively and since we know that $W.\theta_1 \sqsubseteq \theta'$ and $(\theta', j, v) \in \lfloor \tau_1 \rfloor_V$

Therefore we get $(\theta', j, e_1[v/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e}$

(b) $\forall m.\ (W.\theta_2, m, \lambda x.e_2) \in \lfloor \tau_1 \xrightarrow{\ell_e} \tau_2 \rfloor_V$:
Similar reasoning with e_2

5. Case $\forall \alpha.(\ell_e, \tau)$:

Given: $(W, n, \Lambda e_1, \Lambda e_2) \in \lceil \forall \alpha.(\ell_e, \tau) \rceil_V^{\mathcal{A}}$
This means from Definition 1.4 we know that

$\forall W_b \sqsupseteq W, n_b < n, \ell' \in \mathcal{L}.((W_b, n_b, e_1, e_2) \in \lceil \tau[\ell'/\alpha] \rceil_E^{\mathcal{A}})$
$\wedge\ \forall \theta_l \sqsupseteq W.\theta_1, i, \ell'' \in \mathcal{L}.((\theta_l, i, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\ell_e[\ell''/\alpha]})$
$\wedge\ \forall \theta_l \sqsupseteq W.\theta_2, i, \ell'' \in \mathcal{L}.((\theta_l, i, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\ell_e[\ell''/\alpha]})$ (F0)

To prove:

(a) $\forall m.\ (W.\theta_1, m, \Lambda e_1) \in \lfloor \forall \alpha.(\ell_e, \tau) \rfloor_V$:
This means from Definition 1.6 we need to prove:
$\forall \theta'. W.\theta_1 \sqsubseteq \theta'. \forall m' < m. \forall \ell_u \in \mathcal{L}.(\theta', m', e_1) \in \lfloor \tau[\ell_u/\alpha] \rfloor_E^{\ell_e[\ell_u/\alpha]}$
This further means that we are given some θ', m' and ℓ_u s.t $W.\theta_1 \sqsubseteq \theta'$, $m' < m$ and $\ell_u \in \mathcal{L}$
And we need to prove: $(\theta', m', e_1) \in \lfloor \tau[\ell_u/\alpha] \rfloor_E^{\ell_e[\ell_u/\alpha]}$

Instantiating θ_l, i and ℓ'' in the second conjunct of F0 with θ', m' and ℓ_u respectively and since we know that $W.\theta_1 \sqsubseteq \theta'$ and $\ell_u \in \mathcal{L}$

Therefore we get $(\theta', m', e_1) \in \lfloor \tau[\ell_u/\alpha] \rfloor_E^{\ell_e[\ell_u/\alpha]}$

(b) $\forall m.\ (W.\theta_2, m, \Lambda e_2) \in \lfloor \forall \alpha.(\ell_e, \tau) \rfloor_V$:
Symmetric reasoning for e_2

6. Case $c \overset{\ell_e}{\Rightarrow} \tau$:

Given: $(W, n, \nu e_1, \nu e_2) \in \lceil c \overset{\ell_e}{\Rightarrow} \tau \rceil_V^{\mathcal{A}}$

This means from Definition 1.4 we know that

$\forall W_b \sqsupseteq W, n' < n. \mathcal{L} \models c \implies (W_b, n', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$
$\wedge \forall \theta_l \sqsupseteq W.\theta_1, j. \mathcal{L} \models c \implies (\theta_l, j, e_1) \in \lfloor \tau \rfloor_E^{\ell_e})$
$\wedge \forall \theta_l \sqsupseteq W.\theta_2, j. \mathcal{L} \models c \implies (\theta_l, j, e_2) \in \lfloor \tau \rfloor_E^{\ell_e})$ (C0)

To prove:

(a) $\forall m.\ (W.\theta_1, m, \nu e_1) \in \lfloor c \overset{\ell_e}{\Rightarrow} \tau \rfloor_V$:
This means from Definition 1.6 we need to prove:
$\forall \theta'. W.\theta_1 \sqsubseteq \theta'. \forall m' < m. \mathcal{L} \models c \implies (\theta', m', e_1) \in \lfloor \tau \rfloor_E^{\ell_e}$
This further means that we are given some θ' and m' s.t $W.\theta_1 \sqsubseteq \theta'$, $m' < m$ and $\mathcal{L} \models c$
And we need to prove: $(\theta', m', e_1) \in \lfloor \tau \rfloor_E^{\ell_e}$

Instantiating θ_l, j in the second conjunct of C0 with θ', m' respectively and since we know that $W.\theta_1 \sqsubseteq \theta'$ and $\mathcal{L} \models c$

Therefore we get $(\theta', m', e_1) \in \lfloor \tau \rfloor_E^{\ell_e}$

(b) $\forall m.\ (W.\theta_2, m, \nu e_2) \in \lfloor c \overset{\ell_e}{\Rightarrow} \tau \rfloor_V$:
Symmetric reasoning for e_2

7. Case $\mathsf{ref}\ \tau$:

From Definition 1.4 and 1.6

Proof of statement (2)

Let $\tau = \mathsf{A}^{\ell}$
2 cases arise:

1. $\ell \sqsubseteq \mathcal{A}$:

   From IH (statement(1))

2. $\ell \not\sqsubseteq \mathcal{A}$:

   Directly from Definition 1.4

□

Lemma 1.16 (FG: Monotonicity Unary). *The following holds:*
$\forall \theta, \theta', v, m, m'$.

1. $\forall \mathsf{A}.\ (\theta, m, v) \in \lfloor \mathsf{A} \rfloor_V \wedge m' < m \wedge \theta \sqsubseteq \theta' \implies (\theta', m', v) \in \lfloor \mathsf{A} \rfloor_V$

2. $\forall \tau.\ (\theta, m, v) \in \lfloor \tau \rfloor_V \wedge m' < m \wedge \theta \sqsubseteq \theta' \implies (\theta', m', v) \in \lfloor \tau \rfloor_V$

Proof. Proof by simultaneous induction on A and τ
Proof of statement (1)
We analyze the various cases of A in the last step:

1. case b:

   Directly from Definition 1.6

2. case $\tau_1 \times \tau_2$:

   Given: $(\theta, m, (v_1, v_2)) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

   To prove: $(\theta', m', (v_1, v_2)) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

   This means from Definition 1.6 we know that

   $(\theta, m, v_1) \in \lfloor \tau_1 \rfloor_V \wedge (\theta, m, v_2) \in \lfloor \tau_2 \rfloor_V$

   IH1 : $(\theta', m', v_1) \in \lfloor \tau_1 \rfloor_V$

   IH2 : $(\theta', m', v_2) \in \lfloor \tau_2 \rfloor_V$

   We get the desired from IH1, IH2 and Definition 1.6

3. case $\tau_1 + \tau_2$:

   2 cases arise:

   (a) $v = \mathsf{inl}(v_1)$:
   Given: $(\theta, m, (\mathsf{inl}\ v_1)) \in \lfloor \tau_1 + \tau_2 \rfloor_V$
   To prove: $(\theta', m', \mathsf{inl}\ v_1) \in \lfloor \tau_1 + \tau_2 \rfloor_V$
   This means from Definition 1.6 we know that
   $(\theta, m, v_1) \in \lfloor \tau_1 \rfloor_V$
   IH : $(\theta', m', v_1) \in \lfloor \tau_1 \rfloor_V$
   Therefore from IH and Definition 1.6 we get the desired

   (b) $v = \mathsf{inr}(v_2)$
   Symmetric case

4. case $\tau_1 \xrightarrow{\ell_e} \tau_2$:

   Given: $(\theta, m, (\lambda x.e_1)) \in \lfloor \tau_1 \xrightarrow{\ell_e} \tau_2 \rfloor_V$

   To prove: $(\theta', m', (\lambda x.e_1)) \in \lfloor \tau_1 \xrightarrow{\ell_e} \tau_2 \rfloor_V$

   This means from Definition 1.6 we know that

$$\forall \theta''.\theta \sqsubseteq \theta'' \wedge \forall j < m.\forall v.(\theta'', j, v) \in \lfloor \tau_1 \rfloor_V \implies (\theta'', j, e_1[v/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e} \quad (1)$$

   Similarly from Definition 1.6 we know that we are required to prove
   $\forall \theta'''.\theta' \sqsubseteq \theta''' \wedge \forall k < m'.\forall v_1.(\theta''', k, v_1) \in \lfloor \tau_1 \rfloor_V \implies (\theta''', k, e_1[v_1/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e}$

   This means that given some θ''', k and v_1 such that $\theta' \sqsubseteq \theta''' \wedge k < m' \wedge (\theta''', k, v_1) \in \lfloor \tau_1 \rfloor_V$

   And we are required to prove $(\theta''', k, e_1[v_1/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e}$

   Instantiating Equation 75 with θ''', k and v_1 and since we know that $\theta' \sqsubseteq \theta'''$ and $\theta \sqsubseteq \theta'$ therefore we have $\theta \sqsubseteq \theta'''$. Also, we know that $k < m' < m$ and $(\theta''', k, v_1) \in \lfloor \tau_1 \rfloor_V$

   Therefore we get $(\theta''', k, e_1[v_1/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e}$

5. case $\mathsf{ref}\ \tau$:

   From Definition 1.6 and Definition 1.2

6. case $\forall \alpha.(\ell_e, \tau)$:

   Given: $(\theta, m, (\Lambda e_1)) \in \lfloor \forall \alpha.(\ell_e, \tau) \rfloor_V$

   To prove: $(\theta', m', (\Lambda e_1)) \in \lfloor \forall \alpha.(\ell_e, \tau) \rfloor_V$

   This means from Definition 1.6 we know that

$$\forall \theta''.\theta \sqsubseteq \theta'' \wedge \forall j < m.\forall \ell_i \in \mathcal{L}.(\theta'', j, e_1) \in \lfloor \tau[\ell_i/\alpha] \rfloor_E^{\ell_e[\ell_i/\alpha]} \quad (2)$$

   Similarly from Definition 1.6 we know that we are required to prove
   $\forall \theta'''.\theta' \sqsubseteq \theta''' \wedge \forall k < m'.\forall \ell_j \in \mathcal{L}.(\theta''', k, e_1) \in \lfloor \tau[\ell_j/\alpha] \rfloor_E^{\ell_e[\ell_j/\alpha]}$

   This means that given some θ''', k and ℓ_j such that $\theta' \sqsubseteq \theta''' \wedge k < m' \wedge \ell_j \in \mathcal{L}$

   And we are required to prove $(\theta''', k, e_1) \in \lfloor \tau[\ell_j/\alpha] \rfloor_E^{\ell_e[\ell_j/\alpha]}$

   Instantiating Equation 2 with θ''', k and ℓ_j and since we know that $\theta' \sqsubseteq \theta'''$ and $\theta \sqsubseteq \theta'$ therefore we have $\theta \sqsubseteq \theta'''$. Also, we know that $k < m' < m$ and $\ell_j \in \mathcal{L}$

   Therefore we get $(\theta''', k, e_1) \in \lfloor \tau[\ell_j/\alpha] \rfloor_E^{\ell_e[\ell_j/\alpha]}$

7. case $c \overset{\ell_e}{\Rightarrow} \tau$:

   Given: $(\theta, m, (\nu e_1)) \in \lfloor c \overset{\ell_e}{\Rightarrow} \tau \rfloor_V$

   To prove: $(\theta', m', (\nu e_1)) \in \lfloor c \overset{\ell_e}{\Rightarrow} \tau \rfloor_V$

   This means from Definition 1.6 we know that

$$\forall \theta''.\theta \sqsubseteq \theta'' \wedge \forall j < m.\mathcal{L} \models c \implies (\theta'', j, e_1) \in \lfloor \tau \rfloor_E^{\ell_e} \tag{3}$$

Similarly from Definition 1.6 we know that we are required to prove
$\forall \theta'''.\theta' \sqsubseteq \theta''' \wedge \forall k < m'.\mathcal{L} \models c \implies (\theta''', k, e_1) \in \lfloor \tau \rfloor_E^{\ell_e}$

This means that given some θ''', k and ℓ_j such that $\theta' \sqsubseteq \theta''' \wedge k < m' \wedge \ell_j \in \mathcal{L}$

And we are required to prove $(\theta''', k, e_1) \in \lfloor \tau \rfloor_E^{\ell_e}$

Instantiating Equation 3 with θ''', k and since we know that $\theta' \sqsubseteq \theta'''$ and $\theta \sqsubseteq \theta'$ therefore we have $\theta \sqsubseteq \theta'''$. Also, we know that $k < m' < m$ and $\mathcal{L} \models c$

Therefore we get $(\theta''', k, e_1) \in \lfloor \tau \rfloor_E^{\ell_e}$

Proof of statement (2)
Let $\tau = \mathsf{A}^\ell$
Since $\lfloor \mathsf{A}^\ell \rfloor_V = \lfloor \mathsf{A} \rfloor_V$, therefore from IH (statement 1) □

Lemma 1.17 (FG: Monotonicity binary). *The following holds:*
$\forall W, W', v_1, v_2, \mathcal{A}, n, n'$.

1. $\forall \mathsf{A}.\ (W, n, v_1, v_2) \in \lceil \mathsf{A} \rceil_V^{\mathcal{A}} \wedge n' < n \wedge W \sqsubseteq W' \implies (W', n', v_1, v_2) \in \lceil \mathsf{A} \rceil_V^{\mathcal{A}}$
2. $\forall \tau.\ (W, n, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}} \wedge n' < n \wedge W \sqsubseteq W' \implies (W', n', v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$

Proof. Proof by simultaneous induction on A and τ
Proof of statement (1)
We analyze the different cases of A in the last step:

1. Case b:

   From Definition 1.4

2. Case $\tau_1 \times \tau_2$:

   Given: $(W, n, (v_{i1}, v_{i2}), (v_{j1}, v_{j2})) \in \lceil \tau_1 \times \tau_2 \rceil_V^{\mathcal{A}}$
   To prove: $(W', n', (v_{i1}, v_{i2}), (v_{j1}, v_{j2})) \in \lceil \tau_1 \times \tau_2 \rceil_V^{\mathcal{A}}$

   From Definition 1.4 we know that we are given
   $(W, n, v_{i1}, v_{j1}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \wedge (W, n, v_{i2}, v_{j2}) \in \lceil \tau_2 \rceil_V^{\mathcal{A}}$
   IH1 : $(W', n', v_{i1}, v_{j1}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$
   IH2 : $(W', n', v_{i2}, v_{j2}) \in \lceil \tau_2 \rceil_V^{\mathcal{A}}$

   From IH1, IH2 and Definition 1.4 we get the desired.

3. Case $\tau_1 + \tau_2$:

   2 cases arise:

(a) $v_1 = \mathsf{inl}\ v_{i1}$ and $v_2 = \mathsf{inl}\ v_{i2}$:
Given: $(W, n, (\mathsf{inl}\ v_{i1}, \mathsf{inl}\ v_{i2})) \in \lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}}$
To prove: $(W', n', (\mathsf{inl}\ v_{i1}, \mathsf{inl}\ v_{i2})) \in \lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}}$

From Definition 1.4 we know that we are given
$(W, n, v_{i1}, v_{i2}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$
IH : $(W', n', v_{i1}, v_{i2}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$
Therefore from Definition 1.4 we get
$(W', n', \mathsf{inl}\ v_{i1}, \mathsf{inl}\ v_{i2}) \in \lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}}$

(b) $v_1 = \mathsf{inr}(v_{12})$ and $v_2 = \mathsf{inr}(v_{22})$:
Symmetric case

4. Case $\tau_1 \xrightarrow{\ell_e} \tau_2$:

Given: $(W, n, (\lambda x.e_1), (\lambda x.e_2)) \in \lceil \tau_1 \xrightarrow{\ell_e} \tau_2 \rceil_V^{\mathcal{A}}$

To prove: $(\theta', n', (\lambda x.e_1), (\lambda x.e_1)) \in \lceil \tau_1 \xrightarrow{\ell_e} \tau_2 \rceil_V^{\mathcal{A}}$

This means from Definition 1.4 we know that the following holds

$\forall W' \sqsupseteq W, j < n, v_1, v_2.((W', j, v_1, v_2) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \implies (W', j, e_1[v_1/x], e_2[v_2/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}})$ (BM-A0)

$\forall \theta_l \sqsupseteq W.\theta_1, j, v_c.((\theta_l, j, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, j, e_1[v_c/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e})$ (BM-A1)

$\forall \theta_l \sqsupseteq W.\theta_2, j, v_c.((\theta_l, j, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, j, e_2[v_c/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e})$ (BM-A2)

Similarly from Definition 1.4 we know that we are required to prove

(a) $\forall W'' \sqsupseteq W', k < n', v_1', v_2'.((W'', k, v_1', v_2') \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \implies (W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}})$:
This means that we are given some $W'' \sqsupseteq W'$, $k < n'$ and v_1', v_2' s.t
$(W'', k, v_1', v_2') \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$
And we a required to prove: $(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}}$

Instantiating BM-A0 with W'', k and v_1', v_2' we get
$(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}}$

(b) $\forall \theta_l' \sqsupseteq W'.\theta_1, k, v_c'.((\theta_l', k, v_c') \in \lfloor \tau_1 \rfloor_V \implies (\theta_l', k, e_1[v_c'/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e})$:
This means that we are given some $\theta_l' \sqsupseteq W'.\theta_1$, k and v_c' s.t
$(\theta_l', k, v_c') \in \lfloor \tau_1 \rfloor_V$
And we a required to prove: $(\theta_l', k, e_1[v_c'/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e}$

Instantiating BM-A1 with θ_l', k and v_c' we get
$(\theta_l', k, e_1[v_c'/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e}$

(c) $\forall \theta_l' \sqsupseteq W.\theta_2, k, v_c'.((\theta_l', k, v_c') \in \lfloor \tau_1 \rfloor_V \implies (\theta_l', k, e_2[v_c'/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e})$:
This means that we are given some $\theta_l' \sqsupseteq W'.\theta_2$, k and v_c' s.t
$(\theta_l', k, v_c') \in \lfloor \tau_1 \rfloor_V$
And we a required to prove: $(\theta_l', k, e_2[v_c'/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e}$

Instantiating BM-A1 with θ_l', k and v_c' we get
$(\theta_l', k, e_2[v_c'/x]) \in \lfloor \tau_2 \rfloor_E^{\ell_e}$

5. Case $\mathsf{ref}\ \tau$:

   From Definition 1.4 and Definition 1.3

6. Case $\forall\alpha.(\ell_e, \tau)$:

   Given: $(W, n, (\Lambda e_1), (\Lambda e_2)) \in \lceil \forall\alpha.(\ell_e, \tau) \rceil_V^{\mathcal{A}}$

   To prove: $(\theta', n', (\Lambda e_1), (\Lambda e_1)) \in \lceil \forall\alpha.(\ell_e, \tau) \rceil_V^{\mathcal{A}}$

   This means from Definition 1.4 we know that the following holds

   $\forall W' \sqsupseteq W, n' < n, \ell' \in \mathcal{L}.((W', n', e_1, e_2) \in \lceil \tau[\ell'/\alpha] \rceil_E^{\mathcal{A}})$ (BM-F0)

   $\forall \theta_l \sqsupseteq W.\theta_1, j, \ell' \in \mathcal{L}.((\theta_l, j, e_1) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\ell_e[\ell'/\alpha]})$ (BM-F1)

   $\forall \theta_l \sqsupseteq W.\theta_2, j, \ell' \in \mathcal{L}.((\theta_l, j, e_2) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\ell_e[\ell'/\alpha]})$ (BM-F2)

   Similarly from Definition 1.4 we know that we are required to prove

   (a) $\forall W'' \sqsupseteq W', n'' < n', \ell'' \in \mathcal{L}.((W'', n'', e_1, e_2) \in \lceil \tau[\ell''/\alpha] \rceil_E^{\mathcal{A}})$:

   This means that we are given some $W'' \sqsupseteq W'$, $n'' < n'$ and $\ell'' \in \mathcal{L}$

   And we a required to prove: $((W'', n'', e_1, e_2) \in \lceil \tau[\ell''/\alpha] \rceil_E^{\mathcal{A}})$

   Instantiating BM-F0 with W'', n'' and ℓ''. And since $W'' \sqsupseteq W'$ and $W' \sqsupseteq W$ therefore $W'' \sqsupseteq W$. Also since $n'' < n'$ and $n' < n$ therefore $n'' < n$. And finally since $\ell'' \in \mathcal{L}$ therefore we get

   $((W'', n'', e_1, e_2) \in \lceil \tau[\ell''/\alpha] \rceil_E^{\mathcal{A}})$

   (b) $\forall \theta'_l \sqsupseteq W'.\theta_1, k, \ell'' \in \mathcal{L}.((\theta'_l, k, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\ell_e[\ell''/\alpha]})$:

   This means that we are given some $\theta'_l \sqsupseteq W'.\theta_1$, k and $\ell'' \in \mathcal{L}$

   And we a required to prove: $((\theta'_l, k, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\ell_e[\ell''/\alpha]})$

   Instantiating BM-F1 with θ'_l, k and ℓ''. And since $\theta'_l \sqsupseteq W'.\theta_1$ and $W' \sqsupseteq W$ therefore $\theta'_1 \sqsupseteq W.\theta_1$. And since $\ell'' \in \mathcal{L}$ therefore we get

   $((\theta'_l, k, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\ell_e[\ell''/\alpha]})$

   (c) $\forall \theta_l \sqsupseteq W.\theta_2, j, \ell'' \in \mathcal{L}.((\theta'_l, k, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\ell_e[\ell''/\alpha]})$:

   This means that we are given some $\theta'_l \sqsupseteq W'.\theta_2$, k and $\ell'' \in \mathcal{L}$

   And we a required to prove: $((\theta'_l, k, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\ell_e[\ell''/\alpha]})$

   Instantiating BM-F1 with θ'_l, k and ℓ''. And since $\theta'_l \sqsupseteq W'.\theta_2$ and $W' \sqsupseteq W$ therefore $\theta'_2 \sqsupseteq W.\theta_2$. And since $\ell'' \in \mathcal{L}$ therefore we get

   $((\theta'_l, k, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\ell_e[\ell''/\alpha]})$

7. Case $c \overset{\ell_e}{\Rightarrow} \tau$:

   Given: $(W, n, (\nu e_1), (\nu e_2)) \in \lceil c \overset{\ell_e}{\Rightarrow} \tau \rceil_V^{\mathcal{A}}$

   To prove: $(\theta', n', (\nu e_1), (\nu e_1)) \in \lceil c \overset{\ell_e}{\Rightarrow} \tau \rceil_V^{\mathcal{A}}$

   This means from Definition 1.4 we know that the following holds

   $\forall W' \sqsupseteq W, n' < n.\mathcal{L} \models c \implies (W', n', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$ (BM-C0)

   $\forall \theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c \implies (\theta_l, j, e_1) \in \lfloor \tau \rfloor_E^{\ell_e}$ (BM-C1)

   $\forall \theta_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c \implies (\theta_l, j, e_2) \in \lfloor \tau \rfloor_E^{\ell_e}$ (BM-C2)

   Similarly from Definition 1.4 we know that we are required to prove

(a) $\forall W'' \sqsupseteq W', n'' < n.\mathcal{L} \models c \implies (W'', n'', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$:
This means that we are given some $W'' \sqsupseteq W'$, $n'' < n'$ and $\mathcal{L} \models c$
And we a required to prove: $(W'', n'', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$

Instantiating BM-C0 with W'', n''. And since $W'' \sqsupseteq W'$ and $W' \sqsupseteq W$ therefore $W'' \sqsupseteq W$. And since $\mathcal{L} \models c$ therefore we get
$(W'', n'', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$

(b) $\forall \theta'_l \sqsupseteq W'.\theta_1, k.\mathcal{L} \models c \implies (\theta'_l, k, e_1) \in \lfloor \tau \rfloor_E^{\ell_e}$:
This means that we are given some $\theta'_l \sqsupseteq W'.\theta_1$, k and $\mathcal{L} \models c$
And we a required to prove: $(\theta'_l, k, e_1) \in \lfloor \tau \rfloor_E^{\ell_e}$

Instantiating BM-F1 with θ'_l, k. And since $\theta'_l \sqsupseteq W'.\theta_1$ and $W' \sqsupseteq W$ therefore $\theta'_1 \sqsupseteq W.\theta_1$. And since $\mathcal{L} \models c$ therefore we get
$(\theta'_l, k, e_1) \in \lfloor \tau \rfloor_E^{\ell_e}$

(c) $\forall \theta'_l \sqsupseteq W'.\theta_2, k.\mathcal{L} \models c \implies (\theta_l, k, e_2) \in \lfloor \tau \rfloor_E^{\ell_e}$:
This means that we are given some $\theta'_l \sqsupseteq W'.\theta_2$, k and $\mathcal{L} \models c$
And we a required to prove: $(\theta'_l, k, e_2) \in \lfloor \tau \rfloor_E^{\ell_e}$

Instantiating BM-F1 with θ'_l, k. And since $\theta'_l \sqsupseteq W'.\theta_2$ and $W' \sqsupseteq W$ therefore $\theta'_2 \sqsupseteq W.\theta_2$. And since $\mathcal{L} \models c$ therefore we get
$(\theta'_l, k, e_2) \in \lfloor \tau \rfloor_E^{\ell_e}$

Proof of statement (2)

Let $\tau = \mathsf{A}^\ell$
2 cases arise:

1. $\ell \sqsubseteq \mathcal{A}$:

   From IH (statement 1)

2. $\ell \not\sqsubseteq \mathcal{A}$:

   From Lemma 1.16 and Definition 1.4

□

Lemma 1.18 (FG: Unary monotonicity for Γ)**.** $\forall \theta, \theta', \delta, \Gamma, n, n'$.
$(\theta, n, \delta) \in \lfloor \Gamma \rfloor_V \wedge n' < n \wedge \theta \sqsubseteq \theta' \implies (\theta', n', \delta) \in \lfloor \Gamma \rfloor_V$

Proof. Given: $(\theta, n, \delta) \in \lfloor \Gamma \rfloor_V \wedge n' < n \wedge \theta \sqsubseteq \theta'$
To prove: $(\theta', n', \delta) \in \lfloor \Gamma \rfloor_V$

From Definition 1.13 it is given that
$dom(\Gamma) \subseteq dom(\delta) \wedge \forall x \in dom(\Gamma).(\theta, n, \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$

And again from Definition 1.13 we are required to prove that
$dom(\Gamma) \subseteq dom(\delta) \wedge \forall x \in dom(\Gamma).(\theta', n', \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$

- $dom(\Gamma) \subseteq dom(\delta)$:

  Given

- $\forall x \in dom(\Gamma).(\theta', n', \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$:

  Since we know that $\forall x \in dom(\Gamma).(\theta, n, \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$ (given)

  Therefore from Lemma 1.16 we get

  $\forall x \in dom(\Gamma).(\theta', n', \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$

□

Lemma 1.19 (FG: Binary monotonicity for Γ)**.** $\forall W, W', \delta, \Gamma, n, n'.$
$(W, n, \gamma) \in \lfloor \Gamma \rfloor_V \wedge n' < n \wedge W \sqsubseteq W' \implies (W', n', \gamma) \in \lfloor \Gamma \rfloor_V$

Proof. Given: $(W, n, \gamma) \in \lfloor \Gamma \rfloor_V \wedge n' < n \wedge W \sqsubseteq W'$
To prove: $(W', n', \gamma) \in \lfloor \Gamma \rfloor_V$

From Definition 1.14 it is given that
$dom(\Gamma) \subseteq dom(\gamma) \wedge \forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$

And again from Definition 1.13 we are required to prove that
$dom(\Gamma) \subseteq dom(\gamma) \wedge \forall x \in dom(\Gamma).(W', n', \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$

- $dom(\Gamma) \subseteq dom(\gamma)$:

  Given

- $\forall x \in dom(\Gamma).(W', n', \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$:

  Since we know that $\forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$ (given)

  Therefore from Lemma 1.17 we get

  $\forall x \in dom(\Gamma).(W', n', \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$

□

Lemma 1.20 (FG: Unary monotonicity for H)**.** $\forall \theta, H, n, n'.$
$(n, H) \triangleright \theta \wedge n' < n \implies (n', H) \triangleright \theta$

Proof. Given: $(n, H) \triangleright \theta \wedge n' < n$
To prove: $(n', H) \triangleright \theta$

From Definition 1.8 it is given that
$dom(\theta) \subseteq dom(H) \wedge \forall a \in dom(\theta).(\theta, n-1, H(a)) \in \lfloor \theta(a) \rfloor_V$

And again from Definition 1.13 we are required to prove that
$dom(\theta) \subseteq dom(H) \wedge \forall a \in dom(\theta).(\theta, n'-1, H(a)) \in \lfloor \theta'(a) \rfloor_V$

- $dom(\theta) \subseteq dom(H)$:

  Given

- $\forall a \in dom(\theta).(\theta, n'-1, H(a)) \in \lfloor \theta'(a) \rfloor_V$:

  Since we know that $\forall a \in dom(\theta).(\theta, n-1, H(a)) \in \lfloor \theta(a) \rfloor_V$ (given)

  Therefore from Lemma 1.16 we get

  $\forall a \in dom(\theta).(\theta, n'-1, H(a)) \in \lfloor \theta'(a) \rfloor_V$

□

Lemma 1.21 (FG: Binary monotonicity for heaps)**.** $\forall W, H_1, H_2, n, n'$.
$(n, H_1, H_2) \triangleright W \wedge n' < n \implies (n', H_1, H_2) \triangleright W$

Proof. Given: $(n, H_1, H_2) \triangleright W \wedge n' < n \wedge W \sqsubseteq W'$
To prove: $(n', H_1, H_2) \triangleright W$

From Definition 1.9 it is given that
$dom(W.\theta_1) \subseteq dom(H_1) \wedge dom(W.\theta_2) \subseteq dom(H_2) \wedge$
$(W.\hat{\beta}) \subseteq (dom(W.\theta_1) \times dom(W.\theta_2)) \wedge$
$\forall (a_1, a_2) \in (W.\hat{\beta}).(W.\theta_1(a_1) = W.\theta_2(a_2) \wedge$
$(W, n-1, H_1(a_1), H_2(a_2)) \in \lceil W.\theta_1(a_1) \rceil_V^{\mathcal{A}}) \wedge$
$\forall i \in \{1,2\}.\forall m.\forall a_i \in dom(W.\theta_i).(W.\theta_i, m, H_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$

And again from Definition 1.9 we are required to prove:

- $dom(W.\theta_1) \subseteq dom(H_1) \wedge dom(W.\theta_2) \subseteq dom(H_2)$:
  Given
- $(W.\hat{\beta}) \subseteq (dom(W.\theta_1) \times dom(W.\theta_2))$:
  Given
- $\forall (a_1, a_2) \in (W.\hat{\beta}).(W.\theta_1(a_1) = W.\theta_2(a_2)$ and $(W, n'-1, H_1(a_1), H_2(a_2)) \in \lceil W.\theta_1(a_1) \rceil_V^{\mathcal{A}})$:
  $\forall (a_1, a_2) \in (W.\hat{\beta})$.
  - $(W.\theta_1(a_1) = W.\theta_2(a_2)$: Given
  - $(W, n'-1, H_1(a_1), H_2(a_2)) \in \lceil W.\theta_1(a_1) \rceil_V^{\mathcal{A}})$:
    Given and from Lemma 1.17
- $\forall i \in \{1,2\}.\forall m.\forall a_i \in dom(W.\theta_i).(W.\theta_i, m, H_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$:
  Given

□

Theorem 1.22 (FG: Fundamental theorem unary)**.** $\forall \Sigma, \Psi, \Gamma, pc, \theta, \mathcal{L}, e, \tau, \sigma, \delta, n$.
$\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau \wedge$
$\mathcal{L} \models \Psi\ \sigma \wedge$
$(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V \implies$
$(\theta, n, e\ \delta) \in \lfloor \tau\ \sigma \rfloor_E^{pc}$

Proof. Proof by induction on FG typing derivation

1. FG-var:

$$\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash_{pc} x : \tau}\ \text{FG-var}$$

   To prove: $(\theta, n, x\ \delta) \in \lfloor \tau\ \sigma \rfloor_E^{pc}$

   This means that from Definition 1.7 we need to prove

$\forall H.(n, H) \rhd \theta \wedge \forall j < n.(H, e) \Downarrow_j (H', v') \implies$
$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - j, H') \rhd \theta' \wedge (\theta', n - j, v') \in \lfloor \tau \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc)$

This means that given some heap H and $j < n$ s.t $(n, H) \rhd \theta \wedge (H, x\ \delta) \Downarrow_j (H', v')$

<u>It suffices to prove</u>

$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - j, H') \rhd \theta' \wedge (\theta', n - j, v') \in \lfloor \tau \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc)$ (FU-V0)

In order to prove FU-V0 we instantiate θ' with θ. From reduction relation we know that $H' = H$, $v' = \delta(x)$ and $j = 1$

We need to prove the following:

(a) $\theta \sqsubseteq \theta \wedge (n - 1, H) \rhd \theta \wedge (\theta, n - 1, v') \in \lfloor \tau\ \sigma \rfloor_V$:
  - $\theta \sqsubseteq \theta$: From Definition 1.2
  - $(n - 1, H) \rhd \theta$: From Lemma 1.20
  - $(\theta, n - 1, v') \in \lfloor \tau\ \sigma \rfloor_V$:
    Since we are given that $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$ and $v' = \delta(x)$
    Therefore $(\theta, n, v') \in \lfloor \Gamma(x)\ \sigma \rfloor_V$, where $\Gamma(x) = \tau$
    And finally from Lemma 1.16 we get $(\theta, n - 1, v') \in \lfloor \tau\ \sigma \rfloor_V$

(b) $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell')$:
  Since $H' = H$, so we are done

(c) $(\forall a \in dom(\theta') \backslash dom(\theta).\theta(a) \searrow pc)$:
  Since $\theta' = \theta$, so we are done

2. FG-lam:

$$\frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{\ell_e} e_i : \tau_2}{\Sigma; \Psi; \Gamma \vdash_{pc} \lambda x.e_i : (\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp}$$

To prove: $(\theta, \lambda x.e_i\ \delta) \in \lfloor ((\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp)\ \sigma \rfloor_E^{pc}$

This means that from Definition 1.7 we need to prove

$\forall H.(n, H) \rhd \theta \wedge \forall j < n.(H, (\lambda x.e_i)\ \delta) \Downarrow_j (H', v') \implies$
$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - j, H') \rhd \theta' \wedge (\theta', n - j, v') \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc)$

This means that given some heap H and $j < n$ s.t $(n, H) \rhd \theta \wedge (H, (\lambda x.e_i)\ \delta) \Downarrow_j (H', v')$

<u>It suffices to prove</u>

$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - j, H') \rhd \theta' \wedge (\theta', n - j, v') \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc)$ (FU-L0)

<u>IH1</u>:

$\forall \theta_i, v_x, n.\ (\theta_i, n, e_i\ \delta \cup \{x \mapsto v_x\}) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$, s.t $(\theta_i, n, v_x) \in \lfloor \tau_1\ \sigma \rfloor_V$

In order to prove FU-L0 we instantiate θ' with θ. From reduction relation we know that $H' = H$, $j = 0$ and $v' = \lambda x.e_i\ \delta$

(a) $\theta \sqsubseteq \theta \wedge (n, H) \triangleright \theta \wedge (\theta, n, v') \in \lfloor ((\tau_1 \xrightarrow{\ell_e} \tau_2)^{\perp})\ \sigma \rfloor_V$:

- $\theta \sqsubseteq \theta$: From Definition 1.2
- $(n, H) \triangleright \theta$: Given
- $(\theta, n, (\lambda x.e_i)\delta) \in \lfloor ((\tau_1 \xrightarrow{\ell_e} \tau_2)^{\perp})\ \sigma \rfloor_V$:
  From Definition 1.6 it suffices to prove that
  $\forall \theta''. \theta \sqsubseteq \theta'' \wedge \forall j < n. \forall v. (\theta'', j, v) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta'', j, e_i[v/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$

  This means given some θ'', j and v such that $\theta \sqsubseteq \theta''$, $j < n$ and $(\theta'', j, v) \in \lfloor \tau_1\ \sigma \rfloor_V$
  It suffices to prove that $(\theta'', j, e_i[v/x]\ \delta) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$

  Since $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$ and $j < n$ therefore from Lemma 1.18 we have
  $(\theta, j, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

  So we can apply IH1 instantiated with θ'', v and j we get
  $(\theta'', j, e_i[v/x]\ \delta) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$

(b) $(\forall a. H(a) \neq H'(a) \implies \exists \ell'. \theta. \theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell')$:
Since $H' = H$ so we are done

(c) $(\forall a \in dom(\theta') \backslash dom(\theta). \theta(a) \searrow pc)$:
Since $\theta' = \theta$ so we are done

3. FG-app:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 \searrow \ell \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1\ e_2 : \tau_2}$$

To prove: $(\theta, n, (e_1\ e_2)\ \delta) \in \lfloor \tau_2\ \sigma \rfloor_E^{pc}$

This means that from Definition 1.7 we need to prove

$\forall H. (n, H) \triangleright \theta \wedge \forall n' < n. (H, (e_1\ e_2)\ \delta) \Downarrow_{n'} (H', v') \implies$
$\exists \theta'. \theta \sqsubseteq \theta' \wedge (n - n', H') \triangleright \theta' \wedge (\theta', n - n', v') \in \lfloor \tau_2\ \sigma \rfloor_V \wedge$
$(\forall a. H(a) \neq H'(a) \implies \exists \ell'. \theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta). \theta'(a) \searrow pc\ \sigma)$

This means that given some heap H s.t $(n, H) \triangleright \theta \wedge (H, (e_1\ e_2)\ \delta) \Downarrow_{n'} (H', v')$

<u>It suffices to prove</u>

$\exists \theta'. \theta \sqsubseteq \theta' \wedge (n - n', H') \triangleright \theta' \wedge (\theta', n - n', v') \in \lfloor \tau_2\ \sigma \rfloor_V \wedge$
$(\forall a. H(a) \neq H'(a) \implies \exists \ell'. \theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta). \theta'(a) \searrow pc\ \sigma)$ (FU-P0)

<u>IH1</u>:

$\forall n_1, H_1. (n_1, H_1) \triangleright \theta \wedge \forall i < n_1. (H_1, (e_1)\ \delta) \Downarrow_i (H_1', v_1') \implies$
$\exists \theta_1'. \theta \sqsubseteq \theta_1' \wedge (n_1 - i, H_1') \triangleright \theta_1' \wedge (\theta_1', n_1 - i, v_1') \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell}\ \sigma \rfloor_V \wedge$

$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1')\backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$

Instantiating IH1 with n, H and since we know that $(n, H) \rhd \theta \wedge (H, (e_1\ e_2)\ \delta) \Downarrow_{n'} (H', v')$ therefore we have

$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n-i, H_1') \rhd \theta_1' \wedge (\theta_1', n-i, v_1') \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell}\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1')\backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$ (FU-P1)

From evaluation rule we know that $v_1' = \lambda x.e_i$. Since from FU-P1 we know that

$(\theta_1', n-i, \lambda x.e_i) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell}\ \sigma \rfloor_V$

This means from Definition 1.6 we have

$$\forall \theta''.\theta_1' \sqsubseteq \theta'' \wedge \forall j < (n-i).\forall v.(\theta'', j, v) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta'', j, e_i[v/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma} \quad (4)$$

<u>IH2</u>:

$\forall n_2, \forall H_2.(n_2, H_2) \rhd \theta_1' \wedge \forall k < n_2.(H_2, (e_2)\ \delta) \Downarrow_k (H_2', v_2') \implies$
$\exists \theta_2'.\theta_1' \sqsubseteq \theta_2' \wedge (n_2 - k, H_2') \rhd \theta_2' \wedge (\theta_2', n_2 - k, v_2') \in \lfloor (\tau_1)\ \sigma \rfloor_V \wedge$
$(\forall a.H_2(a) \neq H_2'(a) \implies \exists \ell'.\theta_1'(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2')\backslash dom(\theta_1').\theta_2'(a) \searrow pc\ \sigma)$

Instantiating IH2 with $n-i$, H_1' and since we know that $(n-i, H_1') \rhd \theta_1' \wedge (H, (e_1\ e_2)\ \delta) \Downarrow_{n'} (H', v')$ therefore we have

$\exists \theta_2'.\theta_1' \sqsubseteq \theta_2' \wedge (n-i-k, H_2') \rhd \theta_2' \wedge (\theta_2', n-i-k, v_2') \in \lfloor (\tau_1)\ \sigma \rfloor_V \wedge$
$(\forall a.H_2(a) \neq H_2'(a) \implies \exists \ell'.\theta_1'(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2')\backslash dom(\theta_1').\theta_2'(a) \searrow pc\ \sigma)$ (FU-P2)

Instantiating θ'', j and v in Equation 4 with θ_2', $n-i-k$ and v_2' from FU-P2 respectively, we get

$(\theta_2', n-i-k, e_i[v_2'/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$

This means from Definition 1.7 we have

$\forall H_3.(n-i-k, H_3) \rhd \theta_2' \wedge \forall l < (n-i-k).(H_3, e_i[v_2'/x]) \Downarrow_l (H_3', v_3') \implies$
$\exists \theta_3'.\theta_2' \sqsubseteq \theta_3' \wedge ((n-i-k-l), H_3') \rhd \theta_3' \wedge (\theta_3', (n-i-k-l), v_3') \in \lfloor \tau_2\ \sigma \rfloor_V \wedge$
$(\forall a.H_3(a) \neq H_3'(a) \implies \exists \ell'.\theta_2'(a) = \mathsf{A}^{\ell'} \wedge \ell_e\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_3')\backslash dom(\theta_2').\theta_3'(a) \searrow \ell_e\ \sigma)$

Instantiating H_3 with H_2' from FU-P2 and since we know that $((n-i-k), H_2') \rhd \theta_2'$ and since the reduction happens therefore we have

$\exists \theta_3'.\theta_2' \sqsubseteq \theta_3' \wedge ((n-i-k-l), H_3') \rhd \theta_3' \wedge (\theta_3', (n-i-k-l), v_3') \in \lfloor \tau_2\ \sigma \rfloor_V \wedge$
$(\forall a.H_3(a) \neq H_3'(a) \implies \exists \ell'.\theta_2'(a) = \mathsf{A}^{\ell'} \wedge \ell_e\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_3')\backslash dom(\theta_2').\theta_3'(a) \searrow \ell_e\ \sigma)$ (FU-P3)

In order to prove FU-P0 we choose θ' as θ_3' from FU-P3. Also we know that $H' = H_3'$, $v' = v_3'$ and $n' = i + k + l$. Now we are required to show

(a) $\theta \sqsubseteq \theta'_3 \wedge ((n-i-k-l), H'_3) \triangleright \theta'_3 \wedge (\theta'_3, (n-i-k-l), v'_3) \in \lfloor \tau_2\ \sigma \rfloor_V$:

- $\theta \sqsubseteq \theta'_3$:
  Since $\theta \sqsubseteq \theta'_1$ from FU-P1, $\theta'_1 \sqsubseteq \theta'_2$ from FU-P2 and $\theta'_2 \sqsubseteq \theta'_3$ from FU-P3 therefore from Definition 1.2 we get $\theta \sqsubseteq \theta'_3$
- $((n-i-k-l), H'_3) \triangleright \theta'_3$:
  From FU-P3 we get $((n-i-k-l), H'_3) \triangleright \theta'_3$
- $(\theta'_3, (n-i-k-l), v'_3) \in \lfloor \tau_2\ \sigma \rfloor_V$:
  From FU-P3 we get $(\theta'_3, (n-i-k-l), v'_3) \in \lfloor \tau_2\ \sigma \rfloor_V$

(b) $(\forall a \in dom(H).H(a) \neq H'_3(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell')$
Since $pc\ \sigma \sqsubseteq \ell_e\ \sigma$ therefore we get the desired from FU-P1, FU-P2 and FU-P3

(c) $(\forall a \in dom(\theta'_3) \backslash dom(\theta).\theta'_3(a) \searrow pc\ \sigma)$
Since $pc\ \sigma \sqsubseteq \ell_e\ \sigma$ therefore we get the desired from FU-P1, FU-P2 and FU-P3

4. FG-prod:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : \tau_1 \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_2}{\Sigma; \Psi; \Gamma \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^{\perp}}$$

To prove: $(\theta, n, (e_1, e_2)\ \delta) \in \lfloor (\tau_1 \times \tau_2)^{\perp}\ \sigma \rfloor_E^{pc}$

This means that from Definition 1.7 we need to prove

$\forall H.(n, H) \triangleright \theta \wedge \forall n' < n.(H, (e_1, e_2)\ \delta) \Downarrow_{n'} (H', v') \implies$
$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n-n', H') \triangleright \theta' \wedge (\theta', n-n', v') \in \lfloor (\tau_1 \times \tau_2)^{\perp} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$

This means that given some heap H s.t $H \triangleright \theta \wedge (H, (e_1, e_2)\ \delta) \Downarrow_{n'} (H', v')$

<u>It suffices to prove</u>

$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n-n', H') \triangleright \theta' \wedge (\theta', n-n', v') \in \lfloor (\tau_1 \times \tau_2)^{\perp} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$ (FU-PA0)

<u>IH1</u>:

$\forall H_1, n_1.(n_1, H_1) \triangleright \theta \wedge \forall i < n_!.(H_1, (e_1)\ \delta) \Downarrow_i (H'_1, v'_1) \implies$
$\exists \theta'_1.\theta \sqsubseteq \theta'_1 \wedge (n_1 - i, H'_1) \triangleright \theta'_1 \wedge (\theta'_1, n_1 - i, v'_1) \in \lfloor \tau_1\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H'_1(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_1) \backslash dom(\theta).\theta'_1(a) \searrow pc\ \sigma)$

We instantiate IH1 with H and n. And since we know that $(n, H) \triangleright \theta \wedge (H, (e_1, e_2)\ \delta) \Downarrow_{n'}$ (H', v') therefore we have

$\exists \theta'_1.\theta \sqsubseteq \theta'_1 \wedge (n-i, H'_1) \triangleright \theta'_1 \wedge (\theta'_1, n-i, v'_1) \in \lfloor \tau_1\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H'_1(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_1) \backslash dom(\theta).\theta'_1(a) \searrow pc\ \sigma)$ (FU-PA1)

<u>IH2</u>:

$\forall H_2, n_2.(n_2, H_2) \triangleright \theta'_1 \wedge \forall j < n_2.(H_2, (e_2)\ \delta) \Downarrow_k (H'_2, v'_2) \implies$
$\exists \theta'_2.\theta'_1 \sqsubseteq \theta'_2 \wedge (n_2 - j, H'_2) \triangleright \theta'_2 \wedge (\theta'_2, n_2 - j, v'_2) \in \lfloor (\tau_2)\ \sigma \rfloor_V \wedge$

$(\forall a.H_2(a) \neq H_2'(a) \implies \exists \ell'.\theta_1'(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2')\backslash dom(\theta_1').\theta_2'(a) \searrow pc\ \sigma)$

We instantiate IH2 with H_1' and $n - i$. And since we know that $(n - i, H_1') \triangleright \theta_1' \wedge (H, (e_1, e_2)\ \delta) \Downarrow_{n'} (H', v')$ therefore we have

$\exists \theta_2'.\theta_1' \sqsubseteq \theta_2' \wedge (n - i - j, H_2') \triangleright \theta_2' \wedge (\theta_2', n - i - j, v_2') \in \lfloor (\tau_2)\ \sigma \rfloor_V \wedge$
$(\forall a.H_2(a) \neq H_2'(a) \implies \exists \ell'.\theta_1'(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2')\backslash dom(\theta_1').\theta_2'(a) \searrow pc\ \sigma)$ (FU-PA2)

In order to prove FU-PA0 we choose θ' as θ_2' from FU-PA2. Also we know from the evaluation rule, that let $v' = (v_1', v_2')$, $H' = H_2'$ and $n' = i + j + 1$. Now we are required to show

(a) $\theta \sqsubseteq \theta_2' \wedge (n - i - j - 1, H') \triangleright \theta_2' \wedge (\theta_2', n - i - j - 1, v') \in \lfloor (\tau_1 \times \tau_2)^{\perp} \rfloor_V$:
   - $\theta \sqsubseteq \theta_2'$:
     Since $\theta \sqsubseteq \theta_1'$ from FU-PA1 and $\theta_1' \sqsubseteq \theta_2'$ from FU-PA2 therefore from Definition 1.2 we get $\theta \sqsubseteq \theta_2'$
   - $(n - i - j - 1, H_2') \triangleright \theta_2'$:
     From FU-PA2 we get $(n - i - j, H_2') \triangleright \theta_2'$ therefore from Lemma 1.20 we get $(n - i - j - 1, H_2') \triangleright \theta_2'$
   - $(\theta_2', n - i - j, v') \in \lfloor (\tau_1 \times \tau_2)^{\perp}\ \sigma \rfloor_V$:
     From Definition 1.6 it suffices to show
     i. $(\theta_2', n - i - j - 1, v_1') \in \lfloor (\tau_1)\ \sigma \rfloor_V$:
        Since from FU-PA1 we know that $(\theta_1', n-i, v_1') \in \lfloor (\tau_1)\ \sigma \rfloor_V$ and since $\theta_1' \sqsubseteq \theta_2'$ (from FU-PA2) therefore from Lemma 1.16 we get
        $(\theta_2', n - i - j - 1, v_1') \in \lfloor (\tau_1)\ \sigma \rfloor_V$
     ii. $(\theta_2', n - i - j - 1, v_2') \in \lfloor (\tau_2)\ \sigma \rfloor_V$:
        From FU-PA2 we know that $(\theta_2', n - i - j, v_2') \in \lfloor (\tau_2)\ \sigma \rfloor_V$ therefore from Lemma 1.16 we get $(\theta_2', n - i - j - 1, v_2') \in \lfloor (\tau_2)\ \sigma \rfloor_V$

(b) $(\forall a \in dom(H).H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell')$
   From FU-PA1 and FU-PA2

(c) $(\forall a \in dom(\theta_2')\backslash dom(\theta).\theta_2'(a) \searrow pc\ \sigma)$
   From FU-PA1 and FU-PA2

5. FG-fst:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_i : (\tau_1 \times \tau_2)^{\ell} \qquad \Sigma; \Psi \vdash \tau_1 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{fst}(e_i) : \tau_1}$$

To prove: $(\theta, n, \mathsf{fst}(e_i)\ \delta) \in \lfloor \tau_1\ \sigma \rfloor_E^{pc\ \sigma}$

This means that from Definition 1.7 we need to prove

$\forall H.(n, H) \triangleright \theta \wedge \forall n' < n.(H, \mathsf{fst}(e_i)\ \delta) \Downarrow_{n'} (H', v') \implies$
$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \triangleright \theta' \wedge (\theta', n - n', v') \in \lfloor \tau_1\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$

This means that given some heap H s.t $(n, H) \triangleright \theta \wedge (H, \mathsf{fst}(e_i)\ \delta) \Downarrow_{n'} (H', v')$

It suffices to prove

$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \triangleright \theta' \wedge (\theta', n - n', v') \in \lfloor \tau_1\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$ (FU-F0)

IH1:

$\forall H_1, n_1.(n_1, H_1) \triangleright \theta \wedge \forall i < n_1.(H_1, (e_i)\ \delta) \Downarrow_i (H_1', v_1') \implies$
$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n_1 - i, H_1') \triangleright \theta_1' \wedge (\theta_1', n_1 - i, v_1') \in \lfloor (\tau_1 \times \tau_2)^\ell\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$

Instantiating IH1 with H and n. Since we know that $H \triangleright \theta \wedge (H, \mathsf{fst}(e_i)\ \delta) \Downarrow (H', v')$ therefore we have

$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n - i, H_1') \triangleright \theta_1' \wedge (\theta_1', n - i, v_1') \in \lfloor (\tau_1 \times \tau_2)^\ell\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$ (FU-F1)

From evaluation rule we know that $v_1' = (v_1'', v_2'')$

In order to prove FU-F0 we choose θ' as θ_1' from FU-P1. Also we know that $H' = H_1'$ and $v' = v_1''$. Now we are required to show

(a) $\theta \sqsubseteq \theta_1' \wedge (n - i - 1, H_1') \triangleright \theta_1' \wedge (\theta_1', n - i - 1, v_1') \in \lfloor \tau_1\ \sigma \rfloor_V$:
   - $\theta \sqsubseteq \theta_1'$:
     From FU-F1
   - $(n - i - 1, H_1') \triangleright \theta_1'$:
     From FU-F1 we know $(n - i, H_1') \triangleright \theta_1'$ therefore from Lemma 1.20 we get $(n - i - 1, H_1') \triangleright \theta_1'$
   - $(\theta_1', n - i, v_1'') \in \lfloor \tau_1\ \sigma \rfloor_V$:
     Since from FU-F1 we know that $(\theta_1', n - i, (v_1'', v_2'')) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V$
     Therefore from Definition 1.6 we know that $(\theta_1', n - i, v_1'') \in \lfloor \tau_1\ \sigma \rfloor_V$
     From Lemma 1.16 we get $(\theta_1', n - i - 1, v_1'') \in \lfloor \tau_1\ \sigma \rfloor_V$

(b) $(\forall a \in dom(H).H(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell')$
   From FU-F1

(c) $(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$
   From FU-F1

6. FG-snd:

   Symmetric case to FG-fst

7. FG-inl:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_i : \tau_1}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inl}(e_i) : (\tau_1 + \tau_2)^\perp}$$

   To prove: $(\theta, n, \mathsf{inl}(e_i)\ \delta) \in \lfloor (\tau_1 + \tau_2)^\perp\ \sigma \rfloor_E^{pc\ \sigma}$

   This means that from Definition 1.7 we need to prove

$\forall H, n.(n, H) \triangleright \theta \wedge \forall n' < n.(H, \mathsf{inl}(e_i)\ \delta) \Downarrow_{n'} (H', v') \implies$
$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \triangleright \theta' \wedge (\theta', n - n', v') \in \lfloor (\tau_1 + \tau_2)^{\perp} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$

This means that given some heap H and n s.t $(n, H) \triangleright \theta \wedge (H, \mathsf{inl}(e_i)\ \delta) \Downarrow_{n'} (H', v')$

It suffices to prove

$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \triangleright \theta' \wedge (\theta', n - n', v') \in \lfloor (\tau_1 + \tau_2)^{\perp} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$ (FU-LE0)

IH1:

$\forall H_1, n_1.(n_1, H_1) \triangleright \theta \wedge \forall i < n_1.(H_1, (e_i)\ \delta) \Downarrow_i (H_1', v_1') \implies$
$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n_1 - i, H_1') \triangleright \theta_1' \wedge (\theta_1', n_1 - i, v_1') \in \lfloor \tau_1\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$

Instantiating IH1 with H and n. Since we know that $(n, H) \triangleright \theta \wedge (H, \mathsf{inl}(e_i)\ \delta) \Downarrow_{n'} (H', v')$ therefore we have

$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n - i, H_1') \triangleright \theta_1' \wedge (\theta_1', n - i, v_1') \in \lfloor \tau_1\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$ (FU-LE1)

In order to prove FU-LE0 we choose θ' as θ_1' from FU-LE1. Also we know from the evaluation rule, that let $v' = \mathsf{inl}(v_1')$, $H' = H_1'$ and $n' = i + 1$. Now we are required to show

(a) $\theta \sqsubseteq \theta_1' \wedge (n - i - 1, H') \triangleright \theta_1' \wedge (\theta_1', n - i - 1, v') \in \lfloor (\tau_1 + \tau_2) \rfloor_V$:
- $\theta \sqsubseteq \theta_1'$:
  From FU-LE1
- $(n - i - 1, H') \triangleright \theta_1'$:
  From FU-LE1 we know that $(n - i, H') \triangleright \theta_1'$ therefore from Lemma 1.20 we get $(n - i - 1, H') \triangleright \theta_1'$
- $(\theta_1', n - i - 1, v') \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V$:
  Since $v' = \mathsf{inl}(v_1')$ and from FU-LE1 we know that $(\theta_1', n - i, v_1') \in \lfloor \tau_1\ \sigma \rfloor_V$
  Therefore from Definition 1.6 we get $(\theta_1', n - i, v') \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V$
  From Lemma 1.16 we get $(\theta_1', n - i - 1, v') \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V$

(b) $(\forall a \in dom(H).H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell')$
From FU-LE1

(c) $(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$
From FU-LE1

8. FG-inr:

   Symmetric case to FG-inl

9. FG-case:

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e : (\tau_1 + \tau_2)^{\ell} \qquad \Sigma;\Psi;\Gamma, x:\tau_1 \vdash_{pc \sqcup \ell} e_1 : \tau \qquad \Sigma;\Psi;\Gamma, y:\tau_2 \vdash_{pc \sqcup \ell} e_2 : \tau \qquad \Sigma;\Psi \vdash \tau \searrow \ell}{\Sigma;\Psi;\Gamma \vdash_{pc} \mathsf{case}(e, x.e_1, y.e_2) : \tau}$$

To prove: $(\theta, n, (\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta) \in \lfloor \tau\ \sigma \rfloor_E^{pc}$

This means that from Definition 1.7 we need to prove

$\forall H, n.(n, H) \rhd \theta \wedge \forall n' < n.(H, (\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta) \Downarrow_{n'} (H', v') \implies$
$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \rhd \theta' \wedge (\theta', n - n', v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$

This means that given some heap H and n s.t $(n, H) \rhd \theta \wedge (H, (\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta) \Downarrow_{n'} (H', v')$

It suffices to prove

$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \rhd \theta' \wedge (\theta', n - n', v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$ (FU-C0)

IH1:

$\forall H_1, n_1.(n_1, H_1) \rhd \theta \wedge \forall i < n_1.(H_1, (e_c)\ \delta) \Downarrow_i (H_1', v_c') \implies$
$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n_1 - i, H_1') \rhd \theta_1' \wedge (\theta_1', n_1 - i, v_c') \in \lfloor (\tau_1 + \tau_2)^{\ell}\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$

Instantiating IH1 with H and n. Since we know that $H \rhd \theta \wedge (H, (\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta) \Downarrow_{n'} (H', v')$ therefore we have

$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n - i, H_1') \rhd \theta_1' \wedge (\theta_1', n - i, v_c') \in \lfloor (\tau_1 + \tau_2)^{\ell}\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$ (FU-C1)

2 cases arise:

(a) $v_c' = \mathsf{inl}(v_{ci})$:

IH2:

$\forall H_2, n_2.(n_2, H_2) \rhd \theta_1' \wedge \forall j < n_2.(H_2, (e_1)\ \delta \cup \{x \mapsto v_{ci}\}) \Downarrow_j (H_2', v_2') \implies$
$\exists \theta_2'.\theta_1' \sqsubseteq \theta_2' \wedge (n_2 - j, H_2') \rhd \theta_2' \wedge (\theta_2', n_2 - j, v_2') \in \lfloor (\tau)\ \sigma \rfloor_V \wedge$
$(\forall a.H_2(a) \neq H_2'(a) \implies \exists \ell'.\theta_1'(a) = \mathsf{A}^{\ell'} \wedge (pc \sqcup \ell)\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2') \backslash dom(\theta_1').\theta_2'(a) \searrow (pc \sqcup \ell)\ \sigma)$

Instantiating IH2 with H_1' and $n-i$ since we know that $H_1' \rhd \theta_1' \wedge (H, (\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta) \Downarrow (H', v')$ therefore we have

$\exists \theta_2'.\theta_1' \sqsubseteq \theta_2' \wedge (n - i - j, H_2') \rhd \theta_2' \wedge (\theta_2', n - i - j, v_2') \in \lfloor (\tau)\ \sigma \rfloor_V \wedge$
$(\forall a.H_2(a) \neq H_2'(a) \implies \exists \ell'.\theta_1'(a) = \mathsf{A}^{\ell'} \wedge (pc \sqcup \ell)\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2') \backslash dom(\theta_1').\theta_2'(a) \searrow (pc \sqcup \ell)\ \sigma)$ (FU-C2)

In order to prove FU-C0 we choose θ' as θ_2' from FU-C2. Also we know that $H' = H_2'$, $v' = v_2'$ and $n' = i + j + 1$. Now we are required to show

i. $\theta \sqsubseteq \theta'_2 \wedge (n-i-j-1, H'_2) \triangleright \theta'_2 \wedge (\theta'_2, n-i-j-1, v'_2) \in \lfloor \tau\ \sigma \rfloor_V$:

- $\theta \sqsubseteq \theta'_2$:
  Since $\theta \sqsubseteq \theta'_1$ from FU-C1 and $\theta'_1 \sqsubseteq \theta'_2$ from FU-C2 therefore from Definition 1.2 we get $\theta \sqsubseteq \theta'_2$
- $(n-i-j-1, H'_2) \triangleright \theta'_2$:
  From FU-C2 we know that $(n-i-j, H'_2) \triangleright \theta'_2$ therefore from Lemma 1.20 we get $(n-i-j-1, H'_2) \triangleright \theta'_2$
- $(\theta'_2, n-i-j-1, v'_2) \in \lfloor \tau\ \sigma \rfloor_V$:
  From FU-C2 we know that $(\theta'_2, n-i-j, v'_2) \in \lfloor \tau\ \sigma \rfloor_V$ therefore from Lemma 1.16 we get $(\theta'_2, n-i-j-1, v'_2) \in \lfloor \tau\ \sigma \rfloor_V$

ii. $(\forall a \in dom(H).H(a) \neq H'_2(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell')$:
Since from FU-C2 we know that
$(\forall a.H'_1(a) \neq H'_2(a) \implies \exists \ell'.\theta'_1(a) = \mathsf{A}^{\ell'} \wedge (pc \sqcup \ell)\ \sigma \sqsubseteq \ell')$
therefore we also have
$(\forall a.H'_1(a) \neq H'_2(a) \implies \exists \ell'.\theta'_1(a) = \mathsf{A}^{\ell'} \wedge (pc)\ \sigma \sqsubseteq \ell')$

and from FU-C1 we know that
$(\forall a.H(a) \neq H'_1(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge (pc)\ \sigma \sqsubseteq \ell')$

Combining the two we get
$(\forall a \in dom(H).H(a) \neq H'_2(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell')$

iii. $(\forall a \in dom(\theta'_2) \backslash dom(\theta).\theta'_2(a) \searrow pc\ \sigma)$:
Since from FU-C2 we know that
$(\forall a \in dom(\theta'_2) \backslash dom(\theta'_1).\theta'_2(a) \searrow (pc \sqcup \ell)\ \sigma)$
therefore we also have
$(\forall a \in dom(\theta'_2) \backslash dom(\theta'_1).\theta'_2(a) \searrow (pc)\ \sigma)$

and from FU-C1 we know that
$(\forall a \in dom(\theta'_1) \backslash dom(\theta).\theta'_1(a) \searrow (pc \sqcup \ell)\ \sigma)$

Combining the two we get
$(\forall a \in dom(\theta'_2) \backslash dom(\theta).\theta'_2(a) \searrow pc\ \sigma)$

(b) $v'_c = \mathsf{inr}(v_{ci})$:
Symmetric case as $v'_c = \mathsf{inl}(v_{ci})$

10. FG-ref:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_i : \tau \qquad \Sigma; \Psi \vdash \tau \searrow pc}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{new}\ e_i : (\mathsf{ref}\ \tau)^{\perp}}$$

To prove: $(\theta, n, \mathsf{new}\ (e_i)\ \delta) \in \lfloor (\mathsf{ref}\ \tau)^{\perp}\ \sigma \rfloor_E^{pc}$

This means that from Definition 1.7 we need to prove

$\forall H, n.(n, H) \triangleright \theta \wedge \forall n' < n.(H, \mathsf{new}\ (e_i)\ \delta) \Downarrow_{n'} (H', v') \implies$
$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n-n', H') \triangleright \theta' \wedge (\theta', n-n', v') \in \lfloor (\mathsf{ref}\ \tau)^{\perp} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$

This means that given some heap H and n s.t $(n, H) \triangleright \theta \wedge (H, \mathsf{new}\ (e_i)\ \delta) \Downarrow_{n'} (H', v')$

It suffices to prove

$\exists\theta'.\theta \sqsubseteq \theta' \wedge (n-n', H') \rhd \theta' \wedge (\theta', n-n', v') \in \lfloor (\mathsf{ref}\ \tau)^{\perp} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$ (FU-R0)

<u>IH1</u>:

$\forall H_1, n_1.(n_1, H_1) \rhd \theta \wedge \forall i < n_1.(H_1, (e_i)\ \delta) \Downarrow_i (H_1', v_1') \implies$
$\exists\theta_1'.\theta \sqsubseteq \theta_1' \wedge (n_1 - i, H_1') \rhd \theta_1' \wedge (\theta_1', n_1 - i, v_1') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$

Instantiating IH1 with H and n. Since we know that $(n, H) \rhd \theta \wedge (H, \mathsf{new}\ (e_i)\ \delta) \Downarrow_{n'} (H', v')$ therefore we have

$\exists\theta_1'.\theta \sqsubseteq \theta_1' \wedge (n - i, H_1') \rhd \theta_1' \wedge (\theta_1', n - i, v_1') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$ (FU-R1)

From the evaluation rule we know that $H' = H_1'[a \mapsto v_1']$ where $a \notin dom(H_1')$, $v' = a$ and $n' = i + 1$. In order to prove FU-R0 we choose θ' as $\theta_2' = (\theta_1' \cup \{a \mapsto \tau\ \sigma\})$. Now we are required to show

(a) $\theta \sqsubseteq \theta_2' \wedge (n - i - 1, H') \rhd \theta_2' \wedge (\theta_2', n - i - 1, v') \in \lfloor (\mathsf{ref}\ \tau)^{\perp}\ \sigma \rfloor_V$:
- $\theta \sqsubseteq \theta_2'$:
  From FU-R1 we know that $\theta \sqsubseteq \theta_1'$ therefore from Definition 1.2 $\theta \sqsubseteq \theta_2'$
- $(n - i - 1, H') \rhd \theta_2'$:
  From FU-R1 we know that $(n - i, H_1') \rhd \theta_1'$. Therefore from Lemma 1.20 we get $(n - i - 1, H_1') \rhd \theta_1'$.
  We also know that $(\theta_1', n-i, v_1') \in \lfloor \tau\ \sigma \rfloor_V$ (from FU-R1) therefore from Lemma 1.16 we get $(\theta_1', n - i - 1, v_1') \in \lfloor \tau\ \sigma \rfloor_V$
  Since $H' = H_1'[a \mapsto v_1']$ and $\theta_2' = (\theta_1' \cup \{a \mapsto \tau\ \sigma\})$ therefore from Definition 1.8 we get $(n - i - 1, H') \rhd \theta_2'$
- $(\theta_2', n - i - 1, a) \in \lfloor (\mathsf{ref}\ \tau)^{\perp}\ \sigma \rfloor_V$:
  Since $\theta_2'(a) = \tau\ \sigma$ therefore from Definition 1.6 we get $(\theta_2', n - i - 1, a) \in \lfloor (\mathsf{ref}\ \tau)^{\perp}\ \sigma \rfloor_V$

(b) $(\forall a \in dom(H).H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell')$
From FU-R1

(c) $(\forall a \in dom(\theta_2') \backslash dom(\theta).\theta_2'(a) \searrow pc\ \sigma)$:
We get this from FU-R1 and $\tau\ \sigma \searrow pc\ \sigma$ (given)

11. FG-deref:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_i : (\mathsf{ref}\ \tau)^{\ell} \qquad \Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \tau' \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} !e_i : \tau'}$$

To prove: $(\theta, n, (!e_i)\ \delta) \in \lfloor \tau'\ \sigma \rfloor_E^{pc}$

This means that from Definition 1.7 we need to prove

$\forall H, n.(n, H) \rhd \theta \wedge \forall n' < n.(H, (!e_i)\ \delta) \Downarrow_{n'} (H', v') \implies$
$\exists\theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \rhd \theta' \wedge (\theta', n - n', v') \in \lfloor \tau'\ \sigma \rfloor_V \wedge$

$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta).\theta'(a) \searrow pc)$

This means that given some heap H and n s.t $(n, H) \triangleright \theta \wedge (H, (!e_i)\ \delta) \Downarrow_{n'} (H', v')$

It suffices to prove

$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \triangleright \theta' \wedge (\theta', n - n', v') \in \lfloor \tau'\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta).\theta'(a) \searrow pc)$ (FU-D0)

IH1:

$\forall H_1, n_1.(n_1, H_1) \triangleright \theta \wedge \forall i < n_1.(H_1, (e_i)\ \delta) \Downarrow_i (H_1', v_1') \implies$
$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n_1 - i, H_1') \triangleright \theta_1' \wedge (\theta_1', n_1 - i, v_1') \in \lfloor ((\mathsf{ref}\ \tau))^\ell\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1')\backslash dom(\theta).\theta_1'(a) \searrow pc)$

Instantiating IH1 with H and n. Since we know that $(n, H) \triangleright \theta \wedge (H, !(e_i)\ \delta) \Downarrow_{n'} (H', v')$ therefore we have

$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n - i, H_1') \triangleright \theta_1' \wedge (\theta_1', n - i, v_1') \in \lfloor ((\mathsf{ref}\ \tau))^\ell\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1')\backslash dom(\theta).\theta_1'(a) \searrow pc)$ (FU-D1)

In order to prove FU-D0 we choose θ' as θ_1' from FU-D1. Also we know from the evaluation rule, that $H' = H_1'$, $v' = H_1'(a)$, $v_1' = a$ and $n' = i + 1$. Now we are required to show

(a) $\theta \sqsubseteq \theta_1' \wedge (n - i - 1, H') \triangleright \theta_1' \wedge (\theta_1', n - i - 1, v') \in \lfloor \tau\ \sigma \rfloor_V$:
- $\theta \sqsubseteq \theta_1'$:
  From FU-D1
- $(n - i - 1, H') \triangleright \theta_1'$:
  From FU-D1 we know that $(n - i, H') \triangleright \theta_1'$ therefore from Lemma 1.20 we get $(n - i - 1, H') \triangleright \theta_1'$
- $(\theta_1', n - i - 1, v') \in \lfloor \tau'\ \sigma \rfloor_V$:
  Since from FU-D1 we know that $(n - i, H_1') \triangleright \theta_1'$ therefore from the Definition 1.8 we get $(\theta_1', n - i, H_1'(a)) \in \lfloor \tau\ \sigma \rfloor_V$
  From Lemma 1.16 we get $(\theta_1', n - i - 1, H_1'(a)) \in \lfloor \tau\ \sigma \rfloor_V$
  Since $\tau\ \sigma <: \tau'\ \sigma$ therefore from Lemma 1.24 we get $(\theta_1', n - i - 1, H_1'(a)) \in \lfloor \tau'\ \sigma \rfloor_V$

(b) $(\forall a \in dom(H).H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell')$
From FU-D1

(c) $(\forall a \in dom(\theta_1')\backslash dom(\theta).\theta_1'(a) \searrow pc)$
From FU-D1

12. FG-assign:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\mathsf{ref}\ \tau)^\ell \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau \qquad \Sigma; \Psi \vdash \tau \searrow (pc \sqcup \ell)}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 := e_2 : \mathsf{unit}}$$

To prove: $(\theta, n, (e_1 := e_2)\ \delta) \in \lfloor \mathsf{unit}\ \sigma \rfloor_E^{pc}$

This means that from Definition 1.7 we need to prove

$\forall H, n.(n, H) \triangleright \theta \wedge \forall n' < n.(H, (e_1 := e_2)\ \delta) \Downarrow_{n'} (H', v') \implies$
$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \triangleright \theta' \wedge (\theta', n - n', v') \in \lfloor \mathsf{unit} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc)$

This means that given some heap H and n s.t $(n, H) \triangleright \theta \wedge (H, (e_1 := e_2)\ \delta) \Downarrow_{n'} (H', v')$

It suffices to prove

$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \triangleright \theta' \wedge (\theta', n - n', v') \in \lfloor \mathsf{unit} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc)$ (FU-A0)

IH1:

$\forall H_1, n_1.(n_1, H_1) \triangleright \theta \wedge \forall i < n_1.(H_1, (e_1)\ \delta) \Downarrow_i (H_1', v_1') \implies$
$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n_1 - i, H_1') \triangleright \theta_1' \wedge (\theta_1', n_1 - i, v_1') \in \lfloor ((\mathsf{ref}\ \tau))^\ell\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc)$

Instantiating IH1 with H and n. Since we know that $(n, H) \triangleright \theta \wedge (H, (e_1 := e_2)\ \delta) \Downarrow_{n'} (H', v')$ therefore we have

$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n - i, H_1') \triangleright \theta_1' \wedge (\theta_1', n - i, v_1') \in \lfloor ((\mathsf{ref}\ \tau))^\ell\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc)$ (FU-A1)

IH2:

$\forall H_2, n_2.(n_2, H_2) \triangleright \theta_1' \wedge \forall j < n_2.(H_2, (e_2)\ \delta) \Downarrow_j (H_2', v_2') \implies$
$\exists \theta_2'.\theta_1' \sqsubseteq (n_2 - j, \theta_2') \wedge H_2' \triangleright \theta_2' \wedge (\theta_2', n_2 - j, v_2') \in \lfloor (\tau)\ \sigma \rfloor_V \wedge$
$(\forall a.H_2(a) \neq H_2'(a) \implies \exists \ell'.\theta_1'(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2') \backslash dom(\theta_1').\theta_2'(a) \searrow pc)$

Instantiating IH2 with H_1' and since we know that $H_1' \triangleright \theta_1' \wedge (H, (e_1 := e_2)\ \delta) \Downarrow (H', v')$ therefore we have

$\exists \theta_2'.\theta_1' \sqsubseteq (n - i - j, \theta_2') \wedge H_2' \triangleright \theta_2' \wedge (\theta_2', n - i - j, v_2') \in \lfloor (\tau)\ \sigma \rfloor_V \wedge$
$(\forall a.H_2(a) \neq H_2'(a) \implies \exists \ell'.\theta_1'(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2') \backslash dom(\theta_1').\theta_2'(a) \searrow pc)$ (FU-A2)

In order to prove FU-A0 we choose θ' as θ_2' from FU-A2. Also we know from the evaluation rule, assign, that let $v_1' = a_1$, $H' = H_2'[a_1 \mapsto v_2']$, $v' = ()$ and $n' = i + j + 1$. Now we are required to show

(a) $\theta \sqsubseteq \theta_2' \wedge (n - i - j - 1, H') \triangleright \theta_2' \wedge (\theta_2', n - i - j - 1, ()) \in \lfloor \mathsf{unit} \rfloor_V$:

- $\theta \sqsubseteq \theta_2'$:
  Since $\theta \sqsubseteq \theta_1'$ from FU-A1 and $\theta_1' \sqsubseteq \theta_2'$ from FU-A2 therefore from Definition 1.2 we get $\theta \sqsubseteq \theta_2'$
- $(n - i - j - 1, H') \triangleright \theta_2'$:
  From Definition 1.8 it suffices to prove that
  i. $dom(\theta_2') \subseteq dom(H')$: From FU-A2
  ii. $\forall a \in dom(\theta_2').(\theta_2', n - i - j - 1, H'(a)) \in \lfloor \theta_2'(a) \rfloor_V$:
  $\forall a \in dom(\theta_2')$.

- $a = a_1$:
  From FU-A2 (since we know that $(\theta'_2, n-i-j, v'_2) \in \lfloor(\tau)\ \sigma\rfloor_V$)
  Therefore from Lemma 1.16 we get $(\theta'_2, n-i-j-1, v'_2) \in \lfloor(\tau)\ \sigma\rfloor_V$
- $a \neq a_1$:
  From FU-A2 (since we know that $(n-i-j, H'_2) \triangleright \theta'_2$ therefore from Lemma 1.20 we get $(n-i-j-1, H'_2) \triangleright \theta'_2$)

- $(\theta'_2, n-i-j-1, ()) \in \lfloor \mathsf{unit} \rfloor_V$:
  From Definition 1.6

(b) $(\forall a \in dom(H).H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell')$
$\forall a \in dom(H)$.

- $a = a_1$:
  Since we know that $H(a_1) \neq H'(a_1)$ and $\theta(a_1) = \tau = \mathsf{A}^{\ell_i}$ (given)
  It is given that $\tau\ \sigma \searrow pc\ \sigma$ therefore $pc\ \sigma \sqsubseteq \ell_i\ \sigma$
- $a \neq a_1$:
  From FU-A2

(c) $(\forall a \in dom(\theta'_2) \backslash dom(\theta).\theta'_2(a) \searrow pc)$
From FU-A2

13. FG-FI:

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash_{\ell_e} e_i : \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} \Lambda e_i : (\forall \alpha.(\ell_e, \tau))^{\perp}}$$

To prove: $(\theta, n, (\Lambda e_i)\ \delta) \in \lfloor(\forall \alpha.(\ell_e, \tau))^{\perp}\ \sigma\rfloor_E^{pc}$
This means that from Definition 1.7 we need to prove
$\forall H, n.(n, H) \triangleright \theta \wedge \forall n' < n.(H, (\Lambda e_i)\ \delta) \Downarrow_{n'} (H', v') \implies$
$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n-n', H') \triangleright \theta' \wedge (\theta', n-n', v') \in \lfloor(\forall \alpha.(\ell, \tau))^{\perp}\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$
This means that given some heap H and n s.t $(n, H) \triangleright \theta \wedge (H, (\Lambda e_i)\ \delta) \Downarrow (H', v')$
<u>It suffices to prove</u>
$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n-n', H') \triangleright \theta' \wedge (\theta', n-n', v') \in \lfloor(\forall \alpha.(\ell, \tau))^{\perp}\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$ (FU-FI0)

<u>IH1</u>:
$\forall n_1, \theta_i, \ell' \in \mathcal{L}.\ (\theta_i, n_1, e_i\ \delta) \in \lfloor \tau\ \sigma \cup \{\alpha \mapsto \ell''\}\rfloor_E^{\ell_e\ \sigma \cup \{\alpha \mapsto \ell''\}}$

In order to prove FU-FI0 we choose θ' as θ. Also we know from the evaluation rule, that $H' = H$ and $n' = 0$. Now we are required to show

(a) $\theta \sqsubseteq \theta \wedge (n, H) \triangleright \theta \wedge (\theta, n, v') \in \lfloor(\forall \alpha.(\ell_e, \tau))^{\perp}\rfloor_V\ \sigma$:
- $\theta \sqsubseteq \theta$: From Definition 1.2
- $(n, H) \triangleright \theta$: Given

- $(\theta, n, (\Lambda e_i)\delta) \in \lfloor(\forall\alpha.(\ell_e, \tau))^{\perp}\rfloor_V\ \sigma$:
  From Definition 1.6 it suffices to prove that
  $\forall\theta''.\theta \sqsubseteq \theta'' \wedge \forall j < n.\forall \ell_d \in \mathcal{L} \implies (\theta'', j, e_i) \in \lfloor\tau[\ell_d/\alpha]\ \sigma\rfloor_E^{\ell_e[\ell_d/\alpha]\ \sigma}$

  This means given some θ'', j and ℓ_d such that $\theta \sqsubseteq \theta''$, $j < n$ and $\ell_d \in \mathcal{L}$
  It suffices to prove that $(\theta'', j, e_i) \in \lfloor\tau[\ell_d/\alpha]\ \sigma\rfloor_E^{\ell_e[\ell_d/\alpha]\ \sigma}$

  Instantiating IH1 with j, θ'' and ℓ_d we get $(\theta_i, j, e_i\ \delta) \in \lfloor\tau\ \sigma\cup\{\alpha \mapsto \ell_d\}\rfloor_E^{\ell_e\ \sigma\cup\{\alpha\mapsto\ell_d\}}$

(b) $(\forall a.H(a) \neq H'(a) \implies \exists\ell'.\theta.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell')$:
Since $H' = H$ so we are done

(c) $(\forall a \in dom(\theta')\backslash dom(\theta).\theta(a) \searrow pc)$:
Since $\theta' = \theta$ so we are done

14. FG-FE:

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e_i : (\forall\alpha.(\ell_e, \tau))^{\ell} \qquad \ell'' \in \mathrm{FV}(\Sigma) \qquad \Sigma;\Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e[\ell''/\alpha] \qquad \Sigma;\Psi \vdash \tau[\ell''/\alpha] \searrow \ell}{\Sigma;\Psi;\Gamma \vdash_{pc} e_i\ [] : \tau[\ell''/\alpha]}$$

To prove: $(\theta, n, (e_i[])\ \delta) \in \lfloor\tau[\ell''/\alpha]\ \sigma\rfloor_E^{pc}$

This means that from Definition 1.7 we need to prove

$\forall H, n.(n, H) \triangleright \theta \wedge \forall n' < n.(H, (e_i[])\ \delta) \Downarrow_{n'} (H', v') \implies$
$\exists\theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \triangleright \theta' \wedge (\theta', n - n', v') \in \lfloor\tau[\ell''/\alpha]\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists\ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$

This means that given some heap H and n s.t $(n, H) \triangleright \theta \wedge (H, (e_i[])\ \delta) \Downarrow_{n'} (H', v')$

<u>It suffices to prove</u>

$\exists\theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \triangleright \theta' \wedge (\theta', n - n', v') \in \lfloor\tau[\ell''/\alpha]\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists\ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$ (FU-FE0)

<u>IH</u>:

$\forall H_1, n_1.(n_1, H_1) \triangleright \theta \wedge \forall i < n_1.(H_1, (e_i)\ \delta) \Downarrow_i (H_1', v_1') \implies$
$\exists\theta_1'.\theta \sqsubseteq \theta_1' \wedge (n_1 - i, H_1') \triangleright \theta_1' \wedge (\theta_1', n_1 - i, v_1') \in \lfloor(\forall\alpha.(\ell_e, \tau))^{\ell}\ \sigma\rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists\ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1')\backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$

Instantiating IH with H and n. Since we know that $(n, H) \triangleright \theta \wedge (H, (e_i[])\ \delta) \Downarrow_{n'} (H', v')$ therefore we have

$\exists\theta_1'.\theta \sqsubseteq \theta_1' \wedge (n - i, H_1') \triangleright \theta_1' \wedge (\theta_1', n - i, v_1') \in \lfloor(\forall\alpha.(\ell_e, \tau))^{\ell}\ \sigma\rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists\ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1')\backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$ (FU-FE1)

From evaluation rule we know that $v_1' = \Lambda e_{i1}$. Since from FU-FE1 we know that
$(\theta_1', n - i, \Lambda e_{i1}) \in \lfloor(\forall\alpha.(\ell_e, \tau))^{\ell}\ \sigma\rfloor_V$

This means from Definition 1.6 we have

$$\forall \theta''.\theta'_1 \sqsubseteq \theta'' \wedge \forall j < n - i.\forall \ell_g \in \mathcal{L} \implies (\theta'', j, e_{i1}) \in \lfloor \tau[\ell_g/\alpha]\ \sigma \rfloor_E^{\ell_e[\ell_g/\alpha]\ \sigma} \tag{5}$$

Instantiating Equation 5 with θ'_1, $n - i - 1$ and ℓ'' we get

$(\theta'_1, n - i - 1, e_{i1}) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E^{\ell_e[\ell''/\alpha]\ \sigma}$

This means from Definition 1.7 we have

$\forall H_3.(n - i - 1, H_3) \rhd \theta'_1 \wedge \forall k < n - i - 1.(H_3, e_{i1}) \Downarrow_k (H'_3, v'_3) \implies$
$\exists \theta'_3.\theta'_1 \sqsubseteq \theta'_3 \wedge (n - i - 1 - k, H'_3) \rhd \theta'_3 \wedge (\theta'_3, n - i - 1 - k, v'_3) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_V \wedge$
$(\forall a.H_3(a) \neq H'_3(a) \implies \exists \ell'.\theta'_1(a) = \mathsf{A}^{\ell'} \wedge \ell_e\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_3) \backslash dom(\theta'_1).\theta'_3(a) \searrow \ell_e\ \sigma)$

Instantiating H_3 with H'_1 from FU-FE1 and since we know that $(n - i - 1, H'_1) \rhd \theta'_1$ (Lemma 1.20)and since we know that $e_i[]\ \gamma \downarrow_1$ reduces in n' steps where $n' = i + k + 1$ and since $n' < n$ therefore we have $k < n - i - 1$ s.t $(H'_1, e_{i1}) \Downarrow_k (H'_3, v'_3)$. Therefore we get

$\exists \theta'_3.\theta'_1 \sqsubseteq \theta'_3 \wedge (n - i - 1 - k, H'_3) \rhd \theta'_3 \wedge (\theta'_3, n - i - 1 - k, v'_3) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_V \wedge$
$(\forall a.H_3(a) \neq H'_3(a) \implies \exists \ell'.\theta'_1(a) = \mathsf{A}^{\ell'} \wedge \ell_e\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_3) \backslash dom(\theta'_1).\theta'_3(a) \searrow \ell_e\ \sigma)$ (FU-FE2)

In order to prove FU-FE0 we choose θ' as θ'_3 from FU-FE2. Also we know that $H' = H'_3$, $v' = v'_3$ and $n' = i + k + 1$. Now we are required to show

(a) $\theta \sqsubseteq \theta'_3 \wedge (n - i - k - 1, H'_3) \rhd \theta'_3 \wedge (\theta'_3, n - i - k - 1, v'_3) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_V$:
   - $\theta \sqsubseteq \theta'_3$:
     Since $\theta \sqsubseteq \theta'_1$ from FU-FE1 and $\theta'_1 \sqsubseteq \theta'_3$ from FU-FE2 therefore from Definition 1.2 we get $\theta \sqsubseteq \theta'_3$
   - $(n - i - k - 1, H'_3) \rhd \theta'_3$:
     From FU-FE2 we know that $(n - i - k - 1, H'_3) \rhd \theta'_3$
   - $(\theta'_3, n - i - k - 1, v'_3) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_V$:
     From FU-FE2 we know that $(\theta'_3, n - i - k - 1, v'_3) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_V$

(b) $(\forall a \in dom(H).H(a) \neq H'_3(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell')$
   Since $pc\ \sigma \sqsubseteq \ell_e[\ell''/\alpha]\ \sigma$ therefore we get the desired from FU-FE1 and FU-FE2

(c) $(\forall a \in dom(\theta'_3) \backslash dom(\theta).\theta'_3(a) \searrow pc\ \sigma)$
   Since $pc\ \sigma \sqsubseteq \ell_e[\ell''/\alpha]\ \sigma$ therefore we get the desired from FU-FE1 and FU-FE2

15. FG-CI:

$$\frac{\Sigma; \Psi, c; \Gamma \vdash_{\ell_e} e_i : \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} \nu\ e_i : (c \overset{\ell_e}{\Rightarrow} \tau)^\perp}$$

To prove: $(\theta, n, (\nu e_i)\ \delta) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\perp\ \sigma \rfloor_E^{pc}$

This means that from Definition 1.7 we need to prove

$\forall H, n.(n, H) \rhd \theta \wedge \forall n' < n.(H, (\nu e_i)\ \delta) \Downarrow_{n'} (H', v') \implies$
$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \rhd \theta' \wedge (\theta', n - n', v') \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\perp\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$

This means that given some heap H and n s.t $(n, H) \rhd \theta \wedge (H, (\nu e_i)\ \delta) \Downarrow (H', v')$

<u>It suffices to prove</u>

$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \rhd \theta' \wedge (\theta', n - n', v') \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^{\perp}\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$ (FU-CI0)

<u>IH1</u>:

$\forall \theta_i, n_1.\ (\theta_i, n_1, e_i\ \delta) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma}$ such that $\mathcal{L} \models c\ \sigma$

In order to prove FU-FI0 we choose θ' as θ. Also we know from the evaluation rule, that $H' = H$, $v' = \nu\ e_i\ \delta$ and $n' = 0$. Now we are required to show

(a) $\theta \sqsubseteq \theta \wedge (n, H) \rhd \theta \wedge (\theta, n, v') \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^{\perp} \rfloor_V\ \sigma$:
   - $\theta \sqsubseteq \theta$: From Definition 1.2
   - $(n, H) \rhd \theta$: Given
   - $(\theta, n, (\nu e_i)\delta) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^{\perp} \rfloor_V\ \sigma$:
     From Definition 1.6 it suffices to prove that
     $\forall \theta''.\theta \sqsubseteq \theta'' \wedge \forall j < n.\mathcal{L} \models c\ \sigma \implies (\theta'', j, e_i\ \delta) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma}$

     This means given some θ'' such that $\theta \sqsubseteq \theta''$, $j < n$ and $\mathcal{L} \models c$
     It suffices to prove that $(\theta'', j, e_i\ \delta) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma}$

     Instantiating IH1 with θ'' and j we get $(\theta'', j, e_i\ \delta) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma}$

(b) $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell')$:
   Since $H' = H$ so we are done

(c) $(\forall a \in dom(\theta') \backslash dom(\theta).\theta(a) \searrow pc)$:
   Since $\theta' = \theta$ so we are done

16. FG-CE:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_i : (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell} \qquad \Sigma; \Psi \vdash c \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e \qquad \Sigma; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e_i \bullet : \tau}$$

To prove: $(\theta, n, (e_i \bullet)\ \delta) \in \lfloor \tau\ \sigma \rfloor_E^{pc}$

This means that from Definition 1.7 we need to prove

$\forall H, n.(n, H) \rhd \theta \wedge \forall n' < n.(H, (e_i \bullet)\ \delta) \Downarrow_{n'} (H', v') \implies$
$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \rhd \theta' \wedge (\theta', n - n', v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$

This means that given some heap H and n s.t $(n, H) \rhd \theta \wedge (H, (e_i \bullet)\ \delta) \Downarrow_{n'} (H', v')$

<u>It suffices to prove</u>

$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - n', H') \rhd \theta' \wedge (\theta', n - n', v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc\ \sigma)$ (FU-CE0)

<u>IH</u>:

$\forall H_1, n_1.(n_1, H_1) \rhd \theta \wedge \forall i < n_1.(H_1, (e_i)\ \delta) \Downarrow_i (H_1', v_1') \implies$
$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n_1 - i, H_1') \rhd \theta_1' \wedge (\theta_1', n_1 - i, v_1') \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\ell\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$

Instantiating IH with H and n. And since we know that $(n, H) \rhd \theta \wedge (H, (e_i[])\ \delta) \Downarrow_{n'} (H', v')$ therefore we have
$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n - i, H_1') \rhd \theta_1' \wedge (\theta_1', n - i, v_1') \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\ell\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc\ \sigma)$ (FU-CE1)

From evaluation rule we know that $v_1' = \nu e_{i1}$. Since from FU-CE1 we know that
$(\theta_1', n - i, \nu e_{i1}) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\ell\ \sigma \rfloor_V$

This means from Definition 1.6 we have

$$\forall \theta''.\theta_1' \sqsubseteq \theta'' \wedge \forall j < n - i.\mathcal{L} \models c\ \sigma \implies (\theta'', j, e_{i1}) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma} \tag{6}$$

Instantiating Equation 6 with θ_1' and $n - i - 1$ since we know that $\mathcal{L} \models c\ \sigma$ therefore we get
$(\theta_1', n - i - 1, e_{i1}) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma}$

This means from Definition 1.7 we have
$\forall H_3.(n - i - 1, H_3) \rhd \theta_1' \wedge \forall k < n - i - 1.(H_3, e_{i1}) \Downarrow_k (H_3', v_3') \implies$
$\exists \theta_3'.\theta_1' \sqsubseteq \theta_3' \wedge (n - i - 1 - k, H_3') \rhd \theta_3' \wedge (\theta_3', n - i - 1 - k, v_3') \in \lfloor \tau\ \sigma \rfloor_V \wedge (\forall a.H_3(a) \neq H_3'(a) \implies$
$\exists \ell'.\theta_1'(a) = \mathsf{A}^{\ell'} \wedge \ell_e\ \sigma \sqsubseteq \ell') \wedge (\forall a \in dom(\theta_3') \backslash dom(\theta_1').\theta_3'(a) \searrow \ell_e\ \sigma)$

Instantiating H_3 with H_1' from FU-CE1 and since we know that $(n - i - 1, H_1') \rhd \theta_1'$ (Lemma 1.20) and since we know that $e_i \bullet \gamma \downarrow_1$ reduces in n' steps where $n' = i + k + 1$ and since $n' < n$ therefore we have $k < n - i - 1$ s.t $(H_1', e_{i1}) \Downarrow_k (H_3', v_3')$. Therefore we get
$\exists \theta_3'.\theta_1' \sqsubseteq \theta_3' \wedge (n - i - 1 - k, H_3') \rhd \theta_3' \wedge (\theta_3', n - i - 1 - k, v_3') \in \lfloor \tau\ \sigma \rfloor_V \wedge (\forall a.H_3(a) \neq H_3'(a) \implies$
$\exists \ell'.\theta_1'(a) = \mathsf{A}^{\ell'} \wedge \ell_e\ \sigma \sqsubseteq \ell') \wedge (\forall a \in dom(\theta_3') \backslash dom(\theta_1').\theta_3'(a) \searrow \ell_e\ \sigma)$ (FU-CE2)

In order to prove FU-CE0 we choose θ' as θ_3' from FU-CE2. Also we know that $H' = H_3'$, $v' = v_3'$ and $n' = i + k + 1$. Now we are required to show

(a) $\theta \sqsubseteq \theta_3' \wedge (n - i - k - 1, H_3') \rhd \theta_3' \wedge (\theta_3', n - i - k - 1, v_3') \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_V$:
   - $\theta \sqsubseteq \theta_3'$:
     Since $\theta \sqsubseteq \theta_1'$ from FU-CE1 and $\theta_1' \sqsubseteq \theta_3'$ from FU-CE2 therefore from Definition 1.2 we get $\theta \sqsubseteq \theta_3'$
   - $(n - i - k - 1, H_3') \rhd \theta_3'$:
     From FU-CE3 we know that $(n - i - k - 1, H_3') \rhd \theta_3'$
   - $(\theta_3', n - i - k - 1, v_3') \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_V$:
     From FU-CE3 we know that $(\theta_3', n - i - k - 1, v_3') \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_V$

(b) $(\forall a \in dom(H).H(a) \neq H_3'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc\ \sigma \sqsubseteq \ell')$
   Since $pc\ \sigma \sqsubseteq \ell_e\ \sigma$ therefore we get the desired from FU-CE1 and FU-CE2

(c) $(\forall a \in dom(\theta_3')\backslash dom(\theta).\theta_3'(a) \searrow pc\ \sigma)$
Since $pc\ \sigma \sqsubseteq \ell_e\ \sigma$ therefore we get the desired from FU-CE1 and FU-CE2

□

Lemma 1.23 (FG: Expression subtyping with closed labels and types)**.** $\forall pc, pc', \tau.$
$\mathcal{L} \models pc \sqsubseteq pc' \implies \lfloor \tau \rfloor_E^{pc'} \subseteq \lfloor \tau \rfloor_E^{pc}$

Proof. Given: $\mathcal{L} \models pc \sqsubseteq pc'$
To prove: $\lfloor (\tau) \rfloor_E^{pc'} \subseteq \lfloor (\tau) \rfloor_E^{pc}$
This means we need to prove that
$\forall (\theta, n, e) \in \lfloor (\tau) \rfloor_E^{pc'}.\ (\theta, n, e) \in \lfloor (\tau) \rfloor_E^{pc}$

This means given $\forall (\theta, n, e) \in \lfloor (\tau) \rfloor_E^{pc'}$
It suffices to prove that $(\theta, n, e) \in \lfloor (\tau) \rfloor_E^{pc}$

From Definition 1.7 for the chosen θ, n, e we are given:
$\forall H.(n, H) \rhd \theta \wedge \forall j < n.(H, e) \Downarrow_j (H', v') \implies$
$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - j, H') \rhd \theta' \wedge (\theta', n - j, v') \in \lfloor \tau \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc' \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta).\theta'(a) \searrow pc')$ (A)

And we need prove that
$\forall H_1.(n, H_1) \rhd \theta \wedge \forall k < n.(H_1, e) \Downarrow_k (H_1', v') \implies$
$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n - k, H_1') \rhd \theta_1' \wedge (\theta_1', n - k, v') \in \lfloor \tau \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1')\backslash dom(\theta).\theta_1'(a) \searrow pc)$

This means that we are given some H_1 and k such that $(n, H_1) \rhd \theta$, $k < n$ and $(H_1, e) \Downarrow_k (H_1', v')$
It suffices to prove:
$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n - k, H_1') \rhd \theta_1' \wedge (\theta_1', n - k, v') \in \lfloor \tau \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1')\backslash dom(\theta).\theta_1'(a) \searrow pc)$

Instantiate H in (A) with H_1 and then we choose θ_1' as θ'

- $\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - k, H_1') \rhd \theta' \wedge (\theta', n - k, v') \in \lfloor \tau \rfloor_V$:
  Given
- $(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell')$:
  Since $pc \sqsubseteq pc'$ and we are given
  $(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc' \sqsubseteq \ell')$
  Therefore
  $(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell')$
- $(\forall a \in dom(\theta')\backslash dom(\theta).\theta'(a) \searrow pc)$:
  We are given
  $(\forall a \in dom(\theta')\backslash dom(\theta).\theta'(a) \searrow pc')$
  and since $pc \sqsubseteq pc'$ Therefore
  $(\forall a \in dom(\theta')\backslash dom(\theta).\theta'(a) \searrow pc)$

□

Lemma 1.24 (FG: Subtyping unary)**.** *The following holds:*
$\forall \Sigma, \Psi, \sigma.$

1. $\forall \mathsf{A}, \mathsf{A}'.$

   (a) $\Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor (\mathsf{A}\ \sigma) \rfloor_V \subseteq \lfloor (\mathsf{A}'\ \sigma) \rfloor_V$

2. $\forall \tau, \tau'.$

   (a) $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor (\tau\ \sigma) \rfloor_V \subseteq \lfloor (\tau'\ \sigma) \rfloor_V$

   (b) $\forall pc.\ \Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor (\tau\ \sigma) \rfloor_E^{pc} \subseteq \lfloor (\tau'\ \sigma) \rfloor_E^{pc}$

Proof. Proof by simultaneous induction on $\mathsf{A} <: \mathsf{A}'$ and $\tau <: \tau'$
Proof of statement 1(a)
We analyse the different cases of $\mathsf{A} <: \mathsf{A}'$ in the last step:

1. FGsub-arrow:

   Given:
   $$\dfrac{\Sigma; \Psi \vdash \tau_1' <: \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2' \qquad \Sigma; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'}\ \text{FGsub-arrow}$$

   To prove: $\lfloor ((\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma) \rfloor_V \subseteq \lfloor ((\tau_1' \xrightarrow{\ell_e'} \tau_2')\ \sigma) \rfloor_V$

   IH1: $\lfloor (\tau_1'\ \sigma) \rfloor_V \subseteq \lfloor (\tau_1\ \sigma) \rfloor_V$ (Statement 2(a))
   IH2: $\forall pc.\ \lfloor (\tau_2\ \sigma) \rfloor_E^{pc} \subseteq \lfloor (\tau_2'\ \sigma) \rfloor_E^{pc}$ (Statement 2(b))
   It suffices to prove: $\forall (\theta, n, \lambda x.e_i) \in \lfloor ((\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma) \rfloor_V.\ (\theta, n, \lambda x.e_i) \in \lfloor ((\tau_1' \xrightarrow{\ell_e'} \tau_2')\ \sigma) \rfloor_V$

   This means that given some θ, n and $\lambda x.e_i$ s.t $(\theta, n, \lambda x.e_i) \in \lfloor ((\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma) \rfloor_V$
   Therefore from Definition 1.6 we are given:

   $$\forall \theta_1.\theta \sqsubseteq \theta_1 \wedge \forall i < n.\forall v.(\theta_1, i, v) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta_1, i, e_i[v/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma} \tag{7}$$

   And it suffices to prove: $(\theta, n, \lambda x.e_i) \in \lfloor ((\tau_1' \xrightarrow{\ell_e'} \tau_2')\ \sigma) \rfloor_V$

   Again from Definition 1.6, it suffices to prove:
   $\forall \theta_2.\theta \sqsubseteq \theta_2 \wedge \forall j < n.\forall v.(\theta_2, j, v) \in \lfloor \tau_1'\ \sigma \rfloor_V \implies (\theta_2, j, e_i[v/x]) \in \lfloor \tau_2'\ \sigma \rfloor_E^{\ell_e'\ \sigma}$

   This means that given some $\theta_2, j < n, v$ s.t $\theta \sqsubseteq \theta_2$ and $(\theta_2, j, v) \in \lfloor \tau_1'\ \sigma \rfloor_V$
   And we are required to prove: $(\theta_2, j, e_i[v/x]) \in \lfloor \tau_2'\ \sigma \rfloor_E^{\ell_e'\ \sigma}$

   Since $(\theta_2, j, v) \in \lfloor \tau_1'\ \sigma \rfloor_V$ therefore from IH1 we know that $(\theta_2, j, v) \in \lfloor \tau_1\ \sigma \rfloor_V$
   As a result from Equation 7 we know that
   $(\theta_2, j, e_i[v/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$

From IH2, we know that
$(\theta_2, j, e_i[v/x]) \in \lfloor \tau_2' \ \sigma \rfloor_E^{\ell_e \ \sigma}$
Since $\mathcal{L} \models \ell_e' \ \sigma \sqsubseteq \ell_e \ \sigma$ therefore from Lemma 1.23 we know that
$(\theta_2, j, e_i[v/x]) \in \lfloor \tau_2' \ \sigma \rfloor_E^{\ell_e' \ \sigma}$

2. FGsub-prod:
Given:

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'} \text{ FGsub-prod}$$

To prove: $\lfloor ((\tau_1 \times \tau_2) \ \sigma) \rfloor_V \subseteq \lfloor ((\tau_1' \times \tau_2') \ \sigma) \rfloor_V$

IH1: $\lfloor (\tau_1 \ \sigma) \rfloor_V \subseteq \lfloor (\tau_1' \ \sigma) \rfloor_V$ (Statement 2(a))
IH2: $\lfloor (\tau_2 \ \sigma) \rfloor_V \subseteq \lfloor (\tau_2' \ \sigma) \rfloor_V$ (Statement 2(a))
It suffices to prove: $\forall (\theta, n, (v_1, v_2)) \in \lfloor ((\tau_1 \times \tau_2) \ \sigma) \rfloor_V. \ (\theta, n, (v_1, v_2)) \in \lfloor ((\tau_1' \times \tau_2') \ \sigma) \rfloor_V$

This means that given some θ, n and $(v_1, v_2 \ (\theta, (v_1, v_2)) \in \lfloor ((\tau_1 \times \tau_2) \ \sigma) \rfloor_V$
Therefore from Definition 1.6 we are given:

$$(\theta, n, v_1) \in \lfloor \tau_1 \ \sigma \rfloor_V \wedge (\theta, n, v_2) \in \lfloor \tau_2 \ \sigma \rfloor_V \tag{8}$$

And it suffices to prove: $(\theta, (v_1, v_2)) \in \lfloor ((\tau_1' \times \tau_2') \ \sigma) \rfloor_V$

Again from Definition 1.6, it suffices to prove:
$(\theta, n, v_1) \in \lfloor \tau_1' \ \sigma \rfloor_V \wedge (\theta, n, v_2) \in \lfloor \tau_2' \ \sigma \rfloor_V$

Since from Equation 8 we know that $(\theta, n, v_1) \in \lfloor \tau_1 \ \sigma \rfloor_V$ therefore from IH1 we have $(\theta, n, v_1) \in \lfloor \tau_1' \ \sigma \rfloor_V$
Similarly since $(\theta, n, v_2) \in \lfloor \tau_2 \ \sigma \rfloor_V$ from Equation 8 therefore from IH2 we have $(\theta, n, v_2) \in \lfloor \tau_2' \ \sigma \rfloor_V$

3. FGsub-sum:
Given:

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'} \text{ FGsub-sum}$$

To prove: $\lfloor ((\tau_1 + \tau_2) \ \sigma) \rfloor_V \subseteq \lfloor ((\tau_1' + \tau_2') \ \sigma) \rfloor_V$

IH1: $\lfloor (\tau_1 \ \sigma) \rfloor_V \subseteq \lfloor (\tau_1' \ \sigma) \rfloor_V$ (Statement 2(a))
IH2: $\lfloor (\tau_2 \ \sigma) \rfloor_V \subseteq \lfloor (\tau_2' \ \sigma) \rfloor_V$ (Statement 2(a))
It suffices to prove: $\forall (\theta, n, v_s) \in \lfloor ((\tau_1 + \tau_2) \ \sigma) \rfloor_V. \ (\theta, v_s) \in \lfloor ((\tau_1' + \tau_2') \ \sigma) \rfloor_V$

This means that given: $(\theta, n, v_s) \in \lfloor ((\tau_1 + \tau_2) \ \sigma) \rfloor_V$
And it suffices to prove: $(\theta, n, v_s) \in \lfloor ((\tau_1' + \tau_2') \ \sigma) \rfloor_V$

2 cases arise

(a) $v_s = \mathsf{inl}\ v_i$:
From Definition 1.6 we are given:

$$(\theta, n, v_i) \in \lfloor \tau_1\ \sigma \rfloor_V \tag{9}$$

And we are required to prove that:
$(\theta, n, v_i) \in \lfloor \tau_1'\ \sigma \rfloor_V$
From Equation 9 and IH1 we know that
$(\theta, n, v_i) \in \lfloor \tau_1'\ \sigma \rfloor_V$

(b) $v_s = \mathsf{inr}\ v_i$:
From Definition 1.6 we are given:

$$(\theta, n, v_i) \in \lfloor \tau_2\ \sigma \rfloor_V \tag{10}$$

And we are required to prove that:
$(\theta, n, v_i) \in \lfloor \tau_2'\ \sigma \rfloor_V$
From Equation 10 and IH2 we know that
$(\theta, n, v_i) \in \lfloor \tau_2'\ \sigma \rfloor_V$

4. FGsub-forall:
Given:

$$\frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2 \qquad \Sigma, \alpha; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash \forall \alpha.(\ell_e, \tau_1) <: \forall \alpha.(\ell_e', \tau_2)}\ \text{FGsub-forall}$$

To prove: $\lfloor ((\forall \alpha.(\ell_e, \tau_1))\ \sigma) \rfloor_V \subseteq \lfloor (\forall \alpha.(\ell_e', \tau_2))\ \sigma \rfloor_V$

IH1: $\forall pc.\ \lfloor (\tau_1\ \sigma) \rfloor_E^{pc} \subseteq \lfloor (\tau_2\ \sigma) \rfloor_E^{pc}$ (Statement 2(b))
It suffices to prove: $\forall (\theta, n, \Lambda e_i) \in \lfloor ((\forall \alpha.(\ell_e, \tau_1))\ \sigma) \rfloor_V.\ (\theta, n, \Lambda e_i) \in \lfloor ((\forall \alpha.(\ell_e, \tau_1))\ \sigma) \rfloor_V$

This means that given: $(\theta, n, \Lambda e_i) \in \lfloor ((\forall \alpha.(\ell_e, \tau_1))\ \sigma) \rfloor_V$
Therefore from Definition 1.6 we are given:

$$\forall \theta_1.\theta \sqsubseteq \theta_1 \wedge \forall i < n. \forall \ell' \in \mathcal{L} \implies (\theta_1, i, e_i) \in \lfloor \tau_1\ (\sigma \cup [\alpha \mapsto \ell']) \rfloor_E^{\ell_e\ (\sigma \cup [\alpha \mapsto \ell'])} \tag{11}$$

And it suffices to prove: $(\theta, n, \Lambda e_i) \in \lfloor ((\forall \alpha.(\ell_e', \tau_2))\ \sigma) \rfloor_V$

Again from Definition 1.6, it suffices to prove:
$\forall \theta_2.\theta \sqsubseteq \theta_2 \wedge \forall j < n. \forall \ell' \in \mathcal{L} \implies (\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma \cup [\alpha \mapsto \ell']) \rfloor_E^{\ell_e\ (\sigma \cup [\alpha \mapsto \ell'])}$

This means that given some $\theta_2, j < n, \ell' \in \mathcal{L}$ s.t $\theta \sqsubseteq \theta_2$
And we are required to prove: $(\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma \cup [\alpha \mapsto \ell']) \rfloor_E^{\ell_e'\ (\sigma \cup [\alpha \mapsto \ell'])}$

Since we are given $\theta \sqsubseteq \theta_2 \wedge j < n \wedge \ell' \in \mathcal{L}$ therefore from Equation 11 we have
$(\theta_2, j, e_i) \in \lfloor \tau_1\ (\sigma \cup [\alpha \mapsto \ell']) \rfloor_E^{\ell_e\ (\sigma \cup [\alpha \mapsto \ell'])}$
From IH1, we know that

$(\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma \cup [\alpha \mapsto \ell'])\rfloor_E^{\ell_e\ (\sigma \cup [\alpha \mapsto \ell'])}$
Since $\mathcal{L} \models \ell'_e\ (\sigma \cup [\alpha \mapsto \ell']) \sqsubseteq \ell_e\ (\sigma \cup [\alpha \mapsto \ell'])$ therefore from Lemma 1.23 we know that $(\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma \cup [\alpha \mapsto \ell'])\rfloor_E^{\ell'_e\ (\sigma \cup [\alpha \mapsto \ell'])}$

5. FGsub-constraint:
   Given:

$$\frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi \vdash \tau_1 <: \tau_2 \qquad \Sigma; \Psi \vdash \ell'_e \sqsubseteq \ell_e}{\Sigma; \Psi \vdash c_1 \overset{\ell_e}{\Rightarrow} \tau_1 <: c_2 \overset{\ell'_e}{\Rightarrow} \tau_2}\ \text{FGsub-constraint}$$

   To prove: $\lfloor ((c_1 \overset{\ell_e}{\Rightarrow} \tau_1)\ \sigma)\rfloor_V \subseteq \lfloor ((c_2 \overset{\ell'_e}{\Rightarrow} \tau_2))\ \sigma\rfloor_V$

   IH1: $\forall pc.\ \lfloor (\tau_1\ \sigma)\rfloor_E^{pc} \subseteq \lfloor (\tau_2\ \sigma)\rfloor_E^{pc}$ (Statement 2(b))
   It suffices to prove: $\forall (\theta, n, \nu e_i) \in \lfloor ((c_1 \overset{\ell_e}{\Rightarrow} \tau_1)\ \sigma)\rfloor_V.\ (\theta, n, \nu e_i) \in \lfloor ((c_2 \overset{\ell'_e}{\Rightarrow} \tau_2)\ \sigma)\rfloor_V$

   This means that given: $(\theta, n, \nu e_i) \in \lfloor ((c_1 \overset{\ell_e}{\Rightarrow} \tau_1)\ \sigma)\rfloor_V$
   Therefore from Definition 1.6 we are given:

$$\forall \theta_1.\theta \sqsubseteq \theta_1 \wedge \forall i < n.\mathcal{L} \models c_1\ \sigma \implies (\theta_1, i, e_i) \in \lfloor \tau_1\ (\sigma)\rfloor_E^{\ell_e\ \sigma} \tag{12}$$

   And it suffices to prove: $(\theta, n, \nu e_i) \in \lfloor ((c_2 \overset{\ell'_e}{\Rightarrow} \tau_2)\ \sigma)\rfloor_V$

   Again from Definition 1.6, it suffices to prove:
   $\forall \theta_2.\theta \sqsubseteq \theta_2 \wedge \forall j < n.\mathcal{L} \models c_2\ \sigma \implies (\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma)\rfloor_E^{\ell'_e\ \sigma}$

   This means that given some θ_2, j s.t $\theta \sqsubseteq \theta_2 \wedge j < n \wedge \mathcal{L} \models c_2\ \sigma$
   And we are required to prove: $(\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma)\rfloor_E^{\ell'_e\ \sigma}$

   Since we are given $\theta \sqsubseteq \theta_2 \wedge j < n \wedge \mathcal{L} \models c_2\ \sigma$ therefore from Equation 12 we have $(\theta_2, j, e_i) \in \lfloor \tau_1\ (\sigma)\rfloor_E^{\ell_e\ \sigma}$
   From IH1, we know that
   $(\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma)\rfloor_E^{\ell_e\ \sigma}$
   Since $\mathcal{L} \models \ell'_e\ \sigma \sqsubseteq \ell_e\ \sigma$ therefore from Lemma 1.23 we know that
   $(\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma)\rfloor_E^{\ell'_e\ \sigma}$

6. FGsub-ref:
   Given:

$$\frac{}{\Sigma; \Psi \vdash \mathsf{ref}\ \tau <: \mathsf{ref}\ \tau}\ \text{FGsub-ref}$$

   To prove: $\lfloor ((\mathsf{ref}\ \tau)\ \sigma)\rfloor_V \subseteq \lfloor ((\mathsf{ref}\ \tau)\ \sigma)\rfloor_V$

   It suffices to prove: $\forall (\theta, n, a) \in \lfloor ((\mathsf{ref}\ \tau)\ \sigma)\rfloor_V.\ (\theta, n, a) \in \lfloor ((\mathsf{ref}\ \tau)\ \sigma)\rfloor_V$
   Trivial

7. FGsub-base:

   Given:

$$\frac{}{\Sigma; \Psi \vdash \mathsf{b} <: \mathsf{b}} \text{ FGsub-base}$$

   To prove: $\lfloor ((\mathsf{b})\ \sigma) \rfloor_V \subseteq \lfloor ((\mathsf{b})\ \sigma) \rfloor_V$

   Directly from Definition 1.6

8. FGsub-unit:

   Given:

$$\frac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}} \text{ FGsub-unit}$$

   To prove: $\lfloor ((\mathsf{unit})\ \sigma) \rfloor_V \subseteq \lfloor ((\mathsf{unit})\ \sigma) \rfloor_V$

   Directly from Definition 1.6

Proof of statement 2(a)
Given:

$$\frac{\Sigma; \Psi \vdash \ell \sqsubseteq \ell' \qquad \Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}'}{\Sigma; \Psi \vdash \mathsf{A}^{\ell} <: \mathsf{A}'^{\ell'}} \text{ FGsub-label}$$

To prove: $\lfloor ((\mathsf{A}^{\ell})\ \sigma) \rfloor_V \subseteq \lfloor ((\mathsf{A}'^{\ell'}))\ \sigma \rfloor_V$
From Definition 1.6 it suffices to prove: $\lfloor ((\mathsf{A})\ \sigma) \rfloor_V \subseteq \lfloor ((\mathsf{A}'))\ \sigma \rfloor_V$
This we get directly from IH (Statement 1(a))

Proof of statement 2(b)
Given: $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma$
To prove: $\lfloor (\tau\ \sigma) \rfloor_E^{pc} \subseteq \lfloor (\tau'\ \sigma) \rfloor_E^{pc}$
This means we need to prove that
$\forall (\theta, n, e) \in \lfloor (\tau\ \sigma) \rfloor_E^{pc}.\ (\theta, n, e) \in \lfloor (\tau'\ \sigma) \rfloor_E^{pc}$

This means given $(\theta, n, e) \in \lfloor (\tau\ \sigma) \rfloor_E^{pc}$
It suffices to prove that $(\theta, n, e) \in \lfloor (\tau'\ \sigma) \rfloor_E^{pc}$

From Definition 1.7 we know we are given:
$\forall H.(n, H) \triangleright \theta \wedge \forall i < n.(H, e) \Downarrow_i (H', v') \implies$
$\exists \theta'.\theta \sqsubseteq \theta' \wedge (n - i, H') \triangleright \theta' \wedge (\theta', n - i, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc)$ (A)

And we need prove that
$\forall H_1.(n, H_1) \triangleright \theta \wedge \forall j < n.(H_1, e) \Downarrow_j (H_1', v') \implies$
$\exists \theta_1'.\theta \sqsubseteq \theta_1' \wedge (n - j, H_1') \triangleright \theta_1' \wedge (\theta_1', n - j, v') \in \lfloor \tau'\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta).\theta_1'(a) \searrow pc)$

This means that we are given some H_1 and $j < n$ s.t $(n, H_1) \triangleright \theta \wedge (H_1, e) \Downarrow_j (H_1', v')$

It suffices to prove:
$\exists\theta'_1.\theta \sqsubseteq \theta'_1 \wedge (n-j, H'_1) \triangleright \theta'_1 \wedge (\theta'_1, n-j, v') \in \lfloor \tau' \ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H'_1(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_1) \backslash dom(\theta).\theta'_1(a) \searrow pc)$

Instantiate H in (A) with H_1 and i with j then we choose θ'_1 as θ'
Also we have IH1 as $\lfloor \tau \ \sigma \rfloor_V \subseteq \lfloor \tau' \ \sigma \rfloor_V$ (Statement 2(a))

- $\exists\theta'.\theta \sqsubseteq \theta' \wedge (n-j, H'_1) \triangleright \theta' \wedge (\theta', n-j, v') \in \lfloor \tau' \ \sigma \rfloor_V$:

  We are given $\exists\theta'.\theta \sqsubseteq \theta' \wedge (n-j, H'_1) \triangleright \theta' \wedge (\theta', n-j, v') \in \lfloor \tau \ \sigma \rfloor_V$

  From IH1 we know that $\lfloor \tau \ \sigma \rfloor_V \subseteq \lfloor \tau' \ \sigma \rfloor_V$

  Therefore, $\exists\theta'.\theta \sqsubseteq \theta' \wedge (n-j, H'_1) \triangleright \theta' \wedge (\theta', n-j, v') \in \lfloor \tau' \ \sigma \rfloor_V$

- $(\forall a.H_1(a) \neq H'_1(a) \implies \exists \ell'.\theta(a) = \mathsf{A}^{\ell'} \wedge pc \sqsubseteq \ell')$:

  Given

- $(\forall a \in dom(\theta') \backslash dom(\theta).\theta'(a) \searrow pc)$:

  Given

□

Lemma 1.25 (FG: Binary interpretation of Γ implies Unary interpretation of Γ)**.** $\forall W, \gamma, \Gamma, n.$
$(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}} \implies \forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, \gamma \downarrow_i) \in \lfloor \Gamma \rfloor_V$

Proof. Given: $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$
To prove: $\forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, \gamma \downarrow_i) \in \lfloor \Gamma \rfloor_V$

From Definition 1.14 we know that we are given:
$dom(\Gamma) \subseteq dom(\gamma) \wedge \forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$
And we are required to prove:
$\forall i \in \{1, 2\}.\ \forall m.$
$dom(\Gamma) \subseteq dom(\gamma \downarrow_i) \wedge \forall x \in dom(\Gamma).(W.\theta_i, m, \gamma \downarrow_i (x)) \in \lfloor \Gamma(x) \rfloor_V$

<u>Case $i = 1$</u>
Given some m we need to show:

- $dom(\Gamma) \subseteq dom(\gamma \downarrow_i)$:

  $dom(\gamma) = dom(\gamma \downarrow_i)$

  Therefore, $dom(\Gamma) \subseteq (dom(\gamma) = dom(\gamma \downarrow_i))$ (Given)

- $\forall x \in dom(\Gamma).(W.\theta_i, m, \gamma \downarrow_i (x)) \in \lfloor \Gamma(x) \rfloor_V$:

  We are given: $\forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$

  Therefore from Lemma 1.15 we know that

  $\forall m'.(W.\theta_i, m', \gamma \downarrow_i (x)) \in \lfloor \Gamma(x) \rfloor_V$

  Instantiating m' with m we get

  $(W.\theta_i, m, \gamma \downarrow_i (x)) \in \lfloor \Gamma(x) \rfloor_V$

Case $i = 2$
Symmetric case as $i = 1$

□

Theorem 1.26 (FG: Fundamental theorem binary)**.** $\forall \Sigma, \Psi, \Gamma, pc, W, \mathcal{A}, \mathcal{L}, e, \tau, \sigma, \gamma, n.$
$\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau \wedge \mathcal{L} \models \Psi\ \sigma \wedge (W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}} \implies$
$(W, n, e\ (\gamma \downarrow_1), e\ (\gamma \downarrow_2)) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$

Proof. Proof by induction on the typing derivation

1. FG-var:

$$\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash_{pc} x : \tau}\ \text{FG-var}$$

To prove: $(W, n, x\ (\gamma \downarrow_1), x\ (\gamma \downarrow_2)) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$
Say $e_1 = x\ (\gamma \downarrow_1)$ and $e_2 = x\ (\gamma \downarrow_2)$

From Definition of $\lceil \tau \rceil_E^{\mathcal{A}}$ it suffices to prove that

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall j < n.(H_1, e_1) \Downarrow_j (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2') \implies$
$\exists W' \sqsupseteq W.(n - j, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - j, v_1', v_2') \in \lceil \tau \rceil_V^{\mathcal{A}}$

This means given some H_1, H_2 and j s.t $(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge (H_1, e_1) \Downarrow_j (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2')$

We are required to prove: $\exists W' \sqsupseteq W.(n - j, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - j, v_1', v_2') \in \lceil \tau \rceil_V^{\mathcal{A}}$

Here
- $H_1' = H_1$ and $H_2' = H_2$
- $e_1 = v_1' = \gamma(x) \downarrow_1$
- $e_2 = v_2' = \gamma(x) \downarrow_2$
- $j = 1$

We choose $W' = W$.

- $W \sqsubseteq W$: From Definition 1.3
- $(n - 1, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W$:
  Since we know that $(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W$ therefore from Lemma 1.21 we get $(n - 1, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W$
- $(W, n - 1, \gamma(x) \downarrow_1, \gamma(x) \downarrow_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$:
  We are given that $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$ therefore from Lemma 1.19 we get $(W, n - 1, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$
  which means from Definition 1.14 we have
  $(W, n - 1, \gamma(x) \downarrow_1, \gamma(x) \downarrow_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$

2. FG-lam:

$$\frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{\ell_e} e_i : \tau_2}{\Sigma; \Psi; \Gamma \vdash_{pc} \lambda x.e_i : (\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp}$$

To prove: $(W, n, \lambda x.e\ (\gamma \downarrow_1), \lambda x.e\ (\gamma \downarrow_2)) \in \lceil(\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma\rceil_E^{\mathcal{A}}$

Say $e_1 = \lambda x.e\ (\gamma \downarrow_1)$ and $e_2 = \lambda x.e\ (\gamma \downarrow_2)$

From Definition of $\lceil(\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp\ \sigma\rceil_E^{\mathcal{A}}$ it suffices to prove that

$\forall H_1, H_2, j < n.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge (H_1, e_1) \Downarrow_j (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2') \implies$
$\exists W' \sqsupseteq W.(n - j, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - j, v_1', v_2') \in \lceil(\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp\ \sigma\rceil_V^{\mathcal{A}}$

This means that given H_1, H_2 and j s.t $(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge (H_1, e_1) \Downarrow_j (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2')$

It suffices to prove:

$$\exists W' \sqsupseteq W.(n - j, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - j, v_1', v_2') \in \lceil(\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp\ \sigma\rceil_V^{\mathcal{A}} \quad \text{(FB-L0)}$$

IH1:

$\forall W, n.\ (W, n, e\ (\gamma \downarrow_1 \cup \{x \mapsto v_1\}), e\ (\gamma \downarrow_2 \cup \{x \mapsto v_2\})) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}}$

s.t

$(W, n, (v_1, v_2)) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}}$

We know from the evaluation rules that $H_1' = H_1$, $H_2' = H_2$, $v_1' = e_1 = \lambda x.e\ (\gamma \downarrow_1)$, $v_2' = e_2 = \lambda x.e\ (\gamma \downarrow_2)$ and $j = 0$. In order to prove FB-L0 we choose $W' = W$ and we need to prove the following:

- $W \sqsubseteq W$: From Definition 1.3
- $(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W$: Given
- $(W, n, \lambda x.e\ (\gamma \downarrow_1), \lambda x.e\ (\gamma \downarrow_2)) \in \lceil(\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp\ \sigma\rceil_V^{\mathcal{A}}$
  From Definition 1.4 it suffices to prove that:
  $\forall W'' \sqsupseteq W, k < n, v_1, v_2.$
  $((W'', k, v_1, v_2) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}} \implies (W'', k, e\ (\gamma \downarrow_1)[v_1/x], e\ (\gamma \downarrow_2)[v_2/x]) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}}) \wedge$
  $\forall \theta_l \sqsupseteq W.\theta_1, k, v_c.$
  $((\theta_l, k, v_c) \in \lfloor\tau_1\ \sigma\rfloor_V \implies (\theta_l, k, e\ (\gamma \downarrow_1)[v_c/x]) \in \lfloor\tau_2\ \sigma\rfloor_E^{\ell_e\ \sigma}) \wedge$
  $\forall \theta_l \sqsupseteq W.\theta_2, , v_c.$
  $((\theta_l, k, v_c) \in \lfloor\tau_1\ \sigma\rfloor_V \implies (\theta_l, k, e\ (\gamma \downarrow_2)[v_c/x]) \in \lfloor\tau_2\ \sigma\rfloor_E^{\ell_e\ \sigma})$

  This means that we need to prove the following:

  - $\forall W'' \sqsupseteq W, k < n, v_1, v_2.((W'', k, v_1, v_2) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}} \implies$
    $(W'', k, e\ (\gamma \downarrow_1)[v_1/x], e\ (\gamma \downarrow_2)[v_2/x]) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}})$:

    This means given $W'' \sqsupseteq W, k < n, v_1, v_2$ s.t $((W'', k, v_1, v_2) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}}$
    We need to prove: $(W'', k, e\ (\gamma \downarrow_1)[v_1/x], e\ (\gamma \downarrow_2)[v_2/x]) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}}$

We instantiate IH1 with W'' and k
And since $(W'', k, v_1, v_2) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$ therefore we get
$(W'', k, e\ (\gamma \downarrow_1)[v_1/x], e\ (\gamma \downarrow_2)[v_2/x]) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$

– $\forall \theta_l \sqsupseteq W.\theta_1, k, v_c.((\theta_l, k, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V \implies$
$(\theta_l, k, e\ (\gamma \downarrow_1)[v_c/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma})$:

This means that we are given θ_l, k and v_c s.t
$\theta_l \sqsupseteq W.\theta_1$ and $(\theta_l, k, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V$
And we are required to prove:
$(\theta_l, k, e\ (\gamma \downarrow_1)[v_c/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$

It is given to us that
$\forall v_1, v_2.\ (W, n, \gamma \in \lceil \Gamma \rceil_V^{\mathcal{A}}$

Therefore from Lemma 1.25 we know that
$\forall m.\ (W.\theta_1, m, (\gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$

Therefore, we can apply Theorem 1.22 to obtain
$\forall m.\ (W.\theta_1, m, \lambda x.e\ \gamma \downarrow_1) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\perp}\ \sigma \rfloor_V$

From Definition 1.6 it means that we have
$\forall m.\ \forall \theta'. W.\theta_1 \sqsubseteq \theta' \wedge \forall j < m. \forall v.(\theta', j, v) \in \lfloor \tau_1\ \sigma \rfloor_V \implies$
$(\theta', j, e[v/x]\gamma \downarrow_1) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$

We instantiate m with some $l > k$, θ' with θ_l, j with k and v with v_c to get
$W.\theta_1 \sqsubseteq \theta_l \wedge k < l \wedge (\theta_l, k, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta_l, k, e[v_c/x]\gamma \downarrow_1) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$

Since we thow that $W.\theta_1 \sqsubseteq \theta_l \wedge k < l \wedge (\theta_l, k, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V$ therefore we get
$(\theta_l, k, e[v_c/x]\gamma \downarrow_1) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$

– $\forall \theta_l \sqsupseteq W.\theta_2, , v_c.((\theta_l, k, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V \implies$
$(\theta_l, k, e\ (\gamma \downarrow_2)[v_c/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma})$:
Symmetric case as above

3. FG-app:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 \searrow \ell \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1\ e_2 : \tau_2}$$

To prove: $(W, n, (e_1\ e_2)\ (\gamma \downarrow_1), (e_1\ e_2)\ (\gamma \downarrow_2)) \in \lceil (\tau_2)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 1.5 we need to prove:

$\forall H_1, H_2, n' < n.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge (H_1, (e_1\ e_2)(\gamma \downarrow_1)) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, (e_1\ e_2)(\gamma \downarrow_2)) \Downarrow (H_2', v_2') \implies$
$\exists W' \sqsupseteq W.(n - n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v_1', v_2') \in \lceil (\tau_2)\ \sigma \rceil_V^{\mathcal{A}}$
This further means that given $H_1, H_2, n' < n$ s.t
$(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge (H_1, (e_1\ e_2)(\gamma \downarrow_1)) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, (e_1\ e_2)(\gamma \downarrow_2)) \Downarrow (H_2', v_2')$
It suffices to prove

$$\exists W' \sqsupseteq W.(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-n', v_1', v_2') \in \lceil (\tau_2)\ \sigma \rceil_V^{\mathcal{A}} \tag{FB-A0}$$

<u>IH1</u> $(W, n, (e_1)\ (\gamma \downarrow_1), (e_1)\ (\gamma \downarrow_2)) \in \lceil (\tau_1 \overset{\ell_e}{\to} \tau_2)^\ell\ \sigma \rceil_E^{\mathcal{A}}$
This means from Definition 1.5 we get

$\forall H_{i1}, H_{i2}, i < n.(n, H_{i1}, H_{i2}) \overset{\mathcal{A}}{\triangleright} W \wedge (H_{i1}, e_1\ (\gamma \downarrow_1)) \Downarrow_i (H_1', v_1') \wedge (H_{i2}, e_1\ (\gamma \downarrow_2)) \Downarrow (H_2', v_2') \implies \exists W_1' \sqsupseteq W.(n-i, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n-i, v_1', v_2') \in \lceil (\tau_1 \overset{\ell_e}{\to} \tau_2)^\ell\ \sigma \rceil_V^{\mathcal{A}}$

Instantiating H_{i1} with H_1 and H_{i2} with H_2 in IH1 and since the $(e_1\ e_2)$ reduces to value with $\gamma \downarrow_1$ in $n' < n$ steps. Therefore $\exists i < n' < n$ s.t $(H_{i1}, e_1\ (\gamma \downarrow_1)) \Downarrow_i (H_1', v_1')$. $(H_{i2}, e_1\ (\gamma \downarrow_2)) \Downarrow (H_2', v_2')$ is known because $(e_1\ e_2)$ reduces to value with $\gamma \downarrow_2$. Hence we get

$$\exists W_1' \sqsupseteq W.(n-i, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n-i, v_1', v_2') \in \lceil (\tau_1 \overset{\ell_e}{\to} \tau_2)^\ell\ \sigma \rceil_V^{\mathcal{A}} \tag{13}$$

<u>IH2</u>: $(W_1', n-i, (e_2)\ (\gamma \downarrow_1), (e_2)\ (\gamma \downarrow_2)) \in \lceil (\tau_1)\ \sigma \rceil_E^{\mathcal{A}}$
This means from Definition 1.5 we get

$\forall H_{j1}, H_{j2}, j < (n-i).(n-i, H_{j1}, H_{j2}) \overset{\mathcal{A}}{\triangleright} W_1' \wedge (H_1, e_2\ (\gamma \downarrow_1)) \Downarrow_j (H_{j1}', v_{j1}') \wedge (H_2, e_2\ (\gamma \downarrow_2)) \Downarrow (H_{j2}', v_{j2}') \implies \exists W_2' \sqsupseteq W_1'.(n-i-j, H_{j1}', H_{j2}') \overset{\mathcal{A}}{\triangleright} W_2' \wedge (W_2', n-i-j, v_{j1}', v_{j2}') \in \lceil (\tau_1)\ \sigma \rceil_V^{\mathcal{A}}$

Instantiating H_{j1} with H_1' and H_{j2} with H_2' in IH2. Since the $(e_1\ e_2)$ reduces to value with $\gamma \downarrow_1$ in $n' < n$ steps. Also, e_1 reduces to value $\gamma \downarrow_1$ in $i < n'$ steps. Therefore $\exists j < n' - i < n - i$ s.t $(H_{i1}, e_2\ (\gamma \downarrow_1)) \Downarrow_j (H_{j1}', v_{j1}')$. $(H_{i2}, e_2\ (\gamma \downarrow_2)) \Downarrow (H_{j2}', v_{j2}')$ is known because $(e_1\ e_2)$ reduces to value with $\gamma \downarrow_2$. Hence we get

$$\exists W_2' \sqsupseteq W_1'.(n-i-j, H_{j1}', H_{j2}') \overset{\mathcal{A}}{\triangleright} W_2' \wedge (W_2', n-i-j, v_{j1}', v_{j2}') \in \lceil (\tau_1)\ \sigma \rceil_V^{\mathcal{A}} \tag{14}$$

We case analyze on $(W_1', n-i, v_1', v_2') \in \lceil (\tau_1 \overset{\ell_e}{\to} \tau_2)^\ell\ \sigma \rceil_V^{\mathcal{A}}$ from Equation 13

- Case $\ell\ \sigma \sqsubseteq \mathcal{A}$:
  From Definition 1.4 we know that this would mean that
  $(W_1', n-i, v_1', v_2') \in \lceil (\tau_1 \overset{\ell_e}{\to} \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$
  This means
  $(W_1', n-i, v_1', v_2') \in \lceil (\tau_1\ \sigma \overset{\ell_e\ \sigma}{\to} \tau_2\ \sigma) \rceil_V^{\mathcal{A}}$
  Let $v_1' = \lambda x.e_{h1}$ and $v_2' = \lambda x.e_{h2}$

  Again from Definition 1.4 it means that
  $\forall W_{h1}' \sqsupseteq W_1', j_1 < (n-i), v_1, v_2.$
  $((W_{h1}', j_1, v_1, v_2) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \implies (W_{h1}', j_1, e_{h1}[v_1/x], e_{h2}[v_2/x]) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}) \wedge$
  $\forall \theta_{l1} \sqsupseteq W_1'.\theta_1, m_1, v_c.$
  $\wedge ((\theta_{l1}, m_1, v_1) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (W_{h1}'.\theta_1, e_{h1}[v_1/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}) \wedge$
  $\forall \theta_{l1} \sqsupseteq W_1'.\theta_2, m_1, v_c.$
  $\wedge (\theta_{l1}, m_1, v_2) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (W_{h1}'.\theta_2, e_{h2}[v_2/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma})$

We instantiate W'_{h1} with W'_2 obtained from Equation 14. Similarly we also instantiate v_1 and v_2 with v'_{j1} and v'_{j2} respectively from Equation 14, and j_1 with $n-i-j$. And we get
$(W'_2, n-i-j, e_{h1}[v'_{j1}/x], e_{h2}[v'_{j2}/x]) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$

From Definition 1.5 we get

$\forall H_1, H_2, k_e < (n-i-j).(n-i-j, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W'_2 \wedge$
$(H_1, e_{h1}[v'_{j1}/x]) \Downarrow_{k_e} (H'_{f1}, v_{f1}) \wedge (H_2, e_{h2}[v'_{j2}/x]) \Downarrow (H'_{f2}, v_{f2}) \implies$
$\exists W' \sqsupseteq W'_2.(n-i-j-k_e, H'_{f1}, H'_{f2}) \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-i-j-k_e, v_{f1}, v_{f2}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$

Instantiating H_1 with H'_{j1} and H_2 with H'_{j2} obtained from Equation 14. And since we know that $e_1\ e_2$ reduces with $\gamma \downarrow_1$ in $n' < n$ steps. And e_2 reduces to value $\gamma \downarrow_1$ in $j < n'-1 < n-i$ steps. Therefore $\exists k_e = n'-i-j < n-i-j$ s.t $(H_1, e_{h1}[v'_{j1}/x]) \Downarrow_{k_e} (H'_{f1}, v_{f1})$. $(H_2, e_{h2}[v'_{j2}/x]) \Downarrow (H'_{f2}, v_{f2})$ is known because $(e_1\ e_2)$ reduces to value with $\gamma \downarrow_2$. Hence we get

$$\exists W' \sqsupseteq W'_2.((n-i-j-k_e), H'_{f1}, H'_{f2}) \overset{\mathcal{A}}{\triangleright} W' \wedge (W', (n-i-j-k_e), v_{f1}, v_{f2}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}} \tag{15}$$

This concludes the proof in this case.

- Case $\ell\ \sigma \not\sqsubseteq \mathcal{A}$:

  From FB-A0 we know that we need to prove
  $\exists W' \sqsupseteq W.(n-n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-n', v'_1, v'_2) \in \lceil (\tau_2)\ \sigma \rceil_V^{\mathcal{A}}$

  In this case since we know that $\ell\ \sigma \not\sqsubseteq \mathcal{A}$. Let $\tau_2\ \sigma = \mathsf{A}^{\ell_i}$ and since $\tau_2\ \sigma \searrow \ell\ \sigma$ therefore $\ell_i \not\sqsubseteq \mathcal{A}$

  Therefore from Definition 1.4 it will suffice to prove
  $\exists W' \sqsupseteq W.(n-n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W' \wedge (\forall m_1.(W'.\theta_1, m_1, v'_1) \in \lfloor (\tau_2)\ \sigma \rfloor_V) \wedge (\forall m_2.(W'.\theta_1, m_2, v'_2) \in \lfloor (\tau_2)\ \sigma \rfloor_V)$

  This means it suffices to prove
  $(\forall m_1, m_2.\exists W' \sqsupseteq W.(n-n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W' \wedge (W'.\theta_1, m_1, v'_1) \in \lfloor (\tau_2)\ \sigma \rfloor_V) \wedge ((W'.\theta_1, m_2, v'_2) \in \lfloor (\tau_2)\ \sigma \rfloor_V)$

  This means given m_1 and m_2 it suffices to prove:

$$(\exists W' \sqsupseteq W.(n-n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W' \wedge (W'.\theta_1, m_1, v'_1) \in \lfloor (\tau_2)\ \sigma \rfloor_V) \wedge (W'.\theta_1, m_2, v'_2) \in \lfloor (\tau_2)\ \sigma \rfloor_V) \tag{16}$$

  In this case from Definition 1.6 we know that

$$\forall m.(W'_1.\theta_1, m, \lambda x.e_{h1}) \in \lfloor (\tau_1\ \sigma \overset{\ell_e\ \sigma}{\rightarrow} \tau_2\ \sigma) \rfloor_V \tag{17}$$

$$\forall m.(W'_1.\theta_2, m, \lambda x.e_{h2}) \in \lfloor (\tau_1\ \sigma \overset{\ell_e\ \sigma}{\rightarrow} \tau_2\ \sigma) \rfloor_V \tag{18}$$

Applying Definition 1.6 on Equation 17 we get
$\forall m.\ \forall \theta'.\theta \sqsubseteq \theta' \wedge \forall j_1 < m.\forall v.(\theta', j_1, v) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta', j_1, e_{h1}[v/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$
where $\theta = W_1'.\theta_1$

We instantiate m with m_1+2+t_1 where t_1 is the number of steps in which e_{h1} reduces
$\forall \theta'.W_1'.\theta_1 \sqsubseteq \theta' \wedge \forall j_1 < (m_1+1+t_1).\forall v.(\theta', j_1, v) \in \lfloor \tau_1\ \sigma \rfloor_V \implies$
$(\theta', j_1, e_{h1}[v/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$ (FB-AC1)

Since from Equation 14 we have
$(W_2', n-i-j, v_{j1}', v_{j2}') \in \lceil (\tau_1)\ \sigma \rceil_V^{\mathcal{A}}$

Therefore from Lemma 1.15 we get
$\forall m.\ (W_2'.\theta_1, m, v_{j1}') \in \lfloor \tau_1\ \sigma \rfloor_V$

Instantiating m with m_1+1+t_1 we get
$(W_2'.\theta_1, m_1+1+t_1, v_{j1}') \in \lfloor \tau_1\ \sigma \rfloor_V$

Instantiating θ' with $W_2'.\theta_1$, $j1$ with m_1+t_1 and v with v_{j1}' from Equation 14.
Therefore we get $(W_2'.\theta_1, m_1+1+t_1, e_{h1}[v_{j1}'/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$

From Definition 1.7, we get
$\forall H.(m_1+1+t_1, H) \triangleright W_2'.\theta_1 \wedge \forall k_c < (m_1+1+t_1).(H, e_{h1}[v_{j1}'/x]) \Downarrow_{k_c} (H_1', v_1') \implies$
$\exists \theta_1'.W_2'.\theta_1 \sqsubseteq \theta_1' \wedge ((m_1+1+t_1-k_c), H_1') \triangleright \theta_1' \wedge (\theta_1', (m_1+1+t_1-k_c), v_1') \in \lfloor \tau_2\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H_1'(a) \implies \exists \ell'.W_2'.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(W_2'.\theta_1).\theta_1'(a) \searrow (\ell_e\ \sigma))$

Since from Equation 14 we have $(n-i-j, H_{j1}', H_{j1}') \triangleright W_2'$
Therefore from Lemma 1.27 we get $\forall m.(m, H_{j1}') \triangleright W_2'.\theta_1$
Instantiating m with m_1+1+t_1 we get $(m_1+1+t_1, H_{j1}') \triangleright W_2'.\theta_1$

Now instantiating H with H_{j1}' from Equation 14 and k_c with t_1 we get
$\exists \theta_1'.W_2'.\theta_1 \sqsubseteq \theta_1' \wedge ((m_1+1), H_1') \triangleright \theta_1' \wedge (\theta_1', (m_1+1), v_1') \in \lfloor \tau_2\ \sigma \rfloor_V \wedge$
$(\forall a.H_{j1}'(a) \neq H_1'(a) \implies \exists \ell'.W_2'.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(W_2'.\theta_1).\theta_1'(a) \searrow (\ell_e\ \sigma))$ (R1)

Similarly we can apply Definition 1.6 on Equation 18 to get
$\forall m.\ \forall \theta_2'.(m, W_1'.\theta_2) \sqsubseteq \theta_2' \wedge \forall j_2 < m.\forall v.(\theta_2', j_2, v) \in \lfloor \tau_1\ \sigma \rfloor_V \implies$
$(\theta_2', j_2, e_{h2}[v/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$

We instantiate m with m_2+2+t_2 where t_2 is the number of steps in which e_{h2} reduces
$\forall \theta'.W_1'.\theta_2 \sqsubseteq \theta' \wedge \forall j_1 < (m_2+2+t_2).\forall v.(\theta', j_1, v) \in \lfloor \tau_1\ \sigma \rfloor_V \implies$
$(\theta', j_1, e_{h2}[v/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$ (FB-AC2)

Since from Equation 14 we have
$(W_2', n-i-j, v_{j1}', v_{j2}') \in \lceil (\tau_1)\ \sigma \rceil_V^{\mathcal{A}}$

Therefore from Lemma 1.15 we get
$\forall m.\ (W_2'.\theta_2, m, v_{j2}') \in \lfloor \tau_1\ \sigma \rfloor_V$

Instantiating m with m_2+1+t_2 we get
$(W_2'.\theta_2, m_2+1+t_2, v_{j2}') \in \lfloor \tau_1\ \sigma \rfloor_V$

Instantiating θ' with $W_2'.\theta_2$, j_1 with m_2+1+t_2 and v with v_{j2}' from Equation 14 in FB-AC2 we get
$(W_2'.\theta_2, m_2+1+t_2, e_{h2}[v_{j2}'/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$

From Definition 1.7, we get
$\forall H.(m_2+1+t_2, H) \triangleright W_2'.\theta_2 \wedge \forall k_c < (m_2+1+t_2).(H, e_{h2}[v_{j1}'/x]) \Downarrow_{k_c} (H_2', v_2') \implies$
$\exists \theta_2'. W_2'.\theta_2 \sqsubseteq \theta_2' \wedge ((m_2+1+t_2-k_c), H_2') \triangleright \theta_2' \wedge (\theta_2', (m_2+1+t_2-k_c)v_2') \in \lfloor \tau_2\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H_2'(a) \implies \exists \ell'. W_2'.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2')/dom(W_2'.\theta_2).\theta_2'(a) \searrow (\ell_e\ \sigma))$

Since from Equation 14 we have $(n-i-j, H_{j1}', H_{j1}') \triangleright W_2'$
Therefore from Lemma 1.27 we get $\forall m.(m, H_{j2}') \triangleright W_2'.\theta_2$
Instantiating m with m_2+1+t_2 we get $(m_2+1+t_2, H_{j2}') \triangleright W_2'.\theta_2$

Now Instantiating H with H_{j2}' from Equation 14 and and k_c with t_2.
$\exists \theta_2'. W_2'.\theta_2 \sqsubseteq \theta_2' \wedge (m_2+1, H_2') \triangleright \theta_2' \wedge (\theta_2', (m_2+1), v_2') \in \lfloor \tau_2\ \sigma \rfloor_V \wedge$
$(\forall a.H_{j2}'(a) \neq H_2'(a) \implies \exists \ell'. W_2'.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2') \backslash dom(W_2'.\theta_2).\theta_2'(a) \searrow (\ell_e\ \sigma))$ (R2)

In order to prove FB-A0 we choose W' to be $(\theta_1', \theta_2', W_2'.\beta)$. Now we need to show two things:

(a) $(n-n', H_1', H_2') \triangleright W'$:
From Definition 1.9 it suffices to show that
   - $dom(W'.\theta_1) \subseteq dom(H_1') \wedge dom(W.\theta_2) \subseteq dom(H_2')$:
     From R1 we know that $(m_1+1, H_1') \triangleright \theta_1'$, therefore from Definition 1.8 we get $dom(W'.\theta_1) \subseteq dom(H_1')$
     Similarly, from R2 we know that $(m_2+1, H_2') \triangleright \theta_2'$, therefore from Definition 1.8 we get $dom(W'.\theta_2) \subseteq dom(H_2')$
   - $(W'.\hat{\beta}) \subseteq (dom(W'.\theta_1) \times dom(W'.\theta_1))$:
     Since from Equation 14 we know that $(n-i-j, H_{j1}', H_{j2}') \triangleright W_2'$ therefore from Definition 1.9 we know that $(W_2'.\hat{\beta}) \subseteq (dom(W_2'.\theta_1) \times dom(W_2'.\theta_2))$
     From R1 and R2 we know that $W_2'.\theta_1 \sqsubseteq \theta_1'$ and $W_2'.\theta_2 \sqsubseteq \theta_2'$ therefore
     $(W_2'.\hat{\beta}) \subseteq (dom(\theta_1') \times dom(\theta_2'))$
   - $\forall (a_1, a_2) \in (W'.\hat{\beta}). W'.\theta_1(a_1) = W'.\theta_2(a_2) \wedge$
     $(W', n-n'-1, H_1'(a_1), H_2'(a_2)) \in \lceil W'.\theta_1(a_1) \rceil_V^{\mathcal{A}}$:

     4 cases arise for each $(a_1, a_2) \in W_2'.\hat{\beta}$
     i. $H_{j1}'(a_1) = H_1'(a_1) \wedge H_{j2}'(a_2) = H_2'(a_2)$:
        * $W'.\theta_1(a_1) = W'.\theta_2(a_2)$:
          We know from Equation 14 that $(n-i-j, H_{j1}', H_{j2}') \triangleright W_2'$

          Therefore from Definition 1.9 we have
          $\forall (a_1, a_2) \in (W_2'.\hat{\beta}). W_2'.\theta_1(a_1) = W_2'.\theta_2(a_2)$

          Since $W'.\hat{\beta} = W_2'.\hat{\beta}$ by construction therefore
          $\forall (a_1, a_2) \in (W'.\hat{\beta}). W_2'.\theta_1(a_1) = W_2'.\theta_2(a_2)$

          From R1 and R2 we know that $W_2'.\theta_1 \sqsubseteq \theta_1'$ and $W_2'.\theta_2 \sqsubseteq \theta_2'$ respectively.
          Therefore from Definition 1.2
          $\forall (a_1, a_2) \in (W'.\hat{\beta}).\theta_1'(a_1) = \theta_2'(a_2)$

* $(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1)\rceil_V^{\mathcal{A}}$:
  From Equation 14 we know that $(n-i-j, H'_{j1}, H'_{j2}) \overset{\mathcal{A}}{\triangleright} W'_2$
  This means from Definition 1.9 that
  $\forall(a_{i1}, a_{i2}) \in (W'_2.\hat{\beta}).\, W'_2.\theta_1(a_1) = W'_2.\theta_2(a_2) \wedge (W'_2, n-i-j-1, H'_{j1}(a_1), H'_{j2}(a_2)) \in \lceil W'_2.\theta_1(a_1)\rceil_V^{\mathcal{A}}$

  Instantiating with a_1 and a_2 and since $W'_2 \sqsubseteq W'$ and $n-n'-1 < n-i-j-1$ (since $n' = i+j+t_1$ where t_1 is the number of steps taken by e_{h1}, i is the number of steps taken by $e_1\ \gamma \downarrow_1$ to reduce and j is the number of steps taken by $e_2\ \gamma \downarrow_1$ to reduce) therefore from Lemma 1.17 we get
  $(W', n-n'-1, H'_{j1}(a_1), H'_{j2}(a_2)) \in \lceil W'.\theta_1(a_1)\rceil_V^{\mathcal{A}}$

ii. $H'_{j1}(a_1) \neq H'_1(a_1) \vee H'_{j2}(a_2) \neq H'_2(a_2)$:

* $W'.\theta_1(a_1) = W'.\theta_2(a_2)$
  Same reasoning as in the previous case
* $(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1)\rceil_V^{\mathcal{A}}$:
  From R1 and R2 we know that
  $(\forall a.H'_{j1}(a) \neq H'_1(a) \implies \exists \ell'.\, W'_2.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell')$
  $(\forall a.H'_{j2}(a) \neq H'_2(a) \implies \exists \ell'.\, W'_2.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell')$
  This means we have
  $\exists \ell'.\, W'_2.\theta_1(a_1) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell'$ and
  $\exists \ell'.\, W'_2.\theta_2(a_2) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell'$

  Since $pc\ \sigma \sqcup \ell\ \sigma \sqsubseteq \ell_e\ \sigma$ (given) and $\ell\ \sigma \not\sqsubseteq \mathcal{A}$. Therefore, $\ell_e\ \sigma \not\sqsubseteq \mathcal{A}$. And thus, $\ell' \not\sqsubseteq \mathcal{A}$

  Also from R1 and R2, $(m_1+1, H'_1) \triangleright \theta'_1$ and $(m_2+1, H'_2) \triangleright \theta'_2$. Therefore from Definition 1.8 we have
  $(\theta'_1, m_1, H'_1(a_1)) \in \lfloor \theta'_1(a_1)\rfloor_V$ and
  $(\theta'_2, m_2, H'_2(a_1)) \in \lfloor \theta'_2(a_2)\rfloor_V$

  Since m_1 and m_2 are arbitrary indices therefore from Definition 1.4 we get
  $(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil \theta'_1(a_1)\rceil_V^{\mathcal{A}}$

iii. $H'_{j1}(a_1) = H'_1(a_1) \vee H'_{j2}(a_2) \neq H'_2(a_2)$:

* $W'.\theta_1(a_1) = W'.\theta_2(a_2)$
  Same reasoning as in the previous case
* $(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1)\rceil_V^{\mathcal{A}}$:
  From R2 we know that
  $(\forall a.H'_{j2}(a) \neq H'_2(a) \implies \exists \ell'.\, W'_2.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell')$
  This means that a_2 was protected at $\ell_e\ \sigma$ in the world before the modification. Since $pc\ \sigma \sqcup \ell\ \sigma \sqsubseteq \ell_e\ \sigma$ (given) and $\ell\ \sigma \not\sqsubseteq \mathcal{A}$. Therefore, $\ell_e\ \sigma \not\sqsubseteq \mathcal{A}$. And thus, $\ell' \not\sqsubseteq \mathcal{A}$

  Since from Equation 14 we know that $(n-i-j, H'_{j1}, H'_{j2}) \overset{\mathcal{A}}{\triangleright} W'_2$ that means from Definition 1.9 that $(W'_2, n-i-j-1, H'_{j1}(a_1), H'_{j2}(a_2)) \in \lceil W'_2.\theta_1(a_1)\rceil_V^{\mathcal{A}}$. Since $(\ell_e\ \sigma) \sqsubseteq \ell'$ therefore from Definition 1.4 we know that $H'_{j1}(a_1)$ must also be protected at some label $\not\sqsubseteq \mathcal{A}$

  Therefore

$\forall m.\ (W_2'.\theta_1, m, H_{j1}'(a_1)) \in W_2'.\theta_1(a_1)$ (F)
and
$\forall m.\ (W_2'.\theta_2, m, H_{j2}'(a_2)) \in W_2'.\theta_2(a_1)$ (S)

Instantiating the (F) with m_1 and using Lemma 1.16 we get
$(\theta_1', m_1, H_{j1}'(a_1)) \in \theta_1'(a_1)$

Since from R2 we know that $(m_2+1, H_2') \triangleright \theta_2'$ therefore from Definition 1.8 we know that $(\theta_2', m_2, H_2'(a_2)) \in \theta_2'(a_2)$
Therefore from Definition 1.4 we get
$(W', n-n'-1, H_1'(a_1), H_2'(a_2)) \in \lceil \theta_1'(a_1) \rceil_V^{\mathcal{A}}$

iv. $H_{j1}'(a_1) \neq H_1'(a_1) \vee H_{j2}'(a_2) = H_2'(a_2)$:
Symmetric case as above

– $\forall i \in \{1,2\}.\forall m.\forall a_i \in dom(W'.\theta_i).(W'.\theta_i, m, H_i'(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$:

$\underline{i=1}$
This means that given some m we need to prove
$\forall a_i \in dom(W'.\theta_i).(W'.\theta_i, m, H_i'(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$

Like before we instantiate Equation 17 and Equation 18 with $m+2+t_1$ and $m+2+t_2$ respectively. This will give us

$\exists \theta_1'.\, W_2'.\theta_1 \sqsubseteq \theta_1' \wedge ((m_1+1), H_1') \triangleright \theta_1' \wedge (\theta_1', (m_1+1), v_1') \in \lfloor \tau_2\ \sigma \rfloor_V \wedge$
$(\forall a.H_{j1}'(a) \neq H_1'(a) \implies \exists \ell'.\, W_2'.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(W_2'.\theta_1).\theta_1'(a) \searrow (\ell_e\ \sigma))$
and
$\exists \theta_2'.\, W_2'.\theta_2 \sqsubseteq \theta_2' \wedge (m_2+1, H_2') \triangleright \theta_2' \wedge (\theta_2', (m_2+1), v_2') \in \lfloor \tau_2\ \sigma \rfloor_V \wedge$
$(\forall a.H_{j2}'(a) \neq H_2'(a) \implies \exists \ell'.\, W_2'.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2') \backslash dom(W_2'.\theta_2).\theta_2'(a) \searrow (\ell_e\ \sigma))$

Since we have $(m+1, H_1') \triangleright \theta_1'$ and $(m+1, H_2') \triangleright \theta_2'$ therefore we get the desired from Definition 1.8

$\underline{i=2}$
Symmetric to $i=1$

(b) $(W', n-n'-1, v_1', v_2') \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$:
Let $\tau_2 = \mathsf{A}^{\ell_i}$ Since $\tau_2\ \sigma \searrow \ell\ \sigma$ and since $\ell\ \sigma \not\sqsubseteq \mathcal{A}$ therefore $\ell_i\ \sigma \not\sqsubseteq \mathcal{A}$

From R1 and R2 we and Definition 1.4 we get the desired.

4. FG-prod:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : \tau_1 \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_2}{\Sigma; \Psi; \Gamma \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^{\perp}}$$

To prove: $(W, n, (e_1, e_2)\ (\gamma \downarrow_1), (e_1, e_2)\ (\gamma \downarrow_2)) \in \lceil (\tau_1 \times \tau_2)^{\perp}\ \sigma \rceil_E^{\mathcal{A}}$
Say $e_1 = (e_1, e_2)\ (\gamma \downarrow_1)$ and $e_2 = (e_1, e_2)\ (\gamma \downarrow_2)$
From Definition of $\lceil (\tau_1 \times \tau_2)^{\perp}\ \sigma \rceil_E^{\mathcal{A}}$ it suffices to prove that

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, e_1) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2') \implies$
$\exists W'.\, W \sqsubseteq W' \wedge (n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-n', v_1', v_2') \in \lceil (\tau_1 \times \tau_2)^{\perp}\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some H_1, H_2 and $n' < n$ s.t

$(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge (H_1, e_1) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2')$

<u>We are required to prove:</u>

$$\exists W'. W \sqsubseteq W' \wedge (n - n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v_1', v_2') \in \lceil (\tau_1 \times \tau_2)^{\perp} \ \sigma \rceil_V^{\mathcal{A}} \tag{19}$$

<u>IH1</u> $(W, n, (e_1)\ (\gamma \downarrow_1), (e_1)\ (\gamma \downarrow_2)) \in \lceil \tau_1\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 1.5 we get

$\forall H_{p11}, H_{p12}.(n, H_{p11}, H_{p12}) \overset{\mathcal{A}}{\triangleright} W \wedge \forall i < n.(H_{p11}, e_1\ (\gamma \downarrow_1)) \Downarrow_i (H_{p11}', v_{p11}') \wedge (H_{p12}, e_1\ (\gamma \downarrow_2$ $)) \Downarrow (H_{p12}', v_{p12}') \implies$

$\exists W_1' \sqsupseteq W.(n - i, H_{p11}', H_{p12}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n - i, v_{p11}', v_{p12}') \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$

Instantiating H_{p11} with H_1 and H_{p22} with H_2 in IH1 and since the (e_1, e_2) reduces to value with $\gamma \downarrow_1$ in $n' < n$ steps therefore we know that $\exists i < n' < n$ s.t $(H_{p11}, e_1\ (\gamma \downarrow_1)) \Downarrow_i (H_{p11}', v_{p11}')$. Similarly since we know that (e_1, e_2) reduces to value with $\gamma \downarrow_2$ therefore we know that $(H_{p12}, e_1\ (\gamma \downarrow_2)) \Downarrow (H_{p12}', v_{p12}')$. Hence we get

$$\exists W_1' \sqsupseteq W.(n - i, H_{p11}', H_{p12}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n - i, v_{p11}', v_{p12}') \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \tag{20}$$

<u>IH2</u> $(W, n - i, (e_2)\ (\gamma \downarrow_1), (e_2)\ (\gamma \downarrow_2)) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 1.5 we get

$\forall H_{p21}, H_{p22}.(n-i, H_{p21}, H_{p22}) \overset{\mathcal{A}}{\triangleright} W_1' \wedge \forall j < n-i.(H_{p21}, e_2\ (\gamma \downarrow_1)) \Downarrow_j (H_{p21}', v_{p21}') \wedge (H_{p22}, e_2\ (\gamma \downarrow_2$ $)) \Downarrow (H_{p22}', v_{p22}') \implies$

$\exists W_2' \sqsupseteq W_1'.(n - i - j, H_{p21}', H_{p22}') \overset{\mathcal{A}}{\triangleright} W_2' \wedge (W_2', n - i - j, v_{p21}', v_{p22}') \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$

Instantiating H_{p21} with H_{p11}' and H_{p22} with H_{p21}' and in IH2. Since (e_1, e_2) reduces to value with $\gamma \downarrow_1$ in $n' < n$ steps and e_1 has reduced with $i < n'$ steps. Therefore we know that $\exists j < n' - i < n - i$ s.t $(H_{p21}, e_2\ (\gamma \downarrow_1)) \Downarrow_i (H_{p21}', v_{p11}')$. Similarly since we know that (e_1, e_2) reduces to value with $\gamma \downarrow_2$ therefore we know that $(H_{p22}, e_2\ (\gamma \downarrow_2)) \Downarrow (H_{p22}', v_{p22}')$. Hence we get

since the (e_1, e_2) reduces to value with both $\gamma \downarrow_1$ and $\gamma \downarrow_2$ therefore we know that $(H_{p21}, e_2\ (\gamma \downarrow_1)) \Downarrow (H_{p21}', v_{p21}') \wedge (H_{p22}, e_1\ (\gamma \downarrow_2)) \Downarrow (H_{p22}', v_{p22}')$. Hence we get

$$\exists W_2' \sqsupseteq W_1'.(n - i - j, H_{p21}', H_{p22}') \overset{\mathcal{A}}{\triangleright} W_2' \wedge (W_2', n - i - j, v_{p21}', v_{p22}') \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}} \tag{21}$$

In order to prove Equation 19 we instantiate W' in Equation 19 with W_2' we are required to show the following:

- $W \sqsubseteq W_2'$:
  Since $W \sqsubseteq W_1'$ from Equation 20 and $W_1' \sqsubseteq W_2'$ from Equation 21
  Therefore, $W \sqsubseteq W_2'$ from Definition 1.3

- $(n - n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W'$:
  Here $n' = i + j + 1$
  From evaluation rule of products we know that $H'_1 = H'_{p21}$ and $H'_2 = H'_{p22}$
  From Equation 21 we know that $(n - i - j, H'_{p21}, H'_{p22}) \overset{\mathcal{A}}{\triangleright} W'_2$
  Therefore from Lemma 1.21 we get $(n - i - j - 1, H'_{p21}, H'_{p22}) \overset{\mathcal{A}}{\triangleright} W'_2$
- $(W', n - i - j - 1, v'_1, v'_2) \in \lceil (\tau_1 \times \tau_2)^{\perp}\ \sigma \rceil_V^{\mathcal{A}}$:
  From evaluation rule of products we know that $v'_1 = (v'_{p11}, v'_{p21})$ and $v'_2 = (v'_{p12}, v'_{p22})$
  We are required to show
  - $(W'_2, n - i - j - 1, v'_{p11}, v'_{p12}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \wedge (W'_2, n - i - j - 1, v'_{p21}, v'_{p22}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$:
    From Equation 20 and Equation 21 we know that
    $(W'_2, n - i - j, v'_{p11}, v'_{p12}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \wedge (W'_2, n - i - j, v'_{p21}, v'_{p22}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$
    Therefore from Lemma 1.17 we get
    $(W'_2, n - i - j - 1, v'_{p11}, v'_{p12}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \wedge (W'_2, n - i - j - 1, v'_{p21}, v'_{p22}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$

5. FG-fst:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_i : (\tau_1 \times \tau_2)^{\ell} \qquad \Sigma; \Psi \vdash \tau_1 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{fst}(e_i) : \tau_1}$$

To prove: $(W, n, (\mathsf{fst}(e_i))\ (\gamma \downarrow_1), (\mathsf{fst}(e_i))\ (\gamma \downarrow_2)) \in \lceil \tau_1\ \sigma \rceil_E^{\mathcal{A}}$
Say $e_1 = (\mathsf{fst}(e_i))\ (\gamma \downarrow_1)$ and $e_2 = (\mathsf{fst}(e_i))\ (\gamma \downarrow_2)$
From Definition 1.5 it suffices to prove that

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, e_1) \Downarrow_{n'} (H'_1, v'_1) \wedge (H_2, e_2) \Downarrow (H'_2, v'_2) \implies$
$\exists W'. W \sqsubseteq W' \wedge (n - n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v'_1, v'_2) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$

This means that given

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, e_1) \Downarrow_{n'} (H'_1, v'_1) \wedge (H_2, e_2) \Downarrow (H'_2, v'_2)$
We are required to prove:

$$\exists W'. W \sqsubseteq W' \wedge (n - n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v'_1, v'_2) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \tag{22}$$

IH1
$(W, (e_i)\ (\gamma \downarrow_1), (e_i)\ (\gamma \downarrow_2)) \in \lceil (\tau_1 \times \tau_2)^{\ell}\ \sigma \rceil_E^{\mathcal{A}}$
This means from Definition 1.5 we get

$\forall H_{i1}, H_{i2}.(n, H_{i1}, H_{i2}) \overset{\mathcal{A}}{\triangleright} W \wedge \forall i < n.(H_{i1}, e_i\ (\gamma \downarrow_1)) \Downarrow_i (H'_{i1}, v'_{i1}) \wedge (H_{i2}, e_i\ (\gamma \downarrow_2)) \Downarrow (H'_{i2}, v'_{i2}) \implies$
$\exists W'_1 \sqsupseteq W.(n - i, H'_{i1}, H'_{i2}) \overset{\mathcal{A}}{\triangleright} W'_1 \wedge (W'_1, n - i, v'_{i1}, v'_{i2}) \in \lceil (\tau_1 \times \tau_2)^{\ell}\ \sigma \rceil_V^{\mathcal{A}}$
Instantiating H_{i1} with H_1 and H_{i2} with H_2 in IH1 and since the $\mathsf{fst}(e_i)$ reduces to value reduces to value with $\gamma \downarrow_1$ in $n' < n$ steps therefore we know that $\exists i < n' < n$ s.t $(H_{i1}, e_i\ (\gamma \downarrow_1)) \Downarrow_i (H'_{i1}, v'_{i1})$. Similarly since we know that $\mathsf{fst}(e_i)$ reduces to value with $\gamma \downarrow_2$ therefore we know that $(H_{i2}, e_i\ (\gamma \downarrow_2)) \Downarrow (H'_{i2}, v'_{i2})$. Hence we get

$$\exists W_1' \sqsupseteq W.(n-i, H_{i1}', H_{i2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n-i, v_{i1}', v_{i2}') \in \lceil (\tau_1 \times \tau_2)^\ell\ \sigma \rceil_V^{\mathcal{A}} \tag{23}$$

We case analyze on $(W_1', n-i, v_{i1}', v_{i2}') \in \lceil (\tau_1 \times \tau_2)^\ell\ \sigma \rceil_V^{\mathcal{A}}$ from Equation 23

- Case $\ell\ \sigma \sqsubseteq \mathcal{A}$:
  From Definition 1.4 we know that this would mean that
  $(W_1', n-i, v_{i1}', v_{i2}') \in \lceil (\tau_1 \times \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$
  This means
  $(W_1', n-i, v_{i1}', v_{i2}') \in \lceil (\tau_1\ \sigma \times \tau_2\ \sigma) \rceil_V^{\mathcal{A}}$
  Let $v_{i1}' = (v_{i1}, v_{i2})$ and $v_{i2}' = (v_{j1}, v_{j2})$

  Again from Definition 1.4 it means that
  $(W_1', n-i, v_{i1}, v_{j1}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \wedge (W_1', n-i, v_{i2}, v_{j2}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$ (F1)

  Inroder to prove Equation 22 we choose W' as W_1' and from the evaluation rule of fst we know that $H_1' = H_{i1}'$ and $H_2' = H_{i2}'$. Also, from reduction rules we know that $n' = i + 1$. And then we need to show:
  - $W \sqsubseteq W_1'$:
    Directly from Equation 23
  - $(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1'$:
    Since from Equation 23 we know that $(n-i, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1'$
    Therefore from Lemma 1.21 we get $(n-i-1, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1'$
  - $(W_1', n-n', v_1', v_2') \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$:
    From the evaluation rule we know that $v_1' = v_{i1}$ and $v_2' = v_{j1}$
    From F1 we know that $(W_1', n-i, v_{i1}, v_{j1}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$
    Therefore from Lemma 1.17 we get $(W_1', n-i-1, v_{i1}, v_{j1}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$
- Case $\ell\ \sigma \not\sqsubseteq \mathcal{A}$:
  In this case from Definition 1.6 we know that
  (a) $\forall m.\ (W_1'.\theta_1, m, v_{i1}') \in \lfloor (\tau_1\ \sigma \times \tau_2\ \sigma) \rfloor_V$ and
  (b) $\forall m.\ (W_1'.\theta_2, m, v_{i2}') \in \lfloor (\tau_1\ \sigma \times \tau_2\ \sigma) \rfloor_V$
  where
  $v_{i1}' = (v_{i1}, v_{i2})$ and $v_{i2}' = (v_{j1}, v_{j2})$

  Inroder to prove Equation 22 we choose W' as W_1' and from the evaluation rule of fst we know that $H_1' = H_{i1}'$ and $H_2' = H_{i2}'$. And then we need to show:
  - $W \sqsubseteq W_1'$:
    Directly from Equation 23
  - $(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1'$:
    From Equation 23 we know that $(n-i, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1'$
    Therefore from Lemma 1.21 we get
    $(n-i-1, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1'$

– $(W_1', n-n', v_1', v_2') \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$:
From the evaluation rule we know that $v_1' = v_{i1}$ and $v_2' = v_{j1}$
Let $\tau_1 = \mathsf{A}^{\ell_i}$ Since $\tau_1\ \sigma \searrow \ell$ and since $\ell\ \sigma \not\sqsubseteq \mathcal{A}$ therefore $\ell_i\ \sigma \not\sqsubseteq \mathcal{A}$

Therefore from Definition 1.4 it suffices to prove that
$\forall m_1.\ (W_1'.\theta_1, m_1, v_{i1}) \in \lfloor \tau_1\ \sigma \rfloor_V$
and
$\forall m_2.\ (W_1'.\theta_2, m_2, v_{j1}) \in \lfloor \tau_1\ \sigma \rfloor_V$
This means given m_1 and it suffices to prove:

$$(W_1'.\theta_1, m_1, v_{i1}) \in \lfloor \tau_1\ \sigma \rfloor_V \tag{24}$$

Similarly given m_2, it suffices to prove:

$$(W_1'.\theta_2, m_2, v_{j1}) \in \lfloor \tau_1\ \sigma \rfloor_V \tag{25}$$

Instantiating (a) with m_1

$$(W_1'.\theta_1, m_1, v_{i1}) \in \lfloor \tau_1\ \sigma \rfloor_V \wedge (W_1'.\theta_1, m_1, v_{i2}) \in \lfloor \tau_2\ \sigma \rfloor_V \tag{26}$$

Instantiating (b) with m_2

$$(W_1'.\theta_2, m_2, v_{j1}) \in \lfloor \tau_1\ \sigma \rfloor_V \wedge (W_1'.\theta_2, m_2, v_{j2}) \in \lfloor \tau_2\ \sigma \rfloor_V \tag{27}$$

From Equation 26 and Equation 27 we get
$(W_1'.\theta_1, m_1, v_{i1}) \in \lfloor \tau_1\ \sigma \rfloor_V$ and $(W_1'.\theta_2, m_2, v_{j1}) \in \lfloor \tau_1\ \sigma \rfloor_V$

6. FG-snd:

   Symmetric case as FG-fst

7. FG-inl:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_i : \tau_1}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inl}(e_i) : (\tau_1 + \tau_2)^\perp}$$

To prove: $(W, n, (\mathsf{inl}\ (e_i))\ (\gamma \downarrow_1), (\mathsf{inl}\ (e_i))\ (\gamma \downarrow_2)) \in \lceil (\tau_1 + \tau_2)^\perp\ \sigma \rceil_E^{\mathcal{A}}$
Say $e_1 = (\mathsf{inl}\ (e_i))\ (\gamma \downarrow_1)$ and $e_2 = (\mathsf{inl}\ (e_i))\ (\gamma \downarrow_2)$
From Definition of $\lceil (\tau_1 + \tau_2)^\perp\ \sigma \rceil_E^{\mathcal{A}}$ it suffices to prove that

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, e_1) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2') \implies$
$\exists W'. W \sqsubseteq W' \wedge (n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-n', v_1', v_2') \in \lceil (\tau_1 + \tau_2)^\perp\ \sigma \rceil_V^{\mathcal{A}}$

This means that given
$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, e_1) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2')$
<u>We are required to prove:</u>

$$\exists W'. W \sqsubseteq W' \wedge (n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-n', v_1', v_2') \in \lceil (\tau_1 + \tau_2)^\perp\ \sigma \rceil_V^{\mathcal{A}} \tag{28}$$

$\underline{\text{IH1}}$ $(W, (e_i)\ (\gamma \downarrow_1), (e_i)\ (\gamma \downarrow_2)) \in \lceil \tau_1\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 1.5 we get

$\forall H_{i1}, H_{i2}.(n, H_{i1}, H_{i2}) \overset{\mathcal{A}}{\triangleright} W \wedge \forall i < n.(H_{i1}, e_i\ (\gamma \downarrow_1)) \Downarrow_i (H'_{i1}, v'_{i1}) \wedge (H_{i2}, e_i\ (\gamma \downarrow_2)) \Downarrow (H'_{i2}, v'_{i2}) \implies$
$\exists W'_1 \sqsupseteq W.(n-i, H'_{i1}, H'_{i2}) \overset{\mathcal{A}}{\triangleright} W'_1 \wedge (W'_1, n-i, v'_{i1}, v'_{i2}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$

Instantiating H_{i1} with H_1 and H_{i2} with H_2 in IH1 and since the $\mathsf{inl}(e_i)$ reduces to value with $\gamma \downarrow_1$ in $n' < n$ steps therefore we know that $\exists i < n' < n$ s.t $(H_{i1}, e_i\ (\gamma \downarrow_1)) \Downarrow_i (H'_{i1}, v'_{i1})$. Similarly since we know that $\mathsf{inl}(e_i)$ reduces to value with $\gamma \downarrow_2$ therefore we know that $(H_{i2}, e_i\ (\gamma \downarrow_2)) \Downarrow (H'_{i2}, v'_{i2})$. Hence we get

$$\exists W'_1 \sqsupseteq W.(n-i, H'_{i1}, H'_{i2}) \overset{\mathcal{A}}{\triangleright} W'_1 \wedge (W'_1, n-i, v'_{i1}, v'_{i2}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \tag{29}$$

Instantiating W' in Equation 28 with W'_1. Also from reduction relation we know that $n' = i + 1$ we are required to show the following:

- $W \sqsubseteq W'_1$:
  Directly from Equation 29
- $(n - n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W'_1$:
  From Equation 29 we know that $(n-i, H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W'_1$
  Therefore from Lemma 1.21 we get
  $(n-n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W'_1$
- $(W'_1, n-n', v'_1, v'_2) \in \lceil (\tau_1 + \tau_2)^{\perp}\ \sigma \rceil_V^{\mathcal{A}}$:
  From evaluation rule of inl we know that $v'_1 = \mathsf{inl}(v'_{i1})$ and $v'_2 = \mathsf{inl}(v'_{i2})$
  We are required to show
  - $(W'_1, n-n', v'_{i1}, v'_{i2}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$:
    From Equation 29 we know that $(W'_1, n-i, v'_{i1}, v'_{i2}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$
    Therefore from Lemma 1.17 we get
    $(W'_1, n-i-1, v'_{i1}, v'_{i2}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$

8. FG-inr:

   Symmetric case to FG-inl.

9. FG-case:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_i : (\tau_1 + \tau_2)^{\ell} \quad \Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_{i1} : \tau \quad \Sigma; \Psi; \Gamma, y : \tau_2 \vdash_{pc \sqcup \ell} e_{i2} : \tau \quad \Sigma; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{case}(e_i, x.e_{i1}, y.e_{i2}) : \tau}$$

To prove: $(W, (\mathsf{case}(e_i, x.e_{i1}, y.e_{i2}))\ (\gamma \downarrow_1), (\mathsf{case}(e_i, x.e_{i1}, y.e_{i2}))\ (\gamma \downarrow_2)) \in \lceil (\tau)\ \sigma \rceil_E^{\mathcal{A}}$

Say $e_1 = (\mathsf{case}(e_i, x.e_{i1}, y.e_{i2}))\ (\gamma \downarrow_1)$ and $e_2 = (\mathsf{case}(e_i, x.e_{i1}, y.e_{i2}))\ (\gamma \downarrow_2)$

This means from Definition 1.5 we need to prove:

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, e_1) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2') \implies$
$\exists W' \sqsupseteq W.(n - n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v_1', v_2') \in \lceil(\tau)\ \sigma\rceil_V^{\mathcal{A}}$
This further means that given

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, e_1) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2')$
It suffices to prove

$$\exists W' \sqsupseteq W.(n - n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v_1', v_2') \in \lceil(\tau)\ \sigma\rceil_V^{\mathcal{A}} \tag{30}$$

IH1 $(W, n, (e_i)\ (\gamma \downarrow_1), (e_i)\ (\gamma \downarrow_2)) \in \lceil(\tau_1 + \tau_2)^\ell\ \sigma\rceil_E^{\mathcal{A}}$
This means from Definition 1.5 we get

$\forall H_{i1}, H_{i2}.(n, H_{i1}, H_{i2}) \overset{\mathcal{A}}{\triangleright} W \wedge \forall i < n.(H_{i1}, e_i\ (\gamma \downarrow_1)) \Downarrow_i (H_1', v_1') \wedge (H_{i2}, e_i\ (\gamma \downarrow_2)) \Downarrow (H_2', v_2') \implies$

$\exists W_1' \sqsupseteq W.(n - i, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n - i, v_{s1}', v_{s2}') \in \lceil(\tau_1 + \tau_2)^\ell\ \sigma\rceil_V^{\mathcal{A}}$
Instantiating H_{i1} with H_1 and H_{i2} with H_2 in IH1 and since the $(\mathsf{case}(e_i, x.e_{i1}, y.e_{i2}))$ reduces to value with both $\gamma \downarrow_1$ and $\gamma \downarrow_2$ therefore we know that $(H_{i1}, e_i\ (\gamma \downarrow_1)) \Downarrow (H_1', v_1') \wedge (H_{i2}, e_i\ (\gamma \downarrow_2)) \Downarrow (H_2', v_2')$. Hence we get

$$\exists W_1' \sqsupseteq W.(n - i, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n - i, v_{s1}', v_{s2}') \in \lceil(\tau_1 + \tau_2)^\ell\ \sigma\rceil_V^{\mathcal{A}} \tag{31}$$

IH2:
$(W_1', n - i, (e_{i1})\ (\gamma \downarrow_1 \cup \{x \mapsto v_{i1}\}), (e_{i1})\ (\gamma \downarrow_2 \cup \{x \mapsto v_{i2}\})) \in \lceil(\tau)\ \sigma\rceil_E^{\mathcal{A}}$
This means from Definition 1.5 we get

$\forall H_{j1}, H_{j2}.(n - i, H_{j1}, H_{j2}) \overset{\mathcal{A}}{\triangleright} W_1' \wedge \forall j < n - i.(H_1, e_{i1}\ (\gamma \downarrow_1 \cup \{x \mapsto v_{i1}\})) \Downarrow_j (H_{j1}', v_{j1}') \wedge (H_2, e_{i1}\ (\gamma \downarrow_2 \cup \{x \mapsto v_{i2}\})) \Downarrow (H_{j2}', v_{j2}') \implies$
$\exists W_2' \sqsupseteq W_1'.(n - i - j, H_{j1}', H_{j2}') \overset{\mathcal{A}}{\triangleright} W_2' \wedge (W_2', n - i - j, v_{j1}', v_{j2}') \in \lceil(\tau)\ \sigma\rceil_V^{\mathcal{A}}$
Instantiating H_{j1} with H_1' and H_{j2} with H_2' in IH2. Also instantiating W with W_1'. Since the $(\mathsf{case}(e_i, x.e_{i1}, y.e_{i2}))$ reduces to value in both runs therefore we know that $(H_1, e_{i1}\ (\gamma \downarrow_1)) \Downarrow (H_{j1}', v_{j1}') \wedge (H_2, e_{i1}\ (\gamma \downarrow_2)) \Downarrow (H_{j2}', v_{j2}')$. Hence we get

$$\exists W_2' \sqsupseteq W_1'.(n - i - j, H_{j1}', H_{j2}') \overset{\mathcal{A}}{\triangleright} W_2' \wedge (W_2', n - i - j, v_{j1}', v_{j2}') \in \lceil(\tau)\ \sigma\rceil_V^{\mathcal{A}} \tag{32}$$

IH3:
$(W_1', n - i, (e_{i2})\ (\gamma \downarrow_1 \cup \{y \mapsto v_{i1}\}), (e_{i2})\ (\gamma \downarrow_2 \cup \{y \mapsto v_{i2}\})) \in \lceil(\tau)\ \sigma\rceil_E^{\mathcal{A}}$
This means from Definition 1.5 we get

$\forall H_{k1}, H_{k2}.(n - i, H_{k1}, H_{k2}) \overset{\mathcal{A}}{\triangleright} W_1' \wedge \forall k < n - i.(H_1, e_{i2}\ (\gamma \downarrow_1 \cup \{y \mapsto v_{i1}\})) \Downarrow_k (H_{k1}', v_{k1}') \wedge (H_2, e_{i2}\ (\gamma \downarrow_2 \cup \{y \mapsto v_{i2}\})) \Downarrow (H_{k2}', v_{k2}') \implies$
$\exists W_3' \sqsupseteq W_1'.(n - i - k, H_{k1}', H_{k2}') \overset{\mathcal{A}}{\triangleright} W_3' \wedge (W_3', n - i - k, v_{k1}', v_{k2}') \in \lceil(\tau)\ \sigma\rceil_V^{\mathcal{A}}$

Instantiating H_{k1} with H'_1 and H_{k2} with H'_2 in IH2. Also instantiating W with W'_1. Since the $(\mathsf{case}(e_i, x.e_{i2}, y.e_{i2}))$ reduces to value in both runs therefore we know that $(H_1, e_{i2}\ (\gamma\downarrow_1)) \Downarrow (H'_{k1}, v'_{k1}) \wedge (H_2, e_{i2}\ (\gamma\downarrow_2)) \Downarrow (H'_{k2}, v'_{k2})$. Hence we get

$$\exists W'_3 \sqsupseteq W'_1.(n-i-k, H'_{k1}, H'_{k2}) \overset{\mathcal{A}}{\triangleright} W'_3 \wedge (W'_3, n-i-k, v'_{k1}, v'_{k2}) \in \lceil(\tau)\ \sigma\rceil_V^{\mathcal{A}} \tag{33}$$

We case analyze $(W'_1, n-i, v'_1, v'_2) \in \lceil(\tau_1+\tau_2)^\ell\ \sigma\rceil_V^{\mathcal{A}}$ from Equation 31

- Case $\ell\ \sigma \sqsubseteq \mathcal{A}$:
  From Definition 1.4 2 further cases arise:
  - $v'_1 = \mathsf{inl}(v_{i1})$ and $v'_2 = \mathsf{inl}(v_{i2})$:
    In this case from Definition 1.4 we know that $(W, n-i, v_{i1}, v_{i2}) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}}$

    Inorder to prove Equation 30 we choose W' as W'_2 from Equation 32 and from the first evaluation rule of case we know that $H'_1 = H'_{j1}$ and $H'_2 = H'_{j2}$. Also we know from the evaluation rule that $n' = i+j+1$. And then we need to show:
    * $W \sqsubseteq W'_2$:
      Since $W \sqsubseteq W'_1$ from Equation 31 and $W'_1 \sqsubseteq W'_2$ from Equation 32
      Therefore, $W \sqsubseteq W'_2$ from Definition 1.3
    * $(n-n', H'_{j1}, H'_{j2}) \overset{\mathcal{A}}{\triangleright} W'_2$:
      From Equation 32 we know that $(n-i-j, H'_{j1}, H'_{j2}) \overset{\mathcal{A}}{\triangleright} W'_2$
      Therefore from Lemma 1.21 we get
      $(n-i-j-1, H'_{j1}, H'_{j2}) \overset{\mathcal{A}}{\triangleright} W'_2$
    * $(W'_2, n-n', v'_1, v'_2) \in \lceil\tau\ \sigma\rceil_V^{\mathcal{A}}$:
      From the evalaution rule we know that $v'_1 = v'_{j1}$ and $v'_2 = v'_{j2}$
      From Equation 32 we know that $(W'_2, n-i-j, v'_{j1}, v'_{j2}) \in \lceil\tau\ \sigma\rceil_V^{\mathcal{A}}$
      Therefore from Lemma 1.17 we get
      $(W'_2, n-i-j-1, v'_{j1}, v'_{j2}) \in \lceil\tau\ \sigma\rceil_V^{\mathcal{A}}$
  - $v'_1 = \mathsf{inr}(v_{i1})$ and $v'_2 = \mathsf{inr}(v_{i2})$:
    In this case from Definition 1.4 we know that $(W, v_{i1}, v_{i2}) \in \lceil\tau_2\ \sigma\rceil_V^{\mathcal{A}}$

    Inorder to prove Equation 30 we choose W' as W'_3 from Equation 33 and from the second evaluation rule of case we know that $H'_1 = H'_{k1}$ and $H'_2 = H'_{k2}$. Also we know from the evaluation rule that $n' = i+k+1$. And then we need to show:
    * $W \sqsubseteq W'_3$:
      Since $W \sqsubseteq W'_1$ from Equation 31 and $W'_1 \sqsubseteq W'_3$ from Equation 33
      Therefore, $W \sqsubseteq W'_3$ from Definition 1.3
    * $(n-n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W'_3$:
      From Equation 33 we know that $(n-i-k, H'_{k1}, H'_{k2}) \overset{\mathcal{A}}{\triangleright} W'_3$
      Therefore from Lemma 1.21 we get
      $(n-i-k-1, H'_{k1}, H'_{k2}) \overset{\mathcal{A}}{\triangleright} W'_3$
    * $(W'_3, n-n', v'_1, v'_2) \in \lceil\tau\ \sigma\rceil_V^{\mathcal{A}}$:
      From the evalaution rule we know that $v'_1 = v'_{k1}$ and $v'_2 = v'_{k2}$
      From Equation 33 we know that $(W'_3, n-i-k, v'_{k1}, v'_{k2}) \in \lceil\tau\ \sigma\rceil_V^{\mathcal{A}}$
      Therefore from Lemma 1.17 we get
      $(W'_3, n-i-k-1, v'_{k1}, v'_{k2}) \in \lceil\tau\ \sigma\rceil_V^{\mathcal{A}}$

- Case $\ell\ \sigma \not\sqsubseteq \mathcal{A}$:

  The following cases arise:

  (a) Reduction of e_1 happens via Case1 and Reduction of e_2 happens via Case1 :
  Exactly the same reasoning as in the $v_1' = \mathsf{inl}(v_{i1})$ and $v_2' = \mathsf{inl}(v_{i2})$ subscase of the $\ell\ \sigma \not\sqsubseteq \mathcal{A}$ case before.

  (b) Reduction of e_1 happens via Case2 and Reduction of e_2 happens via Case2 :
  Exactly the same reasoning as in the $v_1' = \mathsf{inr}(v_{i1})$ and $v_2' = \mathsf{inr}(v_{i2})$ subscase of the $\ell\ \sigma \not\sqsubseteq \mathcal{A}$ case before.

  (c) Reduction of e_1 happens via Case1 and Reduction of e_2 happens via Case2 :

  From Equation 30 we know that we need to prove
  $\exists W' \sqsupseteq W.(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-n', v_1', v_2') \in \lceil(\tau)\ \sigma\rceil_V^{\mathcal{A}}$

  In this case since we know that $\ell\ \sigma \not\sqsubseteq \mathcal{A}$. Let $\tau\ \sigma = \mathsf{A}^{\ell_i}$ and since $\tau\ \sigma \searrow \ell\ \sigma$ therefore $\ell_i \not\sqsubseteq \mathcal{A}$

  This means inorder to prove $\exists W' \sqsupseteq W.(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-n', v_1', v_2') \in \lceil(\tau)\ \sigma\rceil_V^{\mathcal{A}}$
  From Definition 1.4 it will suffice to prove
  $\exists W' \sqsupseteq W.(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (\forall m_1.(W'.\theta_1, m_1, v_1') \in \lfloor(\tau)\ \sigma\rfloor_V) \wedge (\forall m_2.(W'.\theta_1, m_2, v_2') \in \lfloor(\tau)\ \sigma\rfloor_V)$

  This means it suffices to prove
  $(\forall m_1, m_2.\exists W' \sqsupseteq W.(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W'.\theta_1, m_1, v_1') \in \lfloor(\tau)\ \sigma\rfloor_V) \wedge ((W'.\theta_1, m_2, v_2') \in \lfloor(\tau)\ \sigma\rfloor_V)$

  This means given m_1 and m_2 it suffices to prove:

  $$(\exists W' \sqsupseteq W.(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W'.\theta_1, m_1, v_1') \in \lfloor(\tau)\ \sigma\rfloor_V) \wedge (W'.\theta_1, m_2, v_2') \in \lfloor(\tau)\ \sigma\rfloor_V) \tag{34}$$

  Since we know that $(W, n, \gamma) \in \lceil\Gamma\rceil_V^{\mathcal{A}}$ (given) therefore from Lemma 1.25 we know that $\forall i \in \{1,2\}.\ \forall m.\ (W.\theta_i, m, \gamma\downarrow_i) \in \lfloor\Gamma\rfloor_V$

  Therefore by instantiating it at $m_1 + 1 + j$ we know that

  $$(W.\theta_1, m_1 + 1 + j, \gamma\downarrow_1) \in \lfloor\Gamma\rfloor_V \tag{35}$$

  Next we apply Theorem 1.22 on $e_{i1}\ \gamma\downarrow_1$. Here j is the number of steps in which $e_{i1}\ \gamma\downarrow_1$ reduces. We use $\gamma\downarrow_1 \cup \{x \mapsto v_{s1}'\}$ as the unary substitution to get $(W.\theta_1, m_1 + 1 + j, e_{i1}\ \gamma\downarrow_1 \cup \{x \mapsto v_c'\}) \in \lfloor(\tau)\ \sigma\rfloor_E^{pc}$

  This means from Definition 1.7 we get
  $\forall H_{c2}.(m_1+1+j, H_{c1}) \triangleright W_1.\theta_1 \wedge \forall l_c < (m_1+1+j).(H_{c2}, (e_{i1})\ \gamma\downarrow_1 \cup \{x \mapsto v_c'\}) \Downarrow_{k_c} (H_{c2}', v_c') \implies$
  $\exists \theta_1'.\ W_1.\theta_1 \sqsubseteq \theta_1' \wedge (m_1+1+j-l_c, H_{c2}') \triangleright \theta_1' \wedge (\theta_1', m_1+1+j-l_c, v_c') \in \lfloor(\tau)\ \sigma\rfloor_V \wedge$
  $(\forall a.H_{c2}(a) \neq H_{c2}'(a) \implies \exists \ell'.\ W_1.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (pc \sqcup \ell)\ \sigma \sqsubseteq \ell') \wedge$
  $(\forall a \in dom(\theta_1') \backslash dom(W_1.\theta_1).\theta_1'(a) \searrow (pc \sqcup \ell)\ \sigma)$

  Since from Equaiton 31 we know that $(n-i, H_1', H_2') \triangleright W_1'$ therefore from Lemma 1.27 we get $\forall m.(m, H_1') \triangleright W_1'.\theta_1$

Instantiating m with $m_1 + 1 + j$ we get $(m_1 + 1 + j, H'_1) \rhd W'_1.\theta_1$

Instantiating H_{c2} with H'_1 from Equation 31 and l_c with j we get
$\exists \theta'_1. W_1.\theta_1 \sqsubseteq \theta'_1 \wedge (m_1 + 1, H'_{c2}) \rhd \theta'_1 \wedge (\theta'_1, m_1 + 1, v'_c) \in \lfloor (\tau)\ \sigma \rfloor_V \wedge$
$(\forall a. H_{c2}(a) \neq H'_{c2}(a) \implies \exists \ell'. W_1.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (pc \sqcup \ell)\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_1) \backslash dom(\theta'_1).\theta'_1(a) \searrow (pc \sqcup \ell)\ \sigma)$ (CC1)

Similarly we apply Theorem 1.22 on $e_{i2}\ \gamma \downarrow_2$. Here j_2 is the number of steps in which $e_{i2}\ \gamma \downarrow_2$ reduces. We use $\gamma \downarrow_2 \cup \{y \mapsto v'_{s2}\}$ as the unary substitution to get $(W_1.\theta_2, m_2 + 1 + j_2, e_{i2}\ \gamma \downarrow_1 \cup \{y \mapsto v'_c\}) \in \lfloor (\tau)\ \sigma \rfloor_E^{pc}$

This means from Definition 1.7 we get
$\forall H_{c2}.(m_2+1+j_2, H_{c1}) \rhd W_1.\theta_2 \wedge \forall l_c < m_2+1+j_2.(H_{c2}, (e_{i1})\ \gamma \downarrow_1 \cup \{x \mapsto v'_c\}) \Downarrow_{k_c} (H'_{c2}, v'_c) \implies$
$\exists \theta'_2. W_1.\theta_2 \sqsubseteq \theta'_2 \wedge (m_2+1+j_2-l_c, H'_{c2}) \rhd \theta'_1 \wedge (\theta'_2, m_2+1+j_2-l_c, v'_c) \in \lfloor (\tau)\ \sigma \rfloor_V \wedge$
$(\forall a. H_{c2}(a) \neq H'_{c2}(a) \implies \exists \ell'. W_1.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (pc \sqcup \ell)\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_2) \backslash dom(\theta'_1).\theta'_1(a) \searrow (pc \sqcup \ell)\ \sigma)$

Since from Equaiton 31 we know that $(n-i, H'_1, H'_2) \rhd W'_1$ therefore from Lemma 1.27 we get $\forall m.(m, H'_2) \rhd W'_1.\theta_2$
Instantiating m with $m_2 + 1 + j_2$ we get $(m_2 + 1 + j_2, H'_2) \rhd W'_1.\theta_2$

Instantiating H_{c2} with H'_2 (from Equation 31)and l_c with j_2 to get
$\exists \theta'_2. W_1.\theta_2 \sqsubseteq \theta'_2 \wedge (m_2 + 1, H'_{c2}) \rhd \theta'_2 \wedge (\theta'_2, m_2 + 1, v'_c) \in \lfloor (\tau)\ \sigma \rfloor_V \wedge$
$(\forall a. H_{c2}(a) \neq H'_{c2}(a) \implies \exists \ell'. W_1.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (pc \sqcup \ell)\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_2) \backslash dom(\theta'_1).\theta'_1(a) \searrow (pc \sqcup \ell)\ \sigma)$ (CC2)

We choose
$W_n.\theta_1 = \theta'_1$ (from CC1)
$W_n.\theta_2 = \theta'_2$ (from CC2)
$W_n.\hat{\beta} = W'_1.\hat{\beta}$ (from Equation 31)

In order to prove Equation 30 we choose W' as W_n

i. $(n - n', H'_1, H'_2) \rhd W'$:
   From Definition 1.9 it suffices to show that
   - $dom(W'.\theta_1) \subseteq dom(H'_1) \wedge dom(W.\theta_2) \subseteq dom(H'_2)$:
     From (CC1) we know that $(m_1 + 1, H'_1) \rhd \theta'_1$, therefore from Definition 1.8 we get $dom(W'.\theta_1) \subseteq dom(H'_1)$
     Similarly, from (CC2) we know that $(m_2 + 1, H'_2) \rhd \theta'_2$, therefore from Definition 1.8 we get $dom(W'.\theta_2) \subseteq dom(H'_2)$
   - $(W.\hat{\beta}) \subseteq (dom(W'.\theta_1) \times dom(W'.\theta_1))$:
     Since from Equation 31 we have $(n - i, H'_1, H'_2) \rhd W'_1$ therefore from Definition 1.9 we get $(W'_1.\hat{\beta}) \subseteq (dom(W'_1.\theta_1) \times dom(W'_1.\theta_2))$
     From (CC1) and (CC2) we know that $W'_1.\theta_1 \sqsubseteq \theta'_1$ and $W'_1.\theta_2 \sqsubseteq \theta'_2$ therefore $(W'_1.\hat{\beta}) \subseteq (dom(\theta'_1) \times dom(\theta'_2))$
   - $\forall (a_1, a_2) \in (W'.\hat{\beta}). W'.\theta_1(a_1) = W'.\theta_2(a_2) \wedge$
     $(W', n - n' - 1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1) \rceil_V^A$:

     4 cases arise for each a_1 and a_2

A. $H'_{j1}(a_1) = H'_1(a_1) \wedge H'_{j2}(a_2) = H'_2(a_2)$:

$\underline{W'.\theta_1(a_1) = W'.\theta_2(a_2)}$:

We know from Equation 31 that $(n-i, H'_1, H'_2) \triangleright W'_1$

Therefore from Definition 1.9 we have
$\forall (a_1, a_2) \in (W'_1.\hat{\beta}). W'_1.\theta_1(a_1) = W'_1.\theta_2(a_2)$

Since $W'.\hat{\beta} = W'_1.\hat{\beta}$ by construction therefore
$\forall (a_1, a_2) \in (W'.\hat{\beta}). W'_1.\theta_1(a_1) = W'_1.\theta_2(a_2)$

From (CC1) and (CC2) we know that $W'_1.\theta_1 \sqsubseteq \theta'_1$ and $W'_1.\theta_2 \sqsubseteq \theta'_2$ respectively.
Therefore from Definition 1.2
$\forall (a_1, a_2) \in (W'.\hat{\beta}).\theta'_1(a_1) = \theta'_2(a_2)$

$\underline{(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1) \rceil_V^{\mathcal{A}}}$:

From Equation 31 we know that $(n-i, H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W'_1$
This means from Definition 1.9 that
$\forall (a_{i1}, a_{i2}) \in (W'_1.\hat{\beta}). W'_1.\theta_1(a_1) = W'_1.\theta_2(a_2) \wedge (W'_1, n-i-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'_1.\theta_1(a_1) \rceil_V^{\mathcal{A}}$

Instantiating with a_1 and a_2 and since $W'_1 \sqsubseteq W'$ and $n-n'-1 < n-i-1$ (since $n' = i+t_1+1$ where t_1 is the number of steps taken by e_{i1}, i is the number of steps taken by $e_1\ \gamma \downarrow_1$ to reduce) therefore from Lemma 1.17 we get
$(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1) \rceil_V^{\mathcal{A}}$

B. $H'_{j1}(a_1) \neq H'_1(a_1) \vee H'_{j2}(a_2) \neq H'_2(a_2)$:

$\underline{W'.\theta_1(a_1) = W'.\theta_2(a_2)}$:

Same as before

$\underline{(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1) \rceil_V^{\mathcal{A}}}$:

From (CC1) and (CC2) we know that
$(\forall a. H'_1(a) \neq H'_{c1}(a) \implies \exists \ell'. W'_1.\theta_1(a) = \mathsf{A}^{\ell'} \wedge ((pc \sqcup \ell)\ \sigma) \sqsubseteq \ell')$
$(\forall a. H'_2(a) \neq H'_{c2}(a) \implies \exists \ell'. W'_1.\theta_2(a) = \mathsf{A}^{\ell'} \wedge ((pc \sqcup \ell)\ \sigma) \sqsubseteq \ell')$
This means we have
$\exists \ell'. W'_1.\theta_1(a_1) = \mathsf{A}^{\ell'} \wedge ((pc \sqcup \ell)\ \sigma) \sqsubseteq \ell'$ and
$\exists \ell'. W'_1.\theta_2(a_2) = \mathsf{A}^{\ell'} \wedge ((pc \sqcup \ell)\ \sigma) \sqsubseteq \ell'$

Since $\ell\ \sigma \not\sqsubseteq \mathcal{A}$. Therefore, $(pc \sqcup \ell)\ \sigma \not\sqsubseteq \mathcal{A}$. And thus, $\ell' \not\sqsubseteq \mathcal{A}$

Also from (CC1) and (CC2), $(m_1+1, H'_{c1}) \triangleright \theta'_1$ and $(m_2+1, H'_{c2}) \triangleright \theta'_2$.
Therefore from Definition 1.8 we have
$(\theta'_1, m_1, H'_{c1}(a_1)) \in \lfloor \theta'_1(a_1) \rfloor_V$ and
$(\theta'_2, m_2, H'_{c2}(a_1)) \in \lfloor \theta'_2(a_2) \rfloor_V$

Since m_1 and m_2 are arbitrary indices therefore from Definition 1.4 we get (here $H'_1 = H'_{c1}$ and $H'_2 = H'_{c2}$)
$(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil \theta'_1(a_1) \rceil_V^{\mathcal{A}}$

C. $H'_{j1}(a_1) = H'_1(a_1) \vee H'_{j2}(a_2) \neq H'_2(a_2)$:

$\underline{W'.\theta_1(a_1) = W'.\theta_2(a_2)}$:

Same as before

$\underline{(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1) \rceil_V^{\mathcal{A}}}$:

From (CC2) we know that
$(\forall a.H'_2(a) \neq H'_{c2}(a) \implies \exists \ell'. W'_1.\theta_2(a) = \mathsf{A}^{\ell'} \wedge ((pc \sqcup \ell)\ \sigma) \sqsubseteq \ell')$
This means that a_2 was protected at $(pc \sqcup \ell)\ \sigma$ in the world before the modification. Since $\ell\ \sigma \not\sqsubseteq \mathcal{A}$. Therefore, $(pc \sqcup \ell)\ \sigma \not\sqsubseteq \mathcal{A}$. And thus, $\ell' \not\sqsubseteq \mathcal{A}$

Since from Equation 31 we know that $(n-i, H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W'_1$ that means from Definition 1.9 that $(W'_1, n-i-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'_1.\theta_1(a_1) \rceil^{\mathcal{A}}_V$. Since $((pc \sqcup \ell)\ \sigma) \sqsubseteq \ell'$ therefore from Definition 1.4 we know that $H'_1(a_1)$ must also be protected at some label $\not\sqsubseteq \mathcal{A}$

Therefore
$\forall m.\ (W'_1.\theta_1, m, H'_1(a_1)) \in W'_1.\theta_1(a_1)$ (F)
and
$\forall m.\ (W'_1.\theta_2, m, H'_2(a_2)) \in W'_1.\theta_2(a_1)$ (S)

Instantiating the (F) with m_1 and using Lemma 1.16 we get
$(\theta'_1, m_1, H'_1(a_1)) \in \theta'_1(a_1)$

Since from (CC2) we know that $(m_2+1, H'_{c2}) \triangleright \theta'_2$ therefore from Definition 1.8 we know that $(\theta'_2, m_2, H'_{c2}(a_2)) \in \theta'_2(a_2)$
Therefore from Definition 1.4 we get
$(W', n-n'-1, H'_{c1}(a_1), H'_{c2}(a_2)) \in \lceil \theta'_1(a_1) \rceil^{\mathcal{A}}_V$

D. $H'_{j1}(a_1) \neq H'_1(a_1) \vee H'_{j2}(a_2) = H'_2(a_2)$:
Symmetric case as above

– $\forall i \in \{1,2\}.\forall m.\forall a_i \in dom(W'.\theta_i).(W'.\theta_i, m, H'_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$:

<u>$i = 1$</u>
This means that given some m we need to prove
$\forall a_i \in dom(W'.\theta_i).(W'.\theta_i, m, H'_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$

Like before we apply Theorem 1.22 on $e_{i1}\ \gamma 1$ and $e_{i2}\ \gamma 2$ but this time using $m+1+i$ and $m+1+j$ where i and j are the number of steps in which $e_{i1}\ \gamma 1$ and $e_{i2}\ \gamma 2$ reduces respectively. This will give us

$\exists \theta'_1. W_1.\theta_1 \sqsubseteq \theta'_1 \wedge (m+1, H'_{c2}) \triangleright \theta'_1 \wedge (\theta'_1, m+1, v'_c) \in \lfloor (\tau)\ \sigma \rfloor_V \wedge$
$(\forall a.H_{c2}(a) \neq H'_{c2}(a) \implies \exists \ell'. W_1.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (pc \sqcup \ell)\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_1) \backslash dom(\theta'_1).\theta'_1(a) \searrow (pc \sqcup \ell)\ \sigma)$
and
$\exists \theta'_2. W_1.\theta_2 \sqsubseteq \theta'_2 \wedge (m+1, H'_{c2}) \triangleright \theta'_2 \wedge (\theta'_2, m+1, v'_c) \in \lfloor (\tau)\ \sigma \rfloor_V \wedge$
$(\forall a.H_{c2}(a) \neq H'_{c2}(a) \implies \exists \ell'. W_1.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (pc \sqcup \ell)\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_2) \backslash dom(\theta'_1).\theta'_1(a) \searrow (pc \sqcup \ell)\ \sigma)$

Since we have $(m+1, H'_{c1}) \triangleright \theta'_1$ and $(m+1, H'_{c2}) \triangleright \theta'_2$ therefore we get the desired from Definition 1.8

<u>$i = 2$</u>
Symmetric to $i = 1$

ii. $(W', n-n'-1, v'_1, v'_2) \in \lceil \tau_2\ \sigma \rceil^{\mathcal{A}}_V$:
Let $\tau_2 = \mathsf{A}^{\ell_i}$ Since $\tau_2\ \sigma \searrow \ell\ \sigma$ and since $\ell\ \sigma \not\sqsubseteq \mathcal{A}$ therefore $\ell_i\ \sigma \not\sqsubseteq \mathcal{A}$

From CC1 and CC2 we and Definition 1.4 we get the desired.

(d) Reduction of e_1 happens via Case2 and Reduction of e_2 happens via Case1 :
Symmetric case as before

10. FG-ref:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_i : \tau \qquad \Sigma; \Psi \vdash \tau \searrow pc}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{new}\ e_i : (\mathsf{ref}\ \tau)^{\perp}}$$

To prove: $(W, (\mathsf{new}\ (e_i))\ (\gamma \downarrow_1), (\mathsf{new}\ (e_i))\ (\gamma \downarrow_2)) \in \lceil (\mathsf{ref}\ \tau)^{\perp}\ \sigma \rceil_E^{\mathcal{A}}$

Say $e_1 = (\mathsf{new}\ (e_i))\ (\gamma \downarrow_1)$ and $e_2 = (\mathsf{new}\ (e_i))\ (\gamma \downarrow_2)$

From Definition of $\lceil (\mathsf{ref}\ \tau)^{\perp}\ \sigma \rceil_E^{\mathcal{A}}$ it suffices to prove that

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, e_1) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2') \implies$
$\exists W'. W \sqsubseteq W' \wedge (n - n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v_1', v_2') \in \lceil (\mathsf{ref}\ \tau)^{\perp}\ \sigma \rceil_V^{\mathcal{A}}$

This means that given

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, e_1) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2')$

We are required to prove:

$$\exists W'. W \sqsubseteq W' \wedge (n - n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v_1', v_2') \in \lceil (\mathsf{ref}\ \tau)^{\perp}\ \sigma \rceil_V^{\mathcal{A}} \tag{36}$$

IH1 $(W, n, (e_i)\ (\gamma \downarrow_1), (e_i)\ (\gamma \downarrow_2)) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 1.5 we get

$\forall H_{i1}, H_{i2}.(n, H_{i1}, H_{i2}) \overset{\mathcal{A}}{\triangleright} W \wedge \forall i < n.(H_{i1}, e_i\ (\gamma \downarrow_1)) \Downarrow_i (H_{i1}', v_{i1}') \wedge (H_{i2}, e_i\ (\gamma \downarrow_2)) \Downarrow (H_{i2}', v_{i2}') \implies$
$\exists W_1' \sqsupseteq W.(n - i, H_{i1}', H_{i2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n - i, v_{i1}', v_{i2}') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

Instantiating H_{i1} with H_1 and H_{i2} with H_2 in IH1 and since the $\mathsf{ref}(e_i)$ reduces to value with $\gamma \downarrow_1$ in $n' < n$ steps therefore $\exists i < n' < n.$ s.t $(H_{i1}, e_i\ (\gamma \downarrow_1)) \Downarrow_i (H_{i1}', v_{i1}')$. Similarly since $\mathsf{ref}(e_i)$ reduces with $\gamma \downarrow_2$ therefore we know that $(H_{i2}, e_i\ (\gamma \downarrow_2)) \Downarrow (H_{i2}', v_{i2}')$. Hence we get

$$\exists W_1' \sqsupseteq W.(n - i, H_{i1}', H_{i2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n - i, v_{i1}', v_{i2}') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}} \tag{37}$$

From the evaluation rule of ref we know that $H_1' = H_{i1}' \cup \{a_{n1} \mapsto v_{i1}\}$ and $H_2' = H_{i2}' \cup \{a_{n2} \mapsto v_{i2}\}$

Inorder to prove Equation 36 we instantiate W' with W_n where W_n is

$W_n.\theta_1 = W_1'.\theta_1 \cup \{a_{n1} \mapsto \tau\}$

$W_n.\theta_2 = W_1'.\theta_2 \cup \{a_{n2} \mapsto \tau\}$

$W_n.\hat{\beta} = W_1'.\hat{\beta} \cup \{(a_{n1}, a_{n2})\}$

Also we know that $n' = i + 1$

We are now required to prove

- $W \sqsubseteq W_n$:
  From Equation 37 we know that $W \sqsubseteq W'_1$ and $W'_1 \sqsubseteq W_n$ by construction.
  Therefore from Definition 1.3, $W \sqsubseteq W_n$
- $(n-n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W_n$:
  From Definition 1.9 it suffices to show that
  - $dom(W_n.\theta_1) \subseteq dom(H'_1) \wedge dom(W.\theta_2) \subseteq dom(H'_2)$:
    From Equation 37 and by construction of W_n
  - $(W_n.\hat{\beta}) \subseteq (dom(W_n.\theta_1) \times dom(W_n.\theta_1))$:
    From Equation 37 and by construction of W_n
  - $\forall (a_1, a_2) \in (W_n.\hat{\beta}).\, W_n.\theta_1(a_1) = W_n.\theta_2(a_2) \wedge (W_n, n-n', H'_1(a_1), H'_2(a_2)) \in \lceil W_n.\theta_1(a_1) \rceil_V^{\mathcal{A}}$:
    - $\forall (a_1, a_2) \in (W_n.\hat{\beta}).\, W_n.\theta_1(a_1) = W_n.\theta_2(a_2)$:
      From Equation 37 and by construction of W_n
    - $\forall (a_1, a_2) \in (W_n.\hat{\beta}).(W_n, n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W_n.\theta_1(a_1) \rceil_V^{\mathcal{A}}$:
      From Equation 37 since we know that $(n-i, H'_{i1}, H'_{i2}) \overset{\mathcal{A}}{\triangleright} W'_1$ that means
      $\forall (a_1, a_2) \in (W'_1.\hat{\beta}).(W'_1, n-i-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'_1.\theta_1(a_1) \rceil_V^{\mathcal{A}}$

      Therefore from Lemma 1.17 we get ($n-i-2 = n-n'-1$, since $n' = i+1$)
      $\forall (a_1, a_2) \in (W'_1.\hat{\beta}).(W'_1, n-i-2, H'_1(a_1), H'_2(a_2)) \in \lceil W'_1.\theta_1(a_1) \rceil_V^{\mathcal{A}}$

      Since $W_n.\hat{\beta} = W'_1.\hat{\beta} \cup \{(a_{n1}, a_{n2})\}$ and from Equation 37 we know that $(W'_1, n-i, v'_{i1}, v'_{i2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

      Therefore combining the two we get
      $\forall (a_1, a_2) \in (W_n.\hat{\beta}).(W_n, n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W_n.\theta_1(a_1) \rceil_V^{\mathcal{A}}$
  - $\forall i \in \{1,2\}.\forall a_i \in dom(W_n.\theta_i).\forall m.(W_n, m, H_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$:
    From Equation 37 we have $(n-i, H'_{i1}, H'_{i2}) \overset{\mathcal{A}}{\triangleright} W'_1$ that means from Definition 1.9 we have
    $\forall i \in \{1,2\}.\forall a_i \in dom(W'_1.\theta_i).\forall m.(W_n, m, H_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$

    Also from Equation 37 we know that $(W'_1, n-i, v'_{i1}, v'_{i2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$
    Therefore from Lemma 1.15 and Lemma 1.16 we get
    $\forall m.(W'_1.\theta_1, m, v'_{i1}) \in \lfloor \tau\ \sigma \rfloor_V$
    and
    $\forall m.(W'_1.\theta_2, m, v'_{i2}) \in \lfloor \tau\ \sigma \rfloor_V$

    Combining the two we get
    $\forall i \in \{1,2\}.\forall a_i \in dom(W_n.\theta_i).\forall m.(W_n, m, H_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$
- $(W_n, n-n', v'_1, v'_2) \in \lceil (\mathsf{ref}\ \tau)^{\perp}\ \sigma \rceil_V^{\mathcal{A}}$:
  Here $v'_1 = a_{n1}$ and $v'_2 = a_{n2}$
  Since $(a_{n1}, a_{n2}) \in W_n$ and also $W_n.\theta_1(a_{n1}) = W_n.\theta_1(a_{n1}) = \tau$
  Therefore from Definition 1.4 $(W_n, v'_1, v'_2) \in \lceil (\mathsf{ref}\ \tau)^{\perp}\ \sigma \rceil_V^{\mathcal{A}}$

11. FG-deref:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_i : (\mathsf{ref}\ \tau)^{\ell} \qquad \Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \tau' \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} !e_i : \tau'}$$

To prove: $(W, n, (!(e_i))\ (\gamma \downarrow_1), (!(e_i))\ (\gamma \downarrow_2)) \in \lceil (\tau')\ \sigma \rceil_E^{\mathcal{A}}$

Say $e_1 = (!(e_i))\ (\gamma \downarrow_1)$ and $e_2 = (!(e_i))\ (\gamma \downarrow_2)$

This means from Definition 1.5 we need to prove:

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, !(e_i)(\gamma \downarrow_1)) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, !(e_i)(\gamma \downarrow_2)) \Downarrow (H_2', v_2') \implies$
$\exists W' \sqsupseteq W.(n - n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v_1', v_2') \in \lceil (\tau')\ \sigma \rceil_V^{\mathcal{A}}$
This further means that given

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, !(e_i)(\gamma \downarrow_1)) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, !(e_i)(\gamma \downarrow_2)) \Downarrow (H_2', v_2')$
<u>It suffices to prove</u>

$$\exists W' \sqsupseteq W.(n - n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v_1', v_2') \in \lceil (\tau')\ \sigma \rceil_V^{\mathcal{A}} \tag{38}$$

<u>IH1</u> $(W, n, (e_i)\ (\gamma \downarrow_1), (e_i)\ (\gamma \downarrow_2)) \in \lceil (\mathsf{ref}\ \tau)^\ell\ \sigma \rceil_E^{\mathcal{A}}$
This means from Definition 1.5 we get

$\forall H_{i1}, H_{i2}.(n, H_{i1}, H_{i2}) \overset{\mathcal{A}}{\triangleright} W \wedge \forall i < n.(H_{i1}, e_i\ (\gamma \downarrow_1)) \Downarrow_i (H_1', v_1') \wedge (H_{i2}, e_i\ (\gamma \downarrow_2)) \Downarrow (H_2', v_2') \implies$

$\exists W_1' \sqsupseteq W.(n - i, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n - i, v_1', v_2') \in \lceil (\mathsf{ref}\ \tau)^\ell\ \sigma \rceil_V^{\mathcal{A}}$
Instantiating H_{i1} with H_1 and H_{i2} with H_2 in IH1 and since the $!(e_i)$ reduces to value with both $\gamma \downarrow_1$ in $n' < n$ steps therefore $\exists i < n' < n$ s.t $(H_{i1}, e_i\ (\gamma \downarrow_1)) \Downarrow_i (H_1', v_1')$. Similarly since $!e_i$ reduces to value with $\gamma \downarrow_2$ therefore $(H_{i2}, e_i\ (\gamma \downarrow_2)) \Downarrow (H_2', v_2')$. Hence we get

$$\exists W_1' \sqsupseteq W.(n - i, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n - i, v_1', v_2') \in \lceil (\mathsf{ref}\ \tau)^\ell\ \sigma \rceil_V^{\mathcal{A}} \tag{39}$$

We case analyze on $(W_1', n - i, v_{i1}', v_{i2}') \in \lceil (\mathsf{ref}\ \tau)^\ell\ \sigma \rceil_V^{\mathcal{A}}$ from Equation 39

- Case $\ell\ \sigma \sqsubseteq \mathcal{A}$:
  From Definition 1.4 we know that this would mean that
  $(W_1', n - i, v_{i1}', v_{i2}') \in \lceil (\mathsf{ref}\ \tau)\ \sigma \rceil_V^{\mathcal{A}}$
  This means
  $(W_1', n - i, v_{i1}', v_{i2}') \in \lceil (\mathsf{ref}\ (\tau\ \sigma)) \rceil_V^{\mathcal{A}}$
  Let $v_{i1}' = a_{i1}$ and $v_{i2}' = a_{i2}$

  Again from Definition 1.4 it means that
  $$(a_{i1}, a_{i2}) \in W_1'.\hat{\beta} \wedge W_1'.\theta_1(a_{i1}) = W_1'.\theta_2(a_{i2}) = \tau \tag{D1}$$

  Inorder to prove Equation 38 we instantiate W' with W_1'. Also we know that $n' = i+1$
  - $W_1' \sqsupseteq W$:
    From Equation 39
  - $(n - n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1'$:
    From Equation 39 we know that
    $(n - i, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1'$
    Therefore from Lemma 1.21 we get
    $(n - i - 1, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1'$

– $(W_1', n-n', v_1', v_2') \in \lceil (\tau') \ \sigma \rceil_V^{\mathcal{A}}$:
From the evaluation rule of deref we know that $v_1' = H_1'(a_{i1})$ and $v_1' = H_2'(a_{i2})$

Since from Equation 39 we know that $(n-i, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1'$, therefore from Definition 1.9 we know that
$(W_1', n-i-1, H_1'(a_{i1}), H_2'(a_{i2})) \in \lceil W_1'.\theta_1(a_{i1}) \rceil_V^{\mathcal{A}}$

And from D1 we know that $W_1'.\theta_1(a_{i1}) = W_1'.\theta_2(a_{i2}) = \tau$
Therefore $(W_1', v_1', v_2') \in \lceil (\tau) \ \sigma \rceil_V^{\mathcal{A}}$

Since $\tau \ \sigma <: \tau' \ \sigma$ Therefore from Lemma 1.28, we get
$(W_1', n-i-1, v_1', v_2') \in \lceil (\tau') \ \sigma \rceil_V^{\mathcal{A}}$

- Case $\ell \ \sigma \not\sqsubseteq \mathcal{A}$:
From the evaluation rule of deref we know that $v_{i1}' = a_1$ and $v_{i2}' = a_2$

In this case from Definition 1.4 we know that

$$\forall m_1.(W_1'.\theta_1, m_1, a_1) \in \lfloor (\mathsf{ref}\ \tau) \ \sigma \rfloor_V \tag{40}$$

and

$$\forall m_2.(W_1'.\theta_2, m_2, a_2) \in \lfloor (\mathsf{ref}\ \tau) \ \sigma \rfloor_V \tag{41}$$

Inroder to prove Equation 38 we choose W' as W_1'. And then we need to show:

– $W \sqsubseteq W_1'$:
Directly from Equation 39

– $(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1'$:
From Equation 39 we know that $(n-i, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1'$
Therefore from Lemma 1.21 we get
$(n-i-1, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1'$

– $(W_1', n-n', v_1', v_2') \in \lceil \tau' \ \sigma \rceil_V^{\mathcal{A}}$:
Let $\tau' = \mathsf{A}^{\ell_i}$ Since $\tau' \ \sigma \searrow \ell$ and since $\ell \ \sigma \not\sqsubseteq \mathcal{A}$ therefore $\ell_i \ \sigma \not\sqsubseteq \mathcal{A}$

Therefore from Definition 1.4 it suffices to prove that
$\forall m_1.\ (W_1'.\theta_1, m_1, v_1') \in \lfloor \tau' \ \sigma \rfloor_V$
and
$\forall m_2.\ (W_1'.\theta_2, m_2, v_2') \in \lfloor \tau' \ \sigma \rfloor_V$

This means given m_1 and it suffices to prove:

$$(W_1'.\theta_1, m_1, v_1') \in \lfloor \tau' \ \sigma \rfloor_V \tag{42}$$

Similarly given m_2, it suffices to prove:

$$(W_1'.\theta_2, m_2, v_2') \in \lfloor \tau' \ \sigma \rfloor_V \tag{43}$$

Since from Equation 39 we know that $(n-i, H_1', H_2') \triangleright W_1'$ therefore from Lemma 1.27 we get

$$\forall m_{h1}.(m_{h1}, H_1') \triangleright W_1'.\theta_1 \tag{44}$$

$$\forall m_{h2}.(m_{h2}, H'_2) \triangleright W'_1.\theta_2 \tag{45}$$

Instantiating m_{h1} in Equation 44 with $m_1 + 1$ we get $(m_1, H'_1) \triangleright W'_1.\theta_1$

Therefore from Definition 1.8, we get
$\forall a \in dom(W'_1.\theta_1).(W'_1.\theta_1, m_1, H'_1(a)) \in \lfloor W'_1.\theta_1(a) \rfloor_V$

Instantiating a with a_1 we get $(W'_1.\theta_1, m_1, H'_1(a_1)) \in \lfloor W'_1.\theta_1(a) \rfloor_V$

Since $W'_1.\theta_1(a_{i1}) = \tau$ therefore we get
$(W'_1.\theta_1, m_1, v'_1) \in \lfloor \tau\ \sigma \rfloor_V$
and since $\tau\ \sigma <: \tau'\ \sigma$ therefore from Lemma 1.24 we get
$(W'_1.\theta_1, m_1, v'_1) \in \lfloor \tau'\ \sigma \rfloor_V$

Similarly we also get
$(W'_1.\theta_2, m_2, v'_2) \in \lfloor \tau'\ \sigma \rfloor_V$

Finally from Definition 1.4 we get
$(W'_1, v'_1, v'_2) \in \lceil (\tau')\ \sigma \rceil_V^{\mathcal{A}}$

12. FG-assign:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_{i1} : (\mathsf{ref}\ \tau)^{\ell} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_{i2} : \tau \qquad \Sigma; \Psi \vdash \tau \searrow (pc \sqcup \ell)}{\Sigma; \Psi; \Gamma \vdash_{pc} e_{i1} := e_{i2} : \mathsf{unit}}$$

To prove: $(W, n, (e_{i1} := e_{i2})\ (\gamma \downarrow_1), (e_{i1} := e_{i2})\ (\gamma \downarrow_2)) \in \lceil (\mathsf{unit})\ \sigma \rceil_E^{\mathcal{A}}$
Say $e_1 = (e_{i1} := e_{i2})\ (\gamma \downarrow_1)$ and $e_2 = (e_{i1} := e_{i2})\ (\gamma \downarrow_2)$

This means from Definition 1.5 we need to prove:

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, (e_{i1} := e_{i2})(\gamma \downarrow_1)) \Downarrow_{n'} (H'_1, v'_1) \wedge (H_2, (e_{i1} := e_{i2})(\gamma \downarrow_2$
$)) \Downarrow (H'_2, v'_2) \implies$
$\exists W' \sqsupseteq W.(n - n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v'_1, v'_2) \in \lceil (\mathsf{unit})\ \sigma \rceil_V^{\mathcal{A}}$
This further means that given

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, (e_{i1} := e_{i2})(\gamma \downarrow_1)) \Downarrow_{n'} (H'_1, v'_1) \wedge (H_2, (e_{i1} := e_{i2})(\gamma \downarrow_2$
$)) \Downarrow (H'_2, v'_2)$
<u>It suffices to prove</u>

$$\exists W' \sqsupseteq W.(n - n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v'_1, v'_2) \in \lceil (\mathsf{unit})\ \sigma \rceil_V^{\mathcal{A}} \tag{46}$$

<u>IH1</u> $(W, n, (e_{i1})\ (\gamma \downarrow_1), (e_{i1})\ (\gamma \downarrow_2)) \in \lceil (\mathsf{ref}\ \tau)^{\ell}\ \sigma \rceil_E^{\mathcal{A}}$
This means from Definition 1.5 we get

$\forall H_{i1}, H_{i2}.(n, H_{i1}, H_{i2}) \overset{\mathcal{A}}{\triangleright} W \wedge \forall i < n.(H_{i1}, e_{i1}\ (\gamma \downarrow_1)) \Downarrow_i (H'_{i1}, v'_1) \wedge (H_{i2}, e_{i1}\ (\gamma \downarrow_2)) \Downarrow$
$(H'_{i2}, v'_2) \implies$
$\exists W'_1 \sqsupseteq W.(n - i, H'_{i1}, H'_{i2}) \overset{\mathcal{A}}{\triangleright} W'_1 \wedge (W'_1, n - i, v'_1, v'_2) \in \lceil (\mathsf{ref}\ \tau)^{\ell}\ \sigma \rceil_V^{\mathcal{A}}$
Instantiating H_{i1} with H_1 and H_{i2} with H_2 in IH1 and since the $(e_{i1} := e_{i2})$ reduces to value with both $\gamma \downarrow_1$ in $n' < n$ steps therefore $\exists i < n' < n$ s.t $(H_{i1}, e_{i1}\ (\gamma \downarrow_1)) \Downarrow (H'_{i1}, v'_{i1})$.

Similarly since $(e_{i1} := e_{i2})$ reduces to value with $\gamma \downarrow_2$ therefore we also have $(H_{i2}, e_{i1}\ (\gamma \downarrow_2)) \Downarrow (H'_{i2}, v'_{i2})$. Hence we get

$$\exists W'_1 \sqsupseteq W.(n-i, H'_{i1}, H'_{i2}) \overset{\mathcal{A}}{\triangleright} W'_1 \wedge (W'_1, n-i, v'_{i1}, v'_{i2}) \in \lceil (\mathsf{ref}\ \tau)^{\ell}\ \sigma \rceil^{\mathcal{A}}_{V} \tag{47}$$

<u>IH2</u> $(W, n-i, (e_{i2})\ (\gamma \downarrow_1), (e_{i2})\ (\gamma \downarrow_2)) \in \lceil (\tau)\ \sigma \rceil^{\mathcal{A}}_{E}$
This means from Definition 1.5 we get
$\forall H_{j1}, H_{j2}.(n-i, H_{j1}, H_{j2}) \overset{\mathcal{A}}{\triangleright} W'_1 \wedge \forall j < n-i.(H_{j1}, e_{i2}\ (\gamma \downarrow_1)) \Downarrow_j (H'_{j1}, v'_{j1}) \wedge (H_{j2}, e_{i2}\ (\gamma \downarrow_2)) \Downarrow (H'_{j2}, v'_{j2}) \implies$
$\exists W'_2 \sqsupseteq W'_1.(n-i-j, H'_{j1}, H'_{j2}) \overset{\mathcal{A}}{\triangleright} W'_2 \wedge (W'_2, n-i-j, v'_{j1}, v'_{j2}) \in \lceil (\tau)\ \sigma \rceil^{\mathcal{A}}_{V}$
Instantiating H_{j1} with H'_{i1} and H_{j2} with H'_{i2} in IH2 and since the $(e_{i1} := e_{i2})$ reduces to value with $\gamma \downarrow_1$ in $n' < n$ steps and e_1 reduces $\gamma \downarrow_1$ with $i < n'$ steps therefore $\exists j < (n'-i) < (n-i)$ s.t $(H_{j1}, e_{i2}\ (\gamma \downarrow_1)) \Downarrow (H'_{j1}, v'_{j1})$. Similarly we also have $(H_{j2}, e_{i2}\ (\gamma \downarrow_2)) \Downarrow (H'_{j2}, v'_{j2})$. Hence we get

$$\exists W'_2 \sqsupseteq W'_1.(n-i-j, H'_{j1}, H'_{j2}) \overset{\mathcal{A}}{\triangleright} W'_2 \wedge (W'_2, n-i-j, v'_{j1}, v'_{j2}) \in \lceil (\tau)\ \sigma \rceil^{\mathcal{A}}_{V} \tag{48}$$

We case analyze on $(W'_1, n-i, v'_{i1}, v'_{i2}) \in \lceil (\mathsf{ref}\ \tau)^{\ell}\ \sigma \rceil^{\mathcal{A}}_{V}$ from Equation 47

- Case $\ell\ \sigma \sqsubseteq \mathcal{A}$:
  From Definition 1.4 we know that this would mean that
  $(W'_1, n-i, v'_{i1}, v'_{i2}) \in \lceil (\mathsf{ref}\ \tau)\ \sigma \rceil^{\mathcal{A}}_{V}$
  This means
  $(W'_1, n-i, v'_{i1}, v'_{i2}) \in \lceil (\mathsf{ref}\ (\tau\ \sigma)) \rceil^{\mathcal{A}}_{V}$
  Let $v'_{i1} = a_{i1}$ and $v'_{i2} = a_{i2}$

  Again from Definition 1.4 it means that
  $$(a_{i1}, a_{i2}) \in W'_1.\hat{\beta} \wedge W'_1.\theta_1(a_{i1}) = W'_1.\theta_2(a_{i2}) = \tau\ \sigma \tag{A1}$$

  In order to prove Equation 46 we instantiate W' with W'_2
  - $W'_2 \sqsupseteq W$:
    Since $W'_1 \sqsupseteq W$ from Equation 47 and $W'_2 \sqsupseteq W'_1$ from Equation 48
    Therefore from Definition 1.3 we get $W'_2 \sqsupseteq W$
  - $(n-n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W'_2$:
    From the evaluation rule assign we know that
    $H'_1 = H'_{j1}[a_{i1} \mapsto v'_{j1}]$ and $H'_2 = H'_{j2}[a_{i2} \mapsto v'_{j2}]$

    Inorder to prove $(n-n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W'_2$ we need to show:
    * $dom(W'_2.\theta_1) \subseteq dom(H'_1) \wedge dom(W'_2.\theta_2) \subseteq dom(H'_2)$:
      Directly from Equation 48
    * $W'_2.\hat{\beta} \subseteq (dom(W'_2.\theta_1) \times dom(W'_2.\theta_1))$:
      Directly from Equation 48
    * $\forall (a_1, a_2) \in (W'_2.\hat{\beta}).\ W'_2.\theta_1(a_1) = W'_2.\theta_2(a_2) \wedge$
      $(W'_2, n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W_2.\theta_1(a_1) \rceil^{\mathcal{A}}_{V}$:

(a) $\forall (a_1, a_2) \in (W_2'.\hat{\beta}). W_2'.\theta_1(a_1) = W_2'.\theta_2(a_2)$:
$\forall (a_1, a_2) \in (W_2'.\hat{\beta})$.

i. When $a_1 = a_{i1}$ and $a_2 = a_{i2}$:
From A1 we know that $W_1'.\theta_1(a_1) = W_1'.\theta_2(a_2) = \tau$
and since $W_1' \sqsubseteq W_2'$ therefore from Lemma 1.16 we get $W_2'.\theta_1(a_1) = W_2'.\theta_2(a_2) = \tau$

ii. When $a_1 = a_{i1}$ and $a_2 \neq a_{i2}$: This case cannot arise

iii. When $a_1 \neq a_{i1}$ and $a_2 = a_{i2}$: This case cannot arise

iv. When $a_1 \neq a_{i1}$ and $a_2 \neq a_{i2}$: From Equation 48 and Lemma 1.17

(b) $\forall (a_1, a_2) \in (W_2'.\hat{\beta}).(W_2', n - n', H_1'(a_1), H_2'(a_2)) \in \lceil W_2'.\theta_1(a_1) \rceil_V^{\mathcal{A}}$:
$\forall (a_1, a_2) \in (W_2'.\hat{\beta})$.

i. When $a_1 = a_{i1}$ and $a_2 = a_{i2}$:
Since $H_1'(a_{i1}) = v_{j1}'$ and $H_1'(a_{i2}) = v_{j2}'$
From A1 we know that $W_2'.\theta_1(a_1) = W_2'.\theta_2(a_2) = \tau$
And since from Equation 48 we know that $(W_2', n - i - j, v_{j1}', v_{j2}') \in \lceil (\tau)\ \sigma \rceil_V^{\mathcal{A}}$
Therefore from Lemma 1.17 we get
$(W_2', n - j - i - 1, H_1'(a_1), H_2'(a_2)) \in \lceil W_2.\theta_1(a_1) \rceil_V^{\mathcal{A}}$

ii. When $a_1 = a_{i1}$ and $a_2 \neq a_{i2}$: This case cannot arise

iii. When $a_1 \neq a_{i1}$ and $a_2 = a_{i2}$: This case cannot arise

iv. When $a_1 \neq a_{i1}$ and $a_2 \neq a_{i2}$: From Equation 48 and from Lemma 1.17

* $\forall i \in \{1, 2\}.\forall m.\forall a_i \in dom(W_2'.\theta_i).(W_2'.\theta_i, m, H_i'(a_i)) \in \lfloor W_2'.\theta_i(a_i) \rfloor_V$:
<u>When $i = 1$</u>
Given some m
$\forall a_1 \in dom(W_2'.\theta_1)$.
  · when $a_1 = a_{i1}$:
  From Equation 48 we know that $(W_2', n - i - j, v_{j1}', v_{j2}') \in \lceil (\tau)\ \sigma \rceil_V^{\mathcal{A}}$ thus from Lemma 1.15 we know that
  $\forall m_1.\ (W_2'.\theta_1, m_1, H_1'(a_1)) \in \lfloor W_2'.\theta_1(a_1) \rfloor_V$

  Instantiating with m we get
  $(W_2'.\theta_1, m, H_1'(a_1)) \in \lfloor W_2'.\theta_1(a_1) \rfloor_V$
  · Otherwise:
  From Equation 48 and Lemma 1.27

<u>When $i = 2$</u>
Similar reasoning as with $i = 1$

– $(W_1', n - n', val_1', v_2') \in \lceil (\mathsf{unit})\ \sigma \rceil_V^{\mathcal{A}}$:
From evaluation rule assign we know that $v_1' = v_2' = ()$
Directly from Definition 1.4

- Case $\ell\ \sigma \not\sqsubseteq \mathcal{A}$:
From Definition 1.4 we know that this would mean that

$$\forall m_1.(W_1'.\theta_1, m_1, a_{i1}) \in \lfloor (\mathsf{ref}\ \tau)\ \sigma \rfloor_V \tag{49}$$

$$\forall m_2.(W_1'.\theta_2, m_2, a_{i2}) \in \lfloor (\mathsf{ref}\ \tau)\ \sigma \rfloor_V \tag{50}$$

In order to prove Equation 46 we instantiate W' with W'_2 and then we need to show that:

- $W'_2 \sqsupseteq W$:
  Since $W'_1 \sqsupseteq W$ from Equation 47 and $W'_2 \sqsupseteq W'_1$ from Equation 48
  Therefore from Definition 1.3 we get $W'_2 \sqsupseteq W$
- $(n - n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W'_2$:
  From the evaluation rule assign we know that
  $H'_1 = H'_{j1}[a_{i1} \mapsto v'_{j1}]$ and $H'_2 = H'_{j2}[a_{i2} \mapsto v'_{j2}]$

  In order to prove $(n - n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W'_2$ we need to show:
  * $dom(W'_2.\theta_1) \subseteq dom(H'_1) \wedge dom(W'_2.\theta_2) \subseteq dom(H'_2)$:
    Directly from Equation 48
  * $W'_2.\hat{\beta} \subseteq (dom(W'_2.\theta_1) \times dom(W'_2.\theta_1))$:
    Directly from Equation 48
  * $\forall (a_1, a_2) \in (W'_2.\hat{\beta}). W'_2.\theta_1(a_1) = W'_2.\theta_2(a_2) \wedge (W'_2, n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W_2.\theta_1(a_1) \rceil^{\mathcal{A}}_V$:

  (a) When $(a_{i1}, a_{i2}) \in W'_2.\hat{\beta}$:
  $\forall (a_1, a_2) \in (W'_2.\hat{\beta})$.
   i. When $a_1 = a_{i1}$ and $a_2 = a_{i2}$:
   Instantiating Equation 49 and Equation 50 with $n - n' - 1$ we get $W'_1.\theta_1(a_1) = W'_1.\theta_2(a_2) = \tau$
   and since $W'_1 \sqsubseteq W'_2$ therefore from Definition 1.3 we get $W'_2.\theta_1(a_1) = W'_2.\theta_2(a_2) = \tau$

   From Equation 48 we know that $(W'_2, v'_{j1}, v'_{j2}) \in \lceil (\tau)\ \sigma \rceil^{\mathcal{A}}_V$
   Therefore $(W'_2, H_1(a_{i1})', H_2(a_{i2})') \in \lceil (\tau)\ \sigma \rceil^{\mathcal{A}}_V$
   ii. When $a_1 = a_{i1}$ and $a_2 \neq a_{i2}$: This case cannot arise
   iii. When $a_1 \neq a_{i1}$ and $a_2 = a_{i2}$: This case cannot arise
   iv. When $a_1 \neq a_{i1}$ and $a_2 \neq a_{i2}$: From Equation 48

  (b) When $(a_{i1}, a_{i2}) \notin W'_2.\hat{\beta}$:
  $\forall (a_1, a_2) \in (W'_2.\hat{\beta})$.
   i. When $a_1 = a_{i1}$ and $a_2 = a_{i2}$: This case cannot arise
   ii. When $a_1 = a_{i1}$ and $a_2 \neq a_{i2}$:
   From Equation 48 we know that $(n - i - j, H'_{j1}, H'_{j2}) \overset{\mathcal{A}}{\triangleright} W'_2$ and since $(a_{i1}, a_2) \in W'_2.\hat{\beta}$ therefore from Definition 1.9 we know that

   $$(W'_2.\theta_1(a_{i1}) = W'_2.\theta_2(a_2) \wedge (W'_2, n-i-j-1, H'_{j1}(a_{i1}), H'_{j2}(a_2)) \in \lceil W'_2.\theta_1(a_{i1}) \rceil^{\mathcal{A}}_V) \tag{51}$$

   Instantiating Equation 49 and Equation 50 with $n - i - j - 1$ we get $W'_1.\theta_1(a_{i1}) = \tau\ \sigma$ therefore from monotonicity we also have $W'_2.\theta_1(a_{i1}) = \tau\ \sigma$.
   As a result from Equation 51 we get $W'_2.\theta_2(a_2) = \tau\ \sigma$

   Also since from Equation 51 $(W'_2, n-i-j-1, H'_{j1}(a_{i1}), H'_{j2}(a_2)) \in \lceil \tau\ \sigma \rceil^{\mathcal{A}}_V$ and $\tau\ \sigma \searrow \ell$, $\ell\ \sigma \not\sqsubseteq \mathcal{A}$ therefore from Lemma 1.15 we know that

$$\forall m.(W_2'.\theta_1, m, H_{j1}'(a_{i1})) \in \lfloor \tau\ \sigma \rfloor_V \tag{52}$$

$$\forall m.(W_2'.\theta_2, m, H_{j2}'(a_2)) \in \lfloor \tau\ \sigma \rfloor_V \tag{53}$$

Instantiating m with $n - i - j - 1$ in Equation 52 and Equation 53 to get
$(W_2'.\theta_1, n - i - j - 1, H_{j1}'(a_{i1})) \in \lfloor \tau\ \sigma \rfloor_V$
and
$(W_2'.\theta_2, n - i - j - 1, H_{j2}'(a_2)) \in \lfloor \tau\ \sigma \rfloor_V$
Since $H_1'(a_{i1}) = v_{j1}'$ and $H_2'(a_2) = H_{j2}'(a_2)$
Again from Equation 48 we know that $(W_2', n-i-j, v_{j1}', v_{j2}') \in \lceil (\tau)\ \sigma \rceil_V^{\mathcal{A}}$.
This means from Lemma 1.15 and instantiating it with $n - i - j - 1$ we get

$$(W_2'.\theta_1, n - i - j - 1, v_{j1}') \in \lfloor (\tau)\ \sigma \rfloor_V \tag{54}$$

Therefore from Equation 53 and Equation 54 we have
$(W_2', n - i - j - 1, H_1'(a_{i1}), H_2'(a_2)) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

iii. When $a_1 \neq a_{i1}$ and $a_2 = a_{i2}$:
Symmetric case as (ii)

iv. When $a_1 \neq a_{i1}$ and $a_2 \neq a_{i2}$:
From Equation 48 and Definition 1.9

* $\forall i \in \{1, 2\}.\forall m.\forall a_i \in dom(W_2'.\theta_i).(W_2'.\theta_i, m, H_i'(a_i)) \in \lfloor W_2'.\theta_i(a_i) \rfloor_V$:
<u>When $i = 1$</u>
Given some m
$\forall a_1 \in dom(W_2'.\theta_i)$.
  · when $a_1 = a_{i1}$:
  From Equation 48 we know that $(W_2', v_{j1}', v_{j2}') \in \lceil (\tau)\ \sigma \rceil_V^{\mathcal{A}}$ thus from Lemma 1.15 we know that
  $(W_2'.\theta_1, H_1'(a_1)) \in \lfloor W_2'.\theta_1(a_1) \rfloor_V$
  · Otherwise:
  From Equation 48 and Lemma 1.27

<u>When $i = 2$</u>
Similar reasoning as with $i = 1$

– $(W_1', n - n', v_1', v_2') \in \lceil (\mathsf{unit})\ \sigma \rceil_V^{\mathcal{A}}$:
From evaluation rule assign we know that $v_1' = v_2' = ()$
Directly from Definition 1.4

13. FG-FI:

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash_{\ell_e} e_i : \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} \Lambda e_i : (\forall \alpha.(\ell_e, \tau))^{\perp}}$$

To prove: $(W, n, \Lambda\ e_i\ (\gamma \downarrow_1), \Lambda\ e_i\ (\gamma \downarrow_2)) \in \lceil (\forall \alpha.(\ell_e, \tau))^{\perp}\ \sigma \rceil_E^{\mathcal{A}}$

Say $e_1 = \Lambda\ e_i\ (\gamma \downarrow_1)$ and $e_2 = \Lambda\ e\ (\gamma \downarrow_2)$

From Definition of $\lceil (\forall \alpha.(\ell_e, \tau))^{\perp}\ \sigma \rceil_E^{\mathcal{A}}$ it suffices to prove that

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, e_1) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2') \implies$
$\exists W'. W \sqsubseteq W' \wedge (n - n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v_1', v_2') \in \lceil (\forall \alpha.(\ell_e, \tau))^{\perp}\ \sigma \rceil_V^{\mathcal{A}}$

This means that given $\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, e_1) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2')$

We are required to prove:

$$\exists W'. W \sqsubseteq W' \wedge (n - n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v_1', v_2') \in \lceil (\forall \alpha.(\ell_e, \tau))^{\perp}\ \sigma \rceil_V^{\mathcal{A}} \quad (55)$$

IH1 $(W, n, (e_i)\ (\gamma \downarrow_1), (e_i)\ (\gamma \downarrow_2)) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 1.5 we get

$\forall H_{i1}, H_{i2}.(n, H_{i1}, H_{i2}) \overset{\mathcal{A}}{\triangleright} W \wedge \forall i < n.(H_{i1}, e\ (\gamma \downarrow_1)) \Downarrow_i (H_{i1}', v_{i1}') \wedge (H_{i2}, e\ (\gamma \downarrow_2)) \Downarrow (H_{i2}', v_{i2}') \implies$

$\exists W_1' \sqsupseteq W.(n - i, H_{i1}', H_{i2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n - i, v_{i1}', v_{i2}') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

We know from the evaluation rules that $H_1' = H_1$, $H_2' = H_2$, $v_1' = e_1 = \Lambda e_i\ (\gamma \downarrow_1)$ and $v_2' = e_2 = \Lambda e_i\ (\gamma \downarrow_2)$. We choose $W' = W$ and we know that $n' = 0$ we need to show the following:

- $W \sqsubseteq W$: From Definition 1.3
- $(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W$: Given
- $(W, n, v_1', v_2') \in \lceil (\forall \alpha.(\ell_e, \tau))^{\perp}\ \sigma \rceil_V^{\mathcal{A}}$
  Here $v_1' = \Lambda e_i\ (\gamma \downarrow_1)$ and $v_2' = \Lambda e_i\ (\gamma \downarrow_2)$
  From Definition 1.4 it suffices to prove
  $\forall W' \sqsupseteq W. \forall \ell' \in \mathcal{L}. \forall j < n.$
  $((W', j, e_i(\gamma \downarrow_1), e(\gamma \downarrow_2)) \in \lceil \tau[\ell'/\alpha] \rceil_E^{\mathcal{A}})$
  $\wedge \forall \theta_l \sqsupseteq W.\theta_1, k, \ell'' \in \mathcal{L}.((\theta_l, k, e_i[\ell''/\alpha]) \in \lfloor \tau \rfloor_E^{\ell_e}\ {}^{\sigma})$
  $\wedge \forall \theta_l \sqsupseteq W.\theta_2, k, \ell'' \in \mathcal{L}.((\theta_l, k, e_i[\ell''/\alpha]) \in \lfloor \tau \rfloor_E^{\ell_e}\ {}^{\sigma})$

  This means given some $W' \sqsupseteq W$, $\ell' \in \mathcal{L}$ and $j < n$ we need to show that

  - $\forall W' \sqsupseteq W. \forall \ell' \in \mathcal{L}. \forall j < n.$
    $((W', j, e_i(\gamma \downarrow_1), e(\gamma \downarrow_2)) \in \lceil \tau[\ell'/\alpha] \rceil_E^{\mathcal{A}})$:

    This means that given some $W' \sqsupseteq W, \ell' \in \mathcal{L}, j < n$ we need to prove
    $((W', j, e_i(\gamma \downarrow_1), e(\gamma \downarrow_2)) \in \lceil \tau[\ell'/\alpha] \rceil_E^{\mathcal{A}})$

    From Definition 1.5 it suffices to show that
    $\forall H_{s1}, H_{s2}.(j, H_{s1}, H_{s2}) \overset{\mathcal{A}}{\triangleright} W \wedge \forall m < j.(H_{s1}, e\ (\gamma \downarrow_1)) \Downarrow_m (H_{s1}', v_{s1}') \wedge (H_{s2}, e\ (\gamma \downarrow_2)) \Downarrow (H_{s2}', v_{s2}') \implies$
    $\exists W_1' \sqsupseteq W.(j - m, H_{s1}', H_{s2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', j - m, v_{s1}', v_{s2}') \in \lceil \tau[\ell'/\alpha]\ \sigma \rceil_V^{\mathcal{A}}$

    This means for some H_{s1} and H_{s2} and some $m < j$ we are given $(j, H_{s1}, H_{s2}) \overset{\mathcal{A}}{\triangleright} W \wedge m < j.(H_{s1}, e\ (\gamma \downarrow_1)) \Downarrow_m (H_{s1}', v_{s1}') \wedge (H_{s2}, e\ (\gamma \downarrow_2)) \Downarrow (H_{s2}', v_{s2}')$

    And we need to show that

$\exists W_1' \sqsupseteq W.(j-m, H_{s1}', H_{s2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', j-m, v_{s1}', v_{s2}') \in \lceil \tau[\ell'/\alpha]\ \sigma \rceil_V^{\mathcal{A}}$
We instantiate IH1 with H_{s1}, H_{s2}, m and $\sigma \cup \{\alpha \mapsto \ell'\}$ to obtain
$\exists W_1' \sqsupseteq W.(n-m, H_{i1}', H_{i2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n-m, v_{i1}', v_{i2}') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}} \cup \{\alpha \mapsto \ell'\}$
Since $j < n$ therefore from Lemma 1.21 and Lemma 1.17 we get
$\exists W_1' \sqsupseteq W.(j-m, H_{s1}', H_{s2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', j-m, v_{s1}', v_{s2}') \in \lceil \tau[\ell'/\alpha]\ \sigma \rceil_V^{\mathcal{A}}$

- $\forall \theta_l \sqsupseteq W.\theta_1, k, \ell'' \in \mathcal{L}.((\theta_l, k, e_i[\ell''/\alpha]) \in \lfloor \tau \rfloor_E^{\ell_e\ \sigma})$:
  From Lemma 1.25 we know that $(W'.\theta_1, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$. Therefore, we can apply Theorem 1.22 with $\sigma \cup \{\alpha \mapsto \ell''\}$
  $\forall k.\ (W'.\theta_1, k, e\ \gamma \downarrow_1) \in \lfloor \tau\ (\sigma \cup \{\alpha \mapsto \ell'\}) \rfloor_E^{\ell_e\ (\sigma \cup \{\alpha \mapsto \ell'\})}$
  From Lemma 1.16 we get
  $\forall \theta_l \sqsupseteq W'.\theta_1.\ \forall k.\ (\theta_l, k, e\ \gamma \downarrow_1) \in \lfloor \tau\ (\sigma \cup \{\alpha \mapsto \ell'\}) \rfloor_E^{\ell_e\ (\sigma \cup \{\alpha \mapsto \ell'\})}$
- $\forall \theta_l \sqsupseteq W.\theta_2, k, \ell'' \in \mathcal{L}.((\theta_l, k, e_i[\ell''/\alpha]) \in \lfloor \tau \rfloor_E^{\ell_e\ \sigma})$:
  Similar reasoning as in the previous case

14. FG-FE:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\forall \alpha.(\ell_e, \tau))^{\ell} \qquad \ell'' \in \mathrm{FV}(\Sigma) \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e[\ell''/\alpha] \qquad \Sigma; \Psi \vdash \tau[\ell''/\alpha] \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e\ [] : \tau[\ell''/\alpha]}$$

To prove: $(W, n, (e[])\ (\gamma \downarrow_1), (e[])\ (\gamma \downarrow_2)) \in \lceil (\tau[\ell''/\alpha])\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 1.5 we need to prove:

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, (e[])(\gamma \downarrow_1)) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, (e[])(\gamma \downarrow_2)) \Downarrow (H_2', v_2') \implies$
$\exists W' \sqsupseteq W.(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-n', v_1', v_2') \in \lceil (\tau[\ell''/\alpha])\ \sigma \rceil_V^{\mathcal{A}}$
This further means that given

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, (e[])(\gamma \downarrow_1)) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, (e[])(\gamma \downarrow_2)) \Downarrow (H_2', v_2')$
<u>It suffices to prove</u>

$$\exists W' \sqsupseteq W.(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-n', v_1', v_2') \in \lceil (\tau[\ell''/\alpha])\ \sigma \rceil_V^{\mathcal{A}} \tag{56}$$

<u>IH</u> $(W, n, (e)\ (\gamma \downarrow_1), (e)\ (\gamma \downarrow_2)) \in \lceil (\forall \alpha.(\ell_e, \tau))^{\ell}\ \sigma \rceil_E^{\mathcal{A}}$
This means from Definition 1.5 we get

$\forall H_{i1}, H_{i2}.(n, H_{i1}, H_{i2}) \overset{\mathcal{A}}{\triangleright} W \wedge \forall i < n.(H_{i1}, e\ (\gamma \downarrow_1)) \Downarrow_i (H_{i1}', v_{i1}') \wedge (H_{i2}, e\ (\gamma \downarrow_2)) \Downarrow (H_{i2}', v_{i2}') \implies$

$\exists W_1' \sqsupseteq W.(n-i, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n-i, v_1', v_2') \in \lceil (\forall \alpha.(\ell_e, \tau))^{\ell}\ \sigma \rceil_V^{\mathcal{A}}$
Instantiating H_{i1} with H_1 and H_{i2} with H_2 in IH and since the $(e[])$ reduces to value with $\gamma \downarrow_1$ in $n' < n$ steps therefore $\exists i < n' < n$ s.t $(H_{i1}, e\ (\gamma \downarrow_1)) \Downarrow_i (H_{i1}', v_{i1}')$. Similarly $(e[])$ also reduces to value with $\gamma \downarrow_2$ therefore we also have $(H_{i2}, e\ (\gamma \downarrow_2)) \Downarrow (H_{i2}', v_{i2}')$. Hence we get

$$\exists W_1' \sqsupseteq W.(n-i, H_{i1}', H_{i2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n-i, v_{i1}', v_{i2}') \in \lceil (\forall \alpha.(\ell_e, \tau))^{\ell}\ \sigma \rceil_V^{\mathcal{A}} \tag{57}$$

We case analyze on $(W_1', n-i, v_1', v_2') \in \lceil (\forall \alpha.(\ell_e, \tau))^{\ell}\ \sigma \rceil_V^{\mathcal{A}}$ from Equation 57

- Case $\ell\ \sigma \sqsubseteq \mathcal{A}$:
  In this case from Definition 1.4 we know that
  $(W_1', n-i, v_{i1}', v_{i2}') \in \lceil (\forall \alpha.(\ell_e, \tau))\ \sigma \rceil_V^{\mathcal{A}}$
  Here $v_{i1}' = \Lambda e_{i1}$ and $v_{i2}' = \Lambda e_{i2}$

  This further means that we have
  $\forall W'' \sqsupseteq W_1'.\forall \ell' \in \mathcal{L}.\forall j < n-i.((W'', j, e_{i1}, e_{i2}) \in \lceil \tau[\ell'/\alpha] \rceil_E^{\mathcal{A}})$
  $\wedge \forall \theta_l \sqsupseteq W_1'.\theta_1, j, \ell'' \in \mathcal{L}.((\theta_l, j, e_{i1}) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\ell_e[\ell''/\alpha]\ \sigma})$
  $\wedge \forall \theta_l \sqsupseteq W_1'.\theta_2, j, \ell'' \in \mathcal{L}.((\theta_l, j, e_{i2}) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\ell_e[\ell''/\alpha]\ \sigma})\}$ (E1)

  Instantiating the first conjunct of (E1) with W_1', ℓ'' and $n-i-1$ we get
  $((W_1', n-i-1, e_{i1}, e_{i2}) \in \lceil \tau[\ell'/\alpha]\ \sigma \rceil_E^{\mathcal{A}})$

  Therefore from Definition 1.5 we get
  $\forall H_1, H_2.(n-i-1, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W_1' \wedge \forall k < (n-i-1).(H_1, (e_{i1})(\gamma\downarrow_1)) \Downarrow_k (H_1', v_1') \wedge (H_2, (e_{i2})(\gamma\downarrow_2)) \Downarrow (H_2', v_2') \implies$
  $\exists W''' \sqsupseteq W_1'.((n-i-1)-k, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', (n-i-1)-k, v_1', v_2') \in \lceil (\tau[\ell''/\alpha])\ \sigma \rceil_V^{\mathcal{A}}$

  Instantiating H_1 and H_2 with H_{i1}' and H_{i2}' and since $e[]$ reduces to value with $\gamma\downarrow_1$ in $n' < n$ steps and e with $\gamma\downarrow_1$ reduces in $i < n' < n$ steps. Therefore $\exists k < (n'-i-1)$ steps in which e_{i1} reduces. Also since $e[]$ reduces to value with $\gamma\downarrow_2$ therefore e_{i2} must also reduce. As a result we get
  $\exists W''' \sqsupseteq W_1'.((n-i-1)-k, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', (n-i-1)-k, v_1', v_2') \in \lceil (\tau[\ell''/\alpha])\ \sigma \rceil_V^{\mathcal{A}}$
  Since $n' = i+k+1$ therefore we are done

- Case $\ell\ \sigma \not\sqsubseteq \mathcal{A}$:

  From Equation 56 we know that we need to prove
  $\exists W' \sqsupseteq W.(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-n', v_1', v_2') \in \lceil (\tau[\ell''/\alpha])\ \sigma \rceil_V^{\mathcal{A}}$

  In this case since we know that $\ell\ \sigma \not\sqsubseteq \mathcal{A}$. Let $\tau[\ell''/\alpha]\ \sigma = \mathsf{A}^{\ell_i}$ and since $\tau[\ell''/\alpha]\ \sigma \searrow \ell\ \sigma$ therefore $\ell_i \not\sqsubseteq \mathcal{A}$

  This means in order to prove $\exists W' \sqsupseteq W.(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-n', v_1', v_2') \in \lceil (\tau[\ell''/\alpha])\ \sigma \rceil_V^{\mathcal{A}}$
  From Definition 1.4 it will suffice to prove
  $\exists W' \sqsupseteq W.(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (\forall m_1.(W'.\theta_1, m_1, v_1') \in \lfloor (\tau[\ell''/\alpha])\ \sigma \rfloor_V) \wedge (\forall m_2.(W'.\theta_1, m_2, v_2') \in \lfloor (\tau[\ell''/\alpha])\ \sigma \rfloor_V)$

  This means it suffices to prove
  $(\forall m_1, m_2.\exists W' \sqsupseteq W.(n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W'.\theta_1, m_1, v_1') \in \lfloor (\tau[\ell''/\alpha])\ \sigma \rfloor_V) \wedge ((W'.\theta_1, m_2, v_2') \in \lfloor (\tau[\ell''/\alpha])\ \sigma \rfloor_V)$

This means given m_1 and m_2 it suffices to prove:

$$(\exists W' \sqsupseteq W.(n-n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W' \wedge (W'.\theta_1, m_1, v'_1) \in \lfloor(\tau[\ell''/\alpha])\ \sigma\rfloor_V) \wedge (W'.\theta_1, m_2, v'_2) \in \lfloor(\tau[\ell''/\alpha])\ \sigma \tag{58}$$

In this case from Definition 1.6 we know that

$$\forall m.(W'_1.\theta_1, m, \Lambda e_{h1}) \in \lfloor \forall \alpha.(\ell_e, \tau)\ \sigma \rfloor_V \tag{59}$$

$$\forall m.(W'_1.\theta_2, m, \Lambda e_{h2}) \in \lfloor \forall \alpha.(\ell_e, \tau)\ \sigma \rfloor_V \tag{60}$$

Applying Definition 1.6 on Equation 59 we get
$\forall m.\ \forall \theta'.\theta \sqsubseteq \theta' \wedge \forall j_1 < m.\forall \ell' \in \mathcal{L}.(\theta', j_1, e_{h1}) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\ell_e[\ell'/\alpha]}$ where $\theta = W'_1.\theta_1$

We instantiate m with m_1+2+t_1 where t_1 is the number of steps in which e_{h1} reduces
$\forall \theta'. W'_1.\theta_1 \sqsubseteq \theta' \wedge \forall j_1 < (m_1+2+t_1).\forall \ell' \in \mathcal{L}.(\theta', j_1, e_{h1}) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\ell_e[\ell'/\alpha]}$ (FB-FE1)

Instantiating θ' with $W'_1.\theta_1$, $j1$ with $m_1 + t_1 + 1$ and ℓ' with ℓ''
Therefore we get $(W'_1.\theta_1, m_1 + t_1 + 1, e_{h1}) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E^{\ell_e\ \sigma}$

From Definition 1.7, we get
$\forall H.(m_1 + t_1 + 1, H) \triangleright W'_1.\theta_1 \wedge \forall k_c < (m_1 + t_1 + 1).(H, e_{h1}) \Downarrow_{k_c} (H'_1, v'_1) \implies$
$\exists \theta'_1. W'_1.\theta_1 \sqsubseteq \theta'_1 \wedge ((m_1+t_1+1-k_c), H'_1) \triangleright \theta'_1 \wedge (\theta'_1, (m_1+t_1+1-k_c), v'_1) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'_1(a) \implies \exists \ell'. W'_1.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (\ell_e[\ell''/\alpha]\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_1) \backslash dom(W'_1.\theta_1).\theta'_1(a) \searrow (\ell_e[\ell''/\alpha]\ \sigma))$

Since from Equation 57 we have
$(n - i, H'_{i1}, H'_{i2}) \overset{\mathcal{A}}{\triangleright} W'_1$

Therefore from Lemma 1.27 we get
$\forall m.\ (m, H'_{i1}) \triangleright W'_1.\theta_1$

Instantiating m with $m_1 + 1 + t_1$ we get
$(m_1 + 1 + t_1, H'_{i1}) \triangleright W'_1.\theta_1$

Instantiating H with H'_{j1} from Equation 57 and k_c with t_1, we get
$\exists \theta'_1. W'_1.\theta_1 \sqsubseteq \theta'_1 \wedge ((m_1 + 1), H'_1) \triangleright \theta'_1 \wedge (\theta'_1, (m_1 + 1), v'_1) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'_1(a) \implies \exists \ell'. W'_1.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (\ell_e[\ell''/\alpha]\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_1) \backslash dom(W'_1.\theta_1).\theta'_1(a) \searrow (\ell_e[\ell''/\alpha]\ \sigma))$ (CF1)

Similarly applying Definition 1.6 to Equation 60 we get
$\forall m.\ \forall \theta'.\theta \sqsubseteq \theta' \wedge \forall j_1 < m.\forall \ell' \in \mathcal{L}.(\theta', j_1, e_{h2}[v/x]) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\ell_e[\ell'/\alpha]}$ where $\theta = W'_1.\theta_2$

We instantiate m with m_2+1+t_2 where t_2 is the number of steps in which e_{h2} reduces
$\forall \theta'. W'_1.\theta_2 \sqsubseteq \theta' \wedge \forall j_1 < (m_2+2+t_2).\forall \ell' \in \mathcal{L}.(\theta', j_1, e_{h2}) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\ell_e[\ell'/\alpha]}$ (FB-FE2)

Instantiating θ' with $W'_1.\theta_2$, $j1$ with $m_2 + t_2 + 1$ and ℓ' with ℓ''
Therefore we get $(W'_1.\theta_2, m_2 + t_2 + 1, e_{h2}) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E^{\ell_e[\ell''/\alpha]\ \sigma}$

From Definition 1.7, we get
$\forall H.(m_2 + t_2 + 1, H) \triangleright W_1'.\theta_2 \wedge \forall k_c < (m_2 + t_2 + 1).(H, e_{h2}) \Downarrow_{k_c} (H_2', v_1') \implies$
$\exists \theta_2'. W_1'.\theta_2 \sqsubseteq \theta_2' \wedge ((m_2+t_2+1-k_c), H_2') \triangleright \theta_2' \wedge (\theta_2', (m_2+t_2+1-k_c), v_1') \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H_2'(a) \implies \exists \ell'. W_1'.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e[\ell''/\alpha]\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2') \backslash dom(W_1'.\theta_2).\theta_2'(a) \searrow (\ell_e[\ell''/\alpha]\ \sigma))$

Since from Equation 57 we have
$(n - i, H_{i1}', H_{i2}') \overset{\mathcal{A}}{\triangleright} W_1'$

Therefore from Lemma 1.27 we get
$\forall m.\ (m, H_{i2}') \triangleright W_1'.\theta_2$

Instantiating m with $m_2 + 1 + t_2$ we get
$(m_2 + 1 + t_2, H_{i2}') \triangleright W_1'.\theta_2$

Instantiating H with H_{j2}' from Equation 57 and k_c with t_2, we get
$\exists \theta_2'. W_1'.\theta_2 \sqsubseteq \theta_2' \wedge ((m_2 + 1), H_2') \triangleright \theta_2' \wedge (\theta_2', (m_2 + 1), v_1') \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H_2'(a) \implies \exists \ell'. W_1'.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e[\ell''/\alpha]\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2') \backslash dom(W_1'.\theta_2).\theta_2'(a) \searrow (\ell_e[\ell''/\alpha]\ \sigma))$ (CF2)

In order to prove Equation 56 we choose W' to be $(\theta_1', \theta_2', W_1'.\beta)$. Now we need to show two things:

(a) $(n - n', H_1', H_2') \triangleright W'$:
From Definition 1.9 it suffices to show that
- $dom(W'.\theta_1) \subseteq dom(H_1') \wedge dom(W.\theta_2) \subseteq dom(H_2')$:
From CF1 we know that $(m_1 + 1, H_1') \triangleright \theta_1'$, therefore from Definition 1.8 we get $dom(W'.\theta_1) \subseteq dom(H_1')$
Similarly, from CF2 we know that $(m_2 + 1, H_2') \triangleright \theta_2'$, therefore from Definition 1.8 we get $dom(W'.\theta_2) \subseteq dom(H_2')$
- $(W.\hat{\beta}) \subseteq (dom(W'.\theta_1) \times dom(W'.\theta_1))$:
Since $(n - i, H_{j1}', H_{j2}') \triangleright W_1'$ therefore from Definition 1.9 we know that
$(W_1'.\hat{\beta}) \subseteq (dom(W_1'.\theta_1) \times dom(W_1'.\theta_2))$
From CF1 and CF2 we know that $W_1'.\theta_1 \sqsubseteq \theta_1'$ and $W_1'.\theta_2 \sqsubseteq \theta_2'$ therefore
$(W_1'.\hat{\beta}) \subseteq (dom(\theta_1') \times dom(\theta_2'))$
- $\forall (a_1, a_2) \in (W'.\hat{\beta}). W'.\theta_1(a_1) = W'.\theta_2(a_2) \wedge$
$(W', n - n' - 1, H_1'(a_1), H_2'(a_2)) \in \lceil W'.\theta_1(a_1) \rceil_V^{\mathcal{A}}$:
4 cases arise for each a_1 and a_2
  i. $H_{i1}'(a_1) = H_1'(a_1) \wedge H_{i2}'(a_2) = H_2'(a_2)$:
    * $W'.\theta_1(a_1) = W'.\theta_2(a_2)$:
    We know from Equation 57 that $(n - i, H_{i1}', H_{i2}') \triangleright W_1'$
    Therefore from Definition 1.9 we have
    $\forall (a_1, a_2) \in (W_1'.\hat{\beta}). W_1'.\theta_1(a_1) = W_1'.\theta_2(a_2)$
    Since $W'.\hat{\beta} = W_1'.\hat{\beta}$ by construction therefore
    $\forall (a_1, a_2) \in (W'.\hat{\beta}). W_1'.\theta_1(a_1) = W_1'.\theta_2(a_2)$
    From CF1 and CF2 we know that $W_1'.\theta_1 \sqsubseteq \theta_1'$ and $W_1'.\theta_2 \sqsubseteq \theta_2'$ respectively.
    Therefore from Definition 1.2
    $\forall (a_1, a_2) \in (W'.\hat{\beta}).\theta_1'(a_1) = \theta_2'(a_2)$

* $(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1)\rceil_V^{\mathcal{A}}$:
  From Equation 57 we know that $(n-i, H'_{i1}, H'_{i2}) \overset{\mathcal{A}}{\triangleright} W'_1$
  This means from Definition 1.9 that
  $\forall(a_{i1}, a_{i2}) \in (W'_1.\hat{\beta}). W'_1.\theta_1(a_1) = W'_1.\theta_2(a_2) \wedge (W'_1, n-i-1, H'_{i1}(a_1), H'_{i2}(a_2)) \in \lceil W'_1.\theta_1(a_1)\rceil_V^{\mathcal{A}}$

  Instantiating with a_1 and a_2 and since $W'_1 \sqsubseteq W'$ and $n-n'-1 < n-i-1$ (since $i < n'$) therefore from Lemma 1.17 we get
  $(W', n-n'-1, H'_{i1}(a_1), H'_{i2}(a_2)) \in \lceil W'.\theta_1(a_1)\rceil_V^{\mathcal{A}}$

ii. $H'_{j1}(a_1) \neq H'_1(a_1) \vee H'_{j2}(a_2) \neq H'_2(a_2)$:
* $W'.\theta_1(a_1) = W'.\theta_2(a_2)$:
  Same as in the previous case
* $(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1)\rceil_V^{\mathcal{A}}$:
  From CF1 and CF2 we know that
  $(\forall a.H'_{j1}(a) \neq H'_1(a) \implies \exists \ell'. W'_1.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (\ell_e[\ell''/\alpha]\ \sigma) \sqsubseteq \ell')$
  $(\forall a.H'_{j2}(a) \neq H'_2(a) \implies \exists \ell'. W'_1.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e[\ell''/\alpha]\ \sigma) \sqsubseteq \ell')$
  This means we have
  $\exists \ell'. W'_1.\theta_1(a_1) = \mathsf{A}^{\ell'} \wedge (\ell_e[\ell''/\alpha]\ \sigma) \sqsubseteq \ell'$ and
  $\exists \ell'. W'_1.\theta_2(a_2) = \mathsf{A}^{\ell'} \wedge (\ell_e[\ell''/\alpha]\ \sigma) \sqsubseteq \ell'$

  Since $pc\ \sigma \sqcup \ell\ \sigma \sqsubseteq \ell_e[\ell''/\alpha]\ \sigma$ (given) and $\ell\ \sigma \not\sqsubseteq \mathcal{A}$. Therefore, $\ell_e[\ell''/\alpha]\ \sigma \not\sqsubseteq \mathcal{A}$. And thus, $\ell' \not\sqsubseteq \mathcal{A}$

  Also from CF1 and CF2, $(m_1+1, H'_1) \triangleright \theta'_1$ and $(m_2+1, H'_2) \triangleright \theta'_2$. Therefore from Definition 1.8 we have
  $(\theta'_1, m_1, H'_1(a_1)) \in \lfloor \theta'_1(a_1)\rfloor_V$ and
  $(\theta'_2, m_2, H'_2(a_1)) \in \lfloor \theta'_2(a_2)\rfloor_V$

  Since m_1 and m_2 are arbitrary indices therefore from Definition 1.4 we get
  $(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil \theta'_1(a_1)\rceil_V^{\mathcal{A}}$

iii. $H'_{i1}(a_1) = H'_1(a_1) \vee H'_{i2}(a_2) \neq H'_2(a_2)$:
* $W'.\theta_1(a_1) = W'.\theta_2(a_2)$:
  Same as in the previous case
* $(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1)\rceil_V^{\mathcal{A}}$:
  From CF2 we know that
  $(\forall a.H'_{i2}(a) \neq H'_2(a) \implies \exists \ell'. W'_1.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e[\ell''/\alpha]\ \sigma) \sqsubseteq \ell')$
  This means that a_2 was protected at $\ell_e[\ell''/\alpha]\ \sigma$ in the world before the modification. Since $pc\ \sigma \sqcup \ell\ \sigma \sqsubseteq \ell_e[\ell''/\alpha]\ \sigma$ (given) and $\ell\ \sigma \not\sqsubseteq \mathcal{A}$. Therefore, $\ell_e[\ell''/\alpha]\ \sigma \not\sqsubseteq \mathcal{A}$. And thus, $\ell' \not\sqsubseteq \mathcal{A}$

  Since from Equation 57 we know that $(n-i, H'_{i1}, H'_{i2}) \overset{\mathcal{A}}{\triangleright} W'_1$ that means from Definition 1.9 that $(W'_1, n-i-1, H'_{i1}(a_1), H'_{i2}(a_2)) \in \lceil W'_1.\theta_1(a_1)\rceil_V^{\mathcal{A}}$. Since $(\ell_e[\ell''/\alpha]\ \sigma) \sqsubseteq \ell'$ therefore from Definition 1.4 we know that $H'_{i1}(a_1)$ must also have a label $\not\sqsubseteq \mathcal{A}$

  Therefore
  $\forall m.\ (W'_1.\theta_1, m, H'_{i1}(a_1)) \in W'_1.\theta_1(a_1)$ (F)
  and
  $\forall m.\ (W'_1.\theta_2, m, H'_{i2}(a_2)) \in W'_1.\theta_2(a_1)$ (S)

Instantiating the (F) with m_1 and using Lemma 1.16 we get
$(\theta'_1, m_1, H'_{i1}(a_1)) \in \theta'_1(a_1)$

Since from CF2 we know that $(m_2 + 1, H'_2) \triangleright \theta'_2$ therefore from Definition 1.8 we know that $(\theta'_2, m_2, H'_2(a_2)) \in \theta'_2(a_2)$
Therefore from Definition 1.4 we get
$(W', n - n' - 1, H'_1(a_1), H'_2(a_2)) \in \lceil \theta'_1(a_1) \rceil^{\mathcal{A}}_V$

iv. $H'_{j1}(a_1) \neq H'_1(a_1) \vee H'_{j2}(a_2) = H'_2(a_2)$:
Symmetric case as above

– $\forall i \in \{1, 2\}.\forall m.\forall a_i \in dom(W'.\theta_i).(W'.\theta_i, m, H'_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$

$\underline{i = 1}$
This means that given some m we need to prove
$\forall a_i \in dom(W'.\theta_i).(W'.\theta_i, m, H'_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$

Like before we apply Theorem 1.22 on e_{h1} and e_{h2} but this time $m + 2 + t_1$ and $m + 2 + t_2$ where t_1 and t_2 are the number of steps in which e_{h1} and e_{h2} reduces respectively. This will give us

$\exists\theta'_1. W'_1.\theta_1 \sqsubseteq \theta'_1 \wedge ((m_1 + 1), H'_1) \triangleright \theta'_1 \wedge (\theta'_1, (m_1 + 1), v'_1) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'_1(a) \implies \exists\ell'. W'_1.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (\ell_e[\ell''/\alpha]\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_1)\backslash dom(W'_1.\theta_1).\theta'_1(a) \searrow (\ell_e[\ell''/\alpha]\ \sigma))$
and
$\exists\theta'_2. W'_1.\theta_2 \sqsubseteq \theta'_2 \wedge ((m_2 + 1), H'_2) \triangleright \theta'_2 \wedge (\theta'_2, (m_2 + 1), v'_1) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'_2(a) \implies \exists\ell'. W'_1.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e[\ell''/\alpha]\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_2)\backslash dom(W'_1.\theta_2).\theta'_2(a) \searrow (\ell_e[\ell''/\alpha]\ \sigma))$

Since we have $(m+1, H'_1) \triangleright \theta'_1$ and $(m+1, H'_2) \triangleright \theta'_2$ therefore we get the desired from Definition 1.8

$\underline{i = 2}$
Symmetric to $i = 1$

(b) $(W', n - n' - 1, v'_1, v'_2) \in \lceil \tau[\ell''/\alpha]\ \sigma \rceil^{\mathcal{A}}_V$:
Let $\tau[\ell''/\alpha] = \mathsf{A}^{\ell_i}$ Since $\tau[\ell''/\alpha]\ \sigma \searrow \ell\ \sigma$ and since $\ell\ \sigma \not\sqsubseteq \mathcal{A}$ therefore $\ell_i\ \sigma \not\sqsubseteq \mathcal{A}$

From CF1 and CF2 we and Definition 1.4 we get the desired.

15. FG-CI:

$$\frac{\Sigma; \Psi, c; \Gamma \vdash_{\ell_e} e : \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} \nu\ e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\perp}}$$

To prove: $(W, n, \nu\ e\ (\gamma \downarrow_1), \nu\ e\ (\gamma \downarrow_2)) \in \lceil (c \overset{\ell_e}{\Rightarrow} \tau)^{\perp}\ \sigma \rceil^{\mathcal{A}}_E$

Say $e_1 = \nu\ e\ (\gamma \downarrow_1)$ and $e_2 = \nu\ e\ (\gamma \downarrow_2)$

From Definition of $\lceil (c \overset{\ell_e}{\Rightarrow} \tau)^{\perp}\ \sigma \rceil^{\mathcal{A}}_E$ it suffices to prove that

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, e_1) \Downarrow_{n'} (H'_1, v'_1) \wedge (H_2, e_2) \Downarrow (H'_2, v'_2) \implies$
$\exists W'. W \sqsubseteq W' \wedge (n - n', H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v'_1, v'_2) \in \lceil (c \overset{\ell_e}{\Rightarrow} \tau)^{\perp}\ \sigma \rceil^{\mathcal{A}}_V$

This means that given $\forall H_1, H_2.(n', H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, e_1) \Downarrow_{n'} (H'_1, v'_1) \wedge (H_2, e_2) \Downarrow (H'_2, v'_2)$

We are required to prove:

$$\exists W'. W \sqsubseteq W' \wedge (n-n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-n', v_1', v_2') \in \lceil (c \overset{\ell_e}{\Rightarrow} \tau)^{\perp}\ \sigma \rceil_V^{\mathcal{A}} \tag{61}$$

IH1 $(W, n, (e)\ (\gamma \downarrow_1), (e)\ (\gamma \downarrow_2)) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 1.5 we get

$\forall H_{i1}, H_{i2}.(n, H_{i1}, H_{i2}) \overset{\mathcal{A}}{\triangleright} W \wedge \forall i < n.(H_{i1}, e\,(\gamma \downarrow_1)) \Downarrow_i (H_{i1}', v_{i1}') \wedge (H_{i2}, e\,(\gamma \downarrow_2)) \Downarrow (H_{i2}', v_{i2}') \implies$

$\exists W_1' \sqsupseteq W.(n-i, H_{i1}', H_{i2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n-i, v_{i1}', v_{i2}') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

We know from the evaluation rules that $H_1' = H_1$, $H_2' = H_2$, $v_1' = e_1 = \nu e\ (\gamma \downarrow_1)$ and $v_2' = e_2 = \nu e\ (\gamma \downarrow_2)$. We choose $W' = W$ and we know that $n' = 0$. We need to show the following:

- $W \sqsubseteq W$: From Definition 1.3
- $(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W$: Given
- $(W, n, v_1', v_2') \in \lceil (c \overset{\ell_e}{\Rightarrow} \tau)^{\perp}\ \sigma \rceil_V^{\mathcal{A}}$
  Here $v_1' = \nu e\ (\gamma \downarrow_1)$ and $v_2' = \nu e\ (\gamma \downarrow_2)$
  From Definition 1.4 it suffices to prove
  $\forall W' \sqsupseteq W.\forall j < n.\mathcal{L} \models c\ \sigma \implies (W', j, e\ \gamma \downarrow_1, e\ \gamma \downarrow_2) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}} \wedge$
  $\forall \theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c \implies (\theta_l, e\ \gamma \downarrow_1) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma}) \wedge$
  $\forall \theta_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c \implies (\theta_l, e\ \gamma \downarrow_1) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma}$

  We need to prove:

  - $\forall W' \sqsupseteq W.\forall j < n.\mathcal{L} \models c\ \sigma \implies (W', j, e\ \gamma \downarrow_1, e\ \gamma \downarrow_2) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$:
    This means given some $W' \sqsupseteq W$, $j < n$ and given that $\mathcal{L} \models c\ \sigma$ we need to show that
    $(W', j, e\ \gamma \downarrow_1, e\ \gamma \downarrow_2) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$

    From Definition 1.5 it suffices to show that
    $\forall H_{s1}, H_{s2}.(j, H_{s1}, H_{s2}) \overset{\mathcal{A}}{\triangleright} W \wedge \forall m < j.(H_{s1}, e\ (\gamma \downarrow_1)) \Downarrow_m (H_{s1}', v_{s1}') \wedge (H_{s2}, e\ (\gamma \downarrow_2)) \Downarrow (H_{s2}', v_{s2}') \implies$
    $\exists W_1' \sqsupseteq W.(j-m, H_{s1}', H_{s2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', j-m, v_{s1}', v_{s2}') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

    This means for some H_{s1}, H_{s2}, $m < j$ s.t
    $(H_{s1}, H_{s2}) \overset{\mathcal{A}}{\triangleright} W \wedge (H_{s1}, e\ (\gamma \downarrow_1)) \Downarrow_m (H_{s1}', v_{s1}') \wedge (H_{s2}, e\ (\gamma \downarrow_2)) \Downarrow (H_{s2}', v_{s2}')$

    And we need to show that
    $\exists W_1' \sqsupseteq W.(j-m, H_{s1}', H_{s2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', j-m, v_{s1}', v_{s2}') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$
    We instantiate IH1 with H_{s1}, H_{s2} and m to obtain
    $\exists W_1' \sqsupseteq W.(n-m, H_{s1}', H_{s2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n-m, v_{s1}', v_{s2}') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

    Since $j < n$ therefore from Lemma 1.21 and Lemma 1.17 we get
    $\exists W_1' \sqsupseteq W.(j-m, H_{s1}', H_{s2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', j-m, v_{s1}', v_{s2}') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

- $\forall \theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c \implies (\theta_l, j, e\ \gamma \downarrow_1) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma}$:
  This means given $\theta_l \sqsupseteq W.\theta_1, j, \mathcal{L} \models c$
  We need to prove: $(\theta_l, e\ \gamma \downarrow_1) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma}$
  From Lemma 1.25 we know that $\forall m_1.\ (W'.\theta_1, m_1, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$. Therefore by instantiating m_1 at j we can apply Theorem 1.22 to get
  $(\theta_l, j, e\ \gamma \downarrow_1) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma}$
- $\forall \theta_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c \implies (\theta_l, j, e\ \gamma \downarrow_1) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma}$:
  Symmetric reasoning as in the previous case

16. FG-CE:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (c \overset{\ell_e}{\Rightarrow} \tau)^\ell \qquad \Sigma; \Psi \vdash c \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e \qquad \Sigma; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e \bullet : \tau}$$

To prove: $(W, n, (e\bullet)\ (\gamma \downarrow_1), (e\bullet)\ (\gamma \downarrow_2)) \in \lceil (\tau)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 1.5 we need to prove:

$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, (e\bullet)(\gamma \downarrow_1)) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, (e\bullet)(\gamma \downarrow_2)) \Downarrow (H_2', v_2') \implies$
$\exists W' \sqsupseteq W.(n - n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v_1', v_2') \in \lceil (\tau)\ \sigma \rceil_V^{\mathcal{A}}$
This further means that given
$\forall H_1, H_2.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge \forall n' < n.(H_1, (e\bullet)(\gamma \downarrow_1)) \Downarrow_{n'} (H_1', v_1') \wedge (H_2, (e\bullet)(\gamma \downarrow_2)) \Downarrow (H_2', v_2')$
<u>It suffices to prove</u>

$$\exists W' \sqsupseteq W.(n - n', H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - n', v_1', v_2') \in \lceil (\tau)\ \sigma \rceil_V^{\mathcal{A}} \tag{62}$$

<u>IH</u> $(W, n, (e)\ (\gamma \downarrow_1), (e)\ (\gamma \downarrow_2)) \in \lceil (c \overset{\ell_e}{\Rightarrow} \tau)^\ell\ \sigma \rceil_E^{\mathcal{A}}$
This means from Definition 1.5 we get
$\forall H_{i1}, H_{i2}.(n, H_{i1}, H_{i2}) \overset{\mathcal{A}}{\triangleright} W \wedge \forall i < n.(H_{i1}, e\ (\gamma \downarrow_1)) \Downarrow_i (H_{i1}', v_{i1}') \wedge (H_{i2}, e\ (\gamma \downarrow_2)) \Downarrow (H_{i2}', v_{i2}') \implies$

$\exists W_1' \sqsupseteq W.(n - i, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n - i, v_1', v_2') \in \lceil (c \overset{\ell_e}{\Rightarrow} \tau)^\ell\ \sigma \rceil_V^{\mathcal{A}}$

Instantiating H_{i1} with H_1 and H_{i2} with H_2 in IH and since the $(e\bullet)$ reduces to value with $\gamma \downarrow_1$ in $n' < n$ steps therefore $\exists i < n' < n$ s.t $(H_{i1}, e\ (\gamma \downarrow_1)) \Downarrow_i (H_{i1}', v_{i1}')$. Similarly since $(e\bullet)$ reduces to value with $\gamma \downarrow_2$ therefore also have $(H_{i2}, e\ (\gamma \downarrow_2)) \Downarrow (H_{i2}', v_{i2}')$. Hence we get

$$\exists W_1' \sqsupseteq W.(n - i, H_{i1}', H_{i2}') \overset{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', n - i, v_{i1}', v_{i2}') \in \lceil (c \overset{\ell_e}{\Rightarrow} \tau)^\ell\ \sigma \rceil_V^{\mathcal{A}} \tag{63}$$

We case analyze on $(W_1', n - i, v_1', v_2') \in \lceil (c \overset{\ell_e}{\Rightarrow} \tau)^\ell\ \sigma \rceil_V^{\mathcal{A}}$ from Equation 63

- Case $\ell\ \sigma \sqsubseteq \mathcal{A}$:

  In this case from Definition 1.4 we know that
  $(W_1', n-i, v_{i1}', v_{i2}') \in \lceil (c \stackrel{\ell_e}{\Rightarrow} \tau)^{\ell}\ \sigma \rceil_V^{\mathcal{A}}$
  Here $v_{i1}' = \nu e_{i1}$ and $v_{i2}' = \nu e_{i2}$

  This further means that we have
  $\forall W' \sqsupseteq W. \forall j < n-i. \mathcal{L} \models c\ \sigma \implies ((W', j, e_{i1}, e_{i2}) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}})$
  $\wedge \forall \theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c \implies ((\theta_l, j, e_{i1}) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma})$
  $\wedge \forall \theta_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c \implies ((\theta_l, j, e_{i2}) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma})\}$ (CE1)

  Instantiating the first conjunct of (CE1) with W_1', ℓ'' and $n-i-1$ we get
  $((W_1', n-i-1, e_{i1}, e_{i2}) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}})$

  Therefore from Definition 1.5 we get
  $\forall H_1, H_2.(n-i-1, H_1, H_2) \stackrel{\mathcal{A}}{\triangleright} W_1' \wedge \forall k < (n-i-1).(H_1, (e_{i1})(\gamma\downarrow_1)) \Downarrow_k (H_1', v_1') \wedge (H_2, (e_{i2})(\gamma\downarrow_2)) \Downarrow (H_2', v_2') \implies$
  $\exists W''' \sqsupseteq W_1'.((n-i-1)-k, H_1', H_2') \stackrel{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', (n-i-1)-k, v_1', v_2') \in \lceil (\tau)\ \sigma \rceil_V^{\mathcal{A}}$

  Instantiating H_1 and H_2 with H_{i1}' and H_{i2}' and since $e[]$ reduces to value with $\gamma\downarrow_1$ in $n' < n$ steps and e with $\gamma\downarrow_1$ reduces in $i < n' < n$ steps. Therefore $\exists k < (n'-i-1)$ steps in which e_{i1} reduces. Also since $e[]$ reduces to value with $\gamma\downarrow_2$ therefore e_{i2} must also reduce. As a result we get
  $\exists W''' \sqsupseteq W_1'.((n-i-1)-k, H_1', H_2') \stackrel{\mathcal{A}}{\triangleright} W_1' \wedge (W_1', (n-i-1)-k, v_1', v_2') \in \lceil (\tau[\ell''/\alpha])\ \sigma \rceil_V^{\mathcal{A}}$
  Since $n' = i+k+1$ therefore we are done

- Case $\ell\ \sigma \not\sqsubseteq \mathcal{A}$:

  From Equation 62 we know that we need to prove
  $\exists W' \sqsupseteq W.(n-n', H_1', H_2') \stackrel{\mathcal{A}}{\triangleright} W' \wedge (W', n-n', v_1', v_2') \in \lceil (\tau)\ \sigma \rceil_V^{\mathcal{A}}$

  In this case since we know that $\ell\ \sigma \not\sqsubseteq \mathcal{A}$. Let $\tau\ \sigma = \mathsf{A}^{\ell_i}$ and since $\tau\ \sigma \searrow \ell\ \sigma$ therefore $\ell_i \not\sqsubseteq \mathcal{A}$

  This means in order to prove $\exists W' \sqsupseteq W.(n-n', H_1', H_2') \stackrel{\mathcal{A}}{\triangleright} W' \wedge (W', n-n', v_1', v_2') \in \lceil (\tau)\ \sigma \rceil_V^{\mathcal{A}}$
  From Definition 1.4 it will suffice to prove
  $\exists W' \sqsupseteq W.(n-n', H_1', H_2') \stackrel{\mathcal{A}}{\triangleright} W' \wedge (\forall m_1.(W'.\theta_1, m_1, v_1') \in \lfloor (\tau)\ \sigma \rfloor_V) \wedge (\forall m_2.(W'.\theta_1, m_2, v_2') \in \lfloor (\tau)\ \sigma \rfloor_V)$

  This means it suffices to prove
  $(\forall m_1, m_2. \exists W' \sqsupseteq W.(n-n', H_1', H_2') \stackrel{\mathcal{A}}{\triangleright} W' \wedge (W'.\theta_1, m_1, v_1') \in \lfloor (\tau)\ \sigma \rfloor_V) \wedge ((W'.\theta_1, m_2, v_2') \in \lfloor (\tau)\ \sigma \rfloor_V)$

  This means given m_1 and m_2 it suffices to prove:

  $$(\exists W' \sqsupseteq W.(n-n', H_1', H_2') \stackrel{\mathcal{A}}{\triangleright} W' \wedge (W'.\theta_1, m_1, v_1') \in \lfloor (\tau)\ \sigma \rfloor_V) \wedge (W'.\theta_1, m_2, v_2') \in \lfloor (\tau)\ \sigma \rfloor_V) \tag{64}$$

In this case from Definition 1.6 we know that

$$\forall m.(W_1'.\theta_1, m, \nu e_{h1}) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)\ \sigma \rfloor_V \tag{65}$$

$$\forall m.(W_1'.\theta_2, m, \nu e_{h2}) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)\ \sigma \rfloor_V \tag{66}$$

Applying Definition 1.6 to Equation 65 we get
$\forall m.\ \forall \theta'.\theta \sqsubseteq \theta' \wedge \forall j_1 < m.\mathcal{L} \models c\ \sigma \implies (\theta', j_1, e_{h1}) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma}$ where $\theta = W_1'.\theta_1$

We instantiate m with m_1+2+t_1 where t_1 is the number of steps in which e_{h1} reduces
$\forall \theta'. W_1'.\theta_1 \sqsubseteq \theta' \wedge \forall j_1 < (m_1+2+t_1).\mathcal{L} \models c\ \sigma \implies (\theta', j_1, e_{h1}) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\ell_e[\ell'/\alpha]}$
(FB-CE1)

Instantiating θ' with $W_1'.\theta_1$, $j1$ with m_1+t_1+1 and since we know that $\mathcal{L} \models c\ \sigma$. Therefore we get
$(W_1'.\theta_1, m_1+t_1+1, e_{h1}) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma}$

From Definition 1.7, we get
$\forall H.(m_1+t_1+1, H) \triangleright W_1'.\theta_1 \wedge \forall k_c < (m_1+t_1+1).(H, e_{h1}) \Downarrow_{k_c} (H_1', v_1') \implies$
$\exists \theta_1'. W_1'.\theta_1 \sqsubseteq \theta_1' \wedge ((m_1+t_1+1-k_c), H_1') \triangleright \theta_1' \wedge (\theta_1', (m_1+t_1+1-k_c), v_1') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H_1'(a) \implies \exists \ell'. W_1'.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(W_1'.\theta_1).\theta_1'(a) \searrow (\ell_e\ \sigma))$

Since from Equation 63 we have
$(n-i, H_{i1}', H_{i2}') \overset{\mathcal{A}}{\triangleright} W_1'$

Therefore from Lemma 1.27 we get
$\forall m.\ (m, H_{i1}') \triangleright W_1'.\theta_1$

Instantiating m with m_1+1+t_1 we get
$(m_1+1+t_1, H_{i1}') \triangleright W_1'.\theta_1$

Instantiating H with H_{i1}' from Equation 63 and k_c with t_1, we get
$\exists \theta_1'. W_1'.\theta_1 \sqsubseteq \theta_1' \wedge ((m_1+1), H_1') \triangleright \theta_1' \wedge (\theta_1', (m_1+1), v_1') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H_1'(a) \implies \exists \ell'. W_1'.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(W_1'.\theta_1).\theta_1'(a) \searrow (\ell_e\ \sigma))$ (CCE1)

Similarly applying Definition 1.6 to Equation 66 we get
$\forall m.\ \forall \theta'.\theta \sqsubseteq \theta' \wedge \forall j_1 < m.\forall \ell' \in \mathcal{L}.(\theta', j_1, e_{h2}) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e[\ell'/\alpha]}$ where $\theta = W_1'.\theta_2$

We instantiate m with m_2+2+t_2 where t_2 is the number of steps in which e_{h2} reduces
$\forall \theta'. W_1'.\theta_2 \sqsubseteq \theta' \wedge \forall j_1 < (m_2+2+t_2).\forall \ell' \in \mathcal{L}.(\theta', j_1, e_{h2}) \in \lfloor \tau \rfloor_E^{\ell_e[\ell'/\alpha]}$ (FB-CE2)

Instantiating θ' with $W_1'.\theta_2$, $j1$ with m_2+t_2+1 and ℓ' with ℓ''
Therefore we get $(W_1'.\theta_2, m_2+t_2+1, e_{h2}) \in \lfloor \tau\ \sigma \rfloor_E^{\ell_e\ \sigma}$

From Definition 1.7, we get
$\forall H.(m_2+t_2, H) \triangleright W_1'.\theta_2 \wedge \forall k_c < (m_2+t_2+1).(H, e_{h2}) \Downarrow_{k_c} (H_1', v_1') \implies$
$\exists \theta_2'. W_1'.\theta_2 \sqsubseteq \theta_2' \wedge ((m_2+t_2+1-k_c), H_1') \triangleright \theta_2' \wedge (\theta_2', (m_2+t_2+1-k_c), v_1') \in \lfloor \tau\ \sigma \rfloor_V \wedge$

$(\forall a.H(a) \neq H'_1(a) \implies \exists \ell'. W'_1.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_2)\backslash dom(W'_1.\theta_2).\theta'_2(a) \searrow (\ell_e\ \sigma))$

Since from Equation 63 we have
$(n-i, H'_{i1}, H'_{i2}) \overset{\mathcal{A}}{\triangleright} W'_1$

Therefore from Lemma 1.27 we get
$\forall m.\ (m, H'_{i2}) \triangleright W'_1.\theta_2$

Instantiating m with $m_2 + 1 + t_2$ we get
$(m_2 + 1 + t_2, H'_{i2}) \triangleright W'_1.\theta_2$

Instantiating H with H'_{i2} from Equation 57 and k_c with t_2, we get
$\exists \theta'_2. W'_1.\theta_2 \sqsubseteq \theta'_2 \wedge ((m_2+1), H'_1) \triangleright \theta'_2 \wedge (\theta'_2, (m_2+1), v'_1) \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'_1(a) \implies \exists \ell'. W'_1.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_2)\backslash dom(W'_1.\theta_2).\theta'_2(a) \searrow (\ell_e\ \sigma))$ (CCE2)

In order to prove Equation 62 we choose W' to be $(\theta'_1, \theta'_2, W'_1.\beta)$. Now we need to show two things:

(a) $(n-n', H'_1, H'_2) \triangleright W'$:
From Definition 1.9 it suffices to show that
- $dom(W'.\theta_1) \subseteq dom(H'_1) \wedge dom(W.\theta_2) \subseteq dom(H'_2)$:
From CCE1 we know that $(m_1+1, H'_1) \triangleright \theta'_1$, therefore from Definition 1.8 we get $dom(W'.\theta_1) \subseteq dom(H'_1)$
Similarly, from CCE2 we know that $(m_2+1, H'_2) \triangleright \theta'_2$, therefore from Definition 1.8 we get $dom(W'.\theta_2) \subseteq dom(H'_2)$
- $(W.\hat{\beta}) \subseteq (dom(W'.\theta_1) \times dom(W'.\theta_1))$:
Since $(n-i, H'_{j1}, H'_{j2}) \triangleright W'_1$ therefore from Definition 1.9 we know that
$(W'_1.\hat{\beta}) \subseteq (dom(W'_1.\theta_1) \times dom(W'_1.\theta_2))$

From CCE1 and CCE2 we know that $W'_1.\theta_1 \sqsubseteq \theta'_1$ and $W'_1.\theta_2 \sqsubseteq \theta'_2$ therefore
$(W'_1.\hat{\beta}) \subseteq (dom(\theta'_1) \times dom(\theta'_2))$
- $\forall (a_1, a_2) \in (W'.\hat{\beta}). W'.\theta_1(a_1) = W'.\theta_2(a_2) \wedge$
$(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1) \rceil_V^{\mathcal{A}}$:

4 cases arise for each a_1 and a_2
i. $H'_{i1}(a_1) = H'_1(a_1) \wedge H'_{i2}(a_2) = H'_2(a_2)$:
* $W'.\theta_1(a_1) = W'.\theta_2(a_2)$
We know from Equation 57 that $(n-i, H'_{i1}, H'_{i2}) \triangleright W'_1$

Therefore from Definition 1.9 we have
$\forall (a_1, a_2) \in (W'_1.\hat{\beta}). W'_1.\theta_1(a_1) = W'_1.\theta_2(a_2)$

Since $W'.\hat{\beta} = W'_1.\hat{\beta}$ by construction therefore
$\forall (a_1, a_2) \in (W'.\hat{\beta}). W'_1.\theta_1(a_1) = W'_1.\theta_2(a_2)$

From CCE1 and CCE2 we know that $W'_1.\theta_1 \sqsubseteq \theta'_1$ and $W'_1.\theta_2 \sqsubseteq \theta'_2$ respectively.
Therefore from Definition 1.2
$\forall (a_1, a_2) \in (W'.\hat{\beta}).\theta'_1(a_1) = \theta'_2(a_2)$

* $(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1)\rceil_V^{\mathcal{A}}$:

  From Equation 63 we know that $(n-i, H'_{i1}, H'_{i2}) \overset{\mathcal{A}}{\triangleright} W'_1$

  This means from Definition 1.9 that

  $\forall (a_{i1}, a_{i2}) \in (W'_1.\hat{\beta}). W'_1.\theta_1(a_1) = W'_1.\theta_2(a_2) \wedge (W'_1, n-i-1, H'_{i1}(a_1), H'_{i2}(a_2)) \in \lceil W'_1.\theta_1(a_1)\rceil_V^{\mathcal{A}}$

  Instantiating with a_1 and a_2 and since $W'_1 \sqsubseteq W'$ and $n-n'-1 < n-i-1$ (since $i < n'$) therefore from Lemma 1.17 we get

  $(W', n-n'-1, H'_{i1}(a_1), H'_{i2}(a_2)) \in \lceil W'.\theta_1(a_1)\rceil_V^{\mathcal{A}}$

ii. $H'_{j1}(a_1) \neq H'_1(a_1) \vee H'_{j2}(a_2) \neq H'_2(a_2)$:

* $W'.\theta_1(a_1) = W'.\theta_2(a_2)$

  Same as in the previous case

* $(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1)\rceil_V^{\mathcal{A}}$:

  From CCE1 and CCE2 we know that

  $(\forall a. H'_{j1}(a) \neq H'_1(a) \implies \exists \ell'. W'_1.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell')$

  $(\forall a. H'_{j2}(a) \neq H'_2(a) \implies \exists \ell'. W'_1.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell')$

  This means we have

  $\exists \ell'. W'_1.\theta_1(a_1) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell'$ and

  $\exists \ell'. W'_1.\theta_2(a_2) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell'$

  Since $pc\ \sigma \sqcup \ell\ \sigma \sqsubseteq \ell_e\ \sigma$ (given) and $\ell\ \sigma \not\sqsubseteq \mathcal{A}$. Therefore, $\ell_e\ \sigma \not\sqsubseteq \mathcal{A}$. And thus, $\ell' \not\sqsubseteq \mathcal{A}$

  Also from CCE1 and CCE2, $(m_1+1, H'_1) \triangleright \theta'_1$ and $(m_2+1, H'_2) \triangleright \theta'_2$. Therefore from Definition 1.8 we have

  $(\theta'_1, m_1, H'_1(a_1)) \in \lfloor \theta'_1(a_1)\rfloor_V$ and

  $(\theta'_2, m_2, H'_2(a_1)) \in \lfloor \theta'_2(a_2)\rfloor_V$

  Since m_1 and m_2 are arbitrary indices therefore from Definition 1.4 we get

  $(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil \theta'_1(a_1)\rceil_V^{\mathcal{A}}$

iii. $H'_{i1}(a_1) = H'_1(a_1) \vee H'_{i2}(a_2) \neq H'_2(a_2)$:

* $W'.\theta_1(a_1) = W'.\theta_2(a_2)$

  Same as in the previous case

* $(W', n-n'-1, H'_1(a_1), H'_2(a_2)) \in \lceil W'.\theta_1(a_1)\rceil_V^{\mathcal{A}}$:

  From CCE2 we know that

  $(\forall a. H'_{i2}(a) \neq H'_2(a) \implies \exists \ell'. W'_1.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell')$

  This means that a_2 was protected at $\ell_e\ \sigma$ in the world before the modification. Since $pc\ \sigma \sqcup \ell\ \sigma \sqsubseteq \ell_e\ \sigma$ (given) and $\ell\ \sigma \not\sqsubseteq \mathcal{A}$. Therefore, $\ell_e\ \sigma \not\sqsubseteq \mathcal{A}$. And thus, $\ell' \not\sqsubseteq \mathcal{A}$

  Since from Equation 63 we know that $(n-i, H'_{i1}, H'_{i2}) \overset{\mathcal{A}}{\triangleright} W'_1$ that means from Definition 1.9 that $(W'_1, n-i-1, H'_{i1}(a_1), H'_{i2}(a_2)) \in \lceil W'_1.\theta_1(a_1)\rceil_V^{\mathcal{A}}$. Since $(\ell_e\ \sigma) \sqsubseteq \ell'$ therefore from Definition 1.4 we know that $H'_{i1}(a_1)$ must have a label $\not\sqsubseteq \mathcal{A}$

  Therefore

  $\forall m.\ (W'_1.\theta_1, m, H'_{i1}(a_1)) \in W'_1.\theta_1(a_1)$ (F)

  and

  $\forall m.\ (W'_1.\theta_2, m, H'_{i2}(a_2)) \in W'_1.\theta_2(a_1)$ (S)

Instantiating the (F) with m_1 and using Lemma 1.16 we get
$(\theta_1', m_1, H_{i1}'(a_1)) \in \theta_1'(a_1)$

Since from CCE2 we know that $(m_2 + 1, H_2') \triangleright \theta_2'$ therefore from Definition 1.8 we know that $(\theta_2', m_2, H_2'(a_2)) \in \theta_2'(a_2)$
Therefore from Definition 1.4 we get
$(W', n - n' - 1, H_1'(a_1), H_2'(a_2)) \in \lceil \theta_1'(a_1) \rceil_V^{\mathcal{A}}$

iv. $H_{j1}'(a_1) \neq H_1'(a_1) \vee H_{j2}'(a_2) = H_2'(a_2)$:
Symmetric case as above

– $\forall i \in \{1, 2\}. \forall m. \forall a_i \in dom(W'.\theta_i).(W'.\theta_i, m, H_i'(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$

<u>$i = 1$</u>
This means that given some m we need to prove
$\forall a_i \in dom(W'.\theta_i).(W'.\theta_i, m, H_i'(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$

Like before we apply Theorem 1.22 on e_{h1} and e_{h2} but this time $m + 2 + t_1$ and $m + 2 + t_2$ where t_1 and t_2 are the number of steps in which e_{h1} and e_{h2} reduces respectively. This will give us

$\exists \theta_1'. W_1'.\theta_1 \sqsubseteq \theta_1' \wedge ((m_1 + 1), H_1') \triangleright \theta_1' \wedge (\theta_1', (m_1 + 1), v_1') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a. H(a) \neq H_1'(a) \implies \exists \ell'. W_1'.\theta_1(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(W_1'.\theta_1).\theta_1'(a) \searrow (\ell_e\ \sigma))$
and
$\exists \theta_2'. W_1'.\theta_2 \sqsubseteq \theta_2' \wedge ((m_2 + 1), H_1') \triangleright \theta_2' \wedge (\theta_2', (m_2 + 1), v_1') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a. H(a) \neq H_1'(a) \implies \exists \ell'. W_1'.\theta_2(a) = \mathsf{A}^{\ell'} \wedge (\ell_e\ \sigma) \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2') \backslash dom(W_1'.\theta_2).\theta_2'(a) \searrow (\ell_e\ \sigma))$

Since we have $(m+1, H_1') \triangleright \theta_1'$ and $(m+1, H_2') \triangleright \theta_2'$ therefore we get the desired from Definition 1.8

<u>$i = 2$</u>
Symmetric to $i = 1$

(b) $(W', n - n' - 1, v_1', v_2') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$:
Let $\tau = \mathsf{A}^{\ell_i}$ Since $\tau\ \sigma \searrow \ell\ \sigma$ and since $\ell\ \sigma \not\sqsubseteq \mathcal{A}$ therefore $\ell_i\ \sigma \not\sqsubseteq \mathcal{A}$

From CCE1 and CCE2 we and Definition 1.4 we get the desired.

□

Lemma 1.27 (FG: Binary heap well formedness implies unary heap well formedness)**.** $\forall H_1, H_2, W.$
$(n, H_1, H_2) \triangleright W \implies \forall i \in \{1, 2\}. \forall m.(m, H_i) \triangleright W.\theta_i$

Proof. Directly from Definition 1.9 □

Lemma 1.28 (FG: Subtyping binary)**.** *The following holds:*
$\forall \Sigma, \Psi, \sigma.$

1. $\forall \mathsf{A}, \mathsf{A}'.$

(a) $\Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lceil (\mathsf{A}\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil (\mathsf{A}'\ \sigma) \rceil_V^{\mathcal{A}}$

2. $\forall \tau, \tau'.$

(a) $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lceil (\tau\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil (\tau'\ \sigma) \rceil_V^{\mathcal{A}}$

(b) $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lceil(\tau\ \sigma)\rceil_E^{\mathcal{A}} \subseteq \lceil(\tau'\ \sigma)\rceil_E^{\mathcal{A}}$

Proof. Proof by simultaneous induction on $\mathsf{A} <: \mathsf{A}'$ and $\tau <: \tau'$

Proof of statement 1(a)

We analyse the different cases of A in the last step:

1. FGsub-arrow:

   Given:

$$\frac{\Sigma; \Psi \vdash \tau_1' <: \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2' \qquad \Sigma; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'} \text{FGsub-arrow}$$

   To prove: $\lceil((\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil((\tau_1' \xrightarrow{\ell_e'} \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   IH1: $\lceil(\tau_1'\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau_1\ \sigma)\rceil_V^{\mathcal{A}}$
   IH2: $\lceil(\tau_2\ \sigma)\rceil_E^{\mathcal{A}} \subseteq \lceil(\tau_2'\ \sigma)\rceil_E^{\mathcal{A}}$

   It suffices to prove:

   $\forall (W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil((\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}.\ (W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil((\tau_1' \xrightarrow{\ell_e'} \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   This means that given: $(W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil((\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}$

   And it suffices to prove: $(W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil((\tau_1' \xrightarrow{\ell_e'} \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   From Definition 1.4 we are given:

   $\forall W' \sqsupseteq W, j < n, v_1, v_2.((W', j, v_1, v_2) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}} \implies$
   $(W', j, e_1[v_1/x], e_2[v_2/x]) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}}) \wedge$
   $\forall \theta_l \sqsupseteq W.\theta_1, j, v_c.((\theta_l, j, v_c) \in \lfloor\tau_1\ \sigma\rfloor_V \implies (\theta_l, j, e_1[v_1/x]) \in \lfloor\tau_2\ \sigma\rfloor_E^{\ell_e\ \sigma}) \wedge$
   $\forall \theta_l \sqsupseteq W.\theta_2, j, v_c.((\theta_l, j, v_c) \in \lfloor\tau_1\ \sigma\rfloor_V \implies (\theta_l, j, e_2[v_c/x]) \in \lfloor\tau_2\ \sigma\rfloor_E^{\ell_e\ \sigma})$ (Sub-A1)

   Again from Definition 1.4 we are required to prove:

   $\forall W'' \sqsupseteq W, k < n, v_1', v_2'.((W'', k, v_1', v_2') \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}} \implies (W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2'\ \sigma\rceil_E^{\mathcal{A}}) \wedge$
   $\forall \theta_l' \sqsupseteq W.\theta_1, k, v_c'.((\theta_l', k, v_c') \in \lfloor\tau_1'\ \sigma\rfloor_V \implies (\theta_l', k, e_1[v_c'/x]) \in \lfloor\tau_2'\ \sigma\rfloor_E^{\ell_e'\ \sigma}) \wedge$
   $\forall \theta_l' \sqsupseteq W.\theta_2, k, v_c'.((\theta_l', k, v_c') \in \lfloor\tau_1'\ \sigma\rfloor_V \implies (\theta_l', k, e_2[v_c'/x]) \in \lfloor\tau_2'\ \sigma\rfloor_E^{\ell_e'\ \sigma})$

   This means given some $W'' \sqsupseteq W$, $k < n$ and v_1', v_2' we need to prove:

   (a) $\forall W'' \sqsupseteq W, k < n, v_1', v_2'.((W'', k, v_1', v_2') \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}} \implies (W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2'\ \sigma\rceil_E^{\mathcal{A}})$:
   Given: $W'' \sqsupseteq W$, $k < n$ and v_1', v_2'. We are also given $(W'', k, v_1', v_2') \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}}$
   To prove: $(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2'\ \sigma\rceil_E^{\mathcal{A}}$

   Instantiating the first conjunct of Sub-A1 with W'', k, v_1' and v_2' we get

$$((W'', k, v_1', v_2') \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}} \implies (W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}}) \tag{67}$$

   Since $(W'', k, v_1', v_2') \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}}$ therefore from IH1 we know that $(W'', k, v_1', v_2') \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}}$

   Thus from Equation 67 we get $(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}}$

   Finally using IH2 we get $(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2'\ \sigma\rceil_E^{\mathcal{A}}$

(b) $\forall \theta'_l \sqsupseteq W.\theta_1, k, v'_c.((\theta'_l, k, v'_c) \in \lfloor \tau'_1\ \sigma \rfloor_V \implies (\theta'_l, k, e_1[v'_c/x]) \in \lfloor \tau'_2\ \sigma \rfloor_E^{\ell'_e\ \sigma})$:
Given: $\theta'_l \sqsupseteq W.\theta_1, k, v'_c$. We are also given $(\theta'_l, k, v'_c) \in \lfloor \tau'_1\ \sigma \rfloor_V$
To prove: $(\theta'_l, k, e_1[v'_c/x]) \in \lfloor \tau'_2\ \sigma \rfloor_E^{\ell'_e\ \sigma}$
Since we are given $(\theta'_l, k, v'_c) \in \lfloor \tau'_1\ \sigma \rfloor_V$ and since $\tau'_1\ \sigma <: \tau_1\ \sigma$ therefore from Lemma 1.24 we get

$$(\theta'_l, k, v'_c) \in \lfloor \tau_1\ \sigma \rfloor_V \tag{68}$$

Instantiating the second conjunct of Sub-A1 with θ'_l, k, v'_1 and v'_2 we get

$$((\theta'_l, k, v'_c) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta'_l, e_1[v'_c/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}) \tag{69}$$

Therefore from Equation 68 and 69 we get $(\theta'_l, k, e_1[v'_c/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell_e\ \sigma}$

Since $\tau_2\ \sigma <: \tau'_2\ \sigma$ and $\ell'_e\ \sigma \sqsubseteq \ell_e\ \sigma$ therefore from Lemma 1.24 and 1.23 we get $(\theta'_l, k, e_1[v'_c/x]) \in \lfloor \tau'_2\ \sigma \rfloor_E^{\ell'_e\ \sigma}$

(c) $\forall \theta'_l \sqsupseteq W.\theta_2, k, v'_c.((\theta'_l, k, v'_c) \in \lfloor \tau'_1\ \sigma \rfloor_V \implies (\theta'_l, k, e_2[v'_c/x]) \in \lfloor \tau'_2\ \sigma \rfloor_E^{\ell'_e\ \sigma})$:
Similar reasoning as in the previous case

2. FGsub-prod:

Given:

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau'_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau'_2}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau'_1 \times \tau'_2}\ \text{FGsub-prod}$$

To prove: $\lceil ((\tau_1 \times \tau_2)\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil ((\tau'_1 \times \tau'_2)\ \sigma) \rceil_V^{\mathcal{A}}$

IH1: $\lceil (\tau_1\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil (\tau'_1\ \sigma) \rceil_V^{\mathcal{A}}$
IH2: $\lceil (\tau_2\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil (\tau'_2\ \sigma) \rceil_V^{\mathcal{A}}$
It suffices to prove: $\forall (W, n, (v_1, v_2), (v'_1, v'_2)) \in \lceil ((\tau_1 \times \tau_2)\ \sigma) \rceil_V^{\mathcal{A}}.\ (W, n, (v_1, v_2), (v'_1, v'_2)) \in \lceil ((\tau'_1 \times \tau'_2)\ \sigma) \rceil_V^{\mathcal{A}}$

This means that given: $(W, n, (v_1, v_2), (v'_1, v'_2)) \in \lceil ((\tau_1 \times \tau_2)\ \sigma) \rceil_V^{\mathcal{A}}$
Therefore from Definition 1.4 we are given:

$$(W, n, v_1, v'_1) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \wedge (W, n, v_2, v'_2) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}} \tag{70}$$

And it suffices to prove: $(W, n, (v_1, v_2), (v'_1, v'_2)) \in \lceil ((\tau'_1 \times \tau'_2)\ \sigma) \rceil_V^{\mathcal{A}}$

Again from Definition 1.4, it suffices to prove:
$(W, n, v_1, v'_1) \in \lceil \tau'_1\ \sigma \rceil_V^{\mathcal{A}} \wedge (W, n, v_2, v'_2) \in \lceil \tau'_2\ \sigma \rceil_V^{\mathcal{A}}$

Since from Equation 70 we know that $(W, n, v_1, v'_1) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$ therefore from IH1 we have $(W, n, v_1, v'_1) \in \lceil \tau'_1\ \sigma \rceil_V^{\mathcal{A}}$
Similarly since $(W, n, v_2, v'_2) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$ from Equation 70 therefore from IH2 we have $(W, n, v_2, v'_2) \in \lceil \tau'_2\ \sigma \rceil_V^{\mathcal{A}}$

3. FGsub-sum:

   Given:

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'} \text{ FGsub-sum}$$

   To prove: $\lceil((\tau_1 + \tau_2)\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil((\tau_1' + \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   IH1: $\lceil(\tau_1\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau_1'\ \sigma)\rceil_V^{\mathcal{A}}$
   IH2: $\lceil(\tau_2\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau_2'\ \sigma)\rceil_V^{\mathcal{A}}$
   It suffices to prove: $\forall (W, n, v_{s1}, v_{s2}) \in \lceil((\tau_1 + \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}.\ (W, n, v_{s1}, v_{s2}) \in \lceil((\tau_1' + \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   This means that given: $(W, n, v_{s1}, v_{s2}) \in \lceil((\tau_1 + \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}$
   And it suffices to prove: $(W, n, v_{s1}, v_{s2}) \in \lceil((\tau_1' + \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   2 cases arise

   (a) $v_{s1} = \mathsf{inl}\ v_{i1}$ and $v_{s1} = \mathsf{inl}\ v_{i2}$:
   From Definition 1.4 we are given:

$$(W, n, v_{i1}, v_{i2}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \tag{71}$$

   And we are required to prove that:
   $(W, n, v_{i1}, v_{i2}) \in \lceil \tau_1'\ \sigma \rceil_V^{\mathcal{A}}$
   From Equation 71 and IH1 we know that
   $(W, n, v_{i1}, v_{i2}) \in \lceil \tau_1'\ \sigma \rceil_V^{\mathcal{A}}$

   (b) $v_s = \mathsf{inr}\ v_{i1}$ and $v_{s2} = \mathsf{inr}\ v_{i2}$:
   From Definition 1.4 we are given:

$$(W, n, v_{i1}, v_{i2}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}} \tag{72}$$

   And we are required to prove that:
   $(W, n, v_{i1}, v_{i2}) \in \lceil \tau_2'\ \sigma \rceil_V^{\mathcal{A}}$
   From Equation 72 and IH2 we know that
   $(W, n, v_{i1}, v_{i2}) \in \lceil \tau_2'\ \sigma \rceil_V^{\mathcal{A}}$

4. FGsub-forall:

   Given:

$$\frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2 \qquad \Sigma, \alpha; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash \forall \alpha.(\ell_e, \tau_1) <: \forall \alpha.(\ell_e', \tau_2)} \text{ FGsub-forall}$$

   To prove: $\lceil((\forall \alpha.(\ell_e, \tau_1))\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\forall \alpha.(\ell_e', \tau_2))\ \sigma\rceil_V^{\mathcal{A}}$

   IH1: $\lceil(\tau_1\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau_2\ \sigma)\rceil_V^{\mathcal{A}}$
   IH2: $\lceil(\tau_1\ \sigma)\rceil_E^{\mathcal{A}} \subseteq \lceil(\tau_2\ \sigma)\rceil_E^{\mathcal{A}}$
   It suffices to prove: $\forall (W, n, \Lambda e_1, \Lambda e_2) \in \lceil((\forall \alpha.(\ell_e, \tau_1))\ \sigma)\rceil_V^{\mathcal{A}}.$
   $(W, n, \Lambda e_1, \Lambda e_2) \in \lceil((\forall \alpha.(\ell_e', \tau_2))\ \sigma)\rceil_V^{\mathcal{A}}$

   This means that given: $(W, n, \Lambda e_1, \Lambda e_2) \in \lceil((\forall \alpha.(\ell_e, \tau_1))\ \sigma)\rceil_V^{\mathcal{A}}$

Therefore from Definition 1.4 we are given:
$\forall W' \sqsupseteq W, n' < n, \ell' \in \mathcal{L}.((W', n', e_1, e_2) \in \lceil \tau_1[\ell'/\alpha]\ \sigma \rceil_E^{\mathcal{A}}) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, j, \ell' \in \mathcal{L}.((\theta_l, j, e_1) \in \lfloor \tau_1[\ell'/\alpha] \rfloor_E^{\ell_e[\ell'/\alpha]}) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, j, \ell' \in \mathcal{L}.((\theta_l, j, e_2) \in \lfloor \tau_1[\ell''/\alpha] \rfloor_E^{\ell_e[\ell'/\alpha]})$ (Sub-F1)
And it suffices to prove: $(W, n, \Lambda e_1, \Lambda e_2) \in \lceil ((\forall \alpha.(\ell'_e, \tau_2))\ \sigma) \rceil_V^{\mathcal{A}}$

Again from Definition 1.4, it suffices to prove:
$\forall W'' \sqsupseteq W, n'' < n, \ell'' \in \mathcal{L}.((W'', n'', e_1, e_2) \in \lceil \tau_2[\ell''/\alpha]\ \sigma \rceil_E^{\mathcal{A}}) \wedge$
$\forall \theta'_l \sqsupseteq W.\theta_1, k, \ell'' \in \mathcal{L}.((\theta'_l, k, e_1) \in \lfloor \tau_2[\ell''/\alpha] \rfloor_E^{\ell'_e[\ell''/\alpha]}) \wedge$
$\forall \theta'_l \sqsupseteq W.\theta_2, k, \ell'' \in \mathcal{L}.((\theta'_l, k, e_2) \in \lfloor \tau_2[\ell''/\alpha] \rfloor_E^{\ell'_e[\ell''/\alpha]})$

This means we are required to show:

(a) $\forall W'' \sqsupseteq W, n'' < n, \ell' \in \mathcal{L}.((W'', n', e_1, e_2) \in \lceil \tau_2[\ell'/\alpha]\ \sigma \rceil_E^{\mathcal{A}})$:
By instantiating the first conjunct of Sub-F1 with W'', n'' and ℓ'' we know that the following holds
$((W'', n'', e_1, e_2) \in \lceil \tau_1[\ell''/\alpha]\ \sigma \rceil_E^{\mathcal{A}})$

Therefore from IH1 instantiated at $\sigma \cup \{\alpha \mapsto \ell''\}$
$((W'', n'', e_1, e_2) \in \lceil \tau_2[\ell''/\alpha]\ \sigma \rceil_E^{\mathcal{A}})$

(b) $\forall \theta'_l \sqsupseteq W.\theta_1, k, \ell'' \in \mathcal{L}.((\theta'_l, k, e_1) \in \lfloor \tau_2[\ell''/\alpha] \rfloor_E^{\ell'_e[\ell''/\alpha]})$:
By instantiating the second conjunct of Sub-F1 with θ'_l and ℓ'' we know that the following holds
$((\theta'_l, k, e_1) \in \lfloor \tau_1[\ell''/\alpha]\ \sigma \rfloor_E^{\ell_e[\ell''/\alpha]\ \sigma})$

Since $\tau_1\ \sigma <: \tau_2\ \sigma$ and $\ell'_e\ \sigma \sqsubseteq \ell_e\ \sigma$ therefore from Lemma 1.24 and Lemma 1.23 we know that
$((\theta'_l, k, e1) \in \lfloor \tau_2[\ell''/\alpha]\ \sigma \rfloor_E^{\ell'_e[\ell''/\alpha]\ \sigma})$

(c) $\forall \theta'_l \sqsupseteq W.\theta_2, k, \ell'' \in \mathcal{L}.((\theta'_l, k, e_2) \in \lfloor \tau_2[\ell''/\alpha] \rfloor_E^{\ell'_e[\ell''/\alpha]})$:
Similar reasoning as in the previous case

5. FGsub-constraint:

Given:

$$\frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi, c_2 \vdash \tau_1 <: \tau_2 \qquad \Sigma; \Psi \vdash \ell'_e \sqsubseteq \ell_e}{\Sigma; \Psi \vdash c_1 \overset{\ell_e}{\Rightarrow} \tau_1 <: c_2 \overset{\ell'_e}{\Rightarrow} \tau_2} \text{ FGsub-constraint}$$

To prove: $\lceil ((c_1 \overset{\ell_e}{\Rightarrow} \tau_1)\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil ((c_2 \overset{\ell'_e}{\Rightarrow} \tau_2))\ \sigma \rceil_V^{\mathcal{A}}$

IH: $\lceil (\tau_1\ \sigma) \rceil_E^{\mathcal{A}} \subseteq \lceil (\tau_2\ \sigma) \rceil_E^{\mathcal{A}}$

It suffices to prove: $\forall (W, n, \nu e_1, \nu e_2) \in \lceil ((c_1 \overset{\ell_e}{\Rightarrow} \tau_1)\ \sigma) \rceil_V^{\mathcal{A}}.\ (W, n, \nu e_1, \nu e_2) \in \lceil ((c_2 \overset{\ell'_e}{\Rightarrow} \tau_2)\ \sigma) \rceil_V^{\mathcal{A}}$

This means that given: $(W, n, \nu e_1, \nu e_2) \in \lceil ((c_1 \overset{\ell_e}{\Rightarrow} \tau_1)\ \sigma) \rceil_V^{\mathcal{A}}$
Therefore from Definition 1.4 we are given:

$\forall W' \sqsupseteq W, n' < n.\mathcal{L} \models c_1\ \sigma \implies (W', n', e_1, e_2) \in \lceil \tau_1\ \sigma \rceil_E^{\mathcal{A}} \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, k.\mathcal{L} \models c_1 \implies (\theta_l, k, e_1) \in \lfloor \tau_1\ \sigma \rfloor_E^{\ell_e\ \sigma} \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, k.\mathcal{L} \models c_1 \implies (\theta_l, k, e_2) \in \lfloor \tau_1\ \sigma \rfloor_E^{\ell_e\ \sigma}$ (Sub-C1)

And it suffices to prove: $(W, n, \nu e_1, \nu e_2) \in \lceil ((c_2 \overset{\ell'_e}{\Rightarrow} \tau_2)\ \sigma) \rceil_V^{\mathcal{A}}$

Again from Definition 1.4, it suffices to prove:
$\forall W'' \sqsupseteq W, n'' < n.\mathcal{L} \models c_2\ \sigma \implies (W'', n'', e_1, e_2) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}} \wedge$
$\forall \theta'_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c_2 \implies (\theta'_l, j, e_1) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell'_e\ \sigma} \wedge$
$\forall \theta'_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c_2 \implies (\theta'_l, j, e_2) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell'_e\ \sigma}$

This means that we are required to show the following:

(a) $\forall W'' \sqsupseteq W, n'' < n.\mathcal{L} \models c_2\ \sigma \implies (W'', n'', e_1, e_2) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$:
We are given $W'' \sqsupseteq W, n'' < n$ also we know that $\mathcal{L} \models c_2\ \sigma$ and $c_2\ \sigma \implies c_1\ \sigma$ therefore we also know that $\mathcal{L} \models c_1\ \sigma$
Hence by instantiating the first conjunct of Sub-C1 with W'' and n'' we know that the following holds
$(W'', n'', e_1, e_2) \in \lceil \tau_1\ \sigma \rceil_E^{\mathcal{A}}$
Therefore from IH we get $(W'', n'', e_1, e_2) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$

(b) $\forall \theta'_l \sqsupseteq W.\theta_1, k.\mathcal{L} \models c_2 \implies (\theta'_l, k, e_1) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell'_e\ \sigma}$:
We are given some $\theta'_l \sqsupseteq W.\theta_1, k$, also we know that $\mathcal{L} \models c_2\ \sigma$ and $c_2\ \sigma \implies c_1\ \sigma$ therefore we also know that $\mathcal{L} \models c_1\ \sigma$
Hence by instantiating the second conjunct of Sub-C1 with θ'_l we know that the following holds
$(\theta'_l, k, e_1) \in \lfloor \tau_1\ \sigma \rfloor_E^{\ell_e\ \sigma}$
Since $\tau_1\ \sigma <: \tau_2\ \sigma$ and $\ell'_e\ \sigma \sqsubseteq \ell_e\ \sigma$ therefore from Lemma 1.23 and Lemma 1.24 we get
$(\theta'_l, k, e_1) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell'_e\ \sigma}$

(c) $\forall \theta'_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c_2 \implies (\theta'_l, j, e_2) \in \lfloor \tau_2\ \sigma \rfloor_E^{\ell'_e\ \sigma}$:
Similar reasoning as in the previous case

6. FGsub-ref:

Given:

$$\frac{}{\Sigma; \Psi \vdash \mathsf{ref}\ \tau <: \mathsf{ref}\ \tau}\ \text{FGsub-ref}$$

To prove: $\lceil ((\mathsf{ref}\ \tau)\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil ((\mathsf{ref}\ \tau)\ \sigma) \rceil_V^{\mathcal{A}}$

Directly from Definition 1.4

7. FGsub-base:

Given:

$$\frac{}{\Sigma; \Psi \vdash \mathsf{b} <: \mathsf{b}}\ \text{FGsub-base}$$

To prove: $\lceil ((\mathsf{b})\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil ((\mathsf{b})\ \sigma) \rceil_V^{\mathcal{A}}$

Directly from Definition 1.4

8. FGsub-unit:

   Given:

$$\frac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}} \text{FGsub-unit}$$

   To prove: $\lceil ((\mathsf{unit})\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil ((\mathsf{unit})\ \sigma) \rceil_V^{\mathcal{A}}$

   Directly from Definition 1.4

Proof of statement 2(a)
Given:

$$\frac{\Sigma; \Psi \vdash \ell \sqsubseteq \ell' \qquad \Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}'}{\Sigma; \Psi \vdash \mathsf{A}^{\ell} <: \mathsf{A}'^{\ell'}} \text{FGsub-label}$$

To prove: $\lceil ((\mathsf{A}^{\ell})\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil ((\mathsf{A}'^{\ell'}))\ \sigma \rceil_V^{\mathcal{A}}$
2 cases arise

1. $\ell\ \sigma \sqsubseteq \ell'\ \sigma$:

   From Definition 1.4 it suffices to prove: $\lceil ((\mathsf{A})\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil ((\mathsf{A}'))\ \sigma \rceil_V^{\mathcal{A}}$

   This we get directly from IH (Statement (1))

2. $\ell\ \sigma \not\sqsubseteq \ell'\ \sigma$:

   We need to prove that
   $\forall (W, n, v_1, v_2) \in \lceil \mathsf{A}\ \sigma \rceil_V^{\mathcal{A}}.(W, n, v_1, v_2) \in \lceil \mathsf{A}'\ \sigma \rceil_V^{\mathcal{A}}$

   From Definition 1.4 it suffices to prove:
   $\forall i \in \{1,2\}.\forall m.(W(n).\theta_i, m, v_i) \in \lfloor \mathsf{A}\ \sigma \rfloor_V.\ (W(n).\theta_i, m, v_i) \in \lfloor \mathsf{A} \rfloor_V \in \lfloor \mathsf{A}'\ \sigma \rfloor_V$

   Since $\mathsf{A}\ \sigma <: \mathsf{A}'\ \sigma$ therefore from Lemma 1.24 we get the desired

Proof of statement 2(b)
Given: $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma$
To prove: $\lceil (\tau\ \sigma) \rceil_E^{\mathcal{A}} \subseteq \lceil (\tau'\ \sigma) \rceil_E^{\mathcal{A}}$

This means we need to prove that
$\forall (W, n, e_1, e_2) \in \lceil (\tau\ \sigma) \rceil_E^{\mathcal{A}}.\ (W, n, e_1, e_2) \in \lceil (\tau'\ \sigma) \rceil_E^{\mathcal{A}}$

This means given $\forall (W, n, e_1, e_2) \in \lceil (\tau\ \sigma) \rceil_E^{\mathcal{A}}$
It suffices to prove that $(W, n, e_1, e_2) \in \lceil (\tau'\ \sigma) \rceil_E^{\mathcal{A}}$

From Definition 1.5 we know we are given:
$\forall H_1, H_2, j < n.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge (H_1, e_1) \Downarrow_j (H_1', v_1') \wedge (H_2, e_2) \Downarrow (H_2', v_2') \implies$
$\exists W' \sqsupseteq W.(n - j, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n - j, v_1', v_2') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$ (Sub-exp1)

And we need prove that
$\forall H_{21}, H_{22}, k < n.(n, H_{21}, H_{22}) \overset{\mathcal{A}}{\triangleright} W \wedge (H_{21}, e_1) \Downarrow_k (H_{21}', v_{21}') \wedge (H_{22}, e_2) \Downarrow (H_{22}', v_{22}') \implies$
$\exists W'' \sqsupseteq W.(n - k, H_{21}', H_{22}') \overset{\mathcal{A}}{\triangleright} W'' \wedge (W'', n - k, v_{21}', v_{22}') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

This means that we are given some H_{21}, H_{22} and $k < n$ such that $(n, H_{21}, H_{22}) \overset{\mathcal{A}}{\triangleright} W \wedge (H_{21}, e_1) \Downarrow_k (H_{21}', v_{21}') \wedge (H_{22}, e_2) \Downarrow (H_{22}', v_{22}')$

It suffices to prove:

$$\exists W'' \sqsupseteq W.(n-k, H'_{21}, H'_{22}) \overset{\mathcal{A}}{\triangleright} W'' \wedge (W'', n-k, v'_{21}, v'_{22}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}} \tag{73}$$

Instantiating (Sub-exp1) with H_{21}, H_{22} and k we get

$$\exists W' \sqsupseteq W.(n-k, H'_{21}, H'_{22}) \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-k, v'_{21}, v'_{22}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}} \tag{74}$$

We choose W'' in Equation 73 as W' from Equation 74 and we are done

□

Theorem 1.29 (FG: NI)**.** *Say* bool = (unit + unit)
$\forall v_1, v_2, e, \tau, n_1.$
$\emptyset; \emptyset; \emptyset \vdash_\perp v_1 : \mathsf{bool}^\top \wedge \emptyset; \emptyset; \emptyset \vdash_\perp v_2 : \mathsf{bool}^\top$
$\emptyset; \emptyset; x : \mathsf{bool}^\top \vdash_\perp e : \mathsf{bool}^\perp \wedge$
$(\emptyset, e[v_1/x]) \Downarrow_{n_1} (-, v'_1) \wedge (\emptyset, e[v_2/x]) \Downarrow_{-} (-, v'_2) \implies$
$v'_1 = v'_2$

Proof. Given some
$\emptyset; \emptyset; \emptyset \vdash_\perp v_1 : \mathsf{bool}^\top \wedge \emptyset; \emptyset; \emptyset \vdash_\perp v_2 : \mathsf{bool}^\top$
$\emptyset; \emptyset; x : \mathsf{bool}^\top \vdash_\perp e : \mathsf{bool}^\perp \wedge$
$(\emptyset, e[v_1/x]) \Downarrow_{n_1} (-, v'_1) \wedge (\emptyset, e[v_2/x]) \Downarrow (-, v'_2)$

<u>We need to prove</u>
$v'_1 = v'_2$

From Theorem 1.26 we have
$\forall n.\ (\emptyset, n, v_1, v_2) \in \lceil \mathsf{bool}^\top \rceil_E^\perp$
Therefore from Theorem 1.26 and from Definition 1.14 we have
$\forall n.\ (\emptyset, n, e[v_1/x], e[v_1/x]) \in \lceil \mathsf{bool}^\perp \rceil_E^\perp$

Therefore from Definition 1.5 we know that
$\forall n.\big(\forall H_1, H_2, j < n.(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W \wedge (H_1, e_1) \Downarrow_j (H'_1, v'_1) \wedge (H_2, e_2) \Downarrow (H'_2, v'_2) \implies \exists W' \sqsupseteq W.(n-j, H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W' \wedge (W', n-j, v'_1, v'_2) \in \lceil (\mathsf{unit}+\mathsf{unit})^\perp \rceil_V^{\mathcal{A}}\big)$
Instantiating with $n_1 + 1$ and then with $\emptyset, \emptyset, n_1$ we get
$\exists W' \sqsupseteq W.(1, H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W' \wedge (W', 1, v'_1, v'_2) \in \lceil (\mathsf{unit}+\mathsf{unit})^\perp \rceil_V^{\mathcal{A}}$
Since we have $(W', 1, v'_1, v'_2) \in \lceil (\mathsf{unit}+\mathsf{unit})^\perp \rceil_V^{\mathcal{A}}$ therefore from Definition 1.4 we get $v'_1 = v'_2$
□

2 Coarse-grained IFC enforcement (SLIO*)

2.1 SLIO* type system

2.2 SLIO* semantics

Judgement: $e \Downarrow_i v$ and $(H, e) \Downarrow_i^f (H', v)$

Syntax, types, constraints:

Expressions	e	$::=$	$x \mid \lambda x.e \mid e\ e \mid (e,e) \mid \mathsf{fst}(e) \mid \mathsf{snd}(e) \mid \mathsf{inl}(e) \mid \mathsf{inr}(e) \mid \mathsf{case}(e, x.e, y.e) \mid \mathsf{new}\ e \mid !e \mid e := e \mid () \mid \Lambda e \mid e\ [] \mid \nu\ e \mid e\ \bullet \mid \mathsf{Lb}(e) \mid \mathsf{unlabel}(e) \mid \mathsf{toLabeled}(e) \mid \mathsf{ret}(e) \mid \mathsf{bind}(e, x.e)$
Labels	ℓ	$::=$	$l \mid \alpha \mid \ell \sqcup \ell \mid \ell \sqcap \ell$
Types	τ	$::=$	$\mathsf{b} \mid \tau \to \tau \mid \tau \times \tau \mid \tau + \tau \mid \mathsf{ref}\ \ell\ \tau \mid \mathsf{unit} \mid \forall\alpha.\tau \mid c \Rightarrow \tau \mid \mathsf{Labeled}\ \ell\ \tau \mid \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau$
Constraints	c	$::=$	$\ell \sqsubseteq \ell \mid (c,c)$

Type system: $\boxed{\Sigma; \Psi; \Gamma \vdash e : \tau}$

(All rules of the simply typed lambda-calculus pertaining to the types $\mathsf{b}, \tau \to \tau, \tau \times \tau, \tau + \tau, \mathsf{unit}$ are included.)

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{Lb}(e) : \mathsf{Labeled}\ \ell\ \tau}\ \text{SLIO}^*\text{-label}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{Labeled}\ \ell\ \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{unlabel}(e) : \mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau}\ \text{SLIO}^*\text{-unlabel}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{toLabeled}(e) : \mathbb{SLIO}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau)}\ \text{SLIO}^*\text{-toLabeled}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{ret}(e) : \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau}\ \text{SLIO}^*\text{-ret}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \mathbb{SLIO}\ \ell_i\ \ell\ \tau \qquad \Sigma; \Psi; \Gamma, x : \tau \vdash e_2 : \mathbb{SLIO}\ \ell\ \ell_o\ \tau'}{\Sigma; \Psi; \Gamma \vdash \mathsf{bind}(e_1, x.e_2) : \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau'}\ \text{SLIO}^*\text{-bind}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau' \qquad \Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi; \Gamma \vdash e : \tau}\ \text{SLIO}^*\text{-sub}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{Labeled}\ \ell'\ \tau \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash \mathsf{new}\ e : \mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau)}\ \text{SLIO}^*\text{-ref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{ref}\ \ell\ \tau}{\Sigma; \Psi; \Gamma \vdash !e : \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)}\ \text{SLIO}^*\text{-deref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \mathsf{ref}\ \ell'\ \tau \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \mathsf{Labeled}\ \ell'\ \tau \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash e_1 := e_2 : \mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit}}\ \text{SLIO}^*\text{-assign}$$

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash e : \tau}{\Sigma; \Gamma \vdash \Lambda e : \forall\alpha.\tau}\ \text{SLIO}^*\text{-FI} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : \forall\alpha.\tau \qquad \text{FV}(\ell) \in \Sigma}{\Sigma; \Psi; \Gamma \vdash e\ [] : \tau[\ell/\alpha]}\ \text{SLIO}^*\text{-FE}$$

$$\frac{\Sigma; \Psi, c; \Gamma \vdash e : \tau}{\Sigma; \Gamma \vdash \nu\ e : c \Rightarrow \tau}\ \text{SLIO}^*\text{-CI} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : c \Rightarrow \tau \qquad \Sigma; \Psi \vdash c}{\Sigma; \Psi; \Gamma \vdash e\ \bullet : \tau}\ \text{SLIO}^*\text{-CE}$$

Figure 5: Type system for SLIO*

$$\frac{}{\Sigma; \Psi \vdash \tau <: \tau} \text{ SLIO}^*\text{sub-refl} \qquad \frac{\Sigma; \Psi \vdash \tau_1' <: \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 \to \tau_2 <: \tau_1' \to \tau_2'} \text{ SLIO}^*\text{sub-arrow}$$

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'} \text{ SLIO}^*\text{sub-prod}$$

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'} \text{ SLIO}^*\text{sub-sum}$$

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi \vdash \mathsf{Labeled}\ \ell\ \tau <: \mathsf{Labeled}\ \ell'\ \tau'} \text{ SLIO}^*\text{sub-labeled}$$

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell_i' \sqsubseteq \ell_i \qquad \Sigma; \Psi \vdash \ell_o \sqsubseteq \ell_o'}{\Sigma; \Psi \vdash \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau <: \mathbb{SLIO}\ \ell_i'\ \ell_o'\ \tau'} \text{ SLIO}^*\text{sub-monad}$$

$$\frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash \forall \alpha.\tau_1 <: \forall \alpha.\tau_2} \text{ SLIO}^*\text{sub-forall}$$

$$\frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash c_1 \Rightarrow \tau_1 <: c_2 \Rightarrow \tau_2} \text{ SLIO}^*\text{sub-constraint}$$

Figure 6: SLIO* subtyping

$$\frac{}{\Sigma; \Psi \vdash \mathsf{b}\ WF}\ \text{SLIO}^*\text{-wff-base} \qquad \frac{}{\Sigma; \Psi \vdash \mathsf{unit}\ WF}\ \text{SLIO}^*\text{-wff-unit}$$

$$\frac{\Sigma; \Psi \vdash \tau_1\ WF \qquad \Sigma; \Psi \vdash \tau_2\ WF}{\Sigma; \Psi \vdash (\tau_1 \rightarrow \tau_2)\ WF}\ \text{SLIO}^*\text{-wff-arrow}$$

$$\frac{\Sigma; \Psi \vdash \tau_1\ WF \qquad \Sigma; \Psi \vdash \tau_2\ WF}{\Sigma; \Psi \vdash (\tau_1 \times \tau_2)\ WF}\ \text{SLIO}^*\text{-wff-times}$$

$$\frac{\Sigma; \Psi \vdash \tau_1\ WF \qquad \Sigma; \Psi \vdash \tau_2\ WF}{\Sigma; \Psi \vdash (\tau_1 + \tau_2)\ WF}\ \text{SLIO}^*\text{-wff-sum} \qquad \frac{\text{FV}(\ell) = \emptyset \qquad \text{FV}(\tau) = \emptyset}{\Sigma; \Psi \vdash (\mathsf{ref}\ \ell\ \tau)\ WF}\ \text{SLIO}^*\text{-wff-ref}$$

$$\frac{\Sigma, \alpha; \Psi \vdash \tau\ WF}{\Sigma; \Psi \vdash (\forall \alpha.\ \tau)\ WF}\ \text{SLIO}^*\text{-wff-forall} \qquad \frac{\Sigma; \Psi, c \vdash \tau\ WF}{\Sigma; \Psi \vdash (c \Rightarrow \tau)\ WF}\ \text{SLIO}^*\text{-wff-constraint}$$

$$\frac{\Sigma; \Psi \vdash \tau\ WF \qquad \text{FV}(\ell) \in \Sigma}{\Sigma; \Psi \vdash (\mathsf{Labeled}\ \ell\ \tau)\ WF}\ \text{SLIO}^*\text{-wff-labeled}$$

$$\frac{\Sigma; \Psi \vdash \tau\ WF \qquad \text{FV}(\ell_i) \in \Sigma \qquad \text{FV}(\ell_o) \in \Sigma}{\Sigma; \Psi \vdash (\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau)\ WF}\ \text{SLIO}^*\text{-wff-monad}$$

Figure 7: Well-formedness relation for SLIO*

$$\frac{e_1 \Downarrow_i \lambda x.e_i \qquad e_2 \Downarrow_j v_2 \qquad e_i[v_2/x] \Downarrow_k v_3}{e_1\ e_2 \Downarrow_{i+j+k+1} v_3}\ \text{SLIO}^*\text{-Sem-app}$$

$$\frac{e_1 \Downarrow_i v_1 \qquad e_2 \Downarrow_j v_2}{(e_1, e_2) \Downarrow_{i+j+1} (v_1, v_2)}\ \text{SLIO}^*\text{-Sem-prod} \qquad \frac{e \Downarrow_i (v_1, v_2)}{\mathsf{fst}(e) \Downarrow_{i+1} v_1}\ \text{SLIO}^*\text{-Sem-fst}$$

$$\frac{e \Downarrow_i (v_1, v_2)}{\mathsf{snd}(e) \Downarrow_{i+1} v_2}\ \text{SLIO}^*\text{-Sem-snd} \qquad \frac{e \Downarrow_i v}{\mathsf{inl}(e) \Downarrow_{i+1} \mathsf{inl}(v)}\ \text{SLIO}^*\text{-Sem-inl}$$

$$\frac{e \Downarrow_i v}{\mathsf{inr}(e) \Downarrow_{i+1} \mathsf{inr}(v)}\ \text{SLIO}^*\text{-Sem-inr} \qquad \frac{e \Downarrow_i \mathsf{inl}\ v \qquad e_1[v/x] \Downarrow_j v_1}{\mathsf{case}(e, x.e_1, y.e_2) \Downarrow_{i+j+1} v_1}\ \text{SLIO}^*\text{-Sem-case1}$$

$$\frac{e \Downarrow_i \mathsf{inr}\ v \qquad e_2[v/x] \Downarrow_j v_2}{\mathsf{case}(e, x.e_1, y.e_2) \Downarrow_{i+j+1} v_2}\ \text{SLIO}^*\text{-Sem-case2} \qquad \frac{e \Downarrow_i v}{\mathsf{Lb}(e) \Downarrow_{i+1} \mathsf{Lb}(v)}\ \text{SLIO}^*\text{-Sem-Lb}$$

$$\frac{e \Downarrow_i \Lambda\ e_i \qquad e_i \Downarrow_j v}{e[\,] \Downarrow_{i+j+1} v}\ \text{SLIO}^*\text{-Sem-FE} \qquad \frac{e \Downarrow_i \nu\ e_i \qquad e_i \Downarrow_j v}{e\bullet \Downarrow_{i+j+1} v}\ \text{SLIO}^*\text{-Sem-CE}$$

$$\frac{e \Downarrow_i v}{(H, \mathsf{ret}(e)) \Downarrow^f_{i+1} (H, v)}\ \text{SLIO}^*\text{-Sem-ret}$$

$$\frac{e_1 \Downarrow_i v_1 \qquad (H, v_1) \Downarrow^f_j (H', v_1') \qquad e_2[v_1'/x] \Downarrow_k v_2 \qquad (H', v_2) \Downarrow^f_l (H'', v_2')}{(H, \mathsf{bind}(e_1, x.e_2)) \Downarrow^f_{i+j+k+l+1} (H'', v_2')}\ \text{SLIO}^*\text{-Sem-bind}$$

$$\frac{e \Downarrow_i \mathsf{Lb}(v)}{(H, \mathsf{unlabel}(e)) \Downarrow^f_{i+1} (H, v)}\ \text{SLIO}^*\text{-Sem-unlabel}$$

2.3 Model for SLIO*

$W : ((\mathit{Loc} \mapsto \mathit{Type}) \times (\mathit{Loc} \mapsto \mathit{Type}) \times (\mathit{Loc} \leftrightarrow \mathit{Loc}))$

Definition 2.1 (SLIO*: θ_2 extends θ_1). $\theta_1 \sqsubseteq \theta_2 \triangleq$
$\forall a \in \theta_1.\theta_1(a) = \tau \implies \theta_2(a) = \tau$

Definition 2.2 (SLIO*: W_2 extends W_1). $W_1 \sqsubseteq W_2 \triangleq$

1. $\forall i \in \{1, 2\}.\ W_1.\theta_i \sqsubseteq W_2.\theta_i$
2. $\forall p \in (W_1.\hat{\beta}).p \in (W_2.\hat{\beta})$

Definition 2.3 (SLIO*: Value Equivalence).

$$\mathit{ValEq}(\mathcal{A}, W, \ell, n, v_1, v_2, \tau) \triangleq \begin{cases} (W, n, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}} & \ell \sqsubseteq \mathcal{A} \\ \forall j.(W.\theta_1, j, v_1) \in \lfloor \tau \rfloor_V \wedge & \ell \not\sqsubseteq \mathcal{A} \\ (W.\theta_2, j, v_2) \in \lfloor \tau \rfloor_V & \end{cases}$$

Definition 2.4 (SLIO*: Binary value relation)**.**

$$
\begin{array}{lll}
\lceil \mathsf{b} \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, v_1, v_2) \mid v_1 = v_2 \wedge \{v_1, v_2\} \in [\![\mathsf{b}]\!]\} \\
\lceil \mathsf{unit} \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, (), ()) \mid () \in [\![\mathsf{unit}]\!]\} \\
\lceil \tau_1 \times \tau_2 \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, (v_1, v_2), (v_1', v_2')) \mid (W, n, v_1, v_1') \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \wedge (W, n, v_2, v_2') \in \lceil \tau_2 \rceil_V^{\mathcal{A}}\} \\
\lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, \mathsf{inl}\ v, \mathsf{inl}\ v') \mid (W, n, v, v') \in \lceil \tau_1 \rceil_V^{\mathcal{A}}\} \cup \\
& & \{(W, n, \mathsf{inr}\ v, \mathsf{inr}\ v') \mid (W, n, v, v') \in \lceil \tau_2 \rceil_V^{\mathcal{A}}\} \\
\lceil \tau_1 \to \tau_2 \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, \lambda x.e_1, \lambda x.e_2) \mid \\
& & \forall W' \sqsupseteq W, j < n, v_1, v_2. \\
& & ((W', j, v_1, v_2) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \implies (W', j, e_1[v_1/x], e_2[v_2/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}}) \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_1, v_c, j. \\
& & ((\theta_l, j, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, j, e_1[v_c/x]) \in \lfloor \tau_2 \rfloor_E) \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_2, v_c, j. \\
& & ((\theta_l, j, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, j, e_2[v_c/x]) \in \lfloor \tau_2 \rfloor_E)\} \\
\lceil \forall \alpha.\tau \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, \Lambda e_1, \Lambda e_2) \mid \\
& & \forall W' \sqsupseteq W, j < n, \ell' \in \mathcal{L}. \\
& & ((W', j, e_1, e_2) \in \lceil \tau[\ell'/\alpha] \rceil_E^{\mathcal{A}}) \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_1, \ell'' \in \mathcal{L}, j.(\theta_l, j, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_2, \ell'' \in \mathcal{L}, j.(\theta_l, j, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E\} \\
\lceil c \Rightarrow \tau \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, \nu e_1, \nu e_2) \mid \\
& & \forall W' \sqsupseteq W, j < n. \\
& & \mathcal{L} \models c \implies (W', j, e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}} \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c \implies (\theta_l, j, e_1) \in \lfloor \tau \rfloor_E \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c \implies (\theta_l, j, e_2) \in \lfloor \tau \rfloor_E\} \\
\lceil \mathsf{ref}\ \ell\ \tau \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, a_1, a_2) \mid \\
& & (a_1, a_2) \in W.\hat{\beta} \wedge W.\theta_1(a_1) = W.\theta_2(a_2) = \mathsf{Labeled}\ \ell\ \tau\} \\
\lceil \mathsf{Labeled}\ \ell\ \tau \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, \mathsf{Lb}(v_1), \mathsf{Lb}(v_2)) \mid \mathit{ValEq}(\mathcal{A}, W, \ell, n, v_1, v_2, \tau)\} \\
\lceil \mathbb{SLIO}\ \ell_1\ \ell_2\ \tau \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, v_1, v_2) \mid \\
& & \Big(\forall k \leq n, W_e \sqsupseteq W, H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \\
& & \forall v_1', v_2', j.(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies \\
& & \exists W' \sqsupseteq W_e.(k - j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k - j, \ell_2, v_1', v_2', \tau)\Big) \wedge \\
& & \forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies \\
& & \exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v_l') \in \lfloor \tau \rfloor_V \wedge \\
& & (\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge \\
& & (\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_1)\Big)\}
\end{array}
$$

Definition 2.5 (SLIO*: Binary expression relation)**.**

$$
\lceil \tau \rceil_E^{\mathcal{A}} \triangleq \{(W, n, e_1, e_2) \mid \forall i < n.e_1 \Downarrow_i v_1 \wedge e_2 \Downarrow v_2 \implies (W, n - i, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}\}
$$

Definition 2.6 (SLIO*: Unary value relation).

$$
\begin{array}{lcl}
\lfloor \mathsf{b} \rfloor_V & \triangleq & \{(\theta, m, v) \mid v \in [\![\mathsf{b}]\!]\} \\
\lfloor \mathsf{unit} \rfloor_V & \triangleq & \{(\theta, m, v \mid v \in [\![\mathsf{unit}]\!]\} \\
\lfloor \tau_1 \times \tau_2 \rfloor_V & \triangleq & \{(\theta, m, (v_1, v_2)) \mid (\theta, m, v_1) \in \lfloor \tau_1 \rfloor_V \wedge (\theta, m, v_2) \in \lfloor \tau_2 \rfloor_V\} \\
\lfloor \tau_1 + \tau_2 \rfloor_V & \triangleq & \{(\theta, m, \mathsf{inl}\ v) \mid (\theta, m, v) \in \lfloor \tau_1 \rfloor_V\} \cup \{(\theta, m, \mathsf{inr}\ v) \mid (\theta, m, v) \in \lfloor \tau_2 \rfloor_V\} \\
\lfloor \tau_1 \to \tau_2 \rfloor_V & \triangleq & \{(\theta, m, \lambda x.e) \mid \forall \theta' \sqsupseteq \theta, v, j < m.(\theta', j, v) \in \lfloor \tau_1 \rfloor_V \implies (\theta', j, e[v/x]) \in \lfloor \tau_2 \rfloor_E\} \\
\lfloor \forall \alpha.\tau \rfloor_V & \triangleq & \{(\theta, m, \Lambda e) \mid \forall \theta'.\theta \sqsubseteq \theta', j < m.\forall \ell' \in \mathcal{L}.(\theta', j, e) \in \lfloor \tau[\ell'/\alpha] \rfloor_E\} \\
\lfloor c \Rightarrow \tau) \rfloor_V & \triangleq & \{(\theta, m, \nu e) \mid \mathcal{L} \models c \implies \forall \theta'.\theta \sqsubseteq \theta', j < m.(\theta', j, e) \in \lfloor \tau \rfloor_E\} \\
\lfloor \mathsf{ref}\ \ell\ \tau \rfloor_V & \triangleq & \{(\theta, m, a) \mid \theta(a) = \mathsf{Labeled}\ \ell\ \tau\} \\
\lfloor \mathsf{Labeled}\ \ell\ \tau \rfloor_V & \triangleq & \{(\theta, m, \mathsf{Lb}(v) \mid (\theta, m, v) \in \lfloor \tau \rfloor_V\} \\
\lfloor \mathbb{SLIO}\ \ell_1\ \ell_2\ \tau \rfloor_V & \triangleq & \{(\theta, m, e) \mid \\
& & \forall k \leq m, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v) \Downarrow_j^f (H', v') \wedge j < k \implies \\
& & \exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor \tau \rfloor_V \wedge \\
& & (\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge \\
& & (\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_1)\}
\end{array}
$$

Definition 2.7 (SLIO*: Unary expression relation).

$$\lfloor \tau \rfloor_E \triangleq \{(\theta, n, e) \mid \forall i < n.e \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor \tau \rfloor_V\}$$

Definition 2.8 (SLIO*: Unary heap well formedness).

$$(n, H) \triangleright \theta \triangleq dom(\theta) \subseteq dom(H) \wedge \forall a \in dom(\theta).(\theta, n - 1, H(a)) \in \lfloor \theta(a) \rfloor_V$$

Definition 2.9 (SLIO*: Binary heap well formedness).

$$
\begin{array}{lcl}
(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W & \triangleq & dom(W.\theta_1) \subseteq dom(H_1) \wedge dom(W.\theta_2) \subseteq dom(H_2) \wedge \\
& & (W.\hat{\beta}) \subseteq (dom(W.\theta_1) \times dom(W.\theta_2)) \wedge \\
& & \forall (a_1, a_2) \in (W.\hat{\beta}).(W.\theta_1(a_1) = W.\theta_2(a_2) \wedge \\
& & (W, n - 1, H_1(a_1), H_2(a_2)) \in \lceil W.\theta_1(a_1) \rceil_V^{\mathcal{A}}) \wedge \\
& & \forall i \in \{1, 2\}.\forall m.\forall a_i \in dom(W.\theta_i).(W.\theta_i, m, H_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V
\end{array}
$$

Definition 2.10 (SLIO*: Label substitution). $\sigma : Lvar \mapsto Label$

Definition 2.11 (SLIO*: Value substitution to value pairs). $\gamma : Var \mapsto (Val, Val)$

Definition 2.12 (SLIO*: Value substitution to values). $\delta : Var \mapsto Val$

Definition 2.13 (SLIO*: Unary interpretation of Γ).

$$\lfloor \Gamma \rfloor_V \triangleq \{(\theta, n, \delta) \mid dom(\Gamma) \subseteq dom(\delta) \wedge \forall x \in dom(\Gamma).(\theta, n, \delta(x)) \in \lfloor \Gamma(x) \rfloor_V\}$$

Definition 2.14 (SLIO*: Binary interpretation of Γ).

$$\lceil \Gamma \rceil_V^{\mathcal{A}} \triangleq \{(W, n, \gamma) \mid dom(\Gamma) \subseteq dom(\gamma) \wedge \forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}\}$$

2.4 Soundness proof for SLIO*

Lemma 2.15 (SLIO*: Binary value relation subsumes unary value relation). $\forall W, v_1, v_2, \mathcal{A}, n, \tau.$
$(W, n, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}} \implies \forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, v_i) \in \lfloor \tau \rfloor_V$

Proof. Proof by induction on τ

1. Case b:

   From Definition 2.6

2. Case $\tau_1 \times \tau_2$:

   Given: $(W, n, (v_{i1}, v_{i2}), (v_{j1}, v_{j2})) \in \lceil \tau_1 \times \tau_2 \rceil_V^{\mathcal{A}}$

   To prove:

   $\forall m.\ (W.\theta_1, m, (v_{i1}, v_{i2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$ (P01)

   and

   $\forall m.\ (W.\theta_2, m, (v_{j1}, v_{j2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$ (P02)

   From Definition 2.4 we know that we are given

   $(W, n, v_{i1}, v_{j1}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \wedge (W, n, v_{i2}, v_{j2}) \in \lceil \tau_2 \rceil_V^{\mathcal{A}}$ (P1)

   IH1a: $\forall m_1.\ (W.\theta_1, m_1, v_{i1}) \in \lfloor \tau_1 \rfloor_V$ and

   IH1b: $\forall m_1.\ (W.\theta_2, m_1, v_{j1}) \in \lfloor \tau_1 \rfloor_V$

   IH2a: $\forall m_2.\ (W.\theta_1, m_2, v_{i2}) \in \lfloor \tau_2 \rfloor_V$ and

   IH2b: $\forall m_2.\ (W.\theta_2, m_2, v_{j2}) \in \lfloor \tau_2 \rfloor_V$

   From (P01) we know that given some m we need to prove

   $(W.\theta_1, m, (v_{i1}, v_{i2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

   Similarly from (P02) we know that given some m we need to prove

   $(W.\theta_2, m, (v_{j1}, v_{j2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

   We instantiate IH1a and IH2a with the given m from (P01) to get

   $(W.\theta_1, m, v_{i1}) \in \lfloor \tau_1 \rfloor_V$ and $(W.\theta_1, m, v_{i2}) \in \lfloor \tau_2 \rfloor_V$

   Then from Definition 2.6, we get

   $(W.\theta_1, m, (v_{i1}, v_{i2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

   Similarly we instantiate IH1b and IH2b with the given m from (P02) to get

   $(W.\theta_2, m, v_{j1}) \in \lfloor \tau_1 \rfloor_V$ and $(W.\theta_2, m, v_{j2}) \in \lfloor \tau_2 \rfloor_V$

   Then from Definition 2.6, we get

   $(W.\theta_2, m, (v_{j1}, v_{j2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

3. Case $\tau_1 + \tau_2$:

   2 cases arise:

   (a) $v_1 = \mathsf{inl}(v_{i1})$ and $v_2 = \mathsf{inl}(v_{j1})$

   Given: $(W, n, \mathsf{inl}(v_{i1}), \mathsf{inl}(v_{j1})) \in \lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}}$

   To prove:

   $\forall m.\ (W.\theta_1, m, \mathsf{inl}(v_{i1})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$ (S01)

   and

   $\forall m.\ (W.\theta_2, m, \mathsf{inl}(v_{i2})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$ (S02)

From Definition 2.4 we know that we are given
$(W, n, v_{i1}, v_{j1}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$ (S0)
IH1: $\forall m_1.\ (W.\theta_1, m_1, v_{i1}) \in \lfloor \tau_1 \rfloor_V$ and
IH2: $\forall m_2.\ (W.\theta_2, m_2, v_{j1}) \in \lfloor \tau_1 \rfloor_V$

From (S01) we know that given some m and we are required to prove:
$(W.\theta_1, m, \mathsf{inl}(v_{i1})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$
Also from (S02) we know that given some m and we are required to prove:
$(W.\theta_2, m, \mathsf{inl}(v_{i2})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$

We instantiate IH1 with m from (S01) to get
$(W.\theta_1, m, v_{i1}) \in \lfloor \tau_1 \rfloor_V$
Therefore from Definition 2.6, we get
$(W.\theta_1, m, \mathsf{inl}(v_{i1})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$

We instantiate IH2 with m from (S02) to get
$(W.\theta_2, m, v_{j1}) \in \lfloor \tau_1 \rfloor_V$
Therefore from Definition 2.6, we get
$(W.\theta_2, m, \mathsf{inl}(v_{j1})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$

(b) $v_1 = \mathsf{inr}(v_{i2})$ and $v_2 = \mathsf{inr}(v_{j2})$
Symmetric reasoning as in the (a) case above

4. Case $\tau_1 \to \tau_2$:
Given: $(W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil \tau_1 \to \tau_2 \rceil_V^{\mathcal{A}}$
This means from Definition 2.4 we know that
$\forall W' \sqsupseteq W, j < n, v_1, v_2.((W', j, v_1, v_2) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \implies (W', j, e_1[v_1/x], e_2[v_2/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}})$
$\wedge\ \forall \theta_l \sqsupseteq W.\theta_1, i, v_c.((\theta_l, i, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, i, e_1[v_c/x]) \in \lfloor \tau_2 \rfloor_E)$
$\wedge\ \forall \theta_l \sqsupseteq W.\theta_2, k, v_c.((\theta_l, k, v_2) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, k, e_2[v_c/x]) \in \lfloor \tau_2 \rfloor_E)$ (L0)

To prove:

(a) $\forall m.\ (W.\theta_1, m, \lambda x.e_1) \in \lfloor \tau_1 \to \tau_2 \rfloor_V$:
This means from Definition 2.6 we need to prove:
$\forall \theta'. W.\theta_1 \sqsubseteq \theta' \wedge \forall j < m. \forall v.(\theta', j, v) \in \lfloor \tau_1 \rfloor_V \implies (\theta', j, e_1[v/x]) \in \lfloor \tau_2 \rfloor_E$
This further means that we have some θ', j and v s.t
$W.\theta_1 \sqsubseteq \theta' \wedge j < m \wedge (\theta', j, v) \in \lfloor \tau_1 \rfloor_V$
And we need to prove: $(\theta', j, e_1[v/x]) \in \lfloor \tau_2 \rfloor_E$

Instantiating θ_l, i and v_c in the second conjunct of L0 with θ', j and v respectively and since we know that $W.\theta_1 \sqsubseteq \theta'$ and $(\theta', j, v) \in \lfloor \tau_1 \rfloor_V$

Therefore we get $(\theta', j, e_1[v/x]) \in \lfloor \tau_2 \rfloor_E$

(b) $\forall m.\ (W.\theta_2, m, \lambda x.e_2) \in \lfloor \tau_1 \to \tau_2 \rfloor_V$:
Similar reasoning with e_2

5. Case $\forall\alpha.\tau$:

   Given: $(W, n, \Lambda e_1, \Lambda e_2) \in \lceil \forall\alpha.\tau \rceil_V^{\mathcal{A}}$

   This means from Definition 2.4 we know that

   $\forall W_b \sqsupseteq W, n_b < n, \ell' \in \mathcal{L}.((W_b, n_b, e_1, e_2) \in \lceil \tau[\ell'/\alpha] \rceil_E^{\mathcal{A}})$
   $\wedge\ \forall \theta_l \sqsupseteq W.\theta_1, i, \ell'' \in \mathcal{L}.((\theta_l, i, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$
   $\wedge\ \forall \theta_l \sqsupseteq W.\theta_2, i, \ell'' \in \mathcal{L}.((\theta_l, i, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$ (F0)

   To prove:

   (a) $\forall m.\ (W.\theta_1, m, \Lambda e_1) \in \lfloor \forall\alpha.\tau \rfloor_V$:
   This means from Definition 2.6 we need to prove:
   $\forall \theta'. W.\theta_1 \sqsubseteq \theta'.\forall m' < m.\forall \ell_u \in \mathcal{L}.(\theta', m', e_1) \in \lfloor \tau[\ell_u/\alpha] \rfloor_E$
   This further means that we are given some θ', m' and ℓ_u s.t $W.\theta_1 \sqsubseteq \theta'$, $m' < m$ and $\ell_u \in \mathcal{L}$
   And we need to prove: $(\theta', m', e_1) \in \lfloor \tau[\ell_u/\alpha] \rfloor_E$

   Instantiating θ_l, i and ℓ'' in the second conjunct of F0 with θ', m' and ℓ_u respectively and since we know that $W.\theta_1 \sqsubseteq \theta'$ and $\ell_u \in \mathcal{L}$

   Therefore we get $(\theta', m', e_1) \in \lfloor \tau[\ell_u/\alpha] \rfloor_E$

   (b) $\forall m.\ (W.\theta_2, m, \Lambda e_2) \in \lfloor \forall\alpha.\tau \rfloor_V$:
   Symmetric reasoning for e_2

6. Case $c \Rightarrow \tau$:

   Given: $(W, n, \nu e_1, \nu e_2) \in \lceil c \Rightarrow \tau \rceil_V^{\mathcal{A}}$

   This means from Definition 2.4 we know that

   $\forall W_b \sqsupseteq W, n' < n.\mathcal{L} \models c \implies (W_b, n', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$
   $\wedge \forall \theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c \implies (\theta_l, j, e_1) \in \lfloor \tau \rfloor_E)$
   $\wedge \forall \theta_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c \implies (\theta_l, j, e_2) \in \lfloor \tau \rfloor_E)$ (C0)

   To prove:

   (a) $\forall m.\ (W.\theta_1, m, \nu e_1) \in \lfloor c \Rightarrow \tau \rfloor_V$:
   This means from Definition 2.6 we need to prove:
   $\forall \theta'. W.\theta_1 \sqsubseteq \theta'.\forall m' < m.\mathcal{L} \models c \implies (\theta', m', e_1) \in \lfloor \tau \rfloor_E$
   This further means that we are given some θ' and m' s.t $W.\theta_1 \sqsubseteq \theta'$, $m' < m$ and $\mathcal{L} \models c$
   And we need to prove: $(\theta', m', e_1) \in \lfloor \tau \rfloor_E$

   Instantiating θ_l, j in the second conjunct of C0 with θ', m' respectively and since we know that $W.\theta_1 \sqsubseteq \theta'$ and $\mathcal{L} \models c$

   Therefore we get $(\theta', m', e_1) \in \lfloor \tau \rfloor_E$

   (b) $\forall m.\ (W.\theta_2, m, \nu e_2) \in \lfloor c \Rightarrow \tau \rfloor_V$:
   Symmetric reasoning for e_2

7. Case $\mathsf{ref}\ \ell\ \tau$:

   From Definition 2.4 and 2.6

8. Case $\mathsf{Labeled}\ \ell\ \tau$:

   Given $(W, n, \mathsf{Lb}\, v_1, \mathsf{Lb}\, v_2) \in \lceil \mathsf{Labeled}\ \ell\ \tau \rceil_V^{\mathcal{A}}$

   2 cases arise:

   (a) $\ell \sqsubseteq \mathcal{A}$:

   From Definition 2.3 we know that
   $(W, n, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$

   Therefore from IH we get $\forall m.(W.\theta_1, m, v_1) \in \lfloor \tau \rfloor_V$ and $\forall m.(W.\theta_2, m, v_2) \in \lfloor \tau \rfloor_V$

   (b) $\ell \not\sqsubseteq \mathcal{A}$:

   Directly from Definition 2.3

9. Case $\mathbb{SLIO}\ \ell_1\ \ell_2\ \tau$:

   Given: $(W, n, v_1, v_2) \in \lceil \mathbb{SLIO}\ \ell_1\ \ell_2\ \tau \rceil_V^{\mathcal{A}}$

   This means from Definition 2.4 we know that

$$\Big(\forall k \leq n,\ W_e \sqsupseteq W, H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v_1', v_2', j.$$
$$(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$$
$$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_2, v_1', v_2', \tau)\Big) \wedge$$
$$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$$
$$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau \rfloor_V \wedge$$
$$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$$
$$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_1)\Big) \qquad \text{(CG0)}$$

   To prove: $\forall i \in \{1,2\}.\ \forall m.\ (W.\theta_i, m, v_i) \in \lfloor \mathbb{SLIO}\ \ell_1\ \ell_2\ \tau \rfloor_V$

   This means from Definition 2.6 we need to prove

$$\forall l \in \{1,2\}.\forall m.\Big(\forall k \leq m, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$$
$$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau \rfloor_V \wedge$$
$$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$$
$$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_1)\Big)$$

   <u>Case $l = 1$</u>

   And given some m and $k \leq m, \theta_e \sqsupseteq W.\theta_l, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k$

   We need to prove that

$$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau \rfloor_V \wedge$$
$$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$$
$$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_1)$$

   Instantiating (CG0) with $l = 1$ and the given $k \leq m, \theta_e \sqsupseteq W.\theta_l, H, j$ we get the desired.

   <u>Case $l = 2$</u>

   Symmetric reasoning as in the previous case above

□

Lemma 2.16 (SLIO*: Monotonicity Unary)**.** *The following holds:*
$\forall \theta, \theta', v, m, m', \tau.$
$(\theta, m, v) \in \lfloor \tau \rfloor_V \wedge m' < m \wedge \theta \sqsubseteq \theta' \implies (\theta', m', v) \in \lfloor \tau \rfloor_V$

Proof. Proof by induction on τ

1. case b:

   Directly from Definition 2.6

2. case $\tau_1 \times \tau_2$:

   Given: $(\theta, m, (v_1, v_2)) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

   To prove: $(\theta', m', (v_1, v_2)) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

   This means from Definition 2.6 we know that

   $(\theta, m, v_1) \in \lfloor \tau_1 \rfloor_V \wedge (\theta, m, v_2) \in \lfloor \tau_2 \rfloor_V$

   IH1 : $(\theta', m', v_1) \in \lfloor \tau_1 \rfloor_V$

   IH2 : $(\theta', m', v_2) \in \lfloor \tau_2 \rfloor_V$

   We get the desired from IH1, IH2 and Definition 2.6

3. case $\tau_1 + \tau_2$:

   2 cases arise:

   (a) $v = \mathsf{inl}(v_1)$:
   Given: $(\theta, m, (\mathsf{inl}\ v_1)) \in \lfloor \tau_1 + \tau_2 \rfloor_V$
   To prove: $(\theta', m', \mathsf{inl}\ v_1) \in \lfloor \tau_1 + \tau_2 \rfloor_V$
   This means from Definition 2.6 we know that
   $(\theta, m, v_1) \in \lfloor \tau_1 \rfloor_V$
   IH : $(\theta', m', v_1) \in \lfloor \tau_1 \rfloor_V$
   Therefore from IH and Definition 2.6 we get the desired

   (b) $v = \mathsf{inr}(v_2)$
   Symmetric case

4. case $\tau_1 \to \tau_2$:

   Given: $(\theta, m, (\lambda x.e_1)) \in \lfloor \tau_1 \to \tau_2 \rfloor_V$

   To prove: $(\theta', m', (\lambda x.e_1)) \in \lfloor \tau_1 \to \tau_2 \rfloor_V$

   This means from Definition 2.6 we know that

   $$\forall \theta''.\theta \sqsubseteq \theta'' \wedge \forall j < m.\forall v.(\theta'', j, v) \in \lfloor \tau_1 \rfloor_V \implies (\theta'', j, e_1[v/x]) \in \lfloor \tau_2 \rfloor_E \tag{75}$$

   Similarly from Definition 2.6 we know that we are required to prove

   $\forall \theta'''.\theta' \sqsubseteq \theta''' \wedge \forall k < m'.\forall v_1.(\theta''', k, v_1) \in \lfloor \tau_1 \rfloor_V \implies (\theta''', k, e_1[v_1/x]) \in \lfloor \tau_2 \rfloor_E$

   This means that given some θ''', k and v_1 such that $\theta' \sqsubseteq \theta''' \wedge k < m' \wedge (\theta''', k, v_1) \in \lfloor \tau_1 \rfloor_V$

   And we are required to prove $(\theta''', k, e_1[v_1/x]) \in \lfloor \tau_2 \rfloor_E$

Instantiating Equation 75 with θ''', k and v_1 and since we know that $\theta' \sqsubseteq \theta'''$ and $\theta \sqsubseteq \theta'$ therefore we have $\theta \sqsubseteq \theta'''$. Also, we know that $k < m' < m$ and $(\theta''', k, v_1) \in \lfloor \tau_1 \rfloor_V$

Therefore we get $(\theta''', k, e_1[v_1/x]) \in \lfloor \tau_2 \rfloor_E$

5. case $\mathsf{ref}\ \ell\ \tau$:

   From Definition 2.6 and Definition 2.1

6. case $\forall \alpha.\tau$:

   Given: $(\theta, m, (\Lambda e_1)) \in \lfloor \forall \alpha.\tau \rfloor_V$

   To prove: $(\theta', m', (\Lambda e_1)) \in \lfloor \forall \alpha.\tau \rfloor_V$

   This means from Definition 2.6 we know that

$$\forall \theta''.\theta \sqsubseteq \theta'' \wedge \forall j < m.\forall \ell_i \in \mathcal{L}.(\theta'', j, e_1) \in \lfloor \tau[\ell_i/\alpha] \rfloor_E \tag{76}$$

   Similarly from Definition 2.6 we know that we are required to prove
   $\forall \theta'''.\theta' \sqsubseteq \theta''' \wedge \forall k < m'.\forall \ell_j \in \mathcal{L}.(\theta''', k, e_1) \in \lfloor \tau[\ell_j/\alpha] \rfloor_E$

   This means that given some θ''', k and ℓ_j such that $\theta' \sqsubseteq \theta''' \wedge k < m' \wedge \ell_j \in \mathcal{L}$

   And we are required to prove $(\theta''', k, e_1) \in \lfloor \tau[\ell_j/\alpha] \rfloor_E$

   Instantiating Equation 76 with θ''', k and ℓ_j and since we know that $\theta' \sqsubseteq \theta'''$ and $\theta \sqsubseteq \theta'$ therefore we have $\theta \sqsubseteq \theta'''$. Also, we know that $k < m' < m$ and $\ell_j \in \mathcal{L}$

   Therefore we get $(\theta''', k, e_1) \in \lfloor \tau[\ell_j/\alpha] \rfloor_E$

7. case $c \Rightarrow \tau$:

   Given: $(\theta, m, (\nu e_1)) \in \lfloor c \Rightarrow \tau \rfloor_V$

   To prove: $(\theta', m', (\nu e_1)) \in \lfloor c \Rightarrow \tau \rfloor_V$

   This means from Definition 2.6 we know that

$$\forall \theta''.\theta \sqsubseteq \theta'' \wedge \forall j < m.\mathcal{L} \models c \implies (\theta'', j, e_1) \in \lfloor \tau \rfloor_E \tag{77}$$

   Similarly from Definition 2.6 we know that we are required to prove
   $\forall \theta'''.\theta' \sqsubseteq \theta''' \wedge \forall k < m'.\mathcal{L} \models c \implies (\theta''', k, e_1) \in \lfloor \tau \rfloor_E$

   This means that given some θ''', k and ℓ_j such that $\theta' \sqsubseteq \theta''' \wedge k < m' \wedge \ell_j \in \mathcal{L}$

   And we are required to prove $(\theta''', k, e_1) \in \lfloor \tau \rfloor_E$

   Instantiating Equation 77 with θ''', k and since we know that $\theta' \sqsubseteq \theta'''$ and $\theta \sqsubseteq \theta'$ therefore we have $\theta \sqsubseteq \theta'''$. Also, we know that $k < m' < m$ and $\mathcal{L} \models c$

   Therefore we get $(\theta''', k, e_1) \in \lfloor \tau \rfloor_E$

8. case $\mathsf{Labeled}\ \ell\ \tau$:

   Given: $(\theta, m, (\mathsf{Lb}\, v)) \in \lfloor \mathsf{Labeled}\ \ell\ \tau \rfloor_V$

   To prove: $(\theta', m', (\mathsf{Lb}\, v)) \in \lfloor \mathsf{Labeled}\ \ell\ \tau \rfloor_V$

   This means from Definition 2.6 we know that $(\theta, m, v) \in \lfloor \tau \rfloor_V$

   IH: $(\theta', m', v) \in \lfloor \tau \rfloor_V$

   Therefore from IH and Definition 2.6 we get the desired

9. case $\mathbb{SLIO}\ \ell_1\ \ell_2\ \tau$:

   Given: $(\theta, m, e) \in \lfloor \mathbb{SLIO}\ \ell_1\ \ell_2\ \tau \rfloor_V$

   To prove: $(\theta', m', e) \in \lfloor \mathbb{SLIO}\ \ell_1\ \ell_2\ \tau \rfloor_V$

   This means from Definition 2.6 we know that

   $\forall k \le m, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v) \Downarrow_j^f (H', v') \wedge j < k \implies$
   $\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor \tau \rfloor_V \wedge$
   $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell_1 \sqsubseteq \ell') \wedge$
   $(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_1)$ (LB0)

   Similarly from Definition 2.6 we are required to prove

   $\forall k_1 \le m', \theta_{e1} \sqsupseteq \theta', H_1, j_1.(k_1, H_1) \triangleright \theta_{e1} \wedge (H_1, v_1) \Downarrow_{j_1}^f (H'_1, v'_1) \wedge j_1 < k_1 \implies$
   $\exists \theta' \sqsupseteq \theta_e.(k_1 - j_1, H') \triangleright \theta' \wedge (\theta'_1, k_1 - j_1, v') \in \lfloor \tau \rfloor_V \wedge$
   $(\forall a.H_1(a) \neq H'_1(a) \implies \exists \ell'.\theta_{e1}(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell_1 \sqsubseteq \ell') \wedge$
   $(\forall a \in dom(\theta'_1) \backslash dom(\theta_{e1}).\theta'_1(a) \searrow \ell_1)$

   This means we are given

   $k_1 \le m', \theta_{e1} \sqsupseteq \theta', H_1, j_1$ s.t $(k_1, H) \triangleright \theta_{e1} \wedge (H_1, v_1) \Downarrow_{j_1}^f (H'_1, v'_1) \wedge j_1 < k_1$

   And we are required to prove:

   $\exists \theta' \sqsupseteq \theta_e.(k_1 - j_1, H') \triangleright \theta' \wedge (\theta'_1, k_1 - j_1, v') \in \lfloor \tau \rfloor_V \wedge$
   $(\forall a.H_1(a) \neq H'_1(a) \implies \exists \ell'.\theta_{e1}(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell_1 \sqsubseteq \ell') \wedge$
   $(\forall a \in dom(\theta'_1) \backslash dom(\theta_{e1}).\theta'_1(a) \searrow \ell_1)$

   Instantiating (LB0), k with k_1, θ_e with θ_{e1}, H with H_1 and j with j_1. We know that $k_1 < m' < m$, $\theta \sqsubseteq \theta' \sqsubseteq \theta_{e1}$, $(k_1, H_1) \triangleright \theta_{e1}$, $(H_1, v_1) \Downarrow_{j_1}^f (H'_1, v'_1)$ and $i_1 + j_1 < k_1$. Therefore we get

   $\exists \theta' \sqsupseteq \theta_e.(k_1 - j_1, H') \triangleright \theta' \wedge (\theta'_1, k_1 - j_1, v') \in \lfloor \tau \rfloor_V \wedge$
   $(\forall a.H_1(a) \neq H'_1(a) \implies \exists \ell'.\theta_{e1}(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell_1 \sqsubseteq \ell') \wedge$
   $(\forall a \in dom(\theta'_1) \backslash dom(\theta_{e1}).\theta'_1(a) \searrow \ell_1)$

□

Lemma 2.17 (SLIO*: Monotonicity binary)**.** *The following holds:*
$\forall W, W', v_1, v_2, \mathcal{A}, n, n', \tau.$
$(W, n, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}} \wedge n' < n \wedge W \sqsubseteq W' \implies (W', n', v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$

Proof. Proof by induction on τ

1. Case b, unit:

   From Definition 2.4

2. Case $\tau_1 \times \tau_2$:

   Given: $(W, n, (v_{i1}, v_{i2}), (v_{j1}, v_{j2})) \in \lceil \tau_1 \times \tau_2 \rceil_V^{\mathcal{A}}$

   To prove: $(W', n', (v_{i1}, v_{i2}), (v_{j1}, v_{j2})) \in \lceil \tau_1 \times \tau_2 \rceil_V^{\mathcal{A}}$

   From Definition 2.4 we know that we are given
   $(W, n, v_{i1}, v_{j1}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \wedge (W, n, v_{i2}, v_{j2}) \in \lceil \tau_2 \rceil_V^{\mathcal{A}}$
   IH1 : $(W', n', v_{i1}, v_{j1}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$
   IH2 : $(W', n', v_{i2}, v_{j2}) \in \lceil \tau_2 \rceil_V^{\mathcal{A}}$

   From IH1, IH2 and Definition 2.4 we get the desired.

3. Case $\tau_1 + \tau_2$:

   2 cases arise:

   (a) $v_1 = \mathsf{inl}\ v_{i1}$ and $v_2 = \mathsf{inl}\ v_{i2}$:
   Given: $(W, n, (\mathsf{inl}\ v_{i1}, \mathsf{inl}\ v_{i2})) \in \lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}}$
   To prove: $(W', n', (\mathsf{inl}\ v_{i1}, \mathsf{inl}\ v_{i2})) \in \lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}}$

   From Definition 2.4 we know that we are given
   $(W, n, v_{i1}, v_{i2}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$
   IH : $(W', n', v_{i1}, v_{i2}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$
   Therefore from Definition 2.4 we get
   $(W', n', \mathsf{inl}\ v_{i1}, \mathsf{inl}\ v_{i2}) \in \lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}}$

   (b) $v_1 = \mathsf{inr}(v_{12})$ and $v_2 = \mathsf{inr}(v_{22})$:
   Symmetric case

4. Case $\tau_1 \to \tau_2$:

   Given: $(W, n, (\lambda x.e_1), (\lambda x.e_2)) \in \lceil \tau_1 \to \tau_2 \rceil_V^{\mathcal{A}}$

   To prove: $(\theta', n', (\lambda x.e_1), (\lambda x.e_1)) \in \lceil \tau_1 \to \tau_2 \rceil_V^{\mathcal{A}}$

   This means from Definition 2.4 we know that the following holds

   $\forall W' \sqsupseteq W, j < n, v_1, v_2.((W', j, v_1, v_2) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \implies (W', j, e_1[v_1/x], e_2[v_2/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}})$ (BM-A0)

   $\forall \theta_l \sqsupseteq W.\theta_1, j, v_c.((\theta_l, j, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, j, e_1[v_c/x]) \in \lfloor \tau_2 \rfloor_E)$ (BM-A1)

   $\forall \theta_l \sqsupseteq W.\theta_2, j, v_c.((\theta_l, j, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, j, e_2[v_c/x]) \in \lfloor \tau_2 \rfloor_E)$ (BM-A2)

   Similarly from Definition 2.4 we know that we are required to prove

   (a) $\forall W'' \sqsupseteq W', k < n', v_1', v_2'.((W'', k, v_1', v_2') \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \implies (W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}})$:
   This means that we are given some $W'' \sqsupseteq W'$, $k < n'$ and v_1', v_2' s.t
   $(W'', k, v_1', v_2') \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$
   And we a required to prove: $(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}}$

   Instantiating BM-A0 with W'', k and v_1', v_2' we get
   $(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}}$

(b) $\forall \theta'_l \sqsupseteq W'.\theta_1, k, v'_c.((\theta'_l, k, v'_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta'_l, k, e_1[v'_c/x]) \in \lfloor \tau_2 \rfloor_E)$:
This means that we are given some $\theta'_l \sqsupseteq W'.\theta_1$, k and v'_c s.t
$(\theta'_l, k, v'_c) \in \lfloor \tau_1 \rfloor_V$
And we a required to prove: $(\theta'_l, k, e_1[v'_c/x]) \in \lfloor \tau_2 \rfloor_E$

Instantiating BM-A1 with θ'_l, k and v'_c we get
$(\theta'_l, k, e_1[v'_c/x]) \in \lfloor \tau_2 \rfloor_E$

(c) $\forall \theta'_l \sqsupseteq W.\theta_2, k, v'_c.((\theta'_l, k, v'_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta'_l, k, e_2[v'_c/x]) \in \lfloor \tau_2 \rfloor_E)$:
This means that we are given some $\theta'_l \sqsupseteq W'.\theta_2$, k and v'_c s.t
$(\theta'_l, k, v'_c) \in \lfloor \tau_1 \rfloor_V$
And we a required to prove: $(\theta'_l, k, e_2[v'_c/x]) \in \lfloor \tau_2 \rfloor_E$

Instantiating BM-A1 with θ'_l, k and v'_c we get
$(\theta'_l, k, e_2[v'_c/x]) \in \lfloor \tau_2 \rfloor_E$

5. Case $\mathsf{ref}\ \ell\ \tau$:

From Definition 2.4 and Definition 2.2

6. Case $\forall \alpha.\tau$:

Given: $(W, n, (\Lambda e_1), (\Lambda e_2)) \in \lceil \forall \alpha.\tau \rceil_V^{\mathcal{A}}$

To prove: $(\theta', n', (\Lambda e_1), (\Lambda e_1)) \in \lceil \forall \alpha.\tau \rceil_V^{\mathcal{A}}$

This means from Definition 2.4 we know that the following holds

$\forall W' \sqsupseteq W, n' < n, \ell' \in \mathcal{L}.((W', n', e_1, e_2) \in \lceil \tau[\ell'/\alpha] \rceil_E^{\mathcal{A}})$ (BM-F0)

$\forall \theta_l \sqsupseteq W.\theta_1, j, \ell' \in \mathcal{L}.((\theta_l, j, e_1) \in \lfloor \tau[\ell'/\alpha] \rfloor_E)$ (BM-F1)

$\forall \theta_l \sqsupseteq W.\theta_2, j, \ell' \in \mathcal{L}.((\theta_l, j, e_2) \in \lfloor \tau[\ell'/\alpha] \rfloor_E)$ (BM-F2)

Similarly from Definition 2.4 we know that we are required to prove

(a) $\forall W'' \sqsupseteq W', n'' < n', \ell'' \in \mathcal{L}.((W'', n'', e_1, e_2) \in \lceil \tau[\ell''/\alpha] \rceil_E^{\mathcal{A}})$:
This means that we are given some $W'' \sqsupseteq W'$, $n'' < n'$ and $\ell'' \in \mathcal{L}$
And we a required to prove: $((W'', n'', e_1, e_2) \in \lceil \tau[\ell''/\alpha] \rceil_E^{\mathcal{A}})$

Instantiating BM-F0 with W'', n'' and ℓ''. And since $W'' \sqsupseteq W'$ and $W' \sqsupseteq W$ therefore $W'' \sqsupseteq W$. Also since $n'' < n'$ and $n' < n$ therefore $n'' < n$. And finally since $\ell'' \in \mathcal{L}$ therefore we get
$((W'', n'', e_1, e_2) \in \lceil \tau[\ell''/\alpha] \rceil_E^{\mathcal{A}})$

(b) $\forall \theta'_l \sqsupseteq W'.\theta_1, k, \ell'' \in \mathcal{L}.((\theta'_l, k, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$:
This means that we are given some $\theta'_l \sqsupseteq W'.\theta_1$, k and $\ell'' \in \mathcal{L}$
And we a required to prove: $((\theta'_l, k, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$

Instantiating BM-F1 with θ'_l, k and ℓ''. And since $\theta'_l \sqsupseteq W'.\theta_1$ and $W' \sqsupseteq W$ therefore $\theta'_1 \sqsupseteq W.\theta_1$. And since $\ell'' \in \mathcal{L}$ therefore we get
$((\theta'_l, k, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$

(c) $\forall \theta_l \sqsupseteq W.\theta_2, j, \ell'' \in \mathcal{L}.((\theta_l', k, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$:
This means that we are given some $\theta_l' \sqsupseteq W'.\theta_2$, k and $\ell'' \in \mathcal{L}$
And we a required to prove: $((\theta_l', k, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$

Instantiating BM-F1 with θ_l', k and ℓ''. And since $\theta_l' \sqsupseteq W'.\theta_2$ and $W' \sqsupseteq W$ therefore $\theta_2' \sqsupseteq W.\theta_2$. And since $\ell'' \in \mathcal{L}$ therefore we get
$((\theta_l', k, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$

7. Case $c \Rightarrow \tau$:
Given: $(W, n, (\nu e_1), (\nu e_2)) \in \lceil c \Rightarrow \tau \rceil_V^{\mathcal{A}}$
To prove: $(\theta', n', (\nu e_1), (\nu e_1)) \in \lceil c \Rightarrow \tau \rceil_V^{\mathcal{A}}$
This means from Definition 2.4 we know that the following holds
$\forall W' \sqsupseteq W, n' < n.\mathcal{L} \models c \implies (W', n', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$ (BM-C0)
$\forall \theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c \implies (\theta_l, j, e_1) \in \lfloor \tau \rfloor_E$ (BM-C1)
$\forall \theta_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c \implies (\theta_l, j, e_2) \in \lfloor \tau \rfloor_E$ (BM-C2)

Similarly from Definition 2.4 we know that we are required to prove

(a) $\forall W'' \sqsupseteq W', n'' < n.\mathcal{L} \models c \implies (W'', n'', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$:
This means that we are given some $W'' \sqsupseteq W'$, $n'' < n'$ and $\mathcal{L} \models c$
And we a required to prove: $(W'', n'', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$

Instantiating BM-C0 with W'', n''. And since $W'' \sqsupseteq W'$ and $W' \sqsupseteq W$ therefore $W'' \sqsupseteq W$. And since $\mathcal{L} \models c$ therefore we get
$(W'', n'', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$

(b) $\forall \theta_l' \sqsupseteq W'.\theta_1, k.\mathcal{L} \models c \implies (\theta_l', k, e_1) \in \lfloor \tau \rfloor_E$:
This means that we are given some $\theta_l' \sqsupseteq W'.\theta_1$, k and $\mathcal{L} \models c$
And we a required to prove: $(\theta_l', k, e_1) \in \lfloor \tau \rfloor_E$

Instantiating BM-F1 with θ_l', k. And since $\theta_l' \sqsupseteq W'.\theta_1$ and $W' \sqsupseteq W$ therefore $\theta_1' \sqsupseteq W.\theta_1$. And since $\mathcal{L} \models c$ therefore we get
$(\theta_l', k, e_1) \in \lfloor \tau \rfloor_E$

(c) $\forall \theta_l' \sqsupseteq W'.\theta_2, k.\mathcal{L} \models c \implies (\theta_l, k, e_2) \in \lfloor \tau \rfloor_E$:
This means that we are given some $\theta_l' \sqsupseteq W'.\theta_2$, k and $\mathcal{L} \models c$
And we a required to prove: $(\theta_l', k, e_2) \in \lfloor \tau \rfloor_E$

Instantiating BM-F1 with θ_l', k. And since $\theta_l' \sqsupseteq W'.\theta_2$ and $W' \sqsupseteq W$ therefore $\theta_2' \sqsupseteq W.\theta_2$. And since $\mathcal{L} \models c$ therefore we get
$(\theta_l', k, e_2) \in \lfloor \tau \rfloor_E$

8. Case $\mathsf{Labeled}\ \ell\ \tau$:
Given: $(W, n, (\mathsf{Lb}\, v_1), (\mathsf{Lb}\, v_2)) \in \lceil \mathsf{Labeled}\ \ell\ \tau \rceil_V^{\mathcal{A}}$
To prove: $(W', n', (\mathsf{Lb}\, v_1), (\mathsf{Lb}\, v_2)) \in \lceil \mathsf{Labeled}\ \ell\ \tau \rceil_V^{\mathcal{A}}$
From Definition 2.4 2 cases arise:

(a) $\ell \sqsubseteq \mathcal{A}$:
In this case we know that $(W, n, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$
Therefore from IH we know that $(W', n', v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$
Hence from Definition 2.4 we get $(W', n', (\mathsf{Lb}\, v_1), (\mathsf{Lb}\, v_2)) \in \lceil \mathsf{Labeled}\ \ell\ \tau \rceil_V^{\mathcal{A}}$

(b) $\ell \not\sqsubseteq \mathcal{A}$:
In this case we know that $\forall m.\ (W.\theta_1, m, v_1) \in \lfloor \tau \rfloor_V$ and $(W.\theta_2, m, v_2) \in \lfloor \tau \rfloor_V$
Since $W.\theta_1 \sqsubseteq W'.\theta_1$ (from Definition 2.2). Therefore from Lemma 2.16 we know that $\forall m' < m.\ (W'.\theta_1, m', v_1) \in \lfloor \tau \rfloor_V$
Similarly since $W.\theta_2 \sqsubseteq W'.\theta_2$ (from Definition 2.2). Therefore from Lemma 2.16 we know that
$\forall m' < m.\ (W'.\theta_2, m', v_2) \in \lfloor \tau \rfloor_V$

Finally from Definition 2.4 we get $(W', n', (\mathsf{Lb}\, v_1), (\mathsf{Lb}\, v_2)) \in \lceil \mathsf{Labeled}\ \ell\ \tau \rceil_V^{\mathcal{A}}$

9. Case $\mathbb{SLIO}\ \ell_1\ \ell_2\ \tau$:
<u>Given</u>: $(W, n, v_1, v_2) \in \lceil \mathbb{SLIO}\ \ell_1\ \ell_2\ \tau \rceil_V^{\mathcal{A}}$
<u>To prove</u>: $(W', n', v_1, v_2) \in \lceil \mathbb{SLIO}\ \ell_1\ \ell_2\ \tau \rceil_V^{\mathcal{A}}$

From Definition 2.4 we are given that

$$\Big(\forall k \le n, W_e \sqsupseteq W, H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge$$
$$\forall v_1', v_2', j.(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$$
$$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_2, v_1', v_2', \tau)\Big) \wedge$$
$$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$$
$$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau \rfloor_V \wedge$$
$$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$$
$$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_1)\Big) \qquad \text{(BM-M0)}$$

Similarly from Definition 2.4 it suffices to prove that

(a) $\Big(\forall k \le n, W_e \sqsupseteq W, H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge$
$\forall v_1', v_2', j.(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_2, v_1', v_2', \tau)\Big)$:
This means that given some $k \le n$, $W_e \sqsupseteq W, H_1, H_2, v_1', v_2', j$ s.t
$(k, H_1, H_2) \triangleright W_e \wedge (H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2') \wedge j < k$

It suffices to prove that
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_2, v_1', v_2', \tau)$

Instantiating the first conjunct of (BM-M0) with the given k, $W_e \sqsupseteq W, H_1, H_2, v_1', v_2', j$ and since we know that $n' \le n$ and $W \sqsubseteq W'$ we get the desired

(b) $\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_1)\Big)$:
Similar reasoning as in the previous case but using Lemma 2.16

□

Lemma 2.18 (SLIO*: Unary monotonicity for Γ)**.** $\forall \theta, \theta', \delta, \Gamma, n, n'.$
$(\theta, n, \delta) \in \lfloor \Gamma \rfloor_V \wedge n' < n \wedge \theta \sqsubseteq \theta' \implies (\theta', n', \delta) \in \lfloor \Gamma \rfloor_V$

Proof. Given: $(\theta, n, \delta) \in \lfloor \Gamma \rfloor_V \wedge n' < n \wedge \theta \sqsubseteq \theta'$
To prove: $(\theta', n', \delta) \in \lfloor \Gamma \rfloor_V$

From Definition 2.13 it is given that
$dom(\Gamma) \subseteq dom(\delta) \wedge \forall x \in dom(\Gamma).(\theta, n, \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$

And again from Definition 2.13 we are required to prove that
$dom(\Gamma) \subseteq dom(\delta) \wedge \forall x \in dom(\Gamma).(\theta', n', \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$

- $dom(\Gamma) \subseteq dom(\delta)$:

  Given

- $\forall x \in dom(\Gamma).(\theta', n', \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$:

  Since we know that $\forall x \in dom(\Gamma).(\theta, n, \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$ (given)

  Therefore from Lemma 2.16 we get

  $\forall x \in dom(\Gamma).(\theta', n', \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$

□

Lemma 2.19 (SLIO*: Binary monotonicity for Γ)**.** $\forall W, W', \delta, \Gamma, n, n'.$
$(W, n, \gamma) \in \lfloor \Gamma \rfloor_V \wedge n' < n \wedge W \sqsubseteq W' \implies (W', n', \gamma) \in \lfloor \Gamma \rfloor_V$

Proof. Given: $(W, n, \gamma) \in \lfloor \Gamma \rfloor_V \wedge n' < n \wedge W \sqsubseteq W'$
To prove: $(W', n', \gamma) \in \lfloor \Gamma \rfloor_V$

From Definition 2.14 it is given that
$dom(\Gamma) \subseteq dom(\gamma) \wedge \forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$

And again from Definition 2.13 we are required to prove that
$dom(\Gamma) \subseteq dom(\gamma) \wedge \forall x \in dom(\Gamma).(W', n', \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$

- $dom(\Gamma) \subseteq dom(\gamma)$:

  Given

- $\forall x \in dom(\Gamma).(W', n', \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$:

  Since we know that $\forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$ (given)

  Therefore from Lemma 2.17 we get

  $\forall x \in dom(\Gamma).(W', n', \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$

□

Lemma 2.20 (SLIO*: Unary monotonicity for H)**.** $\forall \theta, H, n, n'.$
$(n, H) \rhd \theta \wedge n' < n \implies (n', H) \rhd \theta$

Proof. Given: $(n, H) \rhd \theta \wedge n' < n$
To prove: $(n', H) \rhd \theta$

From Definition 2.8 it is given that
$dom(\theta) \subseteq dom(H) \wedge \forall a \in dom(\theta).(\theta, n-1, H(a)) \in \lfloor \theta(a) \rfloor_V$

And again from Definition 2.13 we are required to prove that
$dom(\theta) \subseteq dom(H) \wedge \forall a \in dom(\theta).(\theta, n'-1, H(a)) \in \lfloor \theta'(a) \rfloor_V$

- $dom(\theta) \subseteq dom(H)$:

  Given

- $\forall a \in dom(\theta).(\theta, n'-1, H(a)) \in \lfloor \theta'(a) \rfloor_V$:

  Since we know that $\forall a \in dom(\theta).(\theta, n-1, H(a)) \in \lfloor \theta(a) \rfloor_V$ (given)

  Therefore from Lemma 2.16 we get

  $\forall a \in dom(\theta).(\theta, n'-1, H(a)) \in \lfloor \theta'(a) \rfloor_V$

□

Lemma 2.21 (SLIO*: Binary monotonicity for heaps)**.** $\forall W, H_1, H_2, n, n'.$
$(n, H_1, H_2) \rhd W \wedge n' < n \implies (n', H_1, H_2) \rhd W$

Proof. Given: $(n, H_1, H_2) \rhd W \wedge n' < n \wedge W \sqsubseteq W'$
To prove: $(n', H_1, H_2) \rhd W$

From Definition 2.9 it is given that
$dom(W.\theta_1) \subseteq dom(H_1) \wedge dom(W.\theta_2) \subseteq dom(H_2) \wedge$
$(W.\hat{\beta}) \subseteq (dom(W.\theta_1) \times dom(W.\theta_2)) \wedge$
$\forall (a_1, a_2) \in (W.\hat{\beta}).(W.\theta_1(a_1) = W.\theta_2(a_2) \wedge$
$(W, n-1, H_1(a_1), H_2(a_2)) \in \lceil W.\theta_1(a_1) \rceil_V^{\mathcal{A}}) \wedge$
$\forall i \in \{1, 2\}.\forall m.\forall a_i \in dom(W.\theta_i).(W.\theta_i, m, H_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$

And again from Definition 2.9 we are required to prove:

- $dom(W.\theta_1) \subseteq dom(H_1) \wedge dom(W.\theta_2) \subseteq dom(H_2)$:

  Given

- $(W.\hat{\beta}) \subseteq (dom(W.\theta_1) \times dom(W.\theta_2))$:

  Given

- $\forall (a_1, a_2) \in (W.\hat{\beta}).(W.\theta_1(a_1) = W.\theta_2(a_2)$ and $(W, n'-1, H_1(a_1), H_2(a_2)) \in \lceil W.\theta_1(a_1) \rceil_V^{\mathcal{A}})$:

  $\forall (a_1, a_2) \in (W.\hat{\beta}).$

  - $(W.\theta_1(a_1) = W.\theta_2(a_2)$: Given
  - $(W, n'-1, H_1(a_1), H_2(a_2)) \in \lceil W.\theta_1(a_1) \rceil_V^{\mathcal{A}})$:
    Given and from Lemma 2.17

- $\forall i \in \{1, 2\}.\forall m.\forall a_i \in dom(W.\theta_i).(W.\theta_i, m, H_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$:

  Given

□

Theorem 2.22 (SLIO*: Fundamental theorem unary)**.** $\forall \Sigma, \Psi, \Gamma, \theta, \mathcal{L}, e, \tau, \sigma, \delta, n.$
$\Sigma; \Psi; \Gamma \vdash e : \tau \wedge$
$\mathcal{L} \models \Psi\ \sigma \wedge$
$(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V \implies$
$(\theta, n, e\ \delta) \in \lfloor \tau\ \sigma \rfloor_E$

Proof. Proof by induction on SLIO* typing derivation

1. SLIO*-var:

$$\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash x : \tau}\ \text{SLIO*-var}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, x\ \delta) \in \lfloor \tau\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n.x\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor \tau \rfloor_V$

This means that given some $i < n$ s.t $x\ \delta \Downarrow_i v$

(from SLIO*-Sem-val we know that $v = x\ \delta$ and $i = 0$)

It suffices to prove $(\theta, n, x\ \delta) \in \lfloor \tau\ \sigma \rfloor_V$ (FU-V0)

Since $(\theta, n, \delta) \in \lfloor \Gamma'\ \sigma \rfloor_V$ where $\Gamma' = \Gamma \cup \{x : \tau\}$. Therefore from Definition 2.13 we know that $(\theta, n, \delta(x)) \in \lfloor \Gamma'(x)\ \sigma \rfloor_V$

So we are done.

2. SLIO*-lam:

$$\frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash e' : \tau_2}{\Sigma; \Psi; \Gamma \vdash \lambda x.e' : (\tau_1 \to \tau_2)}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \lambda x.e_i\ \delta) \in \lfloor (\tau_1 \to \tau_2)\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n.\lambda x.e'\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor (\tau_1 \to \tau_2)\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $\lambda x.e'\ \delta \Downarrow_i v$

(from SLIO*-Sem-val we know that $v = \lambda x.e'\ \delta$ and $i = 0$)

It suffices to prove

$(\theta, n, \lambda x.e'\ \delta) \in \lfloor (\tau_1 \to \tau_2)\ \sigma \rfloor_V$ (FU-L0)

From Definition 2.6 it further suffices to prove

$\forall \theta'' \sqsupseteq \theta, v', j < n.(\theta'', j, v') \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta'', j, (e'\ \delta)[v'/x]) \in \lfloor \tau_2\ \sigma \rfloor_E$

This means given some θ'', v', j s.t $\theta'' \sqsupseteq \theta$, $j < n$ and $(\theta'', j, v') \in \lfloor \tau_1\ \sigma \rfloor_V$ (FU-L1)

We are required to prove

$(\theta'', j, (e' \ \delta)[v'/x]) \in \lfloor \tau_2 \ \sigma \rfloor_E$

Since $(\theta, n, \delta) \in \lfloor \Gamma \ \sigma \rfloor_V$ therefore from Lemma 2.18 we know that $(\theta, j, \delta) \in \lfloor \Gamma \ \sigma \rfloor_V$ where $j < n$ (from FU-L1)

IH:

$\forall \theta_h, v_x. \ (\theta_h, j, e' \ \delta \cup \{x \mapsto v_x\}) \in \lfloor \tau_2 \ \sigma \rfloor_E$, s.t $(\theta_i, j, v_x) \in \lfloor \tau_1 \ \sigma \rfloor_V$

Instantiating IH with θ'' and v' from (FU-L1) we get $(\theta'', j, (e' \ \delta)[v'/x]) \in \lfloor \tau_2 \ \sigma \rfloor_E$

3. SLIO*-app:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : (\tau_1 \to \tau_2) \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \tau_1}{\Sigma; \Psi; \Gamma \vdash e_1 \ e_2 : \tau_2}$$

Also given is $\mathcal{L} \models \Psi \ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma \ \sigma \rfloor_V$

To prove: $(\theta, n, (e_1 \ e_2) \ \delta) \in \lfloor \tau_2 \ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n.(e_1 \ e_2) \ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor \tau_2 \ \sigma \rfloor_V$

This means that given some $i < n$ s.t $(e_1 \ e_2) \ \delta \Downarrow_i v$

It suffices to prove

$(\theta, n - i, v) \in \lfloor \tau_2 \ \sigma \rfloor_V$ (FU-P0)

IH1:

$\forall j < n.e_1 \ \delta \Downarrow_j v_1 \implies (\theta, n - j, v_1) \in \lfloor (\tau_1 \to \tau_2) \ \sigma \rfloor_V$

Since we know that $(e_1 \ e_2) \ \delta \Downarrow_i v$ therefore $\exists j < i < n$ s.t $e_1 \ \delta \Downarrow_j v_1$. This means we have $(\theta, n - j, v_1) \in \lfloor (\tau_1 \to \tau_2) \ \sigma \rfloor_V$

From SLIO*-Sem-app we know that $v_1 = \lambda x.e'$.Therefore we have

$(\theta, n - j, \lambda x.e') \in \lfloor (\tau_1 \to \tau_2) \ \sigma \rfloor_V$ (FU-P1)

This means from Definition 2.6 we have

$$\forall \theta'' \sqsupseteq \theta \wedge I < (n - j), v.(\theta'', I, v) \in \lfloor \tau_1 \ \sigma \rfloor_V \implies (\theta'', I, e'[v/x]) \in \lfloor \tau_2 \ \sigma \rfloor_E \quad (78)$$

IH2:

$\forall k < (n - j).e_2 \ \delta \Downarrow_k v_2 \implies (\theta, n - j - k, v_2) \in \lfloor \tau_1 \ \sigma \rfloor_V$

Since we know that $(e_1 \ e_2) \ \delta \Downarrow_i v$ therefore $\exists k < i - j$ (since $i < n$ therefore $i - j < n - j$) s.t $e_2 \ \delta \Downarrow_k v_2$. This means we have

$(\theta, n - j - k, v_2) \in \lfloor \tau_1 \ \sigma \rfloor_V$ (FU-P2)

Instantiating Equation 78 with $\theta, (n - j - k), v_2$ and since we know that $(\theta, n - j - k, v_2) \in \lfloor \tau_1 \ \sigma \rfloor_V$ therefore we get

$(\theta, n - j - k, e'[v_2/x]) \in \lfloor \tau_2 \ \sigma \rfloor_E$

This means from Definition 2.7 we have

$\forall J < n - j - k.e'[v_2/x] \Downarrow_J v_f \implies (\theta, n - j - k - J, v_J) \in \lfloor \tau_2 \ \sigma \rfloor_E$

Since we know that $(e_1 \ e_2) \ \delta \Downarrow_i v$ therefore we know that $\exists J < i < n$ s.t $i = j + k + J$ (since $j + k + J < n$ therefore $J < n - j - k$) and $e'[v_2/x] \Downarrow_J v_f$

Therefore we have $(\theta, n - j - k - J, v_J) \in \lfloor \tau_2 \ \sigma \rfloor_E$

Since we know that $i = j + k + J$ and $v = v_J$ therefore we get $(\theta, n - i, v_J) \in \lfloor \tau_2 \ \sigma \rfloor_E$ (so FU-P0 is proved)

4. SLIO*-prod:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \tau_1 \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \tau_2}{\Sigma; \Psi; \Gamma \vdash (e_1, e_2) : (\tau_1 \times \tau_2)}$$

Also given is $\mathcal{L} \models \Psi \ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma \ \sigma \rfloor_V$

To prove: $(\theta, n, (e_1, e_2) \ \delta) \in \lfloor (\tau_1 \times \tau_2) \ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n.(e_1, e_2) \ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor (\tau_1 \times \tau_2) \ \sigma \rfloor_V$

This means that given some $i < n$ s.t $(e_1, e_2) \ \delta \Downarrow_i v$

<u>It suffices to prove</u>

$(\theta, n - i, v) \in \lfloor (\tau_1 \times \tau_2) \ \sigma \rfloor_V$ (FU-PA0)

<u>IH1</u>:

$\forall j < n.e_1 \ \delta \Downarrow_j v_1 \implies (\theta, n - j, v_1) \in \lfloor \tau_1 \ \sigma \rfloor_V$

Since we know that $(e_1, e_2) \ \delta \Downarrow_i v$ therefore $\exists j < i < n$ s.t $e_1 \ \delta \Downarrow_j v_1$. This means we have

$(\theta, n - j, v_1) \in \lfloor \tau_1 \ \sigma \rfloor_V$ (FU-PA1)

<u>IH2</u>:

$\forall k < (n - j).e_2 \ \delta \Downarrow_k v_2 \implies (\theta, n - j - k, v_2) \in \lfloor \tau_2 \ \sigma \rfloor_V$

Since we know that $(e_1 \ e_2) \ \delta \Downarrow_i v$ therefore $\exists k < i - j$ (since $i < n$ therefore $i - j < n - j$) s.t $e_2 \ \delta \Downarrow_k v_2$. This means we have

$(\theta, n - j - k, v_2) \in \lfloor \tau_2 \ \sigma \rfloor_V$ (FU-PA2)

In order to prove (FU-PA0) from SLIO*-Sem-prod we know that $i = j + k + 1$ and $v = (v_1, v_2)$ therefore from Definition 2.6 it suffices to prove

$(\theta, n - j - k - 1, v_1) \in \lfloor \tau_1 \ \sigma \rfloor_V$ and $(\theta, n - j - k - 1, v_2) \in \lfloor \tau_2 \ \sigma \rfloor_V$

We get this from (FU-PA1) and Lemma 2.16 and from (FU-PA2) and Lemma 2.16

5. SLIO*-fst:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : (\tau_1 \times \tau_2)}{\Sigma; \Psi; \Gamma \vdash \mathsf{fst}(e') : \tau_1}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \mathsf{fst}(e')\ \delta) \in \lfloor \tau_1\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n. \mathsf{fst}(e')\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor \tau_1\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $\mathsf{fst}(e')\ \delta \Downarrow_i v$

It suffices to prove

$(\theta, n - i, v) \in \lfloor \tau_1\ \sigma \rfloor_V$ (FU-F0)

IH1:

$\forall j < n. e'\ \delta \Downarrow_j (v_1, v_2) \implies (\theta, n - j, (v_1, v_2)) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V$

Since we know that $\mathsf{fst}(e')\ \delta \Downarrow_i v$ therefore $\exists j < i < n$ s.t $e'\ \delta \Downarrow_j (v_1, v_2)$. This means we have

$(\theta, n - j, (v_1, v_2)) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V$

From Definition 2.6 we know the following holds

$(\theta, n - j, v_1) \in \lfloor \tau_1\ \sigma \rfloor_V$ and $(\theta, n - j, v_2) \in \lfloor \tau_2\ \sigma \rfloor_V$ (FU-F1)

From SLIO*-Sem-fst we know that $v = v_1$ and $i = j + 1$. Therefore from (FU-F0), we are required to prove

$(\theta, n - j - 1, v_1) \in \lfloor \tau_1\ \sigma \rfloor_V$

We get this from (FU-F1) and Lemma 2.16

6. SLIO*-snd:

   Symmetric reasoning as in the SLIO*-fst case above

7. SLIO*-inl:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \tau_1}{\Sigma; \Psi; \Gamma \vdash \mathsf{inl}(e') : (\tau_1 + \tau_2)}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \mathsf{inl}(e')\ \delta) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n. \mathsf{inl}(e')\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $\mathsf{inl}(e')\ \delta \Downarrow_i v$

It suffices to prove

$(\theta, n - i, v) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V$ (FU-LE0)

IH1:

$\forall j < n. e'\ \delta \Downarrow_j v_1 \implies (\theta, n - j, v_1) \in \lfloor \tau_1\ \sigma \rfloor_V$

Since we know that $\mathsf{inl}(e')\ \delta \Downarrow_i v$ therefore $\exists j < i < n$ s.t $e'\ \delta \Downarrow_j v_1$. This means we have

$(\theta, n-j, v_1) \in \lfloor \tau_1\ \sigma \rfloor_V$ (FU-LE1)

From SLIO*-Sem-inl we know that $v = v_1$ and $i = j + 1$. Therefore from (FU-LE0) w we are required to prove

$(\theta, n-j-1, v_1) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V$

From Definition 2.6 it suffices to prove

$(\theta, n-j-1, v_1) \in \lfloor \tau_1\ \sigma \rfloor_V$

We get this from (FU-LE1) and Lemma 2.16

8. SLIO*-inr:

   Symmetric reasoning as in the SLIO*-inl case above

9. SLIO*-case:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_c : (\tau_1 + \tau_2) \qquad \Sigma; \Psi; \Gamma, x : \tau_1 \vdash e_1 : \tau \qquad \Sigma; \Psi; \Gamma, y : \tau_2 \vdash e_2 : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{case}(e, x.e_1, y.e_2) : \tau}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, (\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta) \in \lfloor \tau\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n.(\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor \tau\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $(\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta \Downarrow_i v$

It suffices to prove

$(\theta, n-i, v) \in \lfloor \tau\ \sigma \rfloor_V$ (FU-C0)

IH1:

$\forall j < n.e_c\ \delta \Downarrow_j v_c \implies (\theta, n-j, v_1) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V$

Since we know that $(\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta \Downarrow_i v$ therefore $\exists j < i < n$ s.t $e_c\ \delta \Downarrow_j v_c$. This means we have

$(\theta, n-j, v_c) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V$ (FU-C1)

2 cases arise:

(a) $v_c = \mathsf{inl}(v_l)$:

IH2:

$\forall k < (n-j).e_1\ \delta \cup \{x \mapsto v_l\} \Downarrow_k v_1 \implies (\theta, n-j-k, v_1) \in \lfloor \tau\ \sigma \rfloor_V$

Since we know that $(\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta \Downarrow_i v$ therefore $\exists k < i - j$ (since $i < n$ therefore $i - j < n - j$) s.t $e_1\ \delta \cup \{x \mapsto v_l\} \Downarrow_k v_1$. This means we have

$(\theta, n-j-k, v_1) \in \lfloor \tau\ \sigma \rfloor_V$ (FU-C2)

From SLIO*-Sem-case1 we know that $i = j + k + 1$ and $v = v_1$. Therefore from (FU-C0) it suffices to prove

$(\theta, n-j-k-1, v_1) \in \lfloor \tau\ \sigma \rfloor_V$

We get this from (FU-C2) and Lemma 2.16

(b) $v_c = \mathsf{inr}(v_r)$:
Symmetric reasoning as in the previous case

10. SLIO*-FI:

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash e' : \tau}{\Sigma; \Gamma \vdash \Lambda e' : \forall \alpha.\tau}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \Lambda e'\ \delta) \in \lfloor (\forall \alpha.(\ell_e, \tau))\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n. \Lambda e'\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $\lambda x.e'\ \delta \Downarrow_i v$

(from SLIO*-Sem-val we know that $v = \Lambda e'\ \delta$ and $i = 0$)

It suffices to prove

$(\theta, n, \Lambda e'\ \delta) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V$ (FU-FI0)

From Definition 2.6 it further suffices to prove

$\forall \theta'. \theta \sqsubseteq \theta', j < n. \forall \ell' \in \mathcal{L}. (\theta', j, e'\ \delta) \in \lfloor \tau[\ell'/\alpha] \rfloor_E$

This means given some $\theta', j, \ell' \in \mathcal{L}$ s.t $\theta' \sqsupseteq \theta$, $j < n$ (FU-FI1)

We are required to prove

$(\theta', j, (e'\ \delta)) \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_E$ (FU-FI2)

Since $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$ therefore from Lemma 2.18 we know that $(\theta, j, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$ where $j < n$ (from FU-L1)

IH: $(\theta', j, e'\ \delta) \in \lfloor \tau\ \sigma \cup \{\alpha \mapsto \ell'\} \rfloor_E$

(FU-FI2) is obtained directly from IH

11. SLIO*-CI:

$$\frac{\Sigma; \Psi, c; \Gamma \vdash e' : \tau}{\Sigma; \Gamma \vdash \nu\ e' : c \Rightarrow \tau}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \nu e'\ \delta) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n. \nu e'\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $\nu e'\ \delta \Downarrow_i v$

(from SLIO*-Sem-val we know that $v = \nu e'\ \delta$ and $i = 0$)

It suffices to prove

$(\theta, n, \nu e'\ \delta) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_V$ (FU-CI0)

From Definition 2.6 it further suffices to prove

$\mathcal{L} \models c \implies \forall \theta'.\theta \sqsubseteq \theta', j < n.(\theta', j, e'\ \delta) \in \lfloor \tau \rfloor_E$

This means given $\mathcal{L} \models c$ and some θ', j s.t $\theta' \sqsupseteq \theta$, $j < n$ (FU-CI1)

<u>We are required to prove</u>

$(\theta', j, (e'\ \delta)) \in \lfloor \tau\ \sigma \rfloor_E$ (FU-CI2)

Since $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$ therefore from Lemma 2.18 we know that $(\theta, j, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$ where $j < n$ (from FU-L1). Also we know that $\mathcal{L} \models c\ \sigma$ therefore $\mathcal{L} \models (\Sigma \cup \{c\})\ \sigma$

<u>IH</u>: $(\theta', j, e'\ \delta) \in \lfloor \tau\ \sigma \rfloor_E$

(FU-CI2) is obtained directly from IH

12. SLIO*-FE:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \forall \alpha.\tau \qquad \mathrm{FV}(\ell) \in \Sigma}{\Sigma; \Psi; \Gamma \vdash e'\ [] : \tau[\ell/\alpha]}$$

Also given is $\mathcal{L} \models \Psi\ \sigma\ \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, e'[]\ \delta) \in \lfloor \tau[\ell/\alpha]\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n.e'[]\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor \tau[\ell/\alpha]\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $e'[]\ \delta \Downarrow_i v$

<u>It suffices to prove</u>

$(\theta, n - i, v) \in \lfloor \tau[\ell/\alpha]\ \sigma \rfloor_V$ (FU-FE0)

<u>IH</u>: $(\theta, n, e'\ \delta) \in \lfloor \forall \alpha.\tau \rfloor_E$

From Definition 2.7 we know that

$\forall h_1 < n.e'\ \delta \Downarrow_{h_1} \Lambda e_{h1} \implies (\theta, n - h_1, \Lambda e_{h1}) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V$

Since $e'[]\ \delta$ reduces therefore we know that $\exists h_1 < i < n$ such that $e'\ \delta \Downarrow_{h_1} \Lambda e_i$

Therefore we know that $(\theta, n - h_1, \Lambda e_{h1}) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V$

From Definition 2.6 we know that

$\forall \theta'' \sqsupseteq \theta, x < (n - h_1), \ell_h \in \mathcal{L}.(\theta'', x, e_{h1}) \in \lfloor (\tau[\ell_h/\alpha])\ \sigma \rfloor_E$

Instantiating θ'' with θ, x with $n - h_1 - 1$ and ℓ_h with ℓ. So, we get

$(\theta, n - h_1 - 1, e_{h1}) \in \lfloor (\tau[\ell/\alpha])\ \sigma \rfloor_E$

From Definition 2.7 we know that the following holds

$\forall h_2 < n - h_1 - 1.e_{h1}\ \delta \Downarrow_{h_2} v \implies (\theta, n - h_1 - 1 - h_2, v) \in \lfloor (\tau[\ell/\alpha])\ \sigma \rfloor_V$

Since $e'[]\ \delta$ reduces in i steps therefore from SLIO*-Sem-FE we know that $(i = h_1 + h_2 + 1)$ and since we know that $i < n$ therefore we have $h_2 < n - h_1 - 1$ such that $e_{h1}\ \delta \Downarrow_{h_2} v$. Therefore we get

$(\theta, n - h_1 - 1 - h_2, v) \in \lfloor (\tau[\ell/\alpha])\ \sigma \rfloor_V$

Since $i = h_1 + h_2 + 1$ therefore we get

$(\theta, n - i, v) \in \lfloor (\tau[\ell/\alpha])\ \sigma \rfloor_V$

13. SLIO*-CE:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : c \Rightarrow \tau \qquad \Sigma; \Psi \vdash c}{\Sigma; \Psi; \Gamma \vdash e' \bullet : \tau}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, e' \bullet\ \ \delta) \in \lfloor \tau\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n.e' \bullet\ \ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor \tau\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $e' \bullet\ \ \delta \Downarrow_i v$

It suffices to prove

$(\theta, n - i, v) \in \lfloor \tau\ \sigma \rfloor_V$ (FU-CE0)

IH: $(\theta, n, e'\ \delta) \in \lfloor c \Rightarrow \tau\ \sigma \rfloor_E$

From Definition 2.7 we know that

$\forall h_1 < n.e'\ \delta \Downarrow_{h_1} \nu e_{h1} \implies (\theta, n - h_1, \nu e_{h1}) \in \lfloor c \Rightarrow \tau\ \sigma \rfloor_V$

Since $e' \bullet\ \ \delta$ reduces therefore we know that $\exists h_1 < i < n$ such that $e'\ \delta \Downarrow_{h_1} \nu e_{h_1}$

Therefore we know that $(\theta, n - h_1, \nu e_{h1}) \in \lfloor c \Rightarrow \tau\ \sigma \rfloor_V$

From Definition 2.6 we know that

$\mathcal{L} \models c\ \sigma \implies \forall \theta'' \sqsupseteq \theta, x < (n - h_1).(\theta'', x, e_{h1}) \in \lfloor \tau\ \sigma \rfloor_E$

Since we know that $\mathcal{L} \models c\ \sigma$ and then we instantiate θ'' with θ, x with $n - h_1 - 1$. So, we get

$(\theta, n - h_1 - 1, e_{h1}) \in \lfloor \tau\ \sigma \rfloor_E$

From Definition 2.7 we know that the following holds

$\forall h_2 < n - h_1 - 1.e_{h1}\ \delta \Downarrow_{h_2} v \implies (\theta, n - h_1 - 1 - h_2, v) \in \lfloor \tau\ \sigma \rfloor_V$

Since $e' \bullet\ \delta$ reduces in i steps therefore from SLIO*-Sem-CE we know that $(i = h_1 + h_2 + 1)$ and since we know that $i < n$ therefore we have $h_2 < n - h_1 - 1$ such that $e_{h1}\ \delta \Downarrow_{h_2} v$. Therefore we get

$(\theta, n - h_1 - 1 - h_2, v) \in \lfloor \tau\ \sigma \rfloor_V$

Since we know that $i = h_1 + h_2 + 1$ therefore we get

$(\theta, n - i, v) \in \lfloor \tau\ \sigma \rfloor_V$

14. SLIO*-ref:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \mathsf{Labeled}\ \ell'\ \tau \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash \mathsf{new}\ (e') : \mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau)}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \mathsf{new}\ (e')\ \delta) \in \lfloor \mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n.\mathsf{new}\ (e')\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor \mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $\mathsf{new}\ (e')\ \delta \Downarrow_i v$

(from SLIO*-Sem-val we know that $v = \mathsf{new}\ (e')\ \delta$ and $i = 0$)

<u>It suffices to prove</u>

$(\theta, n, \mathsf{new}\ (e')\ \delta) \in \lfloor \mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V$

From Definition 2.6 it suffices to prove

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, \mathsf{new}\ (e')\ \delta) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor (\mathsf{ref}\ \ell'\ \tau) \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$

This means given some $k \leq n, \theta_e \sqsupseteq \theta, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, \mathsf{new}\ (e')\ \delta) \Downarrow_j^f (H', v') \wedge j < k$.
Also from SLIO*-Sem-ref we know that $v' = a$

It suffices to prove

$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, a) \in \lfloor (\mathsf{ref}\ \ell'\ \tau) \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$ (FU-R0)

<u>IH</u>:

$(\theta_e, k, e'\ \delta) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_E$

From Definition 2.7 this means we have

$\forall l < k.e'\ \delta \Downarrow_l v_h \implies (\theta_e, n-l, v_h) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V$

Since we know that $(H, \mathsf{new}\ (e')) \Downarrow_j^f (H', a)$ therefore from SLIO*-Sem-ref we know that $\exists l < j < k$ s.t $e'\ \delta \Downarrow_l v_h$

Therefore we have

$(\theta_e, n-l, v_h) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V$ (FU-R2)

In order to prove (FU-R0) we choose θ' as $\theta_n = \theta_e \cup \{a \mapsto \mathsf{Labeled}\ \ell'\ \tau\}$

Now we need to prove:

(a) $(k-j, H') \triangleright \theta_n$:
From Definition 2.8 it suffices to prove that
$dom(\theta_n) \subseteq dom(H') \wedge \forall a \in dom(\theta_n).(\theta_n, (k-j)-1, H'(a)) \in \lfloor \theta_n(a) \rfloor_V$

- $dom(\theta_n) \subseteq dom(H')$:
  We know that $dom(H') = dom(H) \cup \{a\}$
  We know that $dom(\theta_n) = dom(\theta_e) \cup \{a\}$
  And $(k, H) \triangleright \theta_e$ therefore from Definition 2.8 we know that $dom(\theta_e) \subseteq dom(H)$
  So we are done
- $\forall a \in dom(\theta_n).(\theta_n, (k-j)-1, H'(a)) \in \lfloor \theta_n(a) \rfloor_V$:
  Since from (FU-R2) we know that $(\theta_h, n-l, v_h) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V$
  Since $\theta_h \sqsubseteq \theta_n$ and $k-j-1 < n-l$ (since $k < n$ and $l < j$) therefore from Lemma 2.16 we know that $(\theta_n, k-j-1, v_h) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V$

(b) $(\theta_n, k-j-1, a) \in \lfloor(\mathsf{ref}\ \ell'\ \tau)\rfloor_V$:
From Definition 2.6 it suffices to prove that $\theta_n(a) = \mathsf{Labeled}\ \ell'\ \tau$
We get this by construction of θ_n

(c) $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell')$:
Holds vacuously

(d) $(\forall a \in dom(\theta_n)\backslash dom(\theta_e).\theta_n(a) \searrow \ell)$:
From SLIO*-ref we know that $\ell \sqsubseteq \ell'$

15. SLIO*-deref:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \mathsf{ref}\ \ell\ \tau}{\Sigma; \Psi; \Gamma \vdash !e' : \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)}$$

Also given is $\mathcal{L} \models \Psi\ \sigma\ \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, (!e')\ \delta) \in \lfloor \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n.!(e')\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V$

(From SLIO*-Sem-val we know that $v = !e'\ \delta$ and $i = 0$)

This means that given some $i < n$ s.t $!e'\ \delta \Downarrow_i !e'\ \delta$

<u>It suffices to prove</u>

$(\theta, n, !e'\ \delta) \in \lfloor \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V$

From Definition 2.6 it suffices to prove

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, (!e'\ \delta)) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell''.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau' \wedge \ell' \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta_e).\theta'(a) \searrow \ell')$

This means given some $k \leq n, \theta_e \sqsupseteq \theta, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, (!e'\ \delta)) \Downarrow_j^f (H', v') \wedge j < k$.

It suffices to prove

$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell''.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau' \wedge \ell' \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta_e).\theta'(a) \searrow \ell')$ (FU-D0)

<u>IH</u>:

$(\theta_e, k, e'\ \delta) \in \lfloor(\mathsf{ref}\ \ell\ \tau)\ \sigma\rfloor_E$

From Definition 2.7 this means we have

$\forall l < k.e'\ \delta \Downarrow_l v_h \implies (\theta_e, k-l, v_h) \in \lfloor(\mathsf{ref}\ \ell\ \tau)\ \sigma\rfloor_V$

Since we know that $(H, !(e')) \Downarrow_j^f (H', a)$ therefore from SLIO*-Sem-deref we know that $\exists l < j < k$ s.t $e'\ \delta \Downarrow_l v_h,\ v_h = a$

Therefore we have

$(\theta_e, k-l, a) \in \lfloor(\mathsf{ref}\ \ell\ \tau)\ \sigma\rfloor_V$ (FU-D1)

In order to prove (FU-D0) we choose θ' as θ_e

Now we need to prove:

(a) $(k-j, H') \triangleright \theta_e$:
From Definition 2.8 it suffices to prove that
$dom(\theta_e) \subseteq dom(H') \wedge \forall a \in dom(\theta_e).(\theta_e, (k-j)-1, H'(a)) \in \lfloor \theta_e(a) \rfloor_V$

- $dom(\theta_e) \subseteq dom(H')$:
And $(k, H) \triangleright \theta_e$ therefore from Definition 2.8 we know that $dom(\theta_e) \subseteq dom(H)$
And since $H' = H$ (from SLIO*-Sem-deref) so we are done
- $\forall a \in dom(\theta_e).(\theta_e, (k-j)-1, H'(a)) \in \lfloor \theta_e(a) \rfloor_V$:
Since we know that $(k, H) \triangleright \theta_e$ therefore from Definition 2.8 we know that
$\forall a \in dom(\theta_e).(\theta_e, k-1, H(a)) \in \lfloor \theta_e(a) \rfloor_V$
Since $H' = H$ and from Lemma 2.16 we get
$\forall a \in dom(\theta_e).(\theta_e, (k-j)-1, H'(a)) \in \lfloor \theta_e(a) \rfloor_V$

(b) $(\theta_e, k-j, v') \in \lfloor (\mathsf{Labeled}\ \ell\ \tau) \rfloor_V$:
From SLIO*-Sem-deref we know that $H = H'$ and $v' = H(a)$
From (FU-D1) and Definition 2.6 we know that $\theta_e(a) = \mathsf{Labeled}\ \ell\ \tau$
Since we know that $(k, H) \triangleright \theta_e$ therefore from Definition 2.8 we know that
$\forall a \in dom(\theta_e).(\theta_e, k-1, H(a)) \in \lfloor \theta_e(a) \rfloor_V$
Since from SLIO*-Sem-deref we know that $j \geq 1$. Therefore from Lemma 2.16 we get
$(\theta_e, k-j, H(a)) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau) \rfloor_V$

(c) $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell \sqsubseteq \ell')$:
Holds vacuously

(d) $(\forall a \in dom(\theta_e) \backslash dom(\theta_e).\theta_e(a) \searrow \ell)$:
Holds vacuously

16. SLIO*-assign:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \mathsf{ref}\ \ell'\ \tau \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \mathsf{Labeled}\ \ell'\ \tau \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash e_1 := e_2 : \mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit}}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, (e_1 := e_2)\ \delta) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit})\ \sigma \rfloor_E^{pc}$

This means that from Definition 1.7 we need to prove

$\forall i < n.(e_1 := e_2)\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit})\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $(e_1 := e_2)\ \delta \Downarrow_i v$.

<u>It suffices to prove</u>

$(\theta, n-i, ()) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit})\ \sigma \rfloor_V$

From Definition 2.6 it suffices to prove

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, (e_1 := e_2)\ \delta) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor (\mathsf{ref}\ \ell'\ \tau) \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$

This means given some $k \leq n, \theta_e \sqsupseteq \theta, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, (e_1 := e_2)\ \delta) \Downarrow_j^f (H', v') \wedge j < k$. Also from SLIO*-Sem-assign we know that $v' = ()$

It suffices to prove

$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, ()) \in \lfloor \mathsf{unit} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$ (FU-A0)

IH1:

$\forall l < k.e_1\ \delta \Downarrow_l v_1 \implies (\theta, k-l, a) \in \lfloor (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V$

Since we know that $(e_1 := e_2)\ \delta \Downarrow_j^f v$ therefore $\exists l < j < k$ s.t $e_1\ \delta \Downarrow_l a$. This means we have

$(\theta, k-l, a) \in \lfloor (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V$ (FU-A1)

IH2:

$\forall m < (k-l).e_2\ \delta \Downarrow_m v_2 \implies (\theta, k-l-m, v_2) \in \lfloor \mathsf{Labeled}\ \ell'\ \tau\ \sigma \rfloor_V$

Since we know that $(e_1 := e_2)\ \delta \Downarrow_j^f v$ therefore $\exists m < j-l$ (since $j < k$ therefore $j-l < k-l$) s.t $e_2\ \delta \Downarrow_k v_2$. This means we have

$(\theta, k-l-m, v_2) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V$ (FU-A2)

In order to prove (FU-A0) we choose θ' as θ_e

Now we need to prove:

(a) $(k-j, H') \triangleright \theta_e$:
From Definition 2.8 it suffices to prove that
$dom(\theta_e) \subseteq dom(H') \wedge \forall a \in dom(\theta_e).(\theta_e, (k-j)-1, H'(a)) \in \lfloor \theta_e(a) \rfloor_V$

- $dom(\theta_e) \subseteq dom(H')$:
  We know that $dom(H') = dom(H)$
  And $(k, H) \triangleright \theta_e$ therefore from Definition 2.8 we know that $dom(\theta_e) \subseteq dom(H)$
  So we are done
- $\forall a \in dom(\theta_e).(\theta_e, (k-j)-1, H'(a)) \in \lfloor \theta_e(a) \rfloor_V$:
  $\forall a \in dom(\theta_e)$.
  i. $H(a) = H'(a)$:
     Since $(k, H) \triangleright \theta_e$ therefore from Definition 2.8 we know that
     $(\theta_e, k-1, H(a)) \in \lfloor \theta_e(a) \rfloor_V$
     Therefore from Lemma 2.16 we get
     $(\theta_e, k-1-j, H(a)) \in \lfloor \theta_e(a) \rfloor_V$
  ii. $H(a) \neq H'(a)$:
     From SLIO*-Sem-assign we know that $H'(a) = v_2$
     From (FU-A1) we know that $\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau$
     Also we know that $j = l + m + 1$
     Since from (FU-A2) we know that
     $(\theta, k-l-m, v_2) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V$
     Therefore we get
     $(\theta, k-j+1, v_2) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V$
     Therefore from Lemma 2.16 we get
     $(\theta, k-j-1, v_2) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V$

(b) $(\theta_e, k-j-1, ()) \in \lfloor \mathsf{unit} \rfloor_V$:
From Definition 2.6

(c) $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell \sqsubseteq \ell')$:
From SLIO*-assign we know that $\ell \sqsubseteq \ell'$

(d) $(\forall a \in dom(\theta_e) \backslash dom(\theta_e).\theta_e(a) \searrow \ell)$:
Holds vacuously

17. SLIO*-label:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{Lb}(e') : \mathsf{Labeled}\ \ell\ \tau}$$

Also given is $\mathcal{L} \models \Psi\ \sigma\ \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$
To prove: $(\theta, n, \mathsf{Lb}(e')\ \delta) \in \lfloor \mathsf{Labeled}\ \ell\ \tau\ \sigma \rfloor_E$
This means that from Definition 2.7 we need to prove
$\forall i < n.\mathsf{Lb}(e')\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor \mathsf{Labeled}\ \ell\ \tau\ \sigma \rfloor_V$

This means we are given some $i < n$ s.t $\mathsf{Lb}(e')\ \delta \Downarrow_i v$ and we are required to prove $(\theta, n-i, v) \in \lfloor \mathsf{Labeled}\ \ell\ \tau\ \sigma \rfloor_V$

Let $v = \mathsf{Lb}(v_i)$. This means from Definition 2.6 we are required to prove $(\theta, n-i, v_i) \in \lfloor \tau\ \sigma \rfloor_V$

<u>IH</u>: $(\theta, n, e'\ \delta) \in \lfloor \tau\ \sigma \rfloor_E$

This means from Definition 2.7 we have
$\forall j < n.e'\ \delta \Downarrow_j v_i \implies (\theta, n-j, v_i) \in \lfloor \tau\ \sigma \rfloor_V$

Since we know that $\mathsf{Lb}(e')\ \delta \Downarrow_i v$ therefore $\exists j < i < n$ s.t $e'\ \delta \Downarrow_j v_i$
Therefore we have $(\theta, n-j, v_i) \in \lfloor \tau\ \sigma \rfloor_V$

From SLIO*-Sem-label we know that $i = j + 1$ therefore from Lemma 2.16 we have $(\theta, n-i, v_i) \in \lfloor \tau\ \sigma \rfloor_V$

18. SLIO*-unlabel:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \mathsf{Labeled}\ \ell\ \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{unlabel}(e') : \mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau}$$

Also given is $\mathcal{L} \models \Psi\ \sigma\ \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$
To prove: $(\theta, n, \mathsf{unlabel}(e')\ \delta) \in \lfloor (\mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau)\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove
$\forall i < n.\mathsf{unlabel}(e')\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor (\mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau)\ \sigma \rfloor_V$
This means that given some $i < n$ s.t $\mathsf{unlabel}(e')\ \delta \Downarrow_i v$
(from SLIO*-Sem-val we know that $v = \mathsf{unlabel}(e')\ \delta$ and $i = 0$)
<u>It suffices to prove</u>

$(\theta, n, \mathsf{unlabel}(e')\ \delta) \in \lfloor(\mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau)\ \sigma\rfloor_V$

From Definition 2.6 it suffices to prove

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \rhd \theta_e \wedge (H, \mathsf{unlabel}(e')\ \delta) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \rhd \theta' \wedge (\theta', k-j, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$

This means given some $k \leq n, \theta_e \sqsupseteq \theta, H, j$ s.t $(k, H) \rhd \theta_e \wedge (H, \mathsf{unlabel}(e')\ \delta) \Downarrow_j^f (H', v') \wedge j < k$. Also from SLIO*-Sem-unlabel we know that $H' = H$

It suffices to prove

$\exists \theta' \sqsupseteq \theta_e.(k-j, H) \rhd \theta' \wedge (\theta', k-j, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$ (FU-U0)

<u>IH</u>:

$(\theta_e, k, e'\ \delta) \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall h_1 < k.e'\ \delta \Downarrow_{h_1} v_h \implies (\theta_e, k - h_1, v_h) \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_V$

Since we know that $(H, \mathsf{unlabel}(e')) \Downarrow_j^f (H, v')$ therefore from SLIO*-Sem-unlabel we know that

$\exists h_1 < j < k$ s.t $e'\ \delta \Downarrow_{h_1} \mathsf{Lb} v'$

This means we have

$(\theta_e, k - h_1, \mathsf{Lb} v') \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_V$

This means from Definition 2.6 we have

$(\theta_e, k - h_1, v') \in \lfloor \tau\ \sigma \rfloor_V$ (FU-U1)

In order to prove (FU-U0) we choose θ' as θ_e. And we a required to prove:

(a) $(k-j, H) \rhd \theta_e$:
Since have $(k, H) \rhd \theta_e$ therefore from Lemma 2.20 we get $(k-j, H) \rhd \theta_e$

(b) $(\theta', k-j, v') \in \lfloor \tau\ \sigma \rfloor_V$:
Since from (FU-U1) we know that $(\theta_e, k - h_1, v') \in \lfloor \tau\ \sigma \rfloor_V$
And since $j = h_1 + 1$, therefore from Lemma 2.16 we get $(\theta_e, k - j, v') \in \lfloor \tau\ \sigma \rfloor_V$

(c) $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell')$:
Holds vacuously

(d) $(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$:
Holds vacuously

19. SLIO*-ret:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{ret}(e') : \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \mathsf{ret}(e')\ \delta) \in \lfloor \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n.\mathsf{ret}(e')\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau\ \sigma \rfloor_V$

This means we are given some $i < n$ s.t $\mathsf{ret}(e')\ \delta \Downarrow_i v$ and we are required to prove $(\theta, n - i, v) \in \lfloor \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau\ \sigma \rfloor_V$

(from SLIO*-Sem-val we know that $v = \mathsf{ret}(e')\ \delta$ and $i = 0$)

<u>It suffices to prove</u>

$(\theta, n, \mathsf{ret}(e')\ \delta) \in \lfloor \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau\ \sigma \rfloor_V$

From Definition 2.6 it suffices to prove

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, \mathsf{ret}(e')\ \delta) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$

This means given some $k \leq n, \theta_e \sqsupseteq \theta, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, \mathsf{ret}(e')\ \delta) \Downarrow_j^f (H', v') \wedge j < k$.
Also from SLIO*-Sem-ret we know that $H' = H$

It suffices to prove

$\exists \theta' \sqsupseteq \theta_e.(k - j, H) \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$ (FU-R0)

<u>IH</u>:

$(\theta_e, k, e'\ \delta) \in \lfloor \tau\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall h_1 < k.e'\ \delta \Downarrow_{h_1} v_h \implies (\theta_e, k - h_1, v_h) \in \lfloor \tau\ \sigma \rfloor_V$

Since we know that $(H, \mathsf{unlabel}(e')) \Downarrow_j^f (H, v')$ therefore from SLIO*-Sem-ret we know that $\exists h_1 < j < k$ s.t $e'\ \delta \Downarrow_{h_1} v'$

This means we have

$(\theta_e, k - h_1, v') \in \lfloor \tau\ \sigma \rfloor_V$ (FU-R1)

In order to prove (FU-U0) we choose θ' as θ_e. And we a required to prove:

(a) $(k - j, H) \triangleright \theta_e$:
Since have $(k, H) \triangleright \theta_e$ therefore from Lemma 2.20 we get $(k - j, H) \triangleright \theta_e$

(b) $(\theta', k - j, v') \in \lfloor \tau\ \sigma \rfloor_V$:
Since from (FU-R1) we know that $(\theta_e, k - h_1, v') \in \lfloor \tau\ \sigma \rfloor_V$
And since $j = h_1 + 1$, therefore from Lemma 2.16 we get $(\theta_e, k - j, v') \in \lfloor \tau\ \sigma \rfloor_V$

(c) $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell')$:
Holds vacuously

(d) $(\forall a \in dom(\theta')\backslash dom(\theta_e).\theta'(a) \searrow \ell)$:
Holds vacuously

20. SLIO*-bind:

$$\frac{\Sigma;\Psi;\Gamma \vdash e_1 : \mathbb{SLIO}\ \ell_i\ \ell\ \tau \qquad \Sigma;\Psi;\Gamma, x:\tau \vdash e_2 : \mathbb{SLIO}\ \ell\ \ell_o\ \tau'}{\Sigma;\Psi;\Gamma \vdash \mathsf{bind}(e_1, x.e_2) : \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau'}$$

Also given is $\mathcal{L} \models \Psi\ \sigma\ \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \mathsf{bind}(e_1, x.e_2)\ \delta) \in \lfloor \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau'\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n.\mathsf{bind}(e_1, x.e_2)\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau'\ \sigma \rfloor_V$

This means we are given some $i < n$ s.t $\mathsf{bind}(e_1, x.e_2)\ \delta \Downarrow_i v$ and we are required to prove $(\theta, n-i, v) \in \lfloor \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau'\ \sigma \rfloor_V$

(from SLIO*-Sem-val we know that $v = \mathsf{bind}(e_1, x.e_2)\ \delta$ and $i = 0$)

Therefore we need to prove

$(\theta, n, v) \in \lfloor \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau'\ \sigma \rfloor_V$

From Definition 2.6 it suffices to prove

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, \mathsf{bind}(e_1, x.e_2)\ \delta) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta_e).\theta'(a) \searrow \ell)$

This means we are given some $k \leq n, \theta_e \sqsupseteq \theta, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, \mathsf{bind}(e_1, x.e_2)\ \delta) \Downarrow_j^f (H', v') \wedge j < k$.

It suffices to prove

$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta_e).\theta'(a) \searrow \ell)$ (FU-B0)

<u>IH1</u>:

$(\theta_e, k, e_1\ \delta) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell\ \tau)\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall h_1 < k.e_1\ \delta \Downarrow_{h_1} v_1 \implies (\theta_e, k-h_1, v_1) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell\ \tau)\ \sigma \rfloor_V$

Since we know that $(H, \mathsf{bind}(e_1, x.e_2)) \Downarrow_j^f (H_1, v_1)$ therefore from SLIO*-Sem-bind we know that

$\exists h_1 < j < k$ s.t $e_1\ \delta \Downarrow_{h_1} v_1$

This means we have

$(\theta_e, k-h_1, v_1) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell\ \tau)\ \sigma \rfloor_V$

From Definition 2.6 we know that

$\forall k_{h1} \leq (k-h_1), \theta'_e \sqsupseteq \theta_e, H, J.(k_{h1}, H) \rhd \theta'_e \wedge (H, v_1) \Downarrow^f_J (H', v'_{h1}) \wedge J < k_{h1} \implies$
$\exists \theta'' \sqsupseteq \theta'_e.(k_{h1} - J, H') \rhd \theta'' \wedge (\theta'', k_{h1} - J, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta'_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'') \backslash dom(\theta'_e).\theta''(a) \searrow \ell)$

Instantiating k_{h1} with $k-h_1$, θ'_e with θ_e. Since we know that $(H, \mathsf{bind}(e_1, x.e_2)) \Downarrow^f_j (H_1, v_1)$ therefore $\exists J < j - h_1 < k - h_1$ s.t $(H, v_1) \Downarrow^f_J (H', v'_{h1})$. And since we already knwo that $(k, H) \rhd \theta_e$ therefore from Lemma 2.20 we get $(k - h_1, H) \rhd \theta_e$

This means we have

$\exists \theta'' \sqsupseteq \theta_e.(k_{h1} - J, H') \rhd \theta'' \wedge (\theta'', k_{h1} - J, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'') \backslash dom(\theta_e).\theta''(a) \searrow \ell)$ (FU-B1)

<u>IH2</u>:

$(\theta'', k - h_1 - J, e_2\ \delta \cup \{x \mapsto v'\}) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell\ \tau')\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall h_2 < k - h_1 - J.e_2\ \delta \cup \{x \mapsto v'\} \Downarrow_{h_2} v'' \implies (\theta'', k - h_1 - J - h_2, v'') \in \lfloor (\mathbb{SLIO}\ \ell\ \ell_o\ \tau')\ \sigma \rfloor_V$

Since we know that $(H, \mathsf{bind}(e_1, x.e_2)) \Downarrow^f_j (H, v_1)$ therefore from SLIO*-Sem-bind we know that

$\exists h_2 < j - h_1 - J < k - h_1 - J$ s.t $e_2\ \delta \cup \{x \mapsto v'\} \Downarrow_{h_2} v''$

This means we have

$(\theta'', k - h_1 - J - h_2, v'') \in \lfloor (\mathbb{SLIO}\ \ell\ \ell_o\ \tau')\ \sigma \rfloor_V$

From Definition 2.6 we know that

$\forall k_{h2} \leq (k - h_1 - J - h_2), \theta'_e \sqsupseteq \theta'', H, J'.(k_{h2}, H) \rhd \theta'_e \wedge (H, v'') \Downarrow^f_{J'} (H'', v'_{h2}) \wedge J' < k_{h2} \implies$
$\exists \theta''' \sqsupseteq \theta'_e.(k_{h2} - J', H'') \rhd \theta''' \wedge (\theta''', k_{h2} - J', v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H''(a) \implies \exists \ell'.\theta'_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta''') \backslash dom(\theta'_e).\theta'''(a) \searrow \ell)$

Since we know that $(H, \mathsf{bind}(e_1, x.e_2)) \Downarrow^f_j (H_1, v_1)$ therefore $\exists v_{h2}, i$ s.t $(v'' \Downarrow_i v_{h2})$. From SLIO*-Sem-val we know that $v_{h2} = v''$ and $i = 0$. Instantiating k_{h2} with $k - h_1 - J - h_2$, θ'_e with θ'', H with H' (from FU-B1) and $\exists J' < j - h_1 - J - h_2 < k - h_1 - J - h_2$ s.t $(H', v_{h2}) \Downarrow^f_J (H'', v'_{h2})$. And since we already know that $(k - h_1, H') \rhd \theta''$ therefore from Lemma 2.20 we get $(k - h_1 - J - h_2, H') \rhd \theta''$

This means we have

$\exists \theta''' \sqsupseteq \theta'_e.(k_{h2} - J', H'') \rhd \theta''' \wedge (\theta''', k_{h2} - J', v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H''(a) \implies \exists \ell'.\theta'_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta''') \backslash dom(\theta'_e).\theta'''(a) \searrow \ell)$ (FU-B2)

We get (FU-B0) by choosing θ' as θ'' (from FU-B2)

21. SLIO*-toLabeled:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{toLabeled}(e') : \mathbb{SLIO}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau)}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \mathsf{toLabeled}(e')\ \delta) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell_i\ \mathsf{Labeled}\ \ell_o\ \tau)\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall i < n. \mathsf{toLabeled}(e')\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell_i\ \mathsf{Labeled}\ \ell_o\ \tau)\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $\mathsf{toLabeled}(e')\ \delta \Downarrow_i v$

(from SLIO*-Sem-val we know that $v = \mathsf{toLabeled}(e')\ \delta$ and $i = 0$)

It suffices to prove

$(\theta, n, \mathsf{toLabeled}(e')\ \delta) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell_i\ \mathsf{Labeled}\ \ell_o\ \tau)\ \sigma \rfloor_V$

From Definition 2.6 it suffices to prove

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \rhd \theta_e \wedge (H, \mathsf{toLabeled}(e')\ \delta) \Downarrow^f_j (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \rhd \theta' \wedge (\theta', k - j, v') \in \lfloor (\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma \rfloor_V \wedge$
$(\forall a. H(a) \neq H'(a) \implies \exists \ell'. \theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e). \theta'(a) \searrow \ell)$

And given some $k \leq n, \theta_e \sqsupseteq \theta, H, j$ s.t $(k, H) \rhd \theta_e \wedge (H, \mathsf{toLabeled}(e')\ \delta) \Downarrow^f_j (H', v') \wedge j < k$.
Also from SLIO*-Sem-tolabeled we know that $H' = H$

It suffices to prove

$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \rhd \theta' \wedge (\theta', k - j, v') \in \lfloor (\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma \rfloor_V \wedge$
$(\forall a. H(a) \neq H'(a) \implies \exists \ell'. \theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e). \theta'(a) \searrow \ell)$ (FU-TL0)

IH:

$(\theta_e, k, e'\ \delta) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau)\ \sigma \rfloor_E$

This means that from Definition 2.7 we need to prove

$\forall h_1 < k. e'\ \delta \Downarrow_{h_1} v_1 \implies (\theta, k - h_1, v_1) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau)\ \sigma \rfloor_V$

Since $H, \mathsf{toLabeled}(e') \Downarrow^f_j H', v'$ therefore from SLIO*-Sem-tolabeled we know that $\exists h_1 < j < k$ s.t $e'\ \delta \Downarrow_{h_1} v_1$

Therefore we get $(\theta, k - h_1, v_1) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau)\ \sigma \rfloor_V$

From Definition 2.6 we know that

$\forall k_{h1} \leq (k - h_1), \theta'_e \sqsupseteq \theta_e, H_h, J.(k_{h1}, H_h) \rhd \theta'_e \wedge (H_h, v_1) \Downarrow^f_J (H', v'_{h1}) \wedge J < k_{h1} \implies$
$\exists \theta'' \sqsupseteq \theta'_e.(k_{h1} - J, H') \rhd \theta'' \wedge (\theta'', k_{h1} - J, v_1) \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a. H_h(a) \neq H'(a) \implies \exists \ell'. \theta'_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'') \backslash dom(\theta'_e). \theta''(a) \searrow \ell)$

Instantiating k_{h1} with $k - h_1$, H_h with H, θ'_e with θ_e. Since we know that $(H, \mathsf{toLabeled}(e')) \Downarrow^f_j (H', v_1)$ therefore $\exists J < j - h_1 < k - h_1$ s.t $(H, v_1) \Downarrow^f_J (H', v'_{h1})$. And since we already knwo that $(k, H) \rhd \theta_e$ therefore from Lemma 2.20 we get $(k - h_1, H) \rhd \theta_e$

This means we have
$\exists\theta'' \sqsupseteq \theta'_e.(k - h_1 - J, H') \triangleright \theta'' \wedge (\theta'', k - h1 - J, v_1) \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists\ell'.\theta'_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'')\backslash dom(\theta'_e).\theta''(a) \searrow \ell)$ (FU-TL1)

In order to prove (FU-TL0) we choose θ' as θ''. Now we need to prove the following

(a) $(k - j, H') \triangleright \theta''$:
Since $(k - h_1 - J, H') \triangleright \theta''$ and $j = h_1 + J + 1$ therefore from Lemma 2.20 we get $(k - j, H') \triangleright \theta''$

(b) $(\theta'', k - j - 1, v') \in \lfloor(\mathsf{Labeled}\ \ell_o\ \tau\ \sigma)\rfloor_V$:
From SLIO*-Sem-tolabeled we know that $v' = \mathsf{toLabeled}(v_1)$
From Definition 2.4 it suffices to prove that $(\theta'', k - j - 1, v_1) \in \lfloor \tau\ \sigma \rfloor_V$

We get this from (FU-TL1) and Lemma 2.16

(c) $(\forall a.H(a) \neq H'(a) \implies \exists\ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell')$:
Directly from (FU-TL1)

(d) $(\forall a \in dom(\theta_n)\backslash dom(\theta_e).\theta_n(a) \searrow \ell)$:
Directly from (FU-TL1)

□

Lemma 2.23 (SLIO*: Subtyping unary)**.** *The following holds:*
$\forall\Sigma, \Psi, \sigma, \tau, \tau'.$

1. $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor(\tau\ \sigma)\rfloor_V \subseteq \lfloor(\tau'\ \sigma)\rfloor_V$

2. $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor(\tau\ \sigma)\rfloor_E \subseteq \lfloor(\tau'\ \sigma)\rfloor_E$

Proof. Proof of Statement (1)
Proof by induction on $\tau <: \tau'$

1. SLIO*sub-arrow:

Given:
$$\frac{\Sigma; \Psi \vdash \tau'_1 <: \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau'_2}{\Sigma; \Psi \vdash \tau_1 \to \tau_2 <: \tau'_1 \to \tau'_2}$$

To prove: $\lfloor((\tau_1 \to \tau_2)\ \sigma)\rfloor_V \subseteq \lfloor((\tau'_1 \to \tau'_2)\ \sigma)\rfloor_V$

IH1: $\lfloor(\tau'_1\ \sigma)\rfloor_V \subseteq \lfloor(\tau_1\ \sigma)\rfloor_V$ (Statement (1))
$\lfloor(\tau_2\ \sigma)\rfloor_E \subseteq \lfloor(\tau'_2\ \sigma)\rfloor_E$ (Sub-A0, From Statement (2))
It suffices to prove: $\forall(\theta, n, \lambda x.e_i) \in \lfloor((\tau_1 \to \tau_2)\ \sigma)\rfloor_V.\ (\theta, n, \lambda x.e_i) \in \lfloor((\tau'_1 \to \tau'_2)\ \sigma)\rfloor_V$

This means that given some θ, n and $\lambda x.e_i$ s.t $(\theta, n, \lambda x.e_i) \in \lfloor((\tau_1 \to \tau_2)\ \sigma)\rfloor_V$
Therefore from Definition 2.6 we are given:

$$\exists\theta_1.\theta \sqsubseteq \theta_1 \wedge \forall i < n.\forall v.(\theta_1, i, v) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta_1, i, e_i[v/x]) \in \lfloor \tau_2\ \sigma \rfloor_E \qquad (79)$$

And it suffices to prove: $(\theta, n, \lambda x.e_i) \in \lfloor((\tau_1' \to \tau_2')\ \sigma)\rfloor_V$

Again from Definition 2.6, it suffices to prove:
$\exists \theta_2.\theta \sqsubseteq \theta_2 \wedge \forall j < n.\forall v.(\theta_2, j, v) \in \lfloor \tau_1'\ \sigma \rfloor_V \implies (\theta_2, j, e_i[v/x]) \in \lfloor \tau_2'\ \sigma \rfloor_E$

This means that given some $\theta_2, j < n, v$ s.t $\theta \sqsubseteq \theta_2$ and $(\theta_2, j, v) \in \lfloor \tau_1'\ \sigma \rfloor_V$
And we are required to prove: $(\theta_2, j, e_i[v/x]) \in \lfloor \tau_2'\ \sigma \rfloor_E$

Since $(\theta_2, j, v) \in \lfloor \tau_1'\ \sigma \rfloor_V$ therefore from IH1 we know that $(\theta_2, j, v) \in \lfloor \tau_1\ \sigma \rfloor_V$
As a result from Equation 79 we know that
$(\theta_2, j, e_i[v/x]) \in \lfloor \tau_2\ \sigma \rfloor_E$
From (Sub-A0), we know that
$(\theta_2, j, e_i[v/x]) \in \lfloor \tau_2'\ \sigma \rfloor_E$

2. SLIO*sub-prod:
Given:

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}$$

To prove: $\lfloor((\tau_1 \times \tau_2)\ \sigma)\rfloor_V \subseteq \lfloor((\tau_1' \times \tau_2')\ \sigma)\rfloor_V$

IH1: $\lfloor(\tau_1\ \sigma)\rfloor_V \subseteq \lfloor(\tau_1'\ \sigma)\rfloor_V$ (Statement (1))
IH2: $\lfloor(\tau_2\ \sigma)\rfloor_V \subseteq \lfloor(\tau_2'\ \sigma)\rfloor_V$ (Statement (1))
It suffices to prove: $\forall(\theta, n, (v_1, v_2)) \in \lfloor((\tau_1 \times \tau_2)\ \sigma)\rfloor_V.\ (\theta, n, (v_1, v_2)) \in \lfloor((\tau_1' \times \tau_2')\ \sigma)\rfloor_V$

This means that given some θ, n and $(v_1, v_2\ (\theta, (v_1, v_2)) \in \lfloor((\tau_1 \times \tau_2)\ \sigma)\rfloor_V$
Therefore from Definition 2.6 we are given:

$$(\theta, n, v_1) \in \lfloor \tau_1\ \sigma \rfloor_V \wedge (\theta, n, v_2) \in \lfloor \tau_2\ \sigma \rfloor_V \tag{80}$$

And it suffices to prove: $(\theta, (v_1, v_2)) \in \lfloor((\tau_1' \times \tau_2')\ \sigma)\rfloor_V$

Again from Definition 2.6, it suffices to prove:
$(\theta, n, v_1) \in \lfloor \tau_1'\ \sigma \rfloor_V \wedge (\theta, n, v_2) \in \lfloor \tau_2'\ \sigma \rfloor_V$

Since from Equation 80 we know that $(\theta, n, v_1) \in \lfloor \tau_1\ \sigma \rfloor_V$ therefore from IH1 we have $(\theta, n, v_1) \in \lfloor \tau_1'\ \sigma \rfloor_V$
Similarly since $(\theta, n, v_2) \in \lfloor \tau_2\ \sigma \rfloor_V$ from Equation 80 therefore from IH2 we have $(\theta, n, v_2) \in \lfloor \tau_2'\ \sigma \rfloor_V$

3. SLIO*sub-sum:

   Given:
$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'}$$

   To prove: $\lfloor((\tau_1 + \tau_2)\ \sigma)\rfloor_V \subseteq \lfloor((\tau_1' + \tau_2')\ \sigma)\rfloor_V$

   IH1: $\lfloor(\tau_1\ \sigma)\rfloor_V \subseteq \lfloor(\tau_1'\ \sigma)\rfloor_V$ (Statement (1))
   IH2: $\lfloor(\tau_2\ \sigma)\rfloor_V \subseteq \lfloor(\tau_2'\ \sigma)\rfloor_V$ (Statement (1))
   It suffices to prove: $\forall(\theta, n, v_s) \in \lfloor((\tau_1 + \tau_2)\ \sigma)\rfloor_V.\ (\theta, v_s) \in \lfloor((\tau_1' + \tau_2')\ \sigma)\rfloor_V$

   This means that given: $(\theta, n, v_s) \in \lfloor((\tau_1 + \tau_2)\ \sigma)\rfloor_V$
   And it suffices to prove: $(\theta, n, v_s) \in \lfloor((\tau_1' + \tau_2')\ \sigma)\rfloor_V$

   2 cases arise

   (a) $v_s = \mathsf{inl}\ v_i$:
   From Definition 2.6 we are given:
$$(\theta, n, v_i) \in \lfloor\tau_1\ \sigma\rfloor_V \tag{81}$$
   And we are required to prove that:
   $(\theta, n, v_i) \in \lfloor\tau_1'\ \sigma\rfloor_V$
   From Equation 81 and IH1 we know that
   $(\theta, n, v_i) \in \lfloor\tau_1'\ \sigma\rfloor_V$

   (b) $v_s = \mathsf{inr}\ v_i$:
   From Definition 2.6 we are given:
$$(\theta, n, v_i) \in \lfloor\tau_2\ \sigma\rfloor_V \tag{82}$$
   And we are required to prove that:
   $(\theta, n, v_i) \in \lfloor\tau_2'\ \sigma\rfloor_V$
   From Equation 82 and IH2 we know that
   $(\theta, n, v_i) \in \lfloor\tau_2'\ \sigma\rfloor_V$

4. SLIO*sub-forall:

   Given:
$$\frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash \forall\alpha.\tau_1 <: \forall\alpha.\tau_2}$$

   To prove: $\lfloor((\forall\alpha.\tau_1)\ \sigma)\rfloor_V \subseteq \lfloor(\forall\alpha.\tau_2)\ \sigma\rfloor_V$

   It suffices to prove: $\forall(\theta, n, \Lambda e_i) \in \lfloor((\forall\alpha.\tau_1)\ \sigma)\rfloor_V.\ (\theta, n, \Lambda e_i) \in \lfloor((\forall\alpha.\tau_2)\ \sigma)\rfloor_V$

   This means that given: $(\theta, n, \Lambda e_i) \in \lfloor((\forall\alpha.\tau_1)\ \sigma)\rfloor_V$
   Therefore from Definition 2.6 we are given:

$$\exists \theta_1.\theta \sqsubseteq \theta_1 \wedge \forall i < n.\forall \ell' \in \mathcal{L} \implies (\theta_1, i, e_i) \in \lfloor \tau_1\ (\sigma \cup [\alpha \mapsto \ell']) \rfloor_E \tag{83}$$

And it suffices to prove: $(\theta, n, \Lambda e_i) \in \lfloor ((\forall \alpha.\tau_2)\ \sigma) \rfloor_V$

Again from Definition 2.6, it suffices to prove:
$\exists \theta_2.\theta \sqsubseteq \theta_2 \wedge \forall j < n.\forall \ell' \in \mathcal{L} \implies (\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma \cup [\alpha \mapsto \ell']) \rfloor_E$

This means that given some $\theta_2, j < n, \ell' \in \mathcal{L}$ s.t $\theta \sqsubseteq \theta_2$
And we are required to prove: $(\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma \cup [\alpha \mapsto \ell']) \rfloor_E$

Since we are given $\theta \sqsubseteq \theta_2 \wedge j < n \wedge \ell' \in \mathcal{L}$ therefore from Equation 83 we have
$(\theta_2, j, e_i) \in \lfloor \tau_1\ (\sigma \cup [\alpha \mapsto \ell']) \rfloor_E$

$\lfloor (\tau_1\ (\sigma \cup [\alpha \mapsto \ell'])) \rfloor_E \subseteq \lfloor (\tau_2\ (\sigma \cup [\alpha \mapsto \ell'])) \rfloor_E$ (Sub-F0, Statement (2))

From (Sub-F0), we know that
$(\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma \cup [\alpha \mapsto \ell']) \rfloor_E$

5. SLIO*sub-constraint:
Given:

$$\frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash c_1 \Rightarrow \tau_1 <: c_2 \Rightarrow \tau_2}$$

To prove: $\lfloor ((c_1 \Rightarrow \tau_1)\ \sigma) \rfloor_V \subseteq \lfloor ((c_2 \Rightarrow \tau_2))\ \sigma \rfloor_V$

It suffices to prove: $\forall (\theta, n, \nu e_i) \in \lfloor ((c_1 \Rightarrow \tau_1)\ \sigma) \rfloor_V.\ (\theta, n, \nu e_i) \in \lfloor ((c_2 \Rightarrow \tau_2)\ \sigma) \rfloor_V$

This means that given: $(\theta, n, \nu e_i) \in \lfloor ((c_1 \Rightarrow \tau_1)\ \sigma) \rfloor_V$
Therefore from Definition 2.6 we are given:

$$\exists \theta_1.\theta \sqsubseteq \theta_1 \wedge \forall i < n.\mathcal{L} \models c_1\ \sigma \implies (\theta_1, i, e_i) \in \lfloor \tau_1\ (\sigma) \rfloor_E \tag{84}$$

And it suffices to prove: $(\theta, n, \nu e_i) \in \lfloor ((c_2 \Rightarrow \tau_2)\ \sigma) \rfloor_V$

Again from Definition 2.6, it suffices to prove:
$\exists \theta_2.\theta \sqsubseteq \theta_2 \wedge \forall j < n.\mathcal{L} \models c_2\ \sigma \implies (\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma) \rfloor_E$

This means that given some θ_2, j s.t $\theta \sqsubseteq \theta_2 \wedge j < n \wedge \mathcal{L} \models c_2\ \sigma$
And we are required to prove: $(\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma) \rfloor_E$

Since we are given $\theta \sqsubseteq \theta_2 \wedge j < n \wedge \mathcal{L} \models c_2\ \sigma$ and $\mathcal{L} \models c_2\ \sigma \implies c_1\ \sigma$ therefore from Equation 84 we have
$(\theta_2, j, e_i) \in \lfloor \tau_1\ (\sigma) \rfloor_E$

$\lfloor (\tau_1\ \sigma) \rfloor_E \subseteq \lfloor (\tau_2\ \sigma) \rfloor_E$ (Sub-C0, Statement (2))

From (Sub-C0), we know that
$(\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma) \rfloor_E$

6. SLIO*sub-label:

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi \vdash \mathsf{Labeled}\ \ell\ \tau <: \mathsf{Labeled}\ \ell'\ \tau'}$$

To prove: $\lfloor((\mathsf{Labeled}\ \ell\ \tau)\ \sigma)\rfloor_V \subseteq \lfloor((\mathsf{Labeled}\ \ell\ '\tau')\ \sigma)\rfloor_V$

IH: $\lfloor(\tau\ \sigma)\rfloor_V \subseteq \lfloor(\tau'\ \sigma)\rfloor_V$ (Statement (1))

It suffices to prove:
$\forall(\theta, n, \mathsf{Lb}(v_i)) \in \lfloor((\mathsf{Labeled}\ \ell\ \tau)\ \sigma)\rfloor_V.\ (\theta, n, \mathsf{Lb}(v_i)) \in \lfloor((\mathsf{Labeled}\ \ell'\ \tau')\ \sigma)\rfloor_V$

This means that given some θ, n and $\mathsf{Lb}(e_i)$ s.t $(\theta, n, \mathsf{Lb}(v_i)) \in \lfloor((\mathsf{Labeled}\ \ell\ \tau)\ \sigma)\rfloor_V$
Therefore from Definition 2.6 we are given:
$(\theta, n, v_i) \in \lfloor(\tau\ \sigma)\rfloor_V$ (SL)
And we are required to prove that
$(\theta, n, \mathsf{Lb}(v_i)) \in \lfloor((\mathsf{Labeled}\ \ell'\ \tau')\ \sigma)\rfloor_V$
From Definition 2.6 it suffices to prove
$(\theta, n, v_i) \in \lfloor(\tau'\ \sigma)\rfloor_V$

We get this directly from (SL) and IH

7. SLIO*sub-CG:

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell_i' \sqsubseteq \ell_i \qquad \Sigma; \Psi \vdash \ell_o \sqsubseteq \ell_o'}{\Sigma; \Psi \vdash \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau <: \mathbb{SLIO}\ \ell_i'\ \ell_o'\ \tau'}$$

To prove: $\lfloor((\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau)\ \sigma)\rfloor_V \subseteq \lfloor((\mathbb{SLIO}\ \ell_i'\ \ell_o'\ \tau')\ \sigma)\rfloor_V$

IH: $\lfloor(\tau\ \sigma)\rfloor_V \subseteq \lfloor(\tau'\ \sigma)\rfloor_V$ (Statement (1))

It suffices to prove:
$\forall(\theta, n, e) \in \lfloor((\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau)\ \sigma)\rfloor_V.\ (\theta, n, e) \in \lfloor((\mathbb{SLIO}\ \ell_i'\ \ell_o'\ \tau')\ \sigma)\rfloor_V$

This means that given some θ, n and e s.t $(\theta, n, e) \in \lfloor((\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau)\ \sigma)\rfloor_V$
Therefore from Definition 2.6 we are given:
$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, e) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor\tau\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i\ \sigma)$ (SC0)

And we are required to prove
$(\theta, n, e) \in \lfloor((\mathbb{SLIO}\ \ell_i'\ \ell_o'\ \tau')\ \sigma)\rfloor_V$

So again from Definition 2.6 we need to prove
$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, e) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor\tau'\ \sigma\rfloor_V \wedge$

$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell'_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell'_i\ \sigma)$

This means we are given some $k \leq n, \theta_e \sqsupseteq \theta, H, j < k$ s.t $(k, H) \triangleright \theta_e \wedge (H, e) \Downarrow_j^f (H', v')$ (SC1)

And we need to prove

$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor \tau'\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell'_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell'_i\ \sigma)$

We instantiate (SC0) with k, θ_e, H, j from (SC1) and we get

$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i\ \sigma)$

Since $\tau\ \sigma <: \tau'\ \sigma$ therefore from IH we get

$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor \tau'\ \sigma \rfloor_V$

And since $\ell'_i \sqsubseteq \ell_i$ therefore we also have

$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell'_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell'_i\ \sigma)$

8. SLIO*sub-base:

   Trivial

Proof of Statement(2)
It suffice to prove that
$\forall (\theta, n, e) \in \lfloor (\tau\ \sigma) \rfloor_E.\ (\theta, n, e) \in \lfloor (\tau'\ \sigma) \rfloor_E$

This means that we are given $(\theta, n, e) \in \lfloor (\tau\ \sigma) \rfloor_E$
From Definition 2.7 it means we have
$\forall i < n.e \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor \tau\ \sigma \rfloor_V$ (Sub-E0)
And we need to prove
$(\theta, n, e) \in \lfloor (\tau'\ \sigma) \rfloor_E$

From Definition 2.7 we need to prove
$\forall i < n.e \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor \tau'\ \sigma \rfloor_V$

This further means that given some $i < n$ s.t $e \Downarrow_i v$, it suffices to prove that
$(\theta, n-i, v) \in \lfloor \tau'\ \sigma \rfloor_V$

Instantiating (Sub-E0) with the given i we get $(\theta, n-i, v) \in \lfloor \tau\ \sigma \rfloor_V$

Finally from Statement(1) we get $(\theta, n-i, v) \in \lfloor \tau'\ \sigma \rfloor_V$

□

Lemma 2.24 (SLIO*: Binary interpretation of Γ implies Unary interpretation of Γ)**.** $\forall W, \gamma, \Gamma, n.$ $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}} \implies \forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, \gamma \downarrow_i) \in \lfloor \Gamma \rfloor_V$

Proof. Given: $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$
To prove: $\forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, \gamma\downarrow_i) \in \lfloor \Gamma \rfloor_V$

From Definition 2.14 we know that we are given:
$dom(\Gamma) \subseteq dom(\gamma) \wedge \forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$
And we are required to prove:
$\forall i \in \{1, 2\}.\ \forall m.$
$dom(\Gamma) \subseteq dom(\gamma\downarrow_i) \wedge \forall x \in dom(\Gamma).(W.\theta_i, m, \gamma\downarrow_i (x)) \in \lfloor \Gamma(x) \rfloor_V$

Case $i = 1$
Given some m we need to show:

- $dom(\Gamma) \subseteq dom(\gamma\downarrow_i)$:

  $dom(\gamma) = dom(\gamma\downarrow_i)$

  Therefore, $dom(\Gamma) \subseteq (dom(\gamma) = dom(\gamma\downarrow_i))$ (Given)

- $\forall x \in dom(\Gamma).(W.\theta_i, m, \gamma\downarrow_i (x)) \in \lfloor \Gamma(x) \rfloor_V$:

  We are given: $\forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$

  Therefore from Lemma 2.15 we know that

  $\forall m'.(W.\theta_i, m', \gamma\downarrow_i (x)) \in \lfloor \Gamma(x) \rfloor_V$

  Instantiating m' with m we get

  $(W.\theta_i, m, \gamma\downarrow_i (x)) \in \lfloor \Gamma(x) \rfloor_V$

Case $i = 2$
Symmetric reasoning as in the $i = 1$ case above

□

Theorem 2.25 (SLIO*: Fundamental theorem binary)**.** $\forall \Sigma, \Psi, \Gamma, pc, W, \mathcal{A}, \mathcal{L}, e, \tau, \sigma, \gamma, n.$
$\Sigma; \Psi; \Gamma \vdash e : \tau \wedge \mathcal{L} \models \Psi\ \sigma \wedge (W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}} \implies$
$(W, n, e\ (\gamma\downarrow_1), e\ (\gamma\downarrow_2)) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$

Proof. Proof by induction on the typing derivation

1. SLIO*-var:

$$\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash x : \tau}\ \text{SLIO*-var}$$

   To prove: $(W, n, x\ (\gamma\downarrow_1), x\ (\gamma\downarrow_2)) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$

   Say $e_1 = x\ (\gamma\downarrow_1)$ and $e_2 = x\ (\gamma\downarrow_2)$

   From Definition 2.5 it suffices to prove that

   $\forall i < n.e_1 \Downarrow_i v_1' \wedge e_2 \Downarrow v_2' \implies (W, n - i, v_1', v_2') \in \lceil \tau \rceil_V^{\mathcal{A}}$

   This means given some $i < n$ s.t $e_1 \Downarrow_i v_1' \wedge e_2 \Downarrow v_2'$

   We are required to prove: $(W, n - i, v_1', v_2') \in \lceil \tau \rceil_V^{\mathcal{A}}$

From SLIO*-Sem-val we know that $x\ (\gamma\downarrow_1) \Downarrow x\ (\gamma\downarrow_1)$ and $x\ (\gamma\downarrow_2) \Downarrow x\ (\gamma\downarrow_2)$

This means $v_1' = x\ (\gamma\downarrow_1)$ and $v_2' = x\ (\gamma\downarrow_2)$

Since $(W, n, \gamma) \in \lceil \tau \rceil_V^{\mathcal{A}}$. Therefore from Definition 2.14 we know that

$(W, n, v_1', v_2') \in \lceil \tau \rceil_V^{\mathcal{A}}$

From Lemma 2.17 we get

$(W, n-i, v_1', v_2') \in \lceil \tau \rceil_V^{\mathcal{A}}$

2. SLIO*-lam:

$$\frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash e_i : \tau_2}{\Sigma; \Psi; \Gamma \vdash \lambda x.e_i : (\tau_1 \to \tau_2)}$$

To prove: $(W, n, \lambda x.e\ (\gamma\downarrow_1), \lambda x.e\ (\gamma\downarrow_2)) \in \lceil (\tau_1 \to \tau_2)\ \sigma \rceil_E^{\mathcal{A}}$

Say $e_1 = \lambda x.e\ (\gamma\downarrow_1)$ and $e_2 = \lambda x.e\ (\gamma\downarrow_2)$

From Definition of $\lceil (\tau_1 \to \tau_2)\ \sigma \rceil_E^{\mathcal{A}}$ it suffices to prove that

$\forall i < n. e_1 \Downarrow_i v_1' \wedge e_2 \Downarrow v_2' \implies (W, n-i, v_1', v_2') \in \lceil \tau \rceil_V^{\mathcal{A}}$

This means given some $i < n$ s.t $e_1 \Downarrow_i v_1' \wedge e_2 \Downarrow v_2'$

From SLIO*-Sem-val we know that $v_1' = (\lambda x.e_i)\gamma\downarrow_1$ and $v_2' = (\lambda x.e_i)\gamma\downarrow_2$

We are required to prove:

$(W, n-i, (\lambda x.e_i)\gamma\downarrow_1, (\lambda x.e_i)\gamma\downarrow_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$

From Definition 2.4 it suffices to prove

$\forall W' \sqsupseteq W, j < n, v_1, v_2.$
$((W', j, v_1, v_2) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \implies (W', j, e_1[v_1/x]\ \gamma\downarrow_1, e_2[v_2/x]\ \gamma\downarrow_1) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, v_c, j.$
$((\theta_l, j, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta_l, j, e_1[v_c/x]\ \gamma\downarrow_1) \in \lfloor \tau_2\ \sigma \rfloor_E) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, v_c, j.$
$((\theta_l, j, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, j, e_2[v_c/x]\ \gamma\downarrow_2) \in \lfloor \tau_2\ \sigma \rfloor_E)$ (FB-L0)

IH:

$\forall W, n.\ (W, n, e_i\ (\gamma\downarrow_1 \cup \{x \mapsto v_1\}), e_i\ (\gamma\downarrow_2 \cup \{x \mapsto v_2\})) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$

s.t

$(W, n, (\gamma \cup \{x \mapsto (v_1, v_2)\})) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$

In order to prove (FB-L0) we need to prove the following:

(a) $\forall W' \sqsupseteq W, j < n, v_1, v_2.$
$((W', j, v_1, v_2) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \implies (W', j, e_1[v_1/x]\ \gamma\downarrow_1, e_2[v_2/x]\ \gamma\downarrow_2) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}})$:

This means given some $W' \sqsupseteq W, j < n, v_1, v_2$ s.t. $(W', j, v_1, v_2) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$

We need to prove $(W', j, e_1[v_1/x]\ \gamma\downarrow_1, e_2[v_2/x]\ \gamma\downarrow_2) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$

We get this by instantiating IH with W' and j

(b) $\forall \theta_l \sqsupseteq W.\theta_1, v_c, j.$
$((\theta_l, j, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta_l, j, e_1[v_c/x]\ \gamma \downarrow_1) \in \lfloor \tau_2\ \sigma \rfloor_E)$:
This means given some $\theta_l \sqsupseteq W.\theta_1, v_c, j$ s.t $(\theta_l, j, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V$
We need to prove: $(\theta_l, j, e_1[v_c/x]\ \gamma \downarrow_1) \in \lfloor \tau_2\ \sigma \rfloor_E$

It is given to us that
$(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$

Therefore from Lemma 2.24 we know that
$\forall m.\ (W.\theta_1, m, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$
Intantiating m with j we get
$(W.\theta_1, j, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$

From Lemma 2.19 we know that
$(\theta_l, j, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$

Since we know that $(\theta_l, j, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V$
Therefore we also have
$(\theta_l, j, \gamma \downarrow_1 \cup \{x \mapsto v_c\}) \in \lfloor \Gamma \cup \{x \mapsto \tau_1\ \sigma\} \rfloor_V$

Therefore, we can apply Theorem 2.22 to obtain
$(\theta_l, j, e[v_c/x]\ \gamma \downarrow_1) \in \lfloor \tau_2\ \sigma \rfloor_V$

(c) $\forall \theta_l \sqsupseteq W.\theta_2, v_c, j.$
$((\theta_l, j, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta_l, j, e_2[v_c/x]\ \gamma \downarrow_2) \in \lfloor \tau_2\ \sigma \rfloor_E)$:
Similar reasoning as in the previous case

3. SLIO*-app:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : (\tau_1 \to \tau_2) \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \tau_1}{\Sigma; \Psi; \Gamma \vdash e_1\ e_2 : \tau_2}$$

To prove: $(W, n, (e_1\ e_2)\ (\gamma \downarrow_1), (e_1\ e_2)\ (\gamma \downarrow_2)) \in \lceil (\tau_2)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:
$\forall i < n.(e_1\ e_2)\ \gamma \Downarrow_i v_{f1} \wedge e_2 \Downarrow v_{f2} \implies (W, n-i, v_{f1}, v_{f2}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$

This further means that given some $i < n$ s.t $(e_1\ e_2)\ \gamma \Downarrow_i v_{f1} \wedge e_2 \Downarrow v_{f2}$
<u>It sufficies to prove</u>:
$(W, n-i, v_{f1}, v_{f2}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$

<u>IH1</u>: $(W, n, (e_1)\ (\gamma \downarrow_1), (e_1)\ (\gamma \downarrow_2)) \in \lceil (\tau_1 \to \tau_2)\ \sigma \rceil_E^{\mathcal{A}}$
This means from Definition 2.5 we know that
$\forall j < n.e_1\ \gamma \downarrow_1 \Downarrow_j v_{h1} \wedge e_1\ \gamma \downarrow_2 \Downarrow v_{h2} \implies (W, n-j, v_{h1}, v_{h2}) \in \lceil (\tau_1 \to \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e_1\ e_2)\ \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists j < i < n$ s.t $e_1\ \gamma \downarrow_1 \Downarrow_j v_{h1}$. Similarly since $(e_1\ e_2)\ \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e_1\ \gamma \downarrow_2 \Downarrow v_{h2}$
This means we have $(W, n-j, v_{h1}, v_{h2}) \in \lceil (\tau_1 \to \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$

From SLIO*-Sem-app we know that $val_{h1} = \lambda x.e_{h1}$ and $val_{h2} = \lambda x.e_{h2}$

From Definition 2.4 this further means

$\forall W' \sqsupseteq W, J < (n-j), v_1, v_2.$
$((W', J, v_1, v_2) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \implies (W', J, e_{h1}[v_1/x], e_{h2}[v_2/x]) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, v_c, j.$
$((\theta_l, j, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta_l, j, e_1[v_c/x]) \in \lfloor \tau_2\ \sigma \rfloor_E) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, v_c, j.$
$((\theta_l, j, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta_l, j, e_2[v_c/x]) \in \lfloor \tau_2\ \sigma \rfloor_E)$ (FB-A1)

<u>IH2</u>: $(W, n-j, (e_2)\ (\gamma \downarrow_1), (e_2)\ (\gamma \downarrow_2)) \in \lceil \tau_1\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we know that

$\forall k < n-j.e_2\ \gamma \downarrow_1 \Downarrow_j v_{h1'} \wedge e_2\ \gamma \downarrow_2 \Downarrow v_{h2'} \implies (W, n-j-k, v_{h1'}, v_{h2'}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e_1\ e_2)\ \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists k < i-j < n-j$ s.t $e_2\ \gamma \downarrow_1 \Downarrow_k v_{h1'}$. Similarly since $(e_1\ e_2)\ \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e_2\ \gamma \downarrow_2 \Downarrow v_{h2'}$

This means we have $(W, n-j-k, v_{h1'}, v_{h2'}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$ (FB-A2)

Instantiating the first conjunct of (FB-A1) as follows W' with W, J with $n-j-k$, v_1 and v_2 with v'_{h1} and v'_{h2} respectively, we obtain

$(W, n-j-k, e_{h1}[v'_{h1}/x], e_{h2}[v'_{h2}/x]) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$

From Definition 2.5

$\forall l < n-j-k.(e_{h1}[v'_{h1}/x])\ \gamma \Downarrow_l v_{f1} \wedge\ e_{h2}[v'_{h2}/x] \Downarrow v_{f2} \implies (W, n-j-k-l, v_{f1}, v_{f2}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e_1\ e_2)\ \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists l < i-j-k < n-j-k$ s.t $e_{h1}[v'_{h1}/x] \Downarrow_l v_{f1}$. Similarly since $(e_1\ e_2)\ \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e_{h2}[v'_{h2}/x] \Downarrow v_{f2}$

Therefore we have $(W, n-j-k-l, v_{f1}, v_{f2}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$

Since $i = j+k+l$ threfore we are done

4. SLIO*-prod:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \tau_1 \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \tau_2}{\Sigma; \Psi; \Gamma \vdash (e_1, e_2) : (\tau_1 \times \tau_2)}$$

To prove: $(W, n, (e_1, e_2)\ (\gamma \downarrow_1), (e_1, e_2)\ (\gamma \downarrow_2)) \in \lceil (\tau_1 \times \tau_2)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:

$\forall i < n.(e_1, e_2)\ \gamma \downarrow_1 \Downarrow_i (v_{f1}, v_{f2}) \wedge (e_1, e_2)\ \gamma \downarrow_2 \Downarrow (v'_{f1}, v'_{f2}) \implies$
$(W, n-i, (v_{f1}, v_{f1}), (v'_{f1}, v'_{f2})) \in \lceil (\tau_1 \times \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $(e_1, e_2)\ \gamma \downarrow_1 \Downarrow_i (v_{f1}, v_{f2}) \wedge (e_1, e_2)\ \gamma \downarrow_2 \Downarrow (v'_{f1}, v'_{f2})$

We are required to prove

$(W, n-i, (v_{f1}, v_{f1}), (v'_{f1}, v'_{f2})) \in \lceil (\tau_1 \times \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$ (FB-P0)

<u>IH1</u>: $(W, n, e_1\ (\gamma \downarrow_1), e_1\ (\gamma \downarrow_2)) \in \lceil \tau_1\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we know that

$\forall j < n.e_1\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge e_1\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies (W, n-j, (v_{f1}, v'_{f1})) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e_1, e_2)\ \gamma \downarrow_1 \Downarrow_i (v_{f1}, v_{f2})$. Therefore $\exists j < i < n$ s.t $e_1\ \gamma \downarrow_1 \Downarrow_j v_{f1}$. Similarly since $(e_1\ e_2)\ \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e_1\ \gamma \downarrow_2 \Downarrow v'_{f1}$

This means we have

$(W, n-j, (v_{f1}, v'_{f1})) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$ (FB-P1)

IH2: $(W, n-j, e_2\ (\gamma \downarrow_1), e_2\ (\gamma \downarrow_2)) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we know that

$\forall k < n-j.e_2\ \gamma \downarrow_1 \Downarrow_i v_{f2} \wedge e_2\ \gamma \downarrow_2 \Downarrow v'_{f2} \implies (W, n-j-k, (v_{f2}, v'_{f2})) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e_1, e_2)\ \gamma \downarrow_1 \Downarrow_i (v_{f1}, v_{f2})$. Therefore $\exists k < i-j < n-j$ s.t $e_2\ \gamma \downarrow_1 \Downarrow_j v_{f2}$. Similarly since $(e_1\ e_2)\ \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e_2\ \gamma \downarrow_2 \Downarrow v'_{f2}$

This means we have

$(W, n-j-k, (v_{f2}, v'_{f2})) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$ (FB-P2)

In order to prove (FB-P0) from Definition 2.4 it suffices to prove that

$(W, n-i, (v_{f1}, v'_{f1})) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$ and $(W, n-i, (v_{f2}, v'_{f2})) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$

Since $i = j + k + 1$ therefore from (FB-P1) and (FB-P2) and from Lemma 2.17 we get

$(W, n-i, (v_{f1}, v_{f1}), (v'_{f1}, v'_{f2})) \in \lceil (\tau_1 \times \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$

5. SLIO*-fst:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : (\tau_1 \times \tau_2)}{\Sigma; \Psi; \Gamma \vdash \mathsf{fst}(e') : \tau_1}$$

To prove: $(W, n, \mathsf{fst}(e')\ (\gamma \downarrow_1), \mathsf{fst}(e')\ (\gamma \downarrow_2)) \in \lceil (\tau_1)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:

$\forall i < n.\mathsf{fst}(e')\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{fst}(e')\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n-i, v_{f1}, v'_{f1}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{fst}(e')\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{fst}(e')\ \gamma \downarrow_2 \Downarrow v'_{f1}$

We are required to prove

$(W, n-i, v_{f1}, v_{f1}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$ (FB-F0)

IH:

$(W, n, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil (\tau_1 \times \tau_2)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we have:

$\forall j < n.e'\ \gamma \downarrow_1 \Downarrow_i (v_{f1}, v_{f2}) \wedge e'\ \gamma \downarrow_2 \Downarrow (v'_{f1}, v'_{f2}) \implies$
$(W, n-j, (v_{f1}, v_{f2}), (v'_{f1}, v'_{f2})) \in \lceil (\tau_1 \times \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $\mathsf{fst}(e')\ \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists j < i < n$ s.t $e'\ \gamma \downarrow_1 \Downarrow_j (v_{f1}, -)$. Similarly since $\mathsf{fst}(e')\ \gamma \downarrow_2 \Downarrow v'_{f1}$ therefore $e'\ \gamma \downarrow_2 \Downarrow (v'_{f1}, -)$

This means we have

$(W, n-j, (v_{f1}, v_{f2}), (v'_{f1}, v'_{f2})) \in \lceil(\tau_1 \times \tau_2)\ \sigma\rceil_V^{\mathcal{A}}$

From Definition 2.4 we know that

$(W, n-j, v_{f1}, v'_{f1}) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}}$

Since from SLIO*-Sem-fst $i = j+1$ therefore from Lemma 2.17 we get

$(W, n-i, v_{f1}, v'_{f1}) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}}$

6. SLIO*-snd:

   Symmetric reasoning as in the SLIO*-fst case above

7. SLIO*-inl:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \tau_1}{\Sigma; \Psi; \Gamma \vdash \mathsf{inl}(e') : (\tau_1 + \tau_2)}$$

To prove: $(W, n, \mathsf{inl}(e')\ (\gamma\downarrow_1), \mathsf{inl}(e')\ (\gamma\downarrow_2)) \in \lceil(\tau_1 + \tau_2)\ \sigma\rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:

$\forall i < n.\mathsf{inl}(e')\ \gamma\downarrow_1\Downarrow_i \mathsf{inl}(v_{f1}) \wedge \mathsf{inl}(e')\ \gamma\downarrow_2\Downarrow \mathsf{inl}(v'_{f1}) \implies$
$(W, n-i, \mathsf{inl}(v_{f1}), \mathsf{inl}(v'_{f1})) \in \lceil(\tau_1 + \tau_2)\ \sigma\rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{inl}(e')\ \gamma\downarrow_1\Downarrow_i \mathsf{inl}(v_{f1}) \wedge \mathsf{fst}(e')\ \gamma\downarrow_2\Downarrow \mathsf{inl}(v'_{f1})$

We are required to prove

$(W, n-i, \mathsf{inl}(v_{f1}), \mathsf{inl}(v_{f1})) \in \lceil(\tau_1 + \tau_2)\ \sigma\rceil_V^{\mathcal{A}}$ (FB-IL0)

<u>IH</u>:

$(W, n, e'\ (\gamma\downarrow_1), e'\ (\gamma\downarrow_2)) \in \lceil(\tau_1 \times \tau_2)\ \sigma\rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we have:

$\forall j < n.e'\ \gamma\downarrow_1\Downarrow_i v_{f1} \wedge e'\ \gamma\downarrow_2\Downarrow v'_{f1} \implies$
$(W, n-j, v_{f1}, v'_{f1}) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}}$

Since we know that $\mathsf{inl}(e')\ \gamma\downarrow_1\Downarrow_i \mathsf{inl}(v_{f1})$. Therefore $\exists j < i < n$ s.t $e'\ \gamma\downarrow_1\Downarrow_j v_{f1}$. Similarly since $\mathsf{fst}(e')\ \gamma\downarrow_2\Downarrow \mathsf{inl}(v'_{f1})$ therefore $e'\ \gamma\downarrow_2\Downarrow v'_{f1}$

This means we have

$(W, n-j, v_{f1}, v'_{f1}) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}}$ (FB-IL1)

In order to prove (FB-IL0) from Definition 2.4 it suffices to prove

$(W, n-i, v_{f1}, v'_{f1}) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}}$

From SLIO*-Sem-inl since $i = j+1$ therefore from (FB-IL1) and Lemma 2.17 we get (FB-IL0)

8. SLIO*-inr:

   Symmetric reasoning as in the SLIO*-inl case above

9. SLIO*-case:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_c : (\tau_1 + \tau_2) \qquad \Sigma; \Psi; \Gamma, x : \tau_1 \vdash e_1 : \tau \qquad \Sigma; \Psi; \Gamma, y : \tau_2 \vdash e_2 : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{case}(e_c, x.e_1, y.e_2) : \tau}$$

To prove: $(W, n, \mathsf{case}(e_c, x.e_1, y.e_2)\ (\gamma \downarrow_1), \mathsf{inl}(e')\ (\gamma \downarrow_2)) \in \lceil (\tau_1 + \tau_2)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:

$\forall i < n.\mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_2 \Downarrow v_{f2} \implies$
$(W, n - i, v_{f1}, v_{f2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_2 \Downarrow v_{f2}$

We are required to prove

$(W, n - i, v_{f1}, v_{f2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$ (FB-C0)

<u>IH1</u>:

$(W, n, e_c\ (\gamma \downarrow_1), e_c\ (\gamma \downarrow_2)) \in \lceil (\tau_1 + \tau_2)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we have:

$\forall j < n.e_c\ \gamma \downarrow_1 \Downarrow_i v_{h1} \wedge e_c\ \gamma \downarrow_2 \Downarrow v'_{h1} \implies$
$(W, n - j, v_{h1}, v'_{h1}) \in \lceil (\tau_1 + \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $\mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists j < i < n$ s.t $e_c\ \gamma \downarrow_1 \Downarrow_j v_{h1}$. Similarly since $\mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_2 \Downarrow v'_{h1}$ therefore $e_c\ \gamma \downarrow_2 \Downarrow v'_{h1}$

This means we have

$(W, n - j, v_{h1}, v'_{h1}) \in \lceil (\tau_1 + \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$ (FB-C1)

2 cases arise

(a) $v_{h1} = \mathsf{inl}(v_1)$ and $v'_{h1} = \mathsf{inl}(v'_1)$:
<u>IH2</u>:
$(W, n, e_c\ (\gamma \downarrow_1), e_c\ (\gamma \downarrow_2)) \in \lceil (\tau_1 + \tau_2)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we have:
$\forall k < n - j.e_1\ \gamma \downarrow_1 \cup \{x \mapsto v_1\} \Downarrow_i v_{h2} \wedge e_1\ \gamma \downarrow_2 \cup \{x \mapsto v'_1\} \Downarrow v'_{h2} \implies$
$(W, n - j - k, v_{h2}, v'_{h2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$
Since we know that $\mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists k < i - j < n - j$ s.t $e_1\ \gamma \downarrow_1 \cup \{x \mapsto v_1\} \Downarrow_j v_{h2}$. Similarly since $\mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_2 \cup \{x \mapsto v'_1\} \Downarrow v'_{h2}$ therefore $e_1\ \gamma \downarrow_2 \Downarrow v'_{h2}$
This means we have
$(W, n - j - k, v_{h2}, v'_{h2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

From SLIO*-Sem-case1 we know that $i = j + k + 1$ therefore from Lemma 2.17 we get (FB-C0)

(b) $v_{h1} = \mathsf{inr}(v_1)$ and $v'_{h1} = \mathsf{inr}(v'_1)$:
Symmetric case

10. SLIO*-FI:

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash e' : \tau}{\Sigma; \Gamma \vdash \Lambda e' : \forall \alpha.\tau}$$

To prove: $(W, n, \Lambda e'\ (\gamma \downarrow_1), \Lambda e'\ (\gamma \downarrow_2)) \in \lceil (\forall \alpha.\tau)\ \sigma \rceil_E^{\mathcal{A}}$

From Definition 2.5 it suffices to prove that

$\forall i < n.(\Lambda e')\gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (\Lambda e')\gamma \downarrow_2 \Downarrow v_{f2} \implies (W, n-i, v_{f1}, v_{f2}) \in \lceil (\forall \alpha.\tau)\ \sigma \rceil_V^{\mathcal{A}}$

This means given some $i < n$ s.t $(\Lambda e')\gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (\Lambda e')\gamma \downarrow_2 \Downarrow v_{f2}$

From SLIO*-Sem-val we know that $v_{f1} = (\Lambda e')\gamma \downarrow_1$ and $v_{f2} = (\Lambda e')\gamma \downarrow_2$

We are required to prove:

$(W, n-i, (\Lambda e')\gamma \downarrow_1, (\Lambda e')\gamma \downarrow_2) \in \lceil (\forall \alpha.\tau)\ \sigma \rceil_V^{\mathcal{A}}$

Let $e_1 = (\Lambda e')\gamma \downarrow_1$ and $e_2 = (\Lambda e')\gamma \downarrow_2$

From Definition 2.4 it suffices to prove

$\forall W' \sqsupseteq W, j < (n-i), \ell' \in \mathcal{L}.((W', j, e_1, e_2) \in \lceil \tau[\ell'/\alpha]\ \sigma \rceil_E^{\mathcal{A}}) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, \ell'' \in \mathcal{L}, j.(\theta_l, j, e_1) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, \ell'' \in \mathcal{L}, j.(\theta_l, j, e_2) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E$ (FB-FI0)

IH: $\forall W, n.\ (W, n, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil \tau\ \sigma \cup \{\alpha \mapsto \ell'\} \rceil_E^{\mathcal{A}}$

In order to prove (FB-FI0) we need to prove the following

(a) $\forall W' \sqsupseteq W, j < (n-i), \ell' \in \mathcal{L}.((W', j, e_1, e_2) \in \lceil \tau[\ell'/\alpha]\ \sigma \rceil_E^{\mathcal{A}})$:
   This means given $W' \sqsupseteq W, j < (n-i), \ell' \in \mathcal{L}$ and we are required to prove
   $(W', j, e_1, e_2) \in \lceil \tau[\ell'/\alpha]\ \sigma \rceil_E^{\mathcal{A}}$
   Instantiating IH with W' and j we get the desired
(b) $\forall \theta_l \sqsupseteq W.\theta_1, \ell'' \in \mathcal{L}, j.(\theta_l, j, e_1) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E$:
   This means given $\theta_l \sqsupseteq W.\theta_1, \ell'' \in \mathcal{L}, j$ and we are required to prove
   $(\theta_l, j, e_1) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E$
   Since from Lemma 2.24
   $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}} \implies \forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, \gamma \downarrow_i) \in \lfloor \Gamma \rfloor_V$
   Therefore we get
   $(W.\theta_1, j, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$
   And from Lemma 2.17 we also get
   $(\theta_l, j, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$
   Therefore we can apply Theorem 2.22 to get
   $(\theta_l, j, e_1) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E$
(c) $\forall \theta_l \sqsupseteq W.\theta_2, \ell'' \in \mathcal{L}, j.(\theta_l, j, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E$:
   Symmetric reasoning as before

11. SLIO*-FE:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \forall \alpha.\tau \qquad \text{FV}(\ell) \in \Sigma}{\Sigma; \Psi; \Gamma \vdash e' \; [] : \tau[\ell/\alpha]}$$

To prove: $(W, n, e'[] \; (\gamma \downarrow_1), e'[] \; (\gamma \downarrow_2)) \in \lceil (\forall \alpha.\tau) \; \sigma \rceil_E^{\mathcal{A}}$

From Definition 2.5 it suffices to prove that

$\forall i < n.(e'[])\gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (e'[])\gamma \downarrow_2 \Downarrow v_{f2} \implies (W, n-i, v_{f1}, v_{f2}) \in \lceil (\tau[\ell/\alpha]) \; \sigma \rceil_V^{\mathcal{A}}$

This means given some $i < n$ s.t $(e'[])\gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (e'[])\gamma \downarrow_2 \Downarrow v_{f2}$

<u>We are required to prove</u>:

$(W, n-i, v_{f1}, v_{f2}) \in \lceil (\tau[\ell/\alpha]) \; \sigma \rceil_V^{\mathcal{A}}$ (FB-FE0)

<u>IH</u>: $(W, n, e' \; (\gamma \downarrow_1), e' \; (\gamma \downarrow_2)) \in \lceil (\forall \alpha.\tau) \; \sigma \rceil_E^{\mathcal{A}}$

From Definition 2.5 it suffices to prove that

$\forall i < n.(e')\gamma \downarrow_1 \Downarrow_i v_{h1} \wedge (e')\gamma \downarrow_2 \Downarrow v_{h2} \implies (W, n-i, v_{h1}, v_{h2}) \in \lceil (\forall \alpha.\tau) \; \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e'[]) \; \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists j < i < n$ s.t $e' \; \gamma \downarrow_1 \Downarrow_j v_{h1}$. Similarly since $(e'[]) \; \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e' \; \gamma \downarrow_2 \Downarrow v_{h2}$

This means we have $(W, n-j, v_{h1}, v_{h2}) \in \lceil (\forall \alpha.\tau) \; \sigma \rceil_V^{\mathcal{A}}$

From SLIO*-Sem-FE we know that $v_{h1} = \Lambda e_{h1}$ and $v_{h2} = \Lambda e_{h2}$

From Definition 2.4 this further means

$\forall W' \sqsupseteq W, k < (n-j), \ell' \in \mathcal{L}.((W', k, e_{h1}, e_{h2}) \in \lceil \tau[\ell'/\alpha] \; \sigma \rceil_E^{\mathcal{A}}) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, \ell'' \in \mathcal{L}, k.(\theta_l, k, e_{h1}) \in \lfloor \tau[\ell''/\alpha] \; \sigma \rfloor_E \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, \ell'' \in \mathcal{L}, k.(\theta_l, k, e_{h2}) \in \lfloor \tau[\ell''/\alpha] \; \sigma \rfloor_E$ (FB-FE1)

Instantiating the first conjunct of (FB-FE1) with W, $n-j-1$ and ℓ we get

$(W, n-j-1, e_{h1}, e_{h2}) \in \lceil \tau[\ell/\alpha] \; \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we know that

$\forall l < n-j-1.(e_{h1}) \Downarrow_l v_{f1} \wedge e_{h2} \Downarrow v_{f2} \implies (W, n-j-1-l, v_{f1}, v_{f2}) \in \lceil (\tau[\ell/\alpha]) \; \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e'[]) \; \gamma \downarrow_1 \Downarrow_i v_{f1}$ therefore from SLIO*-Sem-FE we know that $(i = j+l+1)$ and since we know that $i < n$ therefore we have $l < n-j-1$ s.t $e_{h1} \; \gamma \downarrow_1 \Downarrow_j v_{f1}$. Similarly since $(e'[]) \; \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e_{h2} \; \gamma \downarrow_2 \Downarrow v_{f2}$

Therefore we get

$(W, n-j-1-l, v_{f1}, v_{f2}) \in \lceil (\tau[\ell/\alpha]) \; \sigma \rceil_V^{\mathcal{A}}$ (FB-FE2)

Since we know that $i = j+l+1$ therefore from (FB-FE2) we get (FB-FE0)

12. SLIO*-CI:

$$\frac{\Sigma; \Psi, c; \Gamma \vdash e' : \tau}{\Sigma; \Gamma \vdash \nu \; e' : c \Rightarrow \tau}$$

To prove: $(W, n, \nu e' \; (\gamma \downarrow_1), \nu e' \; (\gamma \downarrow_2)) \in \lceil (c \Rightarrow \tau) \; \sigma \rceil_E^{\mathcal{A}}$

From Definition 2.5 it suffices to prove that

$\forall i < n.(\nu e')\gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (\nu e')\gamma \downarrow_2 \Downarrow v_{f2} \implies (W, n-i, v_{f1}, v_{f2}) \in \lceil (c \Rightarrow \tau)\ \sigma \rceil_V^{\mathcal{A}}$

This means given some $i < n$ s.t $(\nu e')\gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (\nu e')\gamma \downarrow_2 \Downarrow v_{f2}$

From SLIO*-Sem-val we know that $v_{f1} = (\nu e')\gamma \downarrow_1$ and $v_{f2} = (\nu e')\gamma \downarrow_2$

<u>We are required to prove</u>:

$(W, n-i, (\nu e')\gamma \downarrow_1, (\nu e')\gamma \downarrow_2) \in \lceil (c \Rightarrow \tau)\ \sigma \rceil_V^{\mathcal{A}}$

Let $e_1 = (\nu e')\gamma \downarrow_1$ and $e_2 = (\nu e')\gamma \downarrow_2$

From Definition 2.4 it suffices to prove

$\forall W' \sqsupseteq W, j < n.\mathcal{L} \models c \implies (W', j, e_1, e_2) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}} \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c \implies (\theta_l, j, e_1) \in \lfloor \tau\ \sigma \rfloor_E \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c \implies (\theta_l, j, e_2) \in \lfloor \tau\ \sigma \rfloor_E$ (FB-CI0)

<u>IH</u>: $\forall W, n.\ (W, n, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$

In order to prove (FB-CI0) we need to prove the following

(a) $\forall W' \sqsupseteq W, j < n.\mathcal{L} \models c\ \sigma \implies (W', j, e_1, e_2) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$:
 This means given $W' \sqsupseteq W, j < n, \mathcal{L} \models c\ \sigma$ and we are required to prove
 $(W', j, e_1, e_2) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$
 Instantiating IH with W' and j we get the desired

(b) $\forall \theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c\ \sigma \implies (\theta_l, j, e_1) \in \lfloor \tau\ \sigma \rfloor_E$:
 This means given $\theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c\ \sigma$ and we are required to prove
 $(\theta_l, j, e_1) \in \lfloor \tau\ \sigma \rfloor_E$
 Since from Lemma 2.24 $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}} \implies \forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, \gamma \downarrow_i) \in \lfloor \Gamma \rfloor_V$
 Therefore we get
 $(W.\theta_1, j, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$
 And from Lemma 2.17 we also get
 $(\theta_l, j, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$
 Therefore we can apply Theorem 2.22 to get
 $(\theta_l, j, e_1) \in \lfloor \tau\ \sigma \rfloor_E$

(c) $\forall \theta_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c \implies (\theta_l, j, e_2) \in \lfloor \tau\ \sigma \rfloor_E$:
 Symmetric reasoning as before

13. SLIO*-CE:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : c \Rightarrow \tau \qquad \Sigma; \Psi \vdash c}{\Sigma; \Psi; \Gamma \vdash e' \bullet : \tau}$$

To prove: $(W, n, e' \bullet\ (\gamma \downarrow_1), e' \bullet\ (\gamma \downarrow_2)) \in \lceil \tau)\ \sigma \rceil_E^{\mathcal{A}}$

From Definition 2.5 it suffices to prove that

$\forall i < n.(e' \bullet)\gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (e' \bullet)\gamma \downarrow_2 \Downarrow v_{f2} \implies (W, n-i, v_{f1}, v_{f2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

This means given some $i < n$ s.t $(e'\bullet)\gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (e'\bullet)\gamma \downarrow_2 \Downarrow v_{f2}$

We are required to prove:

$(W, n-i, v_{f1}, v_{f2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$ (FB-CE0)

IH: $(W, n, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil (c \Rightarrow \tau)\ \sigma \rceil_E^{\mathcal{A}}$

From Definition 2.5 it suffices to prove that

$\forall i < n. e'\gamma \downarrow_1 \Downarrow_i v_{h1} \wedge e'\gamma \downarrow_2 \Downarrow v_{h2} \implies (W, n-i, v_{h1}, v_{h2}) \in \lceil (c \Rightarrow \tau)\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e'\bullet)\ \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists j < i < n$ s.t $e'\ \gamma \downarrow_1 \Downarrow_j v_{h1}$. Similarly since $(e'\bullet)\ \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e'\ \gamma \downarrow_2 \Downarrow v_{h2}$

This means we have $(W, n-j, v_{h1}, v_{h2}) \in \lceil (c \Rightarrow \tau)\ \sigma \rceil_V^{\mathcal{A}}$

From SLIO*-Sem-CE we know that $v_{h1} = \nu e_{h1}$ and $v_{h2} = \nu e_{h2}$

From Definition 2.4 this further means

$\forall W' \sqsupseteq W, k < n-j. \mathcal{L} \models c\ \sigma \implies (W', k, e_1, e_2) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}} \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, k. \mathcal{L} \models c\ \sigma \implies (\theta_l, k, e_1) \in \lfloor \tau\ \sigma \rfloor_E \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, k. \mathcal{L} \models c\ \sigma \implies (\theta_l, k, e_2) \in \lfloor \tau\ \sigma \rfloor_E$ (FB-CE1)

Instantiating the first conjunct of (FB-CE1) with W, $n-j-1$ and since we know that $\mathcal{L} \models c\ \sigma$ therefore we get

$(W, n-j-1, e_{h1}, e_{h2}) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we know that

$\forall l < n-j-1. (e_{h1}) \Downarrow_l v_{f1} \wedge e_{h2} \Downarrow v_{f2} \implies (W, n-j-1-l, v_{f1}, v_{f2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e'\bullet)\ \gamma \downarrow_1 \Downarrow_i v_{f1}$ therefore from SLIO*-Sem-CE we know that $(i = j+l+1)$ and since we know that $i < n$ therefore we have $l < n-j-1$ s.t $e_{h1}\ \gamma \downarrow_1 \Downarrow_l v_{f1}$. Similarly since $(e'\bullet)\ \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e_{h2}\ \gamma \downarrow_2 \Downarrow v_{f2}$

Therefore we get

$(W, n-j-1-l, v_{f1}, v_{f2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$ (FB-CE2)

Since we know that $i = j+l+1$ therefore from (FB-CE2) we get (FB-CE0)

14. SLIO*-label:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{Lb}(e') : \mathsf{Labeled}\ \ell\ \tau}$$

To prove: $(W, n, \mathsf{Lb}(e')\ (\gamma \downarrow_1), \mathsf{Lb}(e')\ (\gamma \downarrow_2)) \in \lceil \mathsf{Labeled}\ \ell\ \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:

$\forall i < n. \mathsf{Lb}(e')\ \gamma \downarrow_1 \Downarrow_i \mathsf{Lb}(v_{f1}) \wedge \mathsf{Lb}(e')\ \gamma \downarrow_2 \Downarrow \mathsf{Lb}(v'_{f1}) \implies$
$(W, n-i, \mathsf{Lb}(v_{f1}), \mathsf{Lb}(v'_{f1})) \in \lceil \mathsf{Labeled}\ \ell\ \tau\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{Lb}(e')\ \gamma \downarrow_1 \Downarrow_i \mathsf{Lb}(v_{f1}) \wedge \mathsf{Lb}(e')\ \gamma \downarrow_2 \Downarrow \mathsf{Lb}(v'_{f1})$

We are required to prove

$(W, n-i, v_{f1}, v'_{f1}) \in \lceil \mathsf{Labeled}\ \ell\ \tau\ \sigma \rceil_V^{\mathcal{A}}$ (FB-LB0)

IH:

$(W, n, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we have:

$\forall j < n. e'\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge e'\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies (W, n-j, v_{f1}, v'_{f1}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $\mathsf{Lb}(e')\ \gamma \downarrow_1 \Downarrow_i \mathsf{Lb}(v_{f1})$. Therefore $\exists j < i < n$ s.t $e'\ \gamma \downarrow_1 \Downarrow_j v_{f1}$. Similarly since $\mathsf{Lb}(e')\ \gamma \downarrow_2 \Downarrow \mathsf{Lb}(v'_{f1})$ therefore $e'\ \gamma \downarrow_2 \Downarrow v'_{f1}$

This means we have

$(W, n-j, v_{f1}, v'_{f1}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$ (FB-LB1)

In order to prove (FB-LB0) from Definition 2.4 it suffices to prove that

$(W, n-i, v_{f1}, v'_{f1}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

From SLIO*-Sem-label we know that $i = j+1$. Therefore we get the desired from (FB-LB1) and Lemma 2.17

15. SLIO*-unlabel:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \mathsf{Labeled}\ \ell\ \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{unlabel}(e') : \mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau}$$

To prove: $(W, n, \mathsf{unlabel}(e')\ (\gamma \downarrow_1), \mathsf{unlabel}(e')\ (\gamma \downarrow_2)) \in \lceil (\mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:

$\forall i < n. \mathsf{unlabel}(e')\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{unlabel}(e')\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n-i, v_{f1}, v'_{f1}) \in \lceil (\mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau)\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{unlabel}(e')\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{unlabel}(e')\ \gamma \downarrow_2 \Downarrow v'_{f1}$

From SLIO*-Sem-val we know that $v_{f1} = \mathsf{unlabel}(e')\ \gamma \downarrow_1$ and $v'_{f1} = \mathsf{unlabel}(e')\ \gamma \downarrow_2$. Also $i = 0$

We are required to prove

$(W, n, \mathsf{unlabel}(e')\ \gamma \downarrow_1, \mathsf{unlabel}(e')\ \gamma \downarrow_2) \in \lceil (\mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau)\ \sigma \rceil_V^{\mathcal{A}}$

This means from Definition 2.4 we need to prove

Let $e_1 = \mathsf{unlabel}(e')\ \gamma \downarrow_1$ and $e_2 = \mathsf{unlabel}(e')\ \gamma \downarrow_2$

$\Big(\forall k \leq n, W_e \sqsupseteq W. \forall H_1, H_2.(k, H_1, H_2) \rhd W_e \wedge \forall v'_1, v'_2.$
$(H_1, e_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, e_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \rhd W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, (\ell_i \sqcup \ell)\ \sigma, v'_1, v'_2, \tau\ \sigma)\Big) \wedge$
$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \rhd \theta_e \wedge (H, e_l) \Downarrow_j^f (H', v'_l) \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \rhd \theta' \wedge (\theta', k-j, v'_l) \in \lfloor \tau' \rfloor_V \wedge$
$(\forall a. H(a) \neq H'(a) \implies \exists \ell'. \theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i\ \sigma)\Big)$

We need to show

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v_1', v_2'.$
$(H_1, e_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, e_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge ValEq(\mathcal{A}, W', k-j, (\ell_i \sqcup \ell)\ \sigma, v_1', v_2', \tau\ \sigma)$:

Also given is some $k \leq n$, $W_e \sqsupseteq W, H_1, H_2, v_1', v_2', j$ s.t $(k, H_1, H_2) \triangleright W_e$ and $(H_1, e_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, e_2) \Downarrow^f (H_2', v_2') \wedge j < k$

And we are required to prove
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge ValEq(\mathcal{A}, W', k-j, (\ell_i \sqcup \ell)\ \sigma, v_1', v_2', \tau\ \sigma)$ (FB-U0)

<u>IH</u>: $(W_e, k, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we are given
$\forall I < k.e'\ \gamma \downarrow_1 \Downarrow_I \mathsf{Lb}(v_{h1}) \wedge e'\ \gamma \downarrow_2 \Downarrow \mathsf{Lb}(v_{h1}') \implies$
$(W_e, k-I, \mathsf{Lb}(v_{h1}), \mathsf{Lb}(v_{h1}')) \in \lceil(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rceil_V^{\mathcal{A}}$

Since we know that
$(H_1, \mathsf{unlabel}(e')\ \gamma \downarrow_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, \mathsf{unlabel}(e')\ \gamma \downarrow_2) \Downarrow^f (H_2', v_2') \wedge j < k$ therefore
$\exists I < j < k$ s.t $e'\ \gamma \downarrow_1 \Downarrow_I \mathsf{Lb}(v_{h1}) \wedge e'\ \gamma \downarrow_2 \Downarrow \mathsf{Lb}(v_{h1}')$

Therefore we have
$(W_e, k-I, \mathsf{Lb}(v_{h1}), \mathsf{Lb}(v_{h1}')) \in \lceil(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rceil_V^{\mathcal{A}}$

This means from Definition 2.4 we have
$ValEq(\mathcal{A}, W_e, k-I, \ell\ \sigma, v_{h1}, v_{h1}', \tau\ \sigma)$ (FB-U1)

In order to prove (FB-U0) we choose W' as W_e and from SLIO*-Sem-unlabel we know that $H_1' = H_1$ and $H_2' = H_2$. And we already know that $(k, H_1, H_2) \triangleright W_e$. Therefore from Lemma 2.21 we get $(k-j, H_1, H_2) \triangleright W_e$

From SLIO*-Sem-unlabel we know that v_1', v_2' in (FB-U0) is v_{h1}, v_{h1}' respectively. And since from (FB-U1) we know that $ValEq(\mathcal{A}, W_e, k-I, \ell\ \sigma, v_{h1}, v_{h1}', \tau\ \sigma)$. Therefore from Lemma 2.26 we get
$ValEq(\mathcal{A}, W_e, k-j, (\ell_i \sqcup \ell)\ \sigma, v_{h1}, v_{h1}', \tau\ \sigma)$

(b) $\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, e_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i\ \sigma)\Big)$:

<u>Case $l = 1$</u>
Given some $k, \theta_e \sqsupseteq W.\theta_l, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, e_l) \Downarrow_j^f (H', v_l') \wedge j < k$

<u>We need to prove</u>
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i\ \sigma)$

Since $(W, n, \gamma) \in \lceil\Gamma\rceil_V^{\mathcal{A}}$ therefore from Lemma 2.24 we know that
$\forall m.\ (W.\theta_1, m, \gamma \downarrow_1) \in \lfloor\Gamma\rfloor_V$ and $(W.\theta_2, m, \gamma \downarrow_2) \in \lfloor\Gamma\rfloor_V$

Instantiating m with k we get $(W.\theta_1, k, \gamma \downarrow_1) \in \lfloor\Gamma\rfloor_V$

Now we can apply Theorem 2.22 to get
$(W.\theta_1, k, (\mathsf{unlabel}\ e')\gamma \downarrow_1) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_i \sqcup \ell\ \tau)\ \sigma\rfloor_E$

This means from Definition 2.7 we get
$\forall c < k.(\mathsf{unlabel}\ e')\gamma \downarrow_1 \Downarrow_c v \implies (W.\theta_1, k - c, v) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_i \sqcup \ell\ \tau)\ \sigma\rfloor_V$

This further means that given some $c < k$ s.t $(\mathsf{unlabel}\ e')\gamma \downarrow_1 \Downarrow_c v$. From SLIO*-Sem-val we know that $c = 0$ and $v = (\mathsf{unlabel}\ e')\gamma \downarrow_1$

And we have $(W.\theta_1, k, (\mathsf{unlabel}\ e')\gamma \downarrow_1) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_i \sqcup \ell\ \tau)\ \sigma\rfloor_V$

From Definition 2.6 we have
$\forall K \le k, \theta'_e \sqsupseteq W.\theta_1, H_1, J.(K, H_1) \triangleright \theta'_e \wedge (H_1, (\mathsf{unlabel}\ e')\gamma \downarrow_1) \Downarrow^f_J (H', v') \wedge J < K \implies$
$\exists \theta' \sqsupseteq \theta'_e.(K - J, H') \triangleright \theta' \wedge (\theta', K - J, v') \in \lfloor\tau\rfloor_V \wedge$
$(\forall a.H_1(a) \neq H'(a) \implies \exists \ell'.\theta'_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta'_e).\theta'(a) \searrow \ell_1)$

Instantiating K with k, θ'_e with θ_e, H_1 with H and J with j we get the desired

Case $l = 2$
Symmetric reasoning as in the $l = 1$ case above

16. SLIO*-tolabeled:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{toLabeled}(e') : \mathbb{SLIO}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau)}$$

To prove: $(W, n, \mathsf{toLabeled}(e')\ (\gamma \downarrow_1), \mathsf{toLabeled}(e')\ (\gamma \downarrow_2)) \in \lceil\mathbb{SLIO}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rceil^{\mathcal{A}}_E$

This means from Definition 2.5 we need to prove:
$\forall i < n.\mathsf{toLabeled}(e')\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{toLabeled}(e')\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n - i, v_{f1}, v'_{f1}) \in \lceil\mathbb{SLIO}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rceil^{\mathcal{A}}_V$

This means that given some $i < n$ s.t $\mathsf{toLabeled}(e')\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{toLabeled}(e')\ \gamma \downarrow_2 \Downarrow v'_{f1}$
From SLIO*-Sem-val we know that $v_{f1} = \mathsf{toLabeled}(e')\ \gamma \downarrow_1$, $v_{f2} = \mathsf{toLabeled}(e')\ \gamma \downarrow_2$ and $i = 0$

We are required to prove
$(W, n, \mathsf{toLabeled}(e')\ \gamma \downarrow_1, \mathsf{toLabeled}(e')\ \gamma \downarrow_2) \in \lceil\mathbb{SLIO}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rceil^{\mathcal{A}}_V$

Let $v_1 = \mathsf{toLabeled}(e')\ \gamma \downarrow_1$ and $v_2 = \mathsf{toLabeled}(e')\ \gamma \downarrow_2$
This means from Definition 2.4 we are required to prove
$\Big(\forall k \le n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow^f_j (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k - j, \ell_i, v'_1, v'_2, (\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma)\Big) \wedge$
$\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow^f_j (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor(\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rfloor_V \wedge$

$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_i \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i)\Big)$

We need to prove:

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v_1', v_2', j.$
$(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_2, v_1', v_2', (\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma)$:

This means that we are given some $k \leq n$, $W_e \sqsupseteq W, H_1, H_2, v_1', v_2', j < k$ s.t $(k, H_1, H_2) \triangleright W_e$ and $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2')$

<u>And we need to prove</u>
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_o, v_1', v_2', (\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma)$ (FB-TL0)

<u>IH</u>:
$(W_e, k, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:
$\forall J < k.e'\ \gamma \downarrow_1 \Downarrow_J v_{h1} \wedge e'\ \gamma \downarrow_2 \Downarrow v_{h1}' \implies (W_e, n-J, v_{h1}, v_{h1}') \in \lceil \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(H_1, \mathsf{toLabeled}(e')\gamma \downarrow_1) \Downarrow_j (H_1', v_1')$ and $(H_2, \mathsf{toLabeled}(e')\gamma \downarrow_1) \Downarrow_j (H_2', v_2')$. Therefore from SLIO*-Sem-val we know that $\exists J < j < k \leq n$ s.t $e'\ \gamma \downarrow_1 \Downarrow_J v_{h1}$ and similarly we also know that $e'\ \gamma \downarrow_2 \Downarrow v_{h1}'$

This means we have
$(W_e, k-J, v_{h1}, v_{h1}') \in \lceil \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau\ \sigma \rceil_V^{\mathcal{A}}$

From Definition 2.4 we know that
$\Big(\forall k_1 \leq (k-J), W_e'' \sqsupseteq W_e.\forall H_1'', H_2''.(k_1, H_1'', H_2'') \triangleright W_e'' \wedge \forall v_1'', v_2'', m.$
$(H_1'', v_{h1}) \Downarrow_m^f (H_1', v_1'') \wedge (H_2'', v_{h1}') \Downarrow^f (H_2', v_2'') \wedge m < k_1 \implies$
$\exists W' \sqsupseteq W_e''.(k_1 - m, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k_1 - m, \ell_o, v_1'', v_2'', \tau\ \sigma)\Big) \wedge$
$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_i \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i)\Big)$ (FB-TL1)

We instantiate W_e'' with W_e, H_1'' with H_1, H_2'' with H_2 and k_1 with k in (FB-TL1). Since we know that $(H_1, \mathsf{toLabeled}(e')\gamma \downarrow_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, \mathsf{toLabeled}(e')\gamma \downarrow_2) \Downarrow^f (H_2', v_2')$, therefore $\exists m < j < k \leq n$ s.t $(H_1, v_{h1}) \Downarrow_m^f (H_1', v_1') \wedge (H_2, v_{h1}') \Downarrow^f (H_2', v_2')$
This means we have
$\exists W' \sqsupseteq W_e.(k-m, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-m, \ell_o, v_1'', v_2'', \tau\ \sigma)$
(FB-TL2)

In order to prove (FB-TL0) we choose W' as W' from (FB-TL2). Since from SLIO*-Sem-tolabeled we know that $v_1' = \mathsf{Lb}_{\ell_o}(v_1'')$, $v_2' = \mathsf{Lb}_{\ell_o}(v_2'')$ and $j = m+1$, therefore from Lemma 2.21 we get $(k-j, H_1', H_2') \triangleright W'$.
Since we have by assumption that $\ell_i \sqsubseteq \ell_o$ therefore the following cases arise

i. $\ell_i \sqsubseteq \ell_o \sqsubseteq \mathcal{A}$:
In this case from Definition 2.3 it suffices to prove that
$(W', k-j, v_1', v_2') \in \lceil(\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rceil_V^{\mathcal{A}}$
Since $v_1' = \mathsf{Lb}_{\ell_o}(v_1'')$ and $v_2' = \mathsf{Lb}_{\ell_o}(v_2'')$. Therefore from Definition 2.4 it suffices to prove that
$ValEq(\mathcal{A}, W', k-j, \ell_o, v_1'', v_2'', \tau\ \sigma)$
We get this from (FB-TL2) and Lemma 2.26

ii. $(\ell_i \sqsubseteq \ell_o) \not\sqsubseteq \mathcal{A}$:
In this case from Definition 2.3 it suffices to prove that
$\forall m.(W', m, v_1') \in \lfloor(\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rfloor_V$ and $\forall m.(W', m, v_2') \in \lfloor(\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rfloor_V$
Since $\ell_o \not\sqsubseteq \mathcal{A}$ therefore we get this from (FB-TL2), Definition 2.3 and Definition 2.6

iii. $(\ell_i \sqsubseteq \mathcal{A} \sqsubseteq \ell_o)$:
In this case from Definition 2.3 it suffices to prove that
$(W', k-j, v_1', v_2') \in \lceil(\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rceil_V^{\mathcal{A}}$
Since $v_1' = \mathsf{Lb}_{\ell_o}(v_1'')$ and $v_2' = \mathsf{Lb}_{\ell_o}(v_2'')$. Therefore from Definition 2.4 it suffices to prove that
$\forall m.(W', m, v_1'') \in \lfloor\tau\ \sigma\rfloor_V$ and $\forall m.(W', m, v_2'') \in \lfloor\tau\ \sigma\rfloor_V$
We obtain this directly from (FB-TL2) and Definition 2.3

(b) $\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor(\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_i \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta_e).\theta'(a) \searrow \ell_i)\Big)$:

<u>Case $l = 1$</u>
Given some $k, \theta_e \sqsupseteq W.\theta_l, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k$

<u>We need to prove</u>
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta_e).\theta'(a) \searrow \ell_i\ \sigma)$

Since $(W, n, \gamma) \in \lceil\Gamma\rceil_V^{\mathcal{A}}$ therefore from Lemma 2.24 we know that
$\forall m.\ (W.\theta_1, m, \gamma\downarrow_1) \in \lfloor\Gamma\rfloor_V$ and $(W.\theta_2, m, \gamma\downarrow_2) \in \lfloor\Gamma\rfloor_V$

Instantiating m with k we get $(W.\theta_1, k, \gamma\downarrow_1) \in \lfloor\Gamma\rfloor_V$

Now we can apply Theorem 2.22 to get
$(W.\theta_1, k, (\mathsf{toLabeled}\ e')\gamma\downarrow_1) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_i\ \mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rfloor_E$

This means from Definition 2.7 we get
$\forall c < k.(\mathsf{toLabeled}\ e')\gamma\downarrow_1 \Downarrow_c v \implies (W.\theta_1, k-c, v) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_i\ \mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rfloor_V$

Instantiating c with 0 and from SLIO*-Sem-val we know $v = (\mathsf{toLabeled}\ e')\gamma\downarrow_1$

And we have $(W.\theta_1, k, (\mathsf{toLabeled}\ e')\gamma\downarrow_1) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_i\ \mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rfloor_V$

From Definition 2.6 we have
$\forall K \leq k, \theta_e' \sqsupseteq W.\theta_1, H_1, J.(K, H_1) \triangleright \theta_e' \wedge (H_1, (\mathsf{toLabeled}\ e')\gamma\downarrow_1) \Downarrow_J^f (H', v') \wedge J < K \implies$

$\exists\theta' \sqsupseteq \theta'_e.(K-J, H') \triangleright \theta' \wedge (\theta', K-J, v') \in \lfloor \mathsf{Labeled}\ \ell_o\ \tau)\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H'(a) \implies \exists \ell'.\theta'_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta'_e).\theta'(a) \searrow \ell_i\ \sigma)$

Instantiating K with k, θ'_e with θ_e, H_1 with H and J with j we get the desired

<u>Case $l = 2$</u>
Symmetric reasoning as in the $l = 1$ case above

17. SLIO*-ret:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{ret}(e') : \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau}$$

To prove: $(W, n, \mathsf{ret}(e')\ (\gamma \downarrow_1), \mathsf{ret}(e')\ (\gamma \downarrow_2)) \in \lceil \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:
$\forall i < n.\mathsf{ret}(e')\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{ret}(e')\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n-i, v_{f1}, v'_{f1}) \in \lceil \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{ret}(e')\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{ret}(e')\ \gamma \downarrow_2 \Downarrow v'_{f1}$
From SLIO*-Sem-val we know that $v_{f1} = \mathsf{ret}(e')\gamma \downarrow_1$, $v_{f2} = \mathsf{ret}(e')\gamma \downarrow_2$ and $i = 0$
We are required to prove
$(W, n, \mathsf{ret}(e')\gamma \downarrow_1, \mathsf{ret}(e')\gamma \downarrow_2) \in \lceil \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau\ \sigma \rceil_V^{\mathcal{A}}$

Let $v_1 = \mathsf{ret}(e')\gamma \downarrow_1$ and $v_2 = \mathsf{ret}(e')\gamma \downarrow_2$
From Definition 2.4 it suffices to prove
$\Big(\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k-j, \ell_i, v'_1, v'_2, \tau)\Big) \wedge$
$\forall l \in \{1, 2\}.\Big(\forall v, i.\ (e_l \Downarrow_i v_l) \implies$
$\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v'_l) \in \lfloor \tau \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_1)\Big)$

It suffices to prove:

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k-j, \ell_i, v'_1, v'_2, \tau)$:

We are given is some $k \leq n$, $W_e \sqsupseteq W, H_1, H_2, v'_1, v'_2, j < k$ s.t $(k, H_1, H_2) \triangleright W_e$ and $(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2)$

From SLIO*-Sem-ret we know that $H'_1 = H_1$ and $H'_2 = H_2$

<u>And we are required to prove:</u>

$\exists W' \sqsupseteq W_e.(k-j, H_1, H_2) \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_i, v'_1, v'_2, \tau)$ (FB-R0)

IH: $(W_e, n, e'\ (\gamma\downarrow_1), e'\ (\gamma\downarrow_2)) \in \lceil\tau\ \sigma\rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:
$\forall J < k.e'\ \gamma\downarrow_1\Downarrow_J v_{h1} \wedge e'\ \gamma\downarrow_2\Downarrow v'_{h1} \implies (W_e, k-J, v_{h1}, v'_{h1}) \in \lceil\tau\ \sigma\rceil_V^{\mathcal{A}}$

Since we know that $(H_1, \mathsf{ret}(e')\gamma\downarrow_1) \Downarrow_j^f (H_1, v'_1) \wedge (H_2, \mathsf{ret}(e')\gamma\downarrow_2) \Downarrow^f (H_2, v'_2)$, therefore $\exists J < j < k$ s.t $e'\ \gamma\downarrow_1\Downarrow_J v_{h1}$ and similarly $e'\ \gamma\downarrow_2\Downarrow v'_{h1}$.
Therefore we have $(W_e, k-J, v_{h1}, v'_{h1}) \in \lceil\tau\ \sigma\rceil_V^{\mathcal{A}}$ (FB-R1)

In order to prove (FB-R0) we choose W' as W_e and from SLIO*-Sem-ret we know that $v'_1 = v_{h1}$ and $v'_2 = v'_{h1}$. We need to prove the following:

i. $(k-j, H_1, H_2) \triangleright W_e$:
Since we have $(k, H_1, H_2) \triangleright W_e$ therefore from Lemma 2.21 we get
$(k-j, H_1, H_2) \triangleright W_e$

ii. $\mathit{ValEq}(\mathcal{A}, W_e, k-j, \ell_i, v'_1, v'_2, \tau)$:
2 cases arise:

A. $\ell_i \sqsubseteq \mathcal{A}$:
In this case from Definition 2.3 it suffices to prove
$(W_e, k-j, v'_1, v'_2) \in \lceil\tau\ \sigma\rceil_V^{\mathcal{A}}$

Since $j = J+1$ therefore we get this from (FB-R1) and Lemma 2.17

B. $\ell_i \not\sqsubseteq \mathcal{A}$:
In this case from Definition 2.3 it suffices to prove that
$\forall m.(W_e, m, v'_1) \in \lfloor\tau\ \sigma\rfloor_V$ and $\forall m.(W_e, m, v'_2) \in \lfloor\tau\ \sigma\rfloor_V$

We get this From (FB-R1) and Lemma 2.15

(b) $\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k \implies$
$\exists\theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v'_l) \in \lfloor\tau\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists\ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in \mathit{dom}(\theta')\backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_i\ \sigma)$:

Case $l = 1$
Given some $k, \theta_e \sqsupseteq W.\theta_l, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k$

We need to prove
$\exists\theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v'_l) \in \lfloor\tau\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists\ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in \mathit{dom}(\theta')\backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_i\ \sigma)$

Since $(W, n, \gamma) \in \lceil\Gamma\rceil_V^{\mathcal{A}}$ therefore from Lemma 2.24 we know that
$\forall m.\ (W.\theta_1, m, \gamma\downarrow_1) \in \lfloor\Gamma\rfloor_V$ and $(W.\theta_2, m, \gamma\downarrow_2) \in \lfloor\Gamma\rfloor_V$

Instantiating m with k we get $(W.\theta_1, k, \gamma\downarrow_1) \in \lfloor\Gamma\rfloor_V$

Now we can apply Theorem 2.22 to get
$(W.\theta_1, k, (\mathsf{ret}\ e')\gamma\downarrow_1) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_i\ \tau)\ \sigma\rfloor_E$

This means from Definition 2.7 we get
$\forall c < k.(\mathsf{ret}\ e')\gamma\downarrow_1\Downarrow_c v \implies (W.\theta_1, k-c, v) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_i\ \tau)\ \sigma\rfloor_V$

Instantiating c with 0 and from SLIO*-Sem-val we know that $v = (\mathsf{ret}\ e')\gamma \downarrow_1$

And we have $(W.\theta_1, k, (\mathsf{ret}\ e')\gamma \downarrow_1) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_i\ \tau)\ \sigma\rfloor_V$

From Definition 2.6 we have
$\forall K \leq k, \theta'_e \sqsupseteq W.\theta_1, H_1, J.(K, H_1) \triangleright \theta'_e \wedge (H_1, v) \Downarrow^f_J (H', v') \wedge J < K \implies$
$\exists \theta' \sqsupseteq \theta'_e.(K - J, H') \triangleright \theta' \wedge (\theta', K - J, v') \in \lfloor\tau)\ \sigma\rfloor_V \wedge$
$(\forall a.H_1(a) \neq H'(a) \implies \exists \ell'.\theta'_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta'_e).\theta'(a) \searrow \ell_i\ \sigma)$

Instantiating K with k, θ'_e with θ_e, H_1 with H and J with j we get the desired

Case $l = 2$
Symmetric reasoning as in the $l = 1$ case above

18. SLIO*-bind:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_l : \mathbb{SLIO}\ \ell_i\ \ell\ \tau \qquad \Sigma; \Psi; \Gamma, x : \tau \vdash e_b : \mathbb{SLIO}\ \ell\ \ell_o\ \tau'}{\Sigma; \Psi; \Gamma \vdash \mathsf{bind}(e_l, x.e_b) : \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau'}$$

To prove: $(W, n, \mathsf{bind}(e_l, x.e_b)\ (\gamma \downarrow_1), \mathsf{bind}(e_l, x.e_b)\ (\gamma \downarrow_2)) \in \lceil\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau'\ \sigma\rceil^{\mathcal{A}}_E$

This means from Definition 2.5 we need to prove:
$\forall i < n.\mathsf{bind}(e_l, x.e_b)\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{bind}(e_l, x.e_b)\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n - i, v_{f1}, v'_{f1}) \in \lceil\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau'\ \sigma\rceil^{\mathcal{A}}_V$

This means that given some $i < n$ s.t $\mathsf{bind}(e_l, x.e_b)\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{bind}(e_l, x.e_b)\ \gamma \downarrow_2 \Downarrow v'_{f1}$
From SLIO*-Sem-val we know that $v_{f1} = \mathsf{bind}(e_l, x.e_b)\gamma \downarrow_1$, $v_{f2} = \mathsf{bind}(e_l, x.e_b)\gamma \downarrow_2$ and $i = 0$

We are required to prove
$(W, n, \mathsf{bind}(e_l, x.e_b)\gamma \downarrow_1, \mathsf{bind}(e_l, x.e_b)\gamma \downarrow_2) \in \lceil\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau'\ \sigma\rceil^{\mathcal{A}}_V$

Let $v_1 = \mathsf{bind}(e_l, x.e_b)\gamma \downarrow_1$ and $v_2 = \mathsf{bind}(e_1, x.e_b)\gamma \downarrow_2$
This means from Definition 2.4 we need to prove
$\Big(\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow^f_j (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k - j, \ell_o, v'_1, v'_2, \tau\ \sigma)\Big) \wedge$
$\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow^f_j (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor\tau\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'\ \sigma \wedge \ell_i \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i)\Big)$

This means we need to prove:

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2, j.$
$(H_1, v_1) \Downarrow^f_j (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k - j, \ell_o, v'_1, v'_2, \tau\ \sigma)$:

This means we are given some $k \leq n$, $W_e \sqsupseteq W, H_1, H_2$ s.t $(k, H_1, H_2) \triangleright W_e$

Also given some $v_1', v_2', j < k$ s.t $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2')$

<u>And we are required to prove:</u>
$\exists W' \sqsupseteq W_e.(k - j, H_1', H_2') \triangleright W' \wedge ValEq(\mathcal{A}, W', k - j, \ell_o, v_1', v_2', \tau' \ \sigma)$ (FB-B0)

<u>IH1</u>:
$(W_e, k, e_l \ (\gamma \downarrow_1), e_l \ (\gamma \downarrow_2)) \in \lceil \mathbb{SLIO} \ \ell_i \ \ell \ \tau \ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:
$\forall f < k.e_l \ \gamma \downarrow_1 \Downarrow_f v_{h1} \wedge e_l \ \gamma \downarrow_2 \Downarrow v_{h1}' \implies$
$(W_e, k - f, v_{h1}, v_{h1}') \in \lceil \mathbb{SLIO} \ \ell_i \ \ell \ \tau \ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2')$ therefore $\exists f < j < k$ s.t $e_l \ \gamma \downarrow_f \Downarrow_j v_{h1} \wedge e_l \ \gamma \downarrow_2 \Downarrow v_{h1}'$

This means we have
$(W_e, k - f, v_{h1}, v_{h1}') \in \lceil \mathbb{SLIO} \ \ell_i \ \ell \ \tau \ \sigma \rceil_V^{\mathcal{A}}$

This means from Definition 2.4 we have
$\Big(\forall K \leq (k - f), W_e' \sqsupseteq W_e.\forall H_1'', H_2''.(K, H_1'', H_2'') \triangleright W_e' \wedge \forall v_1'', v_2'', J.$
$(H_1'', v_{h1}) \Downarrow_J^f (H_1', v_1'') \wedge (H_2'', v_{h1}') \Downarrow^f (H_2', v_2'') \wedge J < K \implies$
$\exists W'' \sqsupseteq W_e'.(K - J, H_1', H_2') \triangleright W'' \wedge ValEq(\mathcal{A}, W'', K - J, \ell \ \sigma, v_1'', v_2'', \tau \ \sigma)\Big) \wedge$
$\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v_l') \in \lfloor \tau \ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled} \ \ell' \ \tau' \ \sigma \wedge \ell_i \ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i \ \sigma)\Big)$

Instantiating K with $(k - f)$, W_e' with W_e, H_1'' with H_1 and H_2'' with H_2 in the first conjunct of the above equation. Since we know that $(k, H_1, H_2) \triangleright W_e$ therefore from Lemma 2.21 we also have $(k - f, H_1, H_2) \triangleright W_e$

Since we know that $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2')$ therefore $\exists J < j - f < k - f$ s.t $(H_1, v_{h1}) \Downarrow_J^f (H_1', v_1'') \wedge (H_2, v_{h1}') \Downarrow^f (H_2', v_2'')$

This means we have
$\exists W'' \sqsupseteq W_e'.(k - f - J, H_1', H_2') \triangleright W'' \wedge ValEq(\mathcal{A}, W'', k - f - J, \ell \ \sigma, v_1'', v_2'', \tau \ \sigma)$ (FB-B1)

From Definition 2.3 two cases arise:

i. $\ell \ \sigma \sqsubseteq \mathcal{A}$:

   In this case we know that $(W'', k - f - J, v_1'', v_2'') \in \lceil \tau \ \sigma \rceil_V^{\mathcal{A}}$
   <u>IH2</u>:
   $(W'', k - f - J, e_b \ (\gamma \downarrow_1 \cup \{x \mapsto v_1''\}), e_b \ (\gamma \downarrow_2 \cup \{x \mapsto v_2''\})) \in \lceil \mathbb{SLIO} \ \ell \ \ell_o \ \tau' \ \sigma \rceil_E^{\mathcal{A}}$

   This means from Definition 2.5 we need to prove:
   $\forall s < k - f - J.e_b \ (\gamma \downarrow_1 \cup \{x \mapsto v_1''\}) \Downarrow_s v_{h2} \wedge e_b \ (\gamma \downarrow_2 \cup \{x \mapsto v_2''\}) \Downarrow v_{h2}' \implies$
   $(W'', k - f - J - s, v_{h2}, v_{h2}') \in \lceil \mathbb{SLIO} \ \ell \ \ell_o \ \tau' \ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(H_1, \mathsf{bind}(e_l, x.e_b)\ \gamma \downarrow_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, \mathsf{bind}(e_l, x.e_b)\ \gamma \downarrow_2) \Downarrow^f (H_2', v_2')$ therefore $\exists s < j - f - J < k - f - J$ s.t $e_b\ (\gamma \downarrow_1 \cup \{x \mapsto v_1''\}) \Downarrow_s v_{h2} \wedge e_b\ (\gamma \downarrow_2 \cup \{x \mapsto v_2''\}) \Downarrow v_{h2}'$

This means we have
$(W'', k - f - J - s, v_{h2}, v_{h2}') \in \lceil \mathbb{SLIO}\ \ell\ \ell_o\ \tau'\ \sigma \rceil_V^{\mathcal{A}}$

This means from Definition 2.4 we know that
$\Big(\forall K_s \leq (k - f - J - s), W_s \sqsupseteq W''.\forall H_1, H_2.(K_s, H_1, H_2) \triangleright W_s \wedge \forall v_{s1}', v_{s2}', J_s.$
$(H_1, v_{h2}) \Downarrow_{J_s}^f (H_{s1}', v_{s1}') \wedge (H_2, v_{h2}') \Downarrow^f (H_{s2}', v_{s2}') \wedge J_s < K_s \implies$
$\exists W_s' \sqsupseteq W_s.(K_s - J_s, H_{s1}', H_{s2}') \triangleright W_s' \wedge \mathit{ValEq}(\mathcal{A}, W_s', K_s - J_s, \ell_i, v_1', v_2', \tau'\ \sigma)\Big) \wedge$
$\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v_l') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'\ \sigma \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_1)\Big)$

Instantiating K_s with $(k - f - J - s)$, W_s with W'', H_1 with H_1' and H_2' with H_2. Since we know that $(k - f - J, H_1', H_2') \triangleright W''$ therefore from Lemma 2.21 we also have $(k - f - J - s, H_1', H_2') \triangleright W''$

Since we know that $(H_1, \mathsf{bind}(e_l, x.e_b)\ \gamma \downarrow_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, \mathsf{bind}(e_l, x.e_b)\ \gamma \downarrow_2) \Downarrow^f (H_2', v_2')$ therefore $\exists J_s < j - f - J - s < k - f - J - s$ s.t $(H_1', v_1'') \Downarrow_{J_s}^f (H_{s1}', v_{s1}') \wedge (H_2', v_2'') \Downarrow^f (H_{s2}', v_{s2}')$

This means we have
$\exists W_s' \sqsupseteq W_s.(k - f - J - s - J_s, H_{s1}', H_{s2}') \triangleright W_s' \wedge \mathit{ValEq}(\mathcal{A}, W_s', k - f - J - s - J_S, \ell_o, v_{s1}', v_{s2}', \tau'\ \sigma)$ (FB-B2)

In order to prove (FB-B0) we choose W' as W_s'. From SLIO*-Sem-bind we know that $H_1' = H_{s1}'$, $H_2' = H_{s2}'$, $v_1' = v_{s1}'$, $v_2' = v_{s2}'$ and $j = f + J + s + J_s + 1$. And we need to prove:

A. $(k - j, H_{s1}', H_{s2}') \triangleright W_s'$:
Since from (FB-B2) we know that $(k - f - J - s - J_s, H_{s1}', H_{s2}') \triangleright W_s'$ therefore from Lemma 2.21 we get
$(k - j, H_{s1}', H_{s2}') \triangleright W_s'$

B. $\mathit{ValEq}(\mathcal{A}, W_s', k - j, \ell_o, v_{s1}', v_{s2}', \tau'\ \sigma)$:
Since from (FB-B2) we know that $\mathit{ValEq}(\mathcal{A}, W_s', k - f - J - s - J_S, \ell_o, v_{s1}', v_{s2}', \tau'\ \sigma)$ therefore from Lemma 2.26 we get
$\mathit{ValEq}(\mathcal{A}, W_s', k - j, \ell_o, v_{s1}', v_{s2}', \tau'\ \sigma)$

ii. $\ell\ \sigma \not\sqsubseteq \mathcal{A}$:

From (FB-B0) we know that we need to prove
$\exists W' \sqsupseteq W_e.(k - j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k - j, \ell_o, v_1', v_2', \tau'\ \sigma)$
Since $\ell_i\ \sigma \sqsubseteq \ell\ \sigma \sqsubseteq \ell_o\ \sigma$ (by assumption) and $\ell\ \sigma \not\sqsubseteq \mathcal{A}$ therefore we have $\ell_o\ \sigma \not\sqsubseteq \mathcal{A}$

This means that from Definition 2.3 it suffices to prove
$\exists W' \sqsupseteq W_e.(k - j, H_1', H_2') \triangleright W' \wedge \forall m_{u1}.(W'.\theta_1, m_{u1}, v_1') \in \lfloor \tau'\ \sigma \rfloor_V \wedge \forall m_{u2}.(W'.\theta_2, m_{u2}, v_2') \in \lfloor \tau'\ \sigma \rfloor_V$

This means given some m_{u1}, m_{u2} and we need to prove

$\exists W' \sqsupseteq W_e.(k - j, H_1', H_2') \triangleright W' \wedge (W'.\theta_1, m_{u1}, v_1') \in \lfloor \tau' \ \sigma \rfloor_V \wedge (W'.\theta_2, m_{u2}, v_2') \in \lfloor \tau' \ \sigma \rfloor_V$ (FB-B01)

In this case we know that
$\forall m.\ (W''.\theta_1, m, v_1'') \in \lfloor \tau \ \sigma \rfloor_V$ and $\forall m.\ (W''.\theta_2, m, v_2'') \in \lfloor \tau \ \sigma \rfloor_V$ (FB-B3)

Since $\mathsf{bind}(e_l, x.e_b)\gamma \downarrow_1 \Downarrow_j v_1'$ therefore $\exists J_1 < j - f - J < k - f - J$ s.t $(e_b)\gamma \downarrow_1 \cup \{x \mapsto v_1''\} \Downarrow_{J_1} v_1'$. Similarly, $\exists J_1' < j - f - J - J_1 < k - f - J - J_1$ s.t $(H_1', v_1') \Downarrow^f_{J_1'} -$

Instantiating m with $m_{u1} + 1 + J_1 + J_1'$ in the first conjunct of (FB-B3)
$(W''.\theta_1, m_{u1} + 1 + J_1 + J_1', v_1'') \in \lfloor \tau \ \sigma \rfloor_V$

Since $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$ therefore from Lemma 2.24 we know that
$\forall m.\ (W.\theta_1, m, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$

Instantiating m with $m_{u1}+1+J_1+J_1'$ we get $(W.\theta_1, m_{u1}+1+J_1+J_1', \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$

From Lemma 2.18 we know that
$(W''.\theta_1, m_{u1} + 1 + J_1 + J_1', \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$ (FB-B4)

Now we can apply Theorem 2.22 to get
$(W''.\theta_1, m_{u1} + 1 + J_1 + J_1', (e_b)\gamma \downarrow_1 \cup \{x \mapsto v_1''\}) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell_o\ \tau')\ \sigma \rfloor_E$

This means from Definition 2.7 we get
$\forall c_1 < m_{u1} + 1 + J_1 + J_1'.(e_b)\gamma \downarrow_1 \cup \{x \mapsto v_1''\} \Downarrow_{c_1} v_{o1} \implies (W''.\theta_1, m_{u1} + 1 + J_1 + J_1' - c_1, v_{o1}) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell_o\ \tau')\ \sigma \rfloor_V$ (FB-B5)

Instantiating c_1 with J_1 in (FB-B5)
Therefore we have $(W''.\theta_1, m_{u1} + 1 + J_1', v_{o1}) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell_o\ \tau')\ \sigma \rfloor_V$

From Definition 2.6 we have
$\forall K \leq (m_{u1}+1+J_1'), \theta_e' \sqsupseteq W''.\theta_1, H_1, J_2.(K, H_1) \triangleright \theta_e' \wedge (H_1, v_{o1}) \Downarrow^f_{J_2} (H_1'', v_1') \wedge J_2 < K \implies$
$\exists \theta_1' \sqsupseteq \theta_e'.(K - J_2, H_1'') \triangleright \theta_1' \wedge (\theta_1', K - J_2, v_1') \in \lfloor \tau' \ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1''(a) \implies \exists \ell'.\theta_e'(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1')/dom(\theta_e').\theta_1'(a) \searrow \ell_i\ \sigma)$

Instantiating K with $m_{u1} + 1 + J_1'$, θ_e' with $W''.\theta_1$, H_1 with H_1' (from FB-B1) and J_2 with J_1' we get

$\exists \theta_1' \sqsupseteq W''.\theta_1.(m_{u1} + 1, H_1'') \triangleright \theta_1' \wedge (\theta_1', m_{u1} + 1, v_1') \in \lfloor \tau' \ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H_1''(a) \implies \exists \ell'.W''.\theta_1(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1')/dom(\theta_e').\theta_1'(a) \searrow \ell_i\ \sigma)$ (FB-B6)

Since we know that $\mathsf{bind}(e_l, x.e_b)\gamma \downarrow_2 \Downarrow v_2'$. Say this reduction happens in t steps. Therefore $\exists t_1 < t < k \leq n$ s.t $(e_l)\gamma \downarrow_2 \cup \{x \mapsto v_2''\} \Downarrow_{t_1} v_{l2}$ and simialrly $\exists t_2 < t - t_1 < k - t_1$ s.t $(H, v_{l2})\gamma \downarrow_2 \Downarrow^f_{t_2} (H_2'', v_2'')$

Again since $\mathsf{bind}(e_l, x.e_b)\gamma \downarrow_2 \Downarrow_t v_2'$ therefore $\exists J_2 < t - t_1 - t_2 < k - t_1 - t_2$ s.t $(e_b)\gamma \downarrow_2 \cup \{x \mapsto v_2''\} \Downarrow_{J_2} v_2'$. Similarly $\exists J_2' < t - t_1 - t_2 - J_2 < k - t_1 - t_2 - J_2$ s.t $(H_2', v_2') \Downarrow^f_{J_2'} -$

Instantiating the second conjunct of (FB-B3) with $m_{u2} + 1 + J_2 + J_2'$ we get
$(W''.\theta_2, m_{u2} + 1 + J_2 + J_2', v_2'') \in \lfloor \tau \ \sigma \rfloor_V$

Again since $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$ therefore from Lemma 2.24 we know that
$\forall m.\ (W.\theta_2, m, \gamma \downarrow_2) \in \lfloor \Gamma \rfloor_V$

Instantiating m with $m_{u2}+1+J_2+J_2'$ we get $(W.\theta_2, m_{u2}+1+J_2+J_2', \gamma \downarrow_2) \in \lfloor \Gamma \rfloor_V$

From Lemma 2.18 we know that
$(W''.\theta_2, m_{u2} + 1 + J_2 + J_2', \gamma \downarrow_2) \in \lfloor \Gamma \rfloor_V$ (FB-B7)

Now we can apply Theorem 2.22 to get
$(W''.\theta_2, m_{u2} + 1 + J_2 + J_2', (e_b)\gamma \downarrow_2 \cup \{x \mapsto v_2''\}) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell_o\ \tau')\ \sigma \rfloor_E$

This means from Definition 2.7 we get
$\forall c_2 < (m_{u2} + 1 + J_2 + J_2').(e_b)\gamma \downarrow_2 \cup \{x \mapsto v_2''\} \Downarrow_{c_2} v_{o2} \implies (W''.\theta_2, m_{u2} + 1 + J_2 - c_2, v_{o2}) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell_o\ \tau')\ \sigma \rfloor_V$ (FB-B8)

Instantiating c_2 with J_2 in (FB-B8) we get
$(W''.\theta_2, m_{u2} + 1 + J_2', v_{o2}) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell_o\ \tau')\ \sigma \rfloor_V$

From Definition 2.6 we have
$\forall K \leq (m_{u2}+1+J_2'), \theta_e' \sqsupseteq W''.\theta_2, H_2, J_3.(K, H_2) \triangleright \theta_e' \wedge (H_2, v_{o2}) \Downarrow_{J_3}^f (H_2'', v_2') \wedge J_3 < K \implies$
$\exists \theta_2' \sqsupseteq \theta_e'.(K - J_3, H_2'') \triangleright \theta_2' \wedge (\theta_2', K - J_3, v_2') \in \lfloor \tau'\ \sigma \rfloor_V \wedge$
$(\forall a. H_2(a) \neq H_2''(a) \implies \exists \ell'.\theta_e'(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2')/dom(\theta_e').\theta_2'(a) \searrow \ell\ \sigma)$

Instantiating K with $m_{u2} + 1 + J_2'$, θ_e' with $W''.\theta_2$, H_2 with H_2' (from FB-B1) and J_3 with J_2', we get

$\exists \theta_2' \sqsupseteq W''.\theta_2.(m_{u2} + 1, H_2'') \triangleright \theta_2' \wedge (\theta_2', m_{u2} + 1, v_2') \in \lfloor \tau'\ \sigma \rfloor_V \wedge$
$(\forall a. H_2(a) \neq H_2''(a) \implies \exists \ell'. W''.\theta_2(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2')/dom(\theta_e').\theta_2'(a) \searrow \ell\ \sigma)$ (FB-B9)

In order to prove (FB-B01) we chose W' as W_n where W_n is defined as follows:
$W_n.\theta_1 = \theta_1'$ (From (FB-B6))
$W_n.\theta_2 = \theta_2'$ (From (FB-B9))
$W_n.\hat{\beta} = W''.\hat{\beta}$ (From (FB-B1))

It suffices to prove

- $(k - j, H_1'', H_2'') \triangleright W_n$:
  From Definition 2.9 we need to prove the following
  - $dom(W_n.\theta_1) \subseteq dom(H_1'') \wedge dom(W_n.\theta_2) \subseteq dom(H_2'')$:

    From (FB-B6) we know that $(m_{u1}+1, H_1'') \triangleright \theta_1'$ therefore from Definition 2.8 we know that $dom(W_n.\theta_1) \subseteq dom(H_1'')$
    Similarly from (FB-B9) we know that $(m_{u2} + 1, H_2'') \triangleright \theta_2'$ therefore from Definition 2.8 we know that $dom(W_n.\theta_2) \subseteq dom(H_2'')$

  - $(W_n.\hat{\beta}) \subseteq (dom(W_n.\theta_1) \times dom(W_n.\theta_2))$:

    Since from (FB-B1) we know that $(k - f - J, H_1', H_2') \triangleright W''$ therefore from Definition 2.9 we know that $(W''.\hat{\beta}) \subseteq (dom(W''.\theta_1) \times dom(W''.\theta_2))$

    Since from (FB-B6) and (FB-B9) we know that $W''.\theta_1 \sqsubseteq W_n.\theta_1$ and $W''.\theta_2 \sqsubseteq W_n.\theta_2$

    Therefore we get
    $(W_n.\hat{\beta}) \subseteq (dom(W_n.\theta_1) \times dom(W_n.\theta_2))$

– $\forall(a_1, a_2) \in (W_n.\hat{\beta}).(W_n.\theta_1(a_1) = W_n.\theta_2(a_2) \wedge (W_n, k-j-1, H_1''(a_1), H_2''(a_2)) \in \lceil W_n.\theta_1(a_1)\rceil_V^{\mathcal{A}})$:

4 cases arise for each $(a_1, a_2) \in W_n.\hat{\beta}$

A. $H_1'(a_1) = H_1''(a_1) \wedge H_2'(a_2) = H_2''(a_2)$:

<u>To prove:</u>
$W_n.\theta_1(a_1) = W_n.\theta_2(a_2)$:
We know from that $(k - f - J, H_1', H_2') \triangleright W''$

Therefore from Definition 2.9 we have
$\forall(a_1', a_2') \in (W''.\hat{\beta}). W''.\theta_1(a_1') = W''.\theta_2(a_2')$

Since $W_n.\hat{\beta} = W''.\hat{\beta}$ by construction therefore
$\forall(a_1', a_2') \in (W_n.\hat{\beta}). W''.\theta_1(a_1') = W''.\theta_2(a_2')$

From (FB-B6) and (FB-B9) we know that $W''.\theta_1 \sqsubseteq \theta_1'$ and $W''.\theta_2 \sqsubseteq \theta_2'$ respectively.

Therefore from Definition 2.1
$\forall(a_1', a_2') \in (W_n.\hat{\beta}).\theta_1'(a_1) = \theta_2'(a_2)$

<u>To prove:</u>
$(W_n, k - j - 1, H_1''(a_1), H_2''(a_2)) \in \lceil W_n.\theta_1(a_1)\rceil_V^{\mathcal{A}}$:
From (FB-B1) we know that $(k - f - J, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W''$

This means from Definition 2.9 we know that
$\forall(a_{i1}, a_{i2}) \in (W''.\hat{\beta}). W''.\theta_1(a_{i1}) = W''.\theta_2(a_{i2}) \wedge$
$(W'', k - f - J - 1, H_1'(a_{i1}), H_2'(a_{i2})) \in \lceil W''.\theta_1(a_{i1})\rceil_V^{\mathcal{A}}$

Instantiating with a_1 and a_2 and since $W'' \sqsubseteq W_n$ and $k - j - 1 < k - f - J - 1$ (since $j = f + J + J_1 + 1$ therefore from Lemma 2.17 we get
$(W_n, k - j - 1, H_1'(a_1), H_2'(a_2)) \in \lceil W_n.\theta_1(a_1)\rceil_V^{\mathcal{A}}$

B. $H_1'(a_1) \neq H_1''(a_1) \wedge H_2'(a_2) \neq H_2''(a_2)$:

<u>To prove:</u>
$W_n.\theta_1(a_1) = W_n.\theta_2(a_2)$
Same reasoning as in the previous case

<u>To prove:</u>
$(W_n, k - j - 1, H_1''(a_1), H_2''(a_2)) \in \lceil W_n.\theta_1(a_1)\rceil_V^{\mathcal{A}}$
From (FB-B6) and (FB-B9) we know that
$(\forall a.H_1'(a) \neq H_1''(a) \implies \exists \ell'. W''.\theta_1(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge (\ell\ \sigma) \sqsubseteq \ell')$
$(\forall a.H_2'(a) \neq H_2''(a) \implies \exists \ell'. W''.\theta_2(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge (\ell\ \sigma) \sqsubseteq \ell')$
This means we have
$\exists \ell'. W''.\theta_1(a_1) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge (\ell\ \sigma) \sqsubseteq \ell'$ and
$\exists \ell'. W''.\theta_2(a_2) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge (\ell\ \sigma) \sqsubseteq \ell'$

Since $\ell\ \sigma \not\sqsubseteq \mathcal{A}$. Therefore, $\ell' \not\sqsubseteq \mathcal{A}$.

Also from (FB-B6) and (FB-B9), $(m_{u1}+1, H_1'') \triangleright \theta_1'$ and $(m_{u2}+1, H_2'') \triangleright \theta_2'$.
Therefore from Definition 2.8 we have

$(\theta'_1, m_{u1}, H''_1(a_1)) \in \lfloor \theta'_1(a_1) \rfloor_V$ and
$(\theta'_2, m_{u2}, H''_2(a_1)) \in \lfloor \theta'_2(a_2) \rfloor_V$

Since m_{u1} and m_{u2} are arbitrary indices therefore from Definition 2.4 we get
$(W_n, k-j-1, H''_1(a_1), H''_2(a_2)) \in \lceil \theta'_1(a_1) \rceil_V^{\mathcal{A}}$

C. $H'_1(a_1) = H''_1(a_1) \wedge H'_2(a_2) \neq H''_2(a_2)$:

To prove:
$W_n.\theta_1(a_1) = W_n.\theta_2(a_2)$
Same reasoning as in the previous case

To prove:
$(W_n, k-j-1, H''_1(a_1), H''_2(a_2)) \in \lceil W_n.\theta_1(a_1) \rceil_V^{\mathcal{A}}$

From (FB-B9) we know that
$(\forall a.H'_2(a) \neq H''_2(a) \implies \exists \ell'. W''.\theta_2(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge (\ell\ \sigma) \sqsubseteq \ell')$

This means we have
$\exists \ell'. W''.\theta_2(a_2) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge (\ell\ \sigma) \sqsubseteq \ell'$
Since $\ell\ \sigma \not\sqsubseteq \mathcal{A}$. Therefore, $\ell' \not\sqsubseteq \mathcal{A}$.

Since from (FB-B1) we know that $(k-f-J, H'_1, H'_2) \overset{\mathcal{A}}{\triangleright} W''$ that means from Definition 2.9 that $(W'', k-f-J-1, H'_1(a_1), H'_2(a_2)) \in \lceil W''.\theta_1(a_1) \rceil_V^{\mathcal{A}}$.
Since $W''.\theta_1(a_1) = W''.\theta_2(a_2) = \mathsf{Labeled}\ \ell'\ \tau''$ and since $\ell' \not\sqsubseteq \mathcal{A}$ therefore from Definition 2.4 and Definition 2.3 we know that

Therefore
$\forall m.\ (W''.\theta_1, m, H'_1(a_1)) \in W''.\theta_1(a_1)$ (F)

Instantiating the (F) with m_{u1} and using Lemma 2.16 we get
$(\theta'_1, m_{u1}, H'_1(a_1)) \in \theta'_1(a_1)$

Since from (FB-B9) we know that $(m_{u2}+1, H''_2) \triangleright \theta'_2$ therefore from Definition 2.8 we know that $(\theta'_2, m_{u2}, H''_2(a_2)) \in \theta'_2(a_2)$
Therefore from Definition 2.4 we get
$(W', k-j-1, H''_1(a_1), H''_2(a_2)) \in \lceil \theta'_1(a_1) \rceil_V^{\mathcal{A}}$

D. $H'_1(a_1) \neq H''_1(a_1) \wedge H'_2(a_2) = H''_2(a_2)$:
Symmetric reasoning as in the previous case

– $\forall i \in \{1,2\}.\forall m.\forall a_i \in dom(W_n.\theta_i).(W_n.\theta_i, m, H''_i(a_i)) \in \lfloor W_n.\theta_i(a_i) \rfloor_V$:

Case $i = 1$
Given some m we need to prove
$\forall a_i \in dom(W_n.\theta_i).(W_n.\theta_i, m, H''_i(a_i)) \in \lfloor W_n.\theta_i(a_i) \rfloor_V$

This further means that given some $a_1 \in dom(W_n.\theta_i)$ we need to show
$(W_n.\theta_1, m, H''_1(a_1)) \in \lfloor W_n.\theta_1(a_1) \rfloor_V$

Since $W_n.\theta_1 = \theta'_1$, it suffices to prove
$(\theta'_1, m, H''_1(a_1)) \in \lfloor \theta'_1(a_1) \rfloor_V$

Like before we apply Theorem 2.22 on $e_b\ \gamma \downarrow_1 \cup \{x \mapsto v''_1\}$ but this time at $m+1+J_1+J'_1$ to get

$\exists \theta'_1 \sqsupseteq W''.\theta_1.(m+1, H''_1) \triangleright \theta'_1 \wedge (\theta'_1, m_{u1}+1, v'_1) \in \lfloor \tau' \ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H''_1(a) \implies \exists \ell'.W''.\theta_1(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'_1)/dom(\theta'_e).\theta'_1(a) \searrow \ell_i\ \sigma)$

Since we have $(m+1, H''_1) \triangleright \theta'_1$ therefore from Definition 2.8 we get the desired.

Case $i = 2$

Similar reasoning as in the $i = 1$ case

- $(W'.\theta_1, m_{u1}, v'_1) \in \lfloor \tau' \ \sigma \rfloor_V \wedge (W'.\theta_2, m_{u2}, v'_2) \in \lfloor \tau' \ \sigma \rfloor_V$:
  We get this from (FB-B6), (FB-B9) and Lemma 2.16 we get the desired

19. SLIO*-ref:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \mathsf{Labeled}\ \ell'\ \tau \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash \mathsf{new}\ (e') : \mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau)}$$

To prove: $(W, n, \mathsf{new}\ (e')\ (\gamma \downarrow_1), \mathsf{new}\ (e')\ (\gamma \downarrow_2)) \in \lceil (\mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau))\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:
$\forall i < n.\mathsf{new}\ (e')\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{new}\ (e')\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n-i, v_{f1}, v'_{f1}) \in \lceil (\mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau))\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{new}\ (e')\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{new}\ (e')\ \gamma \downarrow_2 \Downarrow v'_{f1}$
From SLIO*-Sem-val we know that $v_{f1} = \mathsf{new}\ (e')\gamma \downarrow_1$, $v_{f2} = \mathsf{new}\ (e')\gamma \downarrow_2$ and $i = 0$
We are required to prove
$(W, n, \mathsf{new}\ (e')\gamma \downarrow_1, \mathsf{new}\ (e')\gamma \downarrow_2) \in \lceil (\mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau))\ \sigma \rceil_V^{\mathcal{A}}$

Let $v_1 = \mathsf{new}\ (e')\gamma \downarrow_1$ and $v_2 = \mathsf{new}\ (e')\gamma \downarrow_2$
From Definition 2.4 we are required to prove
$\Big(\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow^f_j (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k-j, \ell, v'_1, v'_2, (\mathsf{ref}\ \ell'\ \tau)\ \sigma)\Big) \wedge$
$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow^f_j (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v'_l) \in \lfloor (\mathsf{ref}\ \ell'\ \tau) \rfloor_V\ \sigma \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)\Big)$

This means we need to prove the following:

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow^f_j (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k-j, \ell, v'_1, v'_2, (\mathsf{ref}\ \ell'\ \tau)\ \sigma)$:

This means we are given some $k \leq n$, $W_e \sqsupseteq W, H_1, H_2$ s.t $(k, H_1, H_2) \triangleright W_e$

Also we are given some $v'_1, v'_2, j < k$ s.t $(H_1, v_1) \Downarrow^f_j (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2)$

And we are required to prove:

$$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge ValEq(\mathcal{A}, W', k-j, \ell, v_1', v_2', (\mathsf{ref}\ \ell'\ \tau)\ \sigma) \quad \text{(FB-R0)}$$

IH:
$(W_e, k, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil \mathsf{Labeled}\ \ell'\ \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:
$\forall f < k.e'\ \gamma \downarrow_1 \Downarrow_f v_{h1} \wedge e'\ \gamma \downarrow_2 \Downarrow v'_{h1} \implies$
$(W_e, k-f, v_{h1}, v'_{h1}) \in \lceil \mathsf{Labeled}\ \ell'\ \tau\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2')$ therefore $\exists f < j < k$ s.t $e'\ \gamma \downarrow_f \Downarrow_j v_{h1} \wedge e'\ \gamma \downarrow_2 \Downarrow v'_{h1}$

This means we have
$(W_e, k-f, v_{h1}, v'_{h1}) \in \lceil \mathsf{Labeled}\ \ell'\ \tau\ \sigma \rceil_V^{\mathcal{A}}$ (FB-R1)

In order to prove (FB-R0) we choose W' as W_n where
$W_n.\theta_1 = W_e.\theta_1 \cup \{a_1 \mapsto (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma\}$
$W_n.\theta_2 = W_e.\theta_2 \cup \{a_2 \mapsto (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma\}$
$W_n.\hat{\beta} = W_e.\hat{\beta} \cup \{a_1, a_2\}$
Now we need to prove:

i. $(k-j, H_1', H_2') \triangleright W_n$:

From Definition 2.9 it suffices to prove:
$dom(W_n.\theta_1) \subseteq dom(H_1') \wedge dom(W_n.\theta_2) \subseteq dom(H_2') \wedge$
$(W_n.\hat{\beta}) \subseteq (dom(W_n.\theta_1) \times dom(W_n.\theta_2)) \wedge$
$\forall (a_1, a_2) \in (W_n.\hat{\beta}).(W_n.\theta_1(a_1) = W_n.\theta_2(a_2) \wedge$
$(W_n, (k-j)-1, H_1'(a_1), H_2'(a_2)) \in \lceil W_n.\theta_1(a_1) \rceil_V^{\mathcal{A}}) \wedge$
$\forall i \in \{1,2\}.\forall m.\forall a_i \in dom(W_n.\theta_i).(W_n.\theta_i, m, H_i(a_i)) \in \lfloor W_n.\theta_i(a_i) \rfloor_V$
This means we need to prove

- $dom(W_n.\theta_1) \subseteq dom(H_1') \wedge dom(W_n.\theta_2) \subseteq dom(H_2') \wedge (W_n.\hat{\beta}) \subseteq (dom(W_n.\theta_1) \times dom(W_n.\theta_2))$:

  We know that $dom(W_n.\theta_1) = dom(W_e.\theta_1) \cup \{a_1\}$ and $dom(W_n.\theta_2) = dom(W_e.\theta_2) \cup \{a_2\}$
  Also $dom(H_1') = dom(H_1) \cup \{a_1\}$ and $dom(H_2') = dom(H_2) \cup \{a_2\}$
  Therefore from $(k, H_1, H_2) \triangleright W_e$ and from construction of W_n we get the desired.

- $\forall (a_1', a_2') \in (W_n.\hat{\beta}).(W_n.\theta_1(a_1') = W_n.\theta_2(a_2') \wedge$
  $(W_n, k-j-1, H_1'(a_1'), H_2'(a_2')) \in \lceil W_n.\theta_1(a_1') \rceil_V^{\mathcal{A}})$:

  $\forall (a_1', a_2') \in (W_n.\hat{\beta})$.

  A. When $a_1' = a_1$ and $a_2' = a_2$:
  From construction
  $(W_n.\theta_1(a_1) = W_n.\theta_2(a_2) = (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma$

  Since from (FB-R1) we know that $(W_e, k-f, v_{h1}, v'_{h1}) \in \lceil \mathsf{Labeled}\ \ell'\ \tau\ \sigma \rceil_V^{\mathcal{A}}$
  And since from SLIO*-Sem-ref we know that $H_1'(a_1) = v_{h1}$, $H_2'(a_2) = v'_{h1}$ and $j = f + 1$ threfore from Lemma 2.17 we get
  $(W_n, k-j-1, H_1'(a_1), H_2'(a_2)) \in \lceil W_n.\theta_1(a_1) \rceil_V^{\mathcal{A}}$

  B. When $a_1' = a_1$ and $a_2' \neq a_2$: This case cannot arise

C. When $a'_1 \neq a_1$ and $a'_2 = a_2$: This case cannot arise

D. When $a'_1 \neq a_1$ and $a'_2 \neq a_2$:
Since $(k, H_1, H_2) \triangleright W_e$ therefore the desired is obtained directly from Definition 2.9

- $\forall i \in \{1,2\}.\forall m.\forall a'_i \in dom(W_n.\theta_i).(W_n.\theta_i, m, H_i(a'_i)) \in \lfloor W_n.\theta_i(a'_i)\rfloor_V$:
  When $i = 1$
  Given some m
  $\forall a'_1 \in dom(W_n.\theta_1)$.
  - when $a'_1 = a_1$:
    From construction
    $(W_n.\theta_1(a_1) = W_n.\theta_2(a_2) = (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma$

    And from (FB-R1) we know that $(W_e, k - f, v_{h1}, v'_{h1}) \in \lceil \mathsf{Labeled}\ \ell'\ \tau\ \sigma\rceil_V^{\mathcal{A}}$
    Therefore from Lemma 2.15 get the desired
  - Otherwise:
    Since $(k, H_1, H_2) \triangleright W_e$ therefore the desired is obtained directly from Definition 2.9

  When $i = 2$
  Similar reasoning as with $i = 1$

ii. $ValEq(\mathcal{A}, W_n, k - j, \ell, v'_1, v'_2, (\mathsf{ref}\ \ell'\ \tau)\ \sigma)$:
From SLIO*-Sem-ref we know that $v'_1 = a_1$ and $v'_2 = a_2$
2 cases arise:

A. $\ell \sqsubseteq \mathcal{A}$:
In this case from Definition 2.3 it suffices to prove that
$(W_n, k - j, a_1, a_2) \in (\mathsf{ref}\ \ell'\ \tau)\ \sigma$

From Definition 2.4 it suffices to prove
$(a_1, a_2) \in W_n.\hat{\beta} \wedge W_n.\theta_1(a_1) = W_n.\theta_2(a_2) = (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma$
This holds from construciton of W_n

B. $\ell \not\sqsubseteq \mathcal{A}$:
In this case from Definition 2.3 it suffices to prove that
$\forall m.\ (W_n.\theta_1, m, a_1) \in (\mathsf{ref}\ \ell'\ \tau)\ \sigma$ and $(W_n.\theta_2, m, a_2) \in (\mathsf{ref}\ \ell'\ \tau)\ \sigma$

From Definition 2.6 this means for any given m we need to prove that
$W_n.\theta_1(a_1) \in (\mathsf{Labeled}\ \ \ell'\ \tau)\ \sigma$ and $W_n.\theta_2(a_2) \in (\mathsf{Labeled}\ \ \ell'\ \tau)\ \sigma$

This holds from construction of W_n

(b) $\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor(\mathsf{ref}\ \ell'\ \tau)\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_1)$:

<u>Case $l = 1$</u>
Given some $k, \theta_e \sqsupseteq W.\theta_l, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k$

<u>We need to prove</u>
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor(\mathsf{ref}\ \ell'\ \tau)\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i\ \sigma)$

Since $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$ therefore from Lemma 2.24 we know that
$\forall m.\ (W.\theta_1, m, \gamma\downarrow_1) \in \lfloor \Gamma \rfloor_V$ and $(W.\theta_2, m, \gamma\downarrow_2) \in \lfloor \Gamma \rfloor_V$

Instantiating m with k we get $(W.\theta_1, k, \gamma\downarrow_1) \in \lfloor \Gamma \rfloor_V$

Now we can apply Theorem 2.22 to get
$(W.\theta_1, k, (\mathsf{ref}\ (e')\gamma\downarrow_1) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau))\ \sigma \rfloor_E$

This means from Definition 2.7 we get
$\forall c < k.\mathsf{ref}\ (e')\gamma\downarrow_1 \Downarrow_c v \implies (W.\theta_1, k - c, v) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau))\ \sigma \rfloor_V$

This further means that given some $c < k$ s.t $\mathsf{ref}\ (e')\gamma\downarrow_1 \Downarrow_c v$. From SLIO*-Sem-val we know that $c = 0$ and $v = \mathsf{ref}\ (e')\gamma\downarrow_1$

And we have $(W.\theta_1, k, \mathsf{ref}\ (e')\gamma\downarrow_1) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau))\ \sigma \rfloor_V$

From Definition 2.6 we have
$\forall K \leq k, \theta'_e \sqsupseteq W.\theta_1, H_1, J.(K, H_1) \triangleright \theta'_e \wedge (H_1, \mathsf{ref}\ (e')\gamma\downarrow_1) \Downarrow_J^f (H', v') \wedge J < K \implies$
$\exists \theta' \sqsupseteq \theta'_e.(K - J, H') \triangleright \theta' \wedge (\theta', K - J, v') \in \lfloor (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H'(a) \implies \exists \ell'.\theta'_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta'_e).\theta'(a) \searrow \ell_i\ \sigma)$

Instantiating K with k, θ'_e with θ_e, H_1 with H and J with j we get the desired

<u>Case $l = 2$</u>
Symmetric reasoning as in the $l = 1$ case above

20. SLIO*-deref:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \mathsf{ref}\ \ell\ \tau}{\Sigma; \Psi; \Gamma \vdash !e' : \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)}$$

To prove: $(W, n, !e'\ (\gamma\downarrow_1), !e'\ (\gamma\downarrow_2)) \in \lceil \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:
$\forall i < n.!e'\ \gamma\downarrow_1 \Downarrow_i v_{f1} \wedge !e'\ \gamma\downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n - i, v_{f1}, v'_{f1}) \in \lceil \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $!e'\ \gamma\downarrow_1 \Downarrow_i v_{f1} \wedge !e'\ \gamma\downarrow_2 \Downarrow v'_{f1}$
From SLIO*-Sem-val we know that $v_{f1} = !e'\gamma\downarrow_1$, $v_{f2} = !e'\gamma\downarrow_2$ and $i = 0$
We are required to prove
$(W, n, !e'\gamma\downarrow_1, !e'\gamma\downarrow_2) \in \lceil \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rceil_V^{\mathcal{A}}$

Let $v_1 = !e'\gamma\downarrow_1$ and $v_2 = !e'\gamma\downarrow_2$
From Definition 2.4 it suffices to prove
$\Big(\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k - j, \ell'\ \sigma, v'_1, v'_2, (\mathsf{Labeled}\ \ell\ \tau)\ \sigma)\Big) \wedge$

$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k,H) \rhd \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \rhd \theta' \wedge (\theta', k-j, v_l') \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau' \wedge \ell'\ \sigma \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell'\ \sigma)\Big)$

This means we need to prove:

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \rhd W_e \wedge \forall v_1', v_2'.$
$(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \rhd W' \wedge ValEq(\mathcal{A}, W', k-j, \ell'\ \sigma, v_1', v_2', (\mathsf{Labeled}\ \ell\ \tau)\ \sigma)$:

This means we are given is some $k \leq n$, $W_e \sqsupseteq W, H_1, H_2$ s.t $(k, H_1, H_2) \rhd W_e$

Also given some $v_1', v_2', j < k$ s.t $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2')$

<u>And we are required to prove:</u>
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \rhd W' \wedge ValEq(\mathcal{A}, W', k-j, \ell'\ \sigma, v_1', v_2', (\mathsf{Labeled}\ \ \ell\ \tau)\ \sigma)$
(FB-D0)

<u>IH</u>:
$(W_e, k, e'\ (\gamma\downarrow_1), e'\ (\gamma\downarrow_2)) \in \lceil(\mathsf{ref}\ \ell\ \tau)\ \sigma\rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:
$\forall f < k.e_l\ \gamma\downarrow_1\Downarrow_f v_{h1} \wedge e_l\ \gamma\downarrow_2\Downarrow v_{h1}' \implies$
$(W_e, k-f, v_{h1}, v_{h1}') \in \lceil(\mathsf{ref}\ \ell\ \tau)\ \sigma\rceil_V^{\mathcal{A}}$

Since we know that $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2')$ therefore $\exists f < j < k$ s.t $e_l\ \gamma\downarrow_f\Downarrow_j v_{h1} \wedge e_l\ \gamma\downarrow_2\Downarrow v_{h1}'$

This means we have
$(W_e, k-f, v_{h1}, v_{h1}') \in \lceil(\mathsf{ref}\ \ell\ \tau)\ \sigma\rceil_V^{\mathcal{A}}$ (FB-D1)

In order to prove (FB-D0) we choose W' as W_e. Also from SLIO*-Sem-deref we know that $H_1' = H_1$ and $H_2' = H_2$. Also we know that $v_{h1} = a_1$ and $v_{h1}' = a_2$.

- $(k-j, H_1, H_2) \rhd W_e$:
  Since we know that $(k, H_1, H_2) \rhd W_e$ therefore from Lemma 2.21 we get
  $(k-j, H_1, H_2) \rhd W_e$
- $ValEq(\mathcal{A}, W_e, k-j, \ell'\ \sigma, v_1', v_2', (\mathsf{Labeled}\ \ \ell\ \tau)\ \sigma)$:
  From SLIO*-Sem-ref we know that $v_1' = H_1(a_1)$ and $v_2' = H_2(a_2)$
  2 cases arise:
  - $\ell'\ \sigma \sqsubseteq \mathcal{A}$:
    In this case from Definition 2.3 it suffices to prove that
    $(W_e, k-j, v_1', v_2') \in (\mathsf{Labeled}\ \ \ell\ \tau)\ \sigma$

    Since from (FB-D1) we know that $(W_e, k-f, a_1, a_2) \in \lceil\mathsf{ref}\ \ell\ \tau\ \sigma\rceil_V^{\mathcal{A}}$
    Therefore from Definition 2.4 we know that $(a_1, a_2) \in W_e.\hat{\beta} \wedge W_e.\theta_1(a_1) = W_e.\theta_2(a_2) = \mathsf{Labeled}\ \ell\ \tau\ \sigma$

    And since we know that $(k, H_1, H_2) \rhd W_e$ therefore from Definition we know that $(W_e, k, H_1(a_1), H_2(a_2)) \in \lceil\mathsf{Labeled}\ \ \ell\ \tau\ \sigma\rceil_V^{\mathcal{A}}$
    From Lemma 2.17 we get $(W_e, k-j, H_1(a_1), H_2(a_2)) \in \lceil(\mathsf{Labeled}\ \ \ell\ \tau)\ \sigma\rceil_V^{\mathcal{A}}$

– $\ell' \not\sqsubseteq \mathcal{A}$:

In this case from Definition 2.3 it suffices to prove that
$\forall m.\ (W_e.\theta_1, m, H_1(a_1)) \in (\mathsf{Labeled}\ \ \ell\ \tau)\ \sigma$ and $(W_e.\theta_2, m, H_2(a_2)) \in (\mathsf{Labeled}\ \ \ell\ \tau)\ \sigma$ (FB-B2)

Since from (FB-D1) we know that $(W_e, k-f, a_1, a_2) \in \lceil \mathsf{ref}\ \ell\ \tau\ \sigma \rceil_V^{\mathcal{A}}$
Therefore from Definition 2.4 we know that $(a_1, a_2) \in W_e.\hat{\beta} \wedge W_e.\theta_1(a_1) = W_e.\theta_2(a_2) = \mathsf{Labeled}\ \ell\ \tau\ \sigma$

And since we know that $(k, H_1, H_2) \triangleright W_e$ therefore from Definition we know that $(W_e, k, H_1(a_1), H_2(a_2)) \in \lceil \mathsf{Labeled}\ \ \ell\ \tau\ \sigma \rceil_V^{\mathcal{A}}$

Finally from Lemma 2.15 we get (FB-B2)

(b) $\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor (\mathsf{Labeled}\ \ \ell\ \tau)\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau' \wedge \ell'\ \sigma \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell'\ \sigma)$:

Case $l = 1$

Given some $k, \theta_e \sqsupseteq W.\theta_l, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k$

We need to prove
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor (\mathsf{Labeled}\ \ \ell\ \tau)\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau'' \wedge \ell'\ \sigma \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell'\ \sigma)$

Since $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$ therefore from Lemma 2.24 we know that
$\forall m.\ (W.\theta_1, m, \gamma\downarrow_1) \in \lfloor \Gamma \rfloor_V$ and $(W.\theta_2, m, \gamma\downarrow_2) \in \lfloor \Gamma \rfloor_V$

Instantiating m with k we get $(W.\theta_1, k, \gamma\downarrow_1) \in \lfloor \Gamma \rfloor_V$

Now we can apply Theorem 2.22 to get
$(W.\theta_1, k, (!e'\gamma\downarrow_1) \in \lfloor (\mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ \ell\ \tau))\ \sigma \rfloor_E$

This means from Definition 2.7 we get
$\forall c < k.!e'\gamma\downarrow_1 \Downarrow_c v \implies (W.\theta_1, k-c, v) \in \lfloor (\mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ \ell\ \tau))\ \sigma \rfloor_V$

Instantianting c with 0 and from SLIO*-Sem-val we know that $v = !e'\gamma\downarrow_1$

And we have $(W.\theta_1, k, !e'\gamma\downarrow_1) \in \lfloor (\mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ \ell\ \tau))\ \sigma \rfloor_V$

From Definition 2.6 we have
$\forall K \leq k, \theta_e' \sqsupseteq W.\theta_1, H_1, J.(K, H_1) \triangleright \theta_e' \wedge (H_1, v) \Downarrow_J^f (H', v') \wedge J < K \implies$
$\exists \theta' \sqsupseteq \theta_e'.(K-J, H') \triangleright \theta' \wedge (\theta', K-J, v') \in \lfloor (\mathsf{Labeled}\ \ \ell\ \tau)\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H'(a) \implies \exists \ell'.\theta_e'(a) = \mathsf{Labeled}\ \ell''\ \tau'' \wedge \ell'\ \sigma \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e').\theta'(a) \searrow \ell'\ \sigma)$

Instantiating K with k, θ_e' with θ_e, H_1 with H and J with j we get the desired

Case $l = 2$

Symmetric reasoning as in the $l = 1$ case above

21. SLIO*-assign:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_l : \mathsf{ref}\ \ell'\ \tau \qquad \Sigma; \Psi; \Gamma \vdash e_r : \mathsf{Labeled}\ \ell'\ \tau \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash e_l := e_r : \mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit}}$$

To prove: $(W, n, (e_l := e_r)\ (\gamma \downarrow_1), (e_l := e_r)\ (\gamma \downarrow_2)) \in \lceil \mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit}\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:

$\forall i < n.(e_l := e_r)\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (e_l := e_r)\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n - i, v_{f1}, v'_{f1}) \in \lceil \mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit}\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $(e_l := e_r)\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (e_l := e_r)\ \gamma \downarrow_2 \Downarrow v'_{f1}$
From SLIO*-Sem-val we know that $v_{f1} = (e_l := e_r)\gamma \downarrow_1$, $v_{f2} = (e_l := e_r)\gamma \downarrow_2$ and $i = 0$
We are required to prove
$(W, n, (e_l := e_r)\gamma \downarrow_1, (e_l := e_r)\gamma \downarrow_2) \in \lceil \mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit}\ \sigma \rceil_V^{\mathcal{A}}$

Let $e_1 = (e_l : -e_r)\ \gamma \downarrow_1$ and $e_2 = (e_l : -e_r)\ \gamma \downarrow_2$
From Definition 2.4 it suffices to prove
$\Big(\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k - j, \ell, v'_1, v'_2, \mathsf{unit})\Big) \wedge$
$\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor \mathsf{unit} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)\Big)$

This means we need to prove:

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k - j, \ell, v'_1, v'_2, \mathsf{unit})$:

This means we are given some $k \leq n$, $W_e \sqsupseteq W, H_1, H_2$ s.t $(k, H_1, H_2) \triangleright W_e$

And finally given some $v'_1, v'_2, j < k$ s.t $(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2)$

And we are required to prove:
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k - j, \ell, v'_1, v'_2, \mathsf{unit})$
(FB-A0)

IH1:
$(W_e, k, e_l\ (\gamma \downarrow_1), e_l\ (\gamma \downarrow_2)) \in \lceil \mathsf{ref}\ \ell'\ \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:
$\forall f < k.e_l\ \gamma \downarrow_1 \Downarrow_f v_{h1} \wedge e_l\ \gamma \downarrow_2 \Downarrow v'_{h1} \implies$
$(W_e, k - f, v_{h1}, v'_{h1}) \in \lceil \mathsf{ref}\ \ell'\ \tau\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2')$ therefore $\exists f < j < k$ s.t $e_l\ \gamma \downarrow_f \Downarrow_j v_{h1} \wedge e_l\ \gamma \downarrow_2 \Downarrow v_{h1}'$

This means we have
$(W_e, k - f, v_{h1}, v_{h1}') \in \lceil \mathsf{ref}\ \ell'\ \tau\ \sigma \rceil_V^{\mathcal{A}}$ (FB-A1)

<u>IH2</u>:
$(W_e, k - f, e_r\ (\gamma \downarrow_1), e_r\ (\gamma \downarrow_2)) \in \lceil \mathsf{Labeled}\ \ell'\ \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 2.5 we need to prove:
$\forall s < k - f. e'\ \gamma \downarrow_1 \Downarrow_s v_{h2} \wedge e'\ \gamma \downarrow_2 \Downarrow v_{h2}' \implies$
$(W_e, k - f - s, v_{h2}, v_{h2}') \in \lceil \mathsf{Labeled}\ \ell'\ \tau\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2')$ therefore $\exists s < j - f < k - f$ s.t $e_r\ \gamma \downarrow_1 \Downarrow_s v_{h2} \wedge e_r\ \gamma \downarrow_2 \Downarrow v_{h2}'$

This means we have
$(W_e, k - f - s, v_{h2}, v_{h2}') \in \lceil \mathsf{Labeled}\ \ell'\ \tau\ \sigma \rceil_V^{\mathcal{A}}$ (FB-A2)

In order to prove (FB-A0) we choose W' as W_e. Also from SLIO*-Sem-assign we know that $H_1' = H_1[v_{h1} \mapsto v_{h2}]$ and $H_2' = H_2[v_{h1}' \mapsto v_{h2}']$, and $j = f + s + 1$
We need to prove the following:

i. $(k - j, H_1', H_2') \rhd W_e$:

Say $v_{h1} = a_1$ and $v_{h1}' = a_2$

From Definition 2.9 it suffices to prove:
$dom(W_e.\theta_1) \subseteq dom(H_1') \wedge dom(W_e.\theta_2) \subseteq dom(H_2') \wedge$
$(W_e.\hat{\beta}) \subseteq (dom(W_e.\theta_1) \times dom(W_e.\theta_2)) \wedge$
$\forall (a_1, a_2) \in (W_e.\hat{\beta}).(W_e.\theta_1(a_1) = W_e.\theta_2(a_2) \wedge$
$(W_e, (k - j) - 1, H_1'(a_1), H_2'(a_2)) \in \lceil W_e.\theta_1(a_1) \rceil_V^{\mathcal{A}}) \wedge$
$\forall i \in \{1, 2\}. \forall m. \forall a_i \in dom(W_e.\theta_i).(W_e.\theta_i, m, H_i(a_i)) \in \lfloor W_e.\theta_i(a_i) \rfloor_V$
This means we need to prove

- $dom(W_e.\theta_1) \subseteq dom(H_1') \wedge dom(W_e.\theta_2) \subseteq dom(H_2') \wedge (W_e.\hat{\beta}) \subseteq (dom(W_e.\theta_1) \times dom(W_e.\theta_2))$:
  Since $dom(H_1) = dom(H_1')$ and $dom(H_2) = dom(H_2')$, and also we know that $(k, H_1, H_2) \rhd W_e$. Therefore we obtain the desired direclty from Definition 2.9
- $\forall (a_1', a_2') \in (W_e.\hat{\beta}).(W_e.\theta_1(a_1') = W_e.\theta_2(a_2') \wedge$
  $(W_e, k - j - 1, H_1'(a_1'), H_2'(a_2')) \in \lceil W_e.\theta_1(a_1') \rceil_V^{\mathcal{A}})$:

  $\forall (a_1', a_2') \in (W_e.\hat{\beta})$.

  A. When $a_1' = a_1$ and $a_2' = a_2$:
  From (FB-A1) and from Definition 2.4 we get
  $(W_e.\theta_1(a_1) = W_e.\theta_2(a_2) = (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma$

  Since from (FB-A2) we know that $(W_e, k-f-s, v_{h2}, v_{h2}') \in \lceil \mathsf{Labeled}\ \ell'\ \tau\ \sigma \rceil_V^{\mathcal{A}}$
  And since from SLIO*-Sem-assign we know that $H_1'(a_1) = v_{h2}$, $H_2'(a_2) = v_{h2}'$ and $j = f + s + 1$ threfore from Lemma 2.17 we get
  $(W_e, k - j - 1, H_1'(a_1), H_2'(a_2)) \in \lceil W_e.\theta_1(a_1) \rceil_V^{\mathcal{A}}$

  B. When $a_1' = a_1$ and $a_2' \neq a_2$: This case cannot arise

  C. When $a_1' \neq a_1$ and $a_2' = a_2$: This case cannot arise

D. When $a'_1 \neq a_1$ and $a'_2 \neq a_2$:
Since $(k, H_1, H_2) \triangleright W_e$ therefore the desired is obtained directly from Definition 2.9

- $\forall i \in \{1, 2\}.\forall m.\forall a'_i \in dom(W_e.\theta_i).(W_e.\theta_i, m, H_i(a'_i)) \in \lfloor W_e.\theta_i(a'_i) \rfloor_V$:
  <u>When $i = 1$</u>
  Given some m
  $\forall a'_1 \in dom(W_e.\theta_1)$.
  - when $a'_1 = a_1$:
    From (FB-A1) and from Definition 2.4 we get
    $(W_e.\theta_1(a_1) = W_e.\theta_2(a_2) = (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma$

    Since from (FB-A2) we know that $(W_e, k{-}f{-}s, v_{h2}, v'_{h2}) \in \lceil \mathsf{Labeled}\ \ell'\ \tau\ \sigma \rceil_V^{\mathcal{A}}$
    Therefore from Lemma 2.15 get the desired
  - Otherwise:
    Since $(k, H_1, H_2) \triangleright W_e$ therefore the desired is obtained directly from Definition 2.9

  <u>When $i = 2$</u>
  Similar reasoning as with $i = 1$

ii. $ValEq(\mathcal{A}, W_e, k - j, \ell, (), (), \mathsf{unit})$:
Holds directly from Definition 2.3 and Definition 2.4

(b) $\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor \mathsf{unit} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell\ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell\ \sigma)$:

<u>Case $l = 1$</u>
Given some $k, \theta_e \sqsupseteq W.\theta_l, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k$

<u>We need to prove</u>
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor (\mathsf{unit})\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau'' \wedge \ell\ \sigma \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell\ \sigma)$

Since $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$ therefore from Lemma 2.24 we know that
$\forall m.\ (W.\theta_1, m, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$ and $(W.\theta_2, m, \gamma \downarrow_2) \in \lfloor \Gamma \rfloor_V$

Instantiating m with k we get $(W.\theta_1, k, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$

Now we can apply Theorem 2.22 to get
$(W.\theta_1, k, ((e_l := e_r)\gamma \downarrow_1) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell\ (\mathsf{unit}))\ \sigma \rfloor_E$

This means from Definition 2.7 we get
$\forall c < k.(e_l := e_r)\gamma \downarrow_1 \Downarrow_c v \implies (W.\theta_1, k - c, v) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell\ (\mathsf{unit}))\ \sigma \rfloor_V$

Instantiating c with 0 and from SLIO*-Sem-val we know that $v = (e_l := e_r)\gamma \downarrow_1$

And we have $(W.\theta_1, k, (e_l := e_r)\gamma \downarrow_1) \in \lfloor (\mathbb{SLIO}\ \ell\ \ell\ (\mathsf{unit}))\ \sigma \rfloor_V$

From Definition 2.6 we have
$\forall K \leq k, \theta'_e \sqsupseteq W.\theta_1, H_1, J.(K, H_1) \triangleright \theta'_e \wedge (H_1, v) \Downarrow_J^f (H', v') \wedge J < K \implies$
$\exists \theta' \sqsupseteq \theta'_e.(K - J, H') \triangleright \theta' \wedge (\theta', K - J, v') \in \lfloor (\mathsf{Labeled}\ \ \ell\ \tau)\ \sigma \rfloor_V \wedge$

$(\forall a.H_1(a) \neq H'(a) \implies \exists \ell'.\theta'_e(a) = \mathsf{Labeled}\ \ell''\ \tau'' \wedge \ell'\ \sigma \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta'_e).\theta'(a) \searrow \ell'\ \sigma)$

Instantiating K with k, θ'_e with θ_e, H_1 with H and J with j we get the desired

Case $l = 2$
Symmetric reasoning as in the $l = 1$ case above

□

Lemma 2.26 (SLIO*: Equivalence of values)**.** $\forall \mathcal{A}, W, W, \ell, \ell', v_1, v_2, \tau, i, j.$
$ValEq(\mathcal{A}, W, \ell, i, v_1, v_2, \tau) \wedge j < i \wedge \ell \sqsubseteq \ell' \wedge W \sqsubseteq W' \implies$
$ValEq(\mathcal{A}, W', \ell', j, v_1, v_2, \tau)$

Proof. Given that $ValEq(\mathcal{A}, W, \ell, i, v_1, v_2, \tau)$. From Definition 2.3 two cases arise

1. $\ell \sqsubseteq \mathcal{A}$:

   In this case we know that $(W, i, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$

   2 cases arise

   (a) $\ell' \sqsubseteq \mathcal{A}$:
   Since $(W, i, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$ therefore from Lemma 2.17 we know that $(W', j, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$
   And thus from Definition 2.3 we know that $ValEq(\mathcal{A}, W', \ell', j, v_1, v_2, \tau)$

   (b) $\ell' \not\sqsubseteq \mathcal{A}$:
   Since $(W, i, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$ therefore from Lemma 2.15 we know that $\forall i \in \{1, 2\}.\ \forall m.$ $(W.\theta_i, m, v_i) \in \lfloor \tau \rfloor_V$
   And from Lemma 2.16 we know that $\forall i \in \{1, 2\}.\ \forall m.\ (W'.\theta_i, m, v_i) \in \lfloor \tau \rfloor_V$
   Hence from Definition 2.3 we know that $ValEq(\mathcal{A}, W', \ell', j, v_1, v_2, \tau)$

2. $\ell \not\sqsubseteq \mathcal{A}$:

   Given is $\ell \sqsubseteq \ell' \not\sqsubseteq \mathcal{A}$

   In this case we know that $\forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, v_i) \in \lfloor \tau \rfloor_V$

   And from Lemma 2.16 we know that $\forall i \in \{1, 2\}.\ \forall m.\ (W'.\theta_i, m, v_i) \in \lfloor \tau \rfloor_V$

   Hence from Definition 2.3 we know that $ValEq(\mathcal{A}, W', \ell', j, v_1, v_2, \tau)$

□

Lemma 2.27 (SLIO*: Subtyping binary)**.** *The following holds:*
$\forall \Sigma, \Psi, \sigma, \tau, \tau'.$

1. $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lceil(\tau\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau'\ \sigma)\rceil_V^{\mathcal{A}}$

2. $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lceil(\tau\ \sigma)\rceil_E^{\mathcal{A}} \subseteq \lceil(\tau'\ \sigma)\rceil_E^{\mathcal{A}}$

Proof. Proof of statement (1)
Proof by induction on the $\tau <: \tau'$

1. SLIO*sub-arrow:

   Given:

$$\frac{\Sigma; \Psi \vdash \tau_1' <: \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 \rightarrow \tau_2 <: \tau_1' \rightarrow \tau_2'}$$

   To prove: $\lceil((\tau_1 \rightarrow \tau_2)\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil((\tau_1' \rightarrow \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   IH1: $\lceil(\tau_1'\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau_1\ \sigma)\rceil_V^{\mathcal{A}}$ (Statement 1)
   $\lceil(\tau_2\ \sigma)\rceil_E^{\mathcal{A}} \subseteq \lceil(\tau_2'\ \sigma)\rceil_E^{\mathcal{A}}$ (Sub-A0 From Statement 2)

   It suffices to prove:
   $\forall(W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil((\tau_1 \rightarrow \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}.\ (W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil((\tau_1' \rightarrow \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   This means that given: $(W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil((\tau_1 \rightarrow \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}$
   And it suffices to prove: $(W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil((\tau_1' \rightarrow \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   From Definition 2.4 we are given:
   $\forall W' \sqsupseteq W, j < n, v_1, v_2.((W', j, v_1, v_2) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}} \implies$
   $(W', j, e_1[v_1/x], e_2[v_2/x]) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}}) \wedge$
   $\forall\theta_l \sqsupseteq W.\theta_1, j, v_c.((\theta_l, j, v_c) \in \lfloor\tau_1\ \sigma\rfloor_V \implies (\theta_l, j, e_1[v_1/x]) \in \lfloor\tau_2\ \sigma\rfloor_E) \wedge$
   $\forall\theta_l \sqsupseteq W.\theta_2, j, v_c.((\theta_l, j, v_c) \in \lfloor\tau_1\ \sigma\rfloor_V \implies (\theta_l, j, e_2[v_c/x]) \in \lfloor\tau_2\ \sigma\rfloor_E)$ (Sub-A1)

   Again from Definition 2.4 we are required to prove:
   $\forall W'' \sqsupseteq W, k < n, v_1', v_2'.((W'', k, v_1', v_2') \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}} \implies (W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2'\ \sigma\rceil_E^{\mathcal{A}}) \wedge$
   $\forall\theta_l' \sqsupseteq W.\theta_1, k, v_c'.((\theta_l', k, v_c') \in \lfloor\tau_1'\ \sigma\rfloor_V \implies (\theta_l', k, e_1[v_c'/x]) \in \lfloor\tau_2'\ \sigma\rfloor_E) \wedge$
   $\forall\theta_l' \sqsupseteq W.\theta_2, k, v_c'.((\theta_l', k, v_c') \in \lfloor\tau_1'\ \sigma\rfloor_V \implies (\theta_l', k, e_2[v_c'/x]) \in \lfloor\tau_2'\ \sigma\rfloor_E)$

   This means need to prove:

   (a) $\forall W'' \sqsupseteq W, k < n, v_1', v_2'.((W'', k, v_1', v_2') \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}} \implies (W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2'\ \sigma\rceil_E^{\mathcal{A}})$:
   Given: $W'' \sqsupseteq W$, $k < n$ and v_1', v_2'. We are also given $(W'', k, v_1', v_2') \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}}$
   To prove: $(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2'\ \sigma\rceil_E^{\mathcal{A}}$

   Instantiating the first conjunct of Sub-A1 with W'', k, v_1' and v_2' we get

$$((W'', k, v_1', v_2') \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}} \implies (W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}}) \quad (85)$$

   Since $(W'', k, v_1', v_2') \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}}$ therefore from IH1 we know that $(W'', k, v_1', v_2') \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}}$

   Thus from Equation 85 we get $(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}}$

   Finally using (Sub-A0) we get $(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2'\ \sigma\rceil_E^{\mathcal{A}}$

   (b) $\forall\theta_l' \sqsupseteq W.\theta_1, k, v_c'.((\theta_l', k, v_c') \in \lfloor\tau_1'\ \sigma\rfloor_V \implies (\theta_l', k, e_1[v_c'/x]) \in \lfloor\tau_2'\ \sigma\rfloor_E)$:
   Given: $\theta_l' \sqsupseteq W.\theta_1, k, v_c'$. We are also given $(\theta_l', k, v_c') \in \lfloor\tau_1'\ \sigma\rfloor_V$
   To prove: $(\theta_l', k, e_1[v_c'/x]) \in \lfloor\tau_2'\ \sigma\rfloor_E$

Since we are given $(\theta'_l, k, v'_c) \in \lfloor \tau'_1\ \sigma \rfloor_V$ and since $\tau'_1\ \sigma <: \tau_1\ \sigma$ therefore from Lemma 2.23 we get

$$(\theta'_l, k, v'_c) \in \lfloor \tau_1\ \sigma \rfloor_V \tag{86}$$

Instantiating the second conjunct of Sub-A1 with θ'_l, k, v'_1 and v'_2 we get

$$((\theta'_l, k, v'_c) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta'_l, e_1[v'_c/x]) \in \lfloor \tau_2\ \sigma \rfloor_E) \tag{87}$$

Therefore from Equation 86 and 87 we get $(\theta'_l, k, e_1[v'_c/x]) \in \lfloor \tau_2\ \sigma \rfloor_E$

Since $\tau_2\ \sigma <: \tau'_2\ \sigma$ therefore from Lemma 2.23 we get
$(\theta'_l, k, e_1[v'_c/x]) \in \lfloor \tau'_2\ \sigma \rfloor_E$

(c) $\forall \theta'_l \sqsupseteq W.\theta_2, k, v'_c.((\theta'_l, k, v'_c) \in \lfloor \tau'_1\ \sigma \rfloor_V \implies (\theta'_l, k, e_2[v'_c/x]) \in \lfloor \tau'_2\ \sigma \rfloor_E)$:
Similar reasoning as in the previous case

2. SLIO*sub-prod:

Given:

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau'_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau'_2}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau'_1 \times \tau'_2}$$

To prove: $\lceil((\tau_1 \times \tau_2)\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil((\tau'_1 \times \tau'_2)\ \sigma)\rceil_V^{\mathcal{A}}$

IH1: $\lceil(\tau_1\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau'_1\ \sigma)\rceil_V^{\mathcal{A}}$ (Statement (1))

IH2: $\lceil(\tau_2\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau'_2\ \sigma)\rceil_V^{\mathcal{A}}$ (Statement (1))

It suffices to prove: $\forall (W, n, (v_1, v_2), (v'_1, v'_2)) \in \lceil((\tau_1 \times \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}.\ (W, n, (v_1, v_2), (v'_1, v'_2)) \in \lceil((\tau'_1 \times \tau'_2)\ \sigma)\rceil_V^{\mathcal{A}}$

This means that given: $(W, n, (v_1, v_2), (v'_1, v'_2)) \in \lceil((\tau_1 \times \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}$

Therefore from Definition 2.4 we are given:

$$(W, n, v_1, v'_1) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \wedge (W, n, v_2, v'_2) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}} \tag{88}$$

And it suffices to prove: $(W, n, (v_1, v_2), (v'_1, v'_2)) \in \lceil((\tau'_1 \times \tau'_2)\ \sigma)\rceil_V^{\mathcal{A}}$

Again from Definition 2.4, it suffices to prove:
$(W, n, v_1, v'_1) \in \lceil \tau'_1\ \sigma \rceil_V^{\mathcal{A}} \wedge (W, n, v_2, v'_2) \in \lceil \tau'_2\ \sigma \rceil_V^{\mathcal{A}}$

Since from Equation 88 we know that $(W, n, v_1, v'_1) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$ therefore from IH1 we have $(W, n, v_1, v'_1) \in \lceil \tau'_1\ \sigma \rceil_V^{\mathcal{A}}$

Similarly since $(W, n, v_2, v'_2) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$ from Equation 88 therefore from IH2 we have $(W, n, v_2, v'_2) \in \lceil \tau'_2\ \sigma \rceil_V^{\mathcal{A}}$

3. SLIO*sub-sum:

Given:

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau'_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau'_2}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau'_1 + \tau'_2}$$

To prove: $\lceil((\tau_1 + \tau_2)\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil((\tau'_1 + \tau'_2)\ \sigma)\rceil_V^{\mathcal{A}}$

IH1: $\lceil(\tau_1\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau_1'\ \sigma)\rceil_V^{\mathcal{A}}$ (Statement (1))
IH2: $\lceil(\tau_2\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau_2'\ \sigma)\rceil_V^{\mathcal{A}}$ (Statement (1))
It suffices to prove: $\forall(W, n, v_{s1}, v_{s2}) \in \lceil((\tau_1 + \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}.\ (W, n, v_{s1}, v_{s2}) \in \lceil((\tau_1' + \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

This means that given: $(W, n, v_{s1}, v_{s2}) \in \lceil((\tau_1 + \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}$
And it suffices to prove: $(W, n, v_{s1}, v_{s2}) \in \lceil((\tau_1' + \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

2 cases arise

(a) $v_{s1} = \mathsf{inl}\ v_{i1}$ and $v_{s1} = \mathsf{inl}\ v_{i2}$:
From Definition 2.4 we are given:

$$(W, n, v_{i1}, v_{i2}) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}} \tag{89}$$

And we are required to prove that:
$(W, n, v_{i1}, v_{i2}) \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}}$
From Equation 89 and IH1 we know that
$(W, n, v_{i1}, v_{i2}) \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}}$

(b) $v_s = \mathsf{inr}\ v_{i1}$ and $v_{s2} = \mathsf{inr}\ v_{i2}$:
From Definition 2.4 we are given:

$$(W, n, v_{i1}, v_{i2}) \in \lceil\tau_2\ \sigma\rceil_V^{\mathcal{A}} \tag{90}$$

And we are required to prove that:
$(W, n, v_{i1}, v_{i2}) \in \lceil\tau_2'\ \sigma\rceil_V^{\mathcal{A}}$
From Equation 90 and IH2 we know that
$(W, n, v_{i1}, v_{i2}) \in \lceil\tau_2'\ \sigma\rceil_V^{\mathcal{A}}$

4. SLIO*sub-forall:

Given:

$$\frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash \forall\alpha.\tau_1 <: \forall\alpha.\tau_2}$$

To prove: $\lceil((\forall\alpha.\tau_1)\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\forall\alpha.\tau_2)\ \sigma\rceil_V^{\mathcal{A}}$

$\forall\sigma.\ \lceil(\tau_1\ \sigma)\rceil_E^{\mathcal{A}} \subseteq \lceil(\tau_2\ \sigma)\rceil_E^{\mathcal{A}}$ (Sub-F2, From Statement (2))
It suffices to prove: $\forall(W, n, \Lambda e_1, \Lambda e_2) \in \lceil((\forall\alpha.\tau_1)\ \sigma)\rceil_V^{\mathcal{A}}$.
$(W, n, \Lambda e_1, \Lambda e_2) \in \lceil((\forall\alpha.\tau_2)\ \sigma)\rceil_V^{\mathcal{A}}$

This means that given: $(W, n, \Lambda e_1, \Lambda e_2) \in \lceil((\forall\alpha.(\tau_1))\ \sigma)\rceil_V^{\mathcal{A}}$
Therefore from Definition 2.4 we are given:
$\forall W' \sqsupseteq W, n' < n, \ell' \in \mathcal{L}.((W', n', e_1, e_2) \in \lceil\tau_1[\ell'/\alpha]\ \sigma\rceil_E^{\mathcal{A}}) \wedge$
$\forall\theta_l \sqsupseteq W.\theta_1, j, \ell' \in \mathcal{L}.((\theta_l, j, e_1) \in \lfloor\tau_1[\ell'/\alpha]\rfloor_E) \wedge$
$\forall\theta_l \sqsupseteq W.\theta_2, j, \ell' \in \mathcal{L}.((\theta_l, j, e_2) \in \lfloor\tau_1[\ell''/\alpha]\rfloor_E)$ (Sub-F1)
And it suffices to prove: $(W, n, \Lambda e_1, \Lambda e_2) \in \lceil((\forall\alpha.\tau_2)\ \sigma)\rceil_V^{\mathcal{A}}$

Again from Definition 2.4, it suffices to prove:

$\forall W'' \sqsupseteq W, n'' < n, \ell'' \in \mathcal{L}.((W'', n'', e_1, e_2) \in \lceil \tau_2[\ell''/\alpha]\ \sigma \rceil_E^{\mathcal{A}}) \wedge$
$\forall \theta_l' \sqsupseteq W.\theta_1, k, \ell'' \in \mathcal{L}.((\theta_l', k, e_1) \in \lfloor \tau_2[\ell''/\alpha] \rfloor_E) \wedge$
$\forall \theta_l' \sqsupseteq W.\theta_2, k, \ell'' \in \mathcal{L}.((\theta_l', k, e_2) \in \lfloor \tau_2[\ell''/\alpha] \rfloor_E)$

This means we are required to show:

(a) $\forall W'' \sqsupseteq W, n'' < n, \ell' \in \mathcal{L}.((W'', n', e_1, e_2) \in \lceil \tau_2[\ell'/\alpha]\ \sigma \rceil_E^{\mathcal{A}})$:
By instantiating the first conjunct of Sub-F1 with W'', n'' and ℓ'' we know that the following holds
$((W'', n'', e_1, e_2) \in \lceil \tau_1[\ell''/\alpha]\ \sigma \rceil_E^{\mathcal{A}})$

Therefore from Sub-F2 instantiated at $\sigma \cup \{\alpha \mapsto \ell''\}$
$((W'', n'', e_1, e_2) \in \lceil \tau_2[\ell''/\alpha]\ \sigma \rceil_E^{\mathcal{A}})$

(b) $\forall \theta_l' \sqsupseteq W.\theta_1, k, \ell'' \in \mathcal{L}.((\theta_l', k, e_1) \in \lfloor \tau_2[\ell''/\alpha] \rfloor_E)$:
By instantiating the second conjunct of Sub-F1 with θ_l' and ℓ'' we know that the following holds
$((\theta_l', k, e_1) \in \lfloor \tau_1[\ell''/\alpha]\ \sigma \rfloor_E)$

Since $\tau_1\ \sigma \cup \{\alpha \mapsto \ell''\} <: \tau_2\ \sigma \cup \{\alpha \mapsto \ell''\}$ therefore from Lemma 2.23 we know that
$((\theta_l', k, e1) \in \lfloor \tau_2[\ell''/\alpha]\ \sigma \rfloor_E)$

(c) $\forall \theta_l' \sqsupseteq W.\theta_2, k, \ell'' \in \mathcal{L}.((\theta_l', k, e_2) \in \lfloor \tau_2[\ell''/\alpha] \rfloor_E)$:
Similar reasoning as in the previous case

5. SLIO*sub-constraint:

Given:

$$\frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash c_1 \Rightarrow \tau_1 <: c_2 \Rightarrow \tau_2}$$

To prove: $\lceil((c_1 \Rightarrow \tau_1)\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil((c_2 \Rightarrow \tau_2))\ \sigma\rceil_V^{\mathcal{A}}$

$\lceil(\tau_1\ \sigma)\rceil_E^{\mathcal{A}} \subseteq \lceil(\tau_2\ \sigma)\rceil_E^{\mathcal{A}}$ (Sub-C0, From Statement (2))
It suffices to prove: $\forall(W, n, \nu e_1, \nu e_2) \in \lceil((c_1 \Rightarrow \tau_1)\ \sigma)\rceil_V^{\mathcal{A}}$. $(W, n, \nu e_1, \nu e_2) \in \lceil((c_2 \Rightarrow \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}$

This means that given: $(W, n, \nu e_1, \nu e_2) \in \lceil((c_1 \Rightarrow \tau_1)\ \sigma)\rceil_V^{\mathcal{A}}$
Therefore from Definition 2.4 we are given:
$\forall W' \sqsupseteq W, n' < n.\mathcal{L} \models c_1\ \sigma \implies (W', n', e_1, e_2) \in \lceil \tau_1\ \sigma \rceil_E^{\mathcal{A}} \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, k.\mathcal{L} \models c_1 \implies (\theta_l, k, e_1) \in \lfloor \tau_1\ \sigma \rfloor_E \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, k.\mathcal{L} \models c_1 \implies (\theta_l, k, e_2) \in \lfloor \tau_1\ \sigma \rfloor_E$ (Sub-C1)
And it suffices to prove: $(W, n, \nu e_1, \nu e_2) \in \lceil((c_2 \Rightarrow \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}$

Again from Definition 2.4, it suffices to prove:
$\forall W'' \sqsupseteq W, n'' < n.\mathcal{L} \models c_2\ \sigma \implies (W'', n'', e_1, e_2) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}} \wedge$
$\forall \theta_l' \sqsupseteq W.\theta_1, j.\mathcal{L} \models c_2 \implies (\theta_l', j, e_1) \in \lfloor \tau_2\ \sigma \rfloor_E \wedge$
$\forall \theta_l' \sqsupseteq W.\theta_2, j.\mathcal{L} \models c_2 \implies (\theta_l', j, e_2) \in \lfloor \tau_2\ \sigma \rfloor_E$

This means that we are required to show the following:

(a) $\forall W'' \sqsupseteq W, n'' < n.\mathcal{L} \models c_2\ \sigma \implies (W'', n'', e_1, e_2) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$:
We are given $W'' \sqsupseteq W, n'' < n$ also we know that $\mathcal{L} \models c_2\ \sigma$ and $c_2\ \sigma \implies c_1\ \sigma$ therefore we also know that $\mathcal{L} \models c_1\ \sigma$
Hence by instantiating the first conjunct of Sub-C1 with W'' and n'' we know that the following holds
$(W'', n'', e_1, e_2) \in \lceil \tau_1\ \sigma \rceil_E^{\mathcal{A}}$

Therefore from (Sub-C0) we get $(W'', n'', e_1, e_2) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$

(b) $\forall \theta'_l \sqsupseteq W.\theta_1, k.\mathcal{L} \models c_2 \implies (\theta'_l, k, e_1) \in \lfloor \tau_2\ \sigma \rfloor_E$:
We are given some $\theta'_l \sqsupseteq W.\theta_1, k$, also we know that $\mathcal{L} \models c_2\ \sigma$ and $c_2\ \sigma \implies c_1\ \sigma$ therefore we also know that $\mathcal{L} \models c_1\ \sigma$
Hence by instantiating the second conjunct of Sub-C1 with θ'_l we know that the following holds
$(\theta'_l, k, e_1) \in \lfloor \tau_1\ \sigma \rfloor_E$
Since $\tau_1\ \sigma <: \tau_2\ \sigma$ therefore from Lemma 2.23 we get
$(\theta'_l, k, e_1) \in \lfloor \tau_2\ \sigma \rfloor_E$

(c) $\forall \theta'_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c_2 \implies (\theta'_l, j, e_2) \in \lfloor \tau_2\ \sigma \rfloor_E$:
Similar reasoning as in the previous case

6. SLIO*sub-label:

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi \vdash \mathsf{Labeled}\ \ell\ \tau <: \mathsf{Labeled}\ \ell'\ \tau'}$$

To prove: $\lceil ((\mathsf{Labeled}\ \ell\ \tau)\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil ((\mathsf{Labeled}\ \ell\ '\tau')\ \sigma) \rceil_V^{\mathcal{A}}$

IH: $\lceil (\tau\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil (\tau'\ \sigma) \rceil_V^{\mathcal{A}}$

It suffices to prove: $\forall (W, n, \mathsf{Lb}(v_1), \mathsf{Lb}(v_2)) \in \lceil ((\mathsf{Labeled}\ \ell\ \tau)\ \sigma) \rceil_V^{\mathcal{A}}.\ (W, n, \mathsf{Lb}(v_1), \mathsf{Lb}(v_2)) \in \lceil ((\mathsf{Labeled}\ \ell\ '\tau')\ \sigma) \rceil_V^{\mathcal{A}}$

This means we are given $(W, n, \mathsf{Lb}(v_1), \mathsf{Lb}(v_2)) \in \lceil ((\mathsf{Labeled}\ \ell\ \tau)\ \sigma) \rceil_V^{\mathcal{A}}$
From Definition 2.4 it means we have $\mathit{ValEq}(\mathcal{A}, W, \ell\ \sigma, n, v_1, v_2, \tau\ \sigma)$ (Sub-L0)
and it suffices to prove $(W, n, \mathsf{Lb}(v_1), \mathsf{Lb}(v_2)) \in \lceil ((\mathsf{Labeled}\ \ell\ '\tau')\ \sigma) \rceil_V^{\mathcal{A}}$
Again from Definition 2.4 it means w need to prove that
$\mathit{ValEq}(\mathcal{A}, W, \ell'\ \sigma, n, \mathsf{Lb}(v_1), \mathsf{Lb}_\ell(v_2), \tau'\ \sigma)$

Since we have (Sub-L0) and $\ell\ \sigma \sqsubseteq \ell'\ \sigma$ therefore from Lemma 2.26 we have
$\mathit{ValEq}(\mathcal{A}, W, \ell'\ \sigma, n, \mathsf{Lb}(v_1), \mathsf{Lb}_\ell(v_2), \tau\ \sigma)$

2 cases arise:

(a) $\ell'\ \sigma \sqsubseteq \mathcal{A}$:
In this case from Definition 2.3 we know that $(W, n, v_1, v_2) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$
From IH we also know that $(W, n, v_1, v_2) \in \lceil \tau'\ \sigma \rceil_V^{\mathcal{A}}$
And from Definition 2.4 we get $\mathit{ValEq}(\mathcal{A}, W, \ell'\ \sigma, n, \mathsf{Lb}(v_1), \mathsf{Lb}_\ell(v_2), \tau'\ \sigma)$

(b) $\ell' \ \sigma \not\sqsubseteq \mathcal{A}$:

In this case from Definition 2.3 we know that $\forall j. \ (W.\theta_1, j, v_1) \in \lfloor \tau \ \sigma \rfloor_V$ and $(W.\theta_2, j, v_2) \in \lfloor \tau \ \sigma \rfloor_V$

Since $\tau \ \sigma <: \tau' \ \sigma$ therefore from Lemma 2.23 we get $(W.\theta_1, j, v_1) \in \lfloor \tau' \ \sigma \rfloor_V$ and $(W.\theta_2, j, v_2) \in \lfloor \tau' \ \sigma \rfloor_V$

And from Definition 2.4 we get $\mathit{ValEq}(\mathcal{A}, W, \ell' \ \sigma, n, \mathsf{Lb}(v_1), \mathsf{Lb}_\ell(v_2), \tau' \ \sigma)$

7. SLIO*sub-CG:

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell_i' \sqsubseteq \ell_i \qquad \Sigma; \Psi \vdash \ell_o \sqsubseteq \ell_o'}{\Sigma; \Psi \vdash \mathbb{SLIO} \ \ell_i \ \ell_o \ \tau <: \mathbb{SLIO} \ \ell_i' \ \ell_o' \ \tau'}$$

To prove: $\lceil ((\mathbb{SLIO} \ \ell_i \ \ell_o \ \tau) \ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil ((\mathbb{SLIO} \ \ell_i' \ \ell_o' \ \tau') \ \sigma) \rceil_V^{\mathcal{A}}$

IH: $\lceil (\tau \ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil (\tau' \ \sigma) \rceil_V^{\mathcal{A}}$

It suffices to prove: $\forall (W, n, e_1, e_2) \in \lceil ((\mathbb{SLIO} \ \ell_i \ \ell_o \ \tau) \ \sigma) \rceil_V^{\mathcal{A}}. \ (W, n, e_1, e_2) \in \lceil ((\mathbb{SLIO} \ \ell_i' \ \ell_o' \ \tau') \ \sigma) \rceil_V^{\mathcal{A}}$

This means we are given $(W, n, e_1, e_2) \in \lceil ((\mathbb{SLIO} \ \ell_i \ \ell_o \ \tau) \ \sigma) \rceil_V^{\mathcal{A}}$

From Definition 2.4 it means we have

$\Big(\forall k \leq n, W_e \sqsupseteq W, H_1, H_2.(k, H_1, H_2) \rhd W_e \wedge \forall v_1', v_2', j.$
$(H_1, e_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, e_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \rhd W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_o \ \sigma, v_1', v_2', \tau \ \sigma)\Big) \wedge$
$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \rhd \theta_e \wedge (H, e_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \rhd \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau \ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled} \ \ell' \ \tau' \wedge \ell_i \ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_i \ \sigma)\Big)$ (Sub-CG0)

And we need to prove

$(W, n, e_1, e_2) \in \lceil ((\mathbb{SLIO} \ \ell_i' \ \ell_o' \ \tau') \ \sigma) \rceil_V^{\mathcal{A}}$

Again from Definition 2.4 it means we need to prove

$\Big(\forall k \leq n, W_e \sqsupseteq W, H_1, H_2.(k, H_1, H_2) \rhd W_e \wedge \forall v_1', v_2', j.$
$(H_1, e_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, e_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \rhd W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_o' \ \sigma, v_1', v_2', \tau' \ \sigma)\Big) \wedge$
$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \rhd \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \rhd \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau' \ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled} \ \ell' \ \tau'' \wedge \ell_i' \ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_i' \ \sigma)\Big)$

It means we need to prove:

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \rhd W_e \wedge \forall v_1', v_2', j.$
$(H_1, e_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, e_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \rhd W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_o \ \sigma, v_1', v_2', \tau' \ \sigma)$:

This means we are given $k \leq n$, $W_e \sqsupseteq W, H_1, H_2, v_1', v_2', j < k$ s.t
$(k, H_1, H_2) \triangleright W_e$, $(H_1, e_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, e_2) \Downarrow^f (H_2', v_2')$

And we need to prove
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_o' \ \sigma, v_1', v_2', \tau' \ \sigma)$

Instantiating the first conjuct of (Sub-CG0) to get
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_o \ \sigma, v_1', v_2', \tau \ \sigma)$ (Sub-CG1)

Since from (Sub-CG1) $\mathit{ValEq}(\mathcal{A}, W', k-j, \ell_o \ \sigma, v_1', v_2', \tau \ \sigma)$
Therefore from Lemma 2.26 we get $\mathit{ValEq}(\mathcal{A}, W', k-j, \ell_o' \ \sigma, v_1', v_2', \tau \ \sigma)$

(b) $\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, e_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau' \ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell' \ \tau'' \wedge \ell_i \ \sigma \sqsubseteq \ell') \wedge$
$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_i \ \sigma)$:

Case $l = 1$

Here we are given $k, \theta_e \sqsupseteq \theta, H, j < k$ s.t $(k, H) \triangleright \theta_e \wedge (H, e_l) \Downarrow_j^f (H', v_l')$

And we need to prove

i. $\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau' \ \sigma \rfloor_V$:
Instantiating the second conjunct of (Sub-CG0) with the given k, θ_e, H, j to get
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau \ \sigma \rfloor_V$

Since $\tau \ \sigma <: \tau' \ \sigma$ therefore from Lemma 2.23 we get $(\theta', k-j, v_l') \in \lfloor \tau' \ \sigma \rfloor_V$

ii. $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell' \ \tau'' \wedge \ell_i' \ \sigma \sqsubseteq \ell')$:
Instantiating the second conjunct of (Sub-CG0) with the given v, i, k, θ_e, H, j to get
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell' \ \tau'' \wedge \ell_i \ \sigma \sqsubseteq \ell')$
Since $\ell_i' \ \sigma \sqsubseteq \ell_i \ \sigma$ therefore we also get
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell' \ \tau'' \wedge \ell_i' \ \sigma \sqsubseteq \ell')$

iii. $(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_i' \ \sigma)$:
Instantiating the second conjunct of (Sub-CG0) with the given v, i, k, θ_e, H, j to get
$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_i \ \sigma)$
Since $\ell_i' \ \sigma \sqsubseteq \ell_i \ \sigma$ therefore we also get
$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_i' \ \sigma)$

Case $l = 2$

Symmetric reasoning as in the previous $l = 1$ case

8. SLIO*sub-base:
Trivial

Proof of Statement (2)
It suffice to prove that
$\forall (W, n, e_1, e_2) \in \lceil (\tau \ \sigma) \rceil_E^{\mathcal{A}}. \ (W, n, e_1, e_2) \in \lceil (\tau' \ \sigma) \rceil_E^{\mathcal{A}}$

This means given $(W, n, e_1, e_2) \in \lceil (\tau \ \sigma) \rceil_E^{\mathcal{A}}$

From Definition 2.5 it means we have
$\forall i < n.e_1 \Downarrow_i v_1 \wedge e_2 \Downarrow v_2 \implies (W, n-i, v_1, v_2) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$ (Sub-E0)

And it suffices to prove $(W, n, e_1, e_2) \in \lceil (\tau'\ \sigma) \rceil_E^{\mathcal{A}}$
Again from Definition 2.5 it means we need to prove
$\forall i < n.e_1 \Downarrow_i v_1 \wedge e_2 \Downarrow v_2 \implies (W, n-i, v_1, v_2) \in \lceil \tau'\ \sigma \rceil_V^{\mathcal{A}}$

This means that given $i < n$ s.t $e_1 \Downarrow_i v_1 \wedge e_2 \Downarrow v_2$ we need to prove $(W, n-i, v_1, v_2) \in \lceil \tau'\ \sigma \rceil_V^{\mathcal{A}}$

Instantiating (Sub-E0) with the given i we get $(W, n-i, v_1, v_2) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

From Statement (1) we get $(W, n-i, v_1, v_2) \in \lceil \tau'\ \sigma \rceil_V^{\mathcal{A}}$ □

Theorem 2.28 (SLIO*: NI). *Say* $\mathsf{bool} = (\mathsf{unit} + \mathsf{unit})$
$\forall v_1, v_2, e, \tau, n.$
$\emptyset \vdash v_1 : \mathsf{Labeled}\ \top\ \mathsf{bool} \wedge \emptyset \vdash v_2 : \mathsf{Labeled}\ \top\ \mathsf{bool} \wedge$
$x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e : \mathbb{SLIO}\ \bot\ \bot\ \mathsf{bool} \wedge$
$(\emptyset, e[v_1/x]) \Downarrow_{n'}^f (-, v_1') \wedge (\emptyset, e[v_2/x]) \Downarrow_{n'}^f (-, v_2') \implies$
$v_1' = v_2'$

Proof. Given some
$\emptyset \vdash v_1 : \mathsf{Labeled}\ \top\ \mathsf{bool} \wedge \emptyset \vdash v_2 : \mathsf{Labeled}\ \top\ \mathsf{bool} \wedge$
$x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e : \mathbb{SLIO}\ \bot\ \bot\ \mathsf{bool} \wedge$
$(\emptyset, e[v_1/x]) \Downarrow_{n'}^f (-, v_1') \wedge (\emptyset, e[v_2/x]) \Downarrow_{-}^f (-, v_2')$

And we need to prove
$v_1' = v_2'$

From Theorem 2.25 we know that
$\forall n.(\emptyset, n, v_1, v_2) \in \lceil \mathsf{Labeled}\ \top\ \mathsf{bool} \rceil_E^{\bot}$
Similarly from Theorem 2.25 and Definition 2.14 we also get
$\forall n.(\emptyset, n, e[v_1/x], e[v_2/x]) \in \lceil \mathbb{SLIO}\ \bot\ \bot\ \mathsf{bool} \rceil_E^{\bot}$

From Definition 2.5 we get
$\forall n.\forall i < n.e[v_1/x] \Downarrow_i v_{11} \wedge e[v_2/x] \Downarrow v_{22} \implies (\emptyset, n-i, v_{11}, v_{22}) \in \lceil \mathbb{SLIO}\ \bot\ \bot\ \mathsf{bool} \rceil_V^{\bot}$

Instantiating it with $n' + 1$ and then with 0, from CG-val we have $v_{11} = e[v_1/x]$ and $v_{22} = e[v_2/x]$
Therefore we have
$(\emptyset, n' + 1, e[v_1/x], e[v_2/x]) \in \lceil \mathbb{SLIO}\ \bot\ \bot\ \mathsf{bool} \rceil_V^{\bot}$

From Definition 2.6 we have
$\Big(\forall k \leq (n'+1), W_e \sqsupseteq \emptyset, H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge$
$\forall v_1'', v_2'', j.(H_1, e[v_1/x]) \Downarrow_j^f (H_1', v_1'') \wedge (H_2, e[v_2/x]) \Downarrow^f (H_2', v_2'') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\bot, W', k-j, \bot, v_1', v_2', \mathsf{b})\Big) \wedge$
$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \mathsf{b} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \bot \sqsubseteq \ell') \wedge$
$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \bot)\Big)$

Instantiating the first conjunct with $n' + 1, \emptyset, \emptyset, \emptyset$.
Since we know that
$(\emptyset, e[v_1/x]) \Downarrow_{n'}^{f} (-, v_1') \wedge n' < n \wedge (\emptyset, e[v_2/x]) \Downarrow_{n'}^{f} (-, v_2')$

Therefore we instantiate v_1'' with v_1', v_2'' with v_2', j with n' to get
$\exists W' \sqsupseteq \emptyset.(n - n', H_1', H_2') \triangleright W' \wedge ValEq(\bot, W', k - j, \bot, v_1', v_2', \mathsf{bool})$

From Definition 2.3 and Definition 2.6 we get $v_1' = v_2'$

□

3 Translations between FG and SLIO*

3.1 Translation from SLIO* to FG

3.1.1 Type directed translation from SLIO* to FG

SLIO* types are translated into FG types by the following definition of $[\![\cdot]\!]$

$$[\![\mathsf{b}]\!] = \mathsf{b}^{\perp}$$
$$[\![\tau_1 \to \tau_2]\!] = ([\![\tau_1]\!] \xrightarrow{\top} [\![\tau_2]\!])^{\perp} \qquad [\![\mathsf{ref}\ \ell\ \tau]\!] = (\mathsf{ref}\ ([\![\tau]\!] + \mathsf{unit})^{\ell})^{\perp}$$
$$[\![\tau_1 \times \tau_2]\!] = ([\![\tau_1]\!] \times [\![\tau_2]\!])^{\perp} \qquad [\![\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau]\!] = (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau]\!] + \mathsf{unit})^{\ell_o})^{\perp}$$
$$[\![\tau_1 + \tau_2]\!] = ([\![\tau_1]\!] + [\![\tau_2]\!])^{\perp} \qquad [\![c \Rightarrow \tau]\!] = (c \overset{\top}{\Rightarrow} [\![\tau]\!])^{\perp}$$
$$[\![\mathsf{Labeled}\ \ell\ \tau]\!] = ([\![\tau]\!] + \mathsf{unit})^{\ell} \qquad [\![\forall\alpha.\tau]\!] = (\forall\alpha.(\top, [\![\tau]\!]))^{\perp}$$

The translation judgment for expressions is of the form $\boxed{\Sigma; \Psi; \Gamma \vdash_{pc} e_C : \tau_C \rightsquigarrow e_F}$. Its rules are shown below.

$$\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash x : \tau \rightsquigarrow x}\ \text{var}$$

$$\frac{\Sigma; \Psi; \Gamma, x : \tau \vdash e : \tau' \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \lambda x.e : \tau \to \tau' \rightsquigarrow \lambda x.e_F}\ \text{lam}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \tau \to \tau' \rightsquigarrow e_{F1} \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \tau \rightsquigarrow e_{F2}}{\Sigma; \Psi; \Gamma \vdash e_1\ e_2 : \tau' \rightsquigarrow e_{F1}\ e_{F2}}\ \text{app}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \tau_1 \rightsquigarrow e_{F1} \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \tau_2 \rightsquigarrow e_{F2}}{\Sigma; \Psi; \Gamma \vdash (e_1, e_2) : (\tau_1 \times \tau_2) \rightsquigarrow (e_{F1}, e_{F2})}\ \text{prod}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau_1 \times \tau_2 \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{fst}(e) : \tau_1 \rightsquigarrow \mathsf{fst}(e_F)}\ \text{fst}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau_1 \times \tau_2 \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{snd}(e) : \tau_1 \rightsquigarrow \mathsf{snd}(e_F)}\ \text{snd}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau_1 \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{inl}(e) : \tau_1 + \tau_2 \rightsquigarrow \mathsf{inl}(e_F)}\ \text{inl}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau_1 \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{inr}(e) : \tau_1 + \tau_2 \rightsquigarrow \mathsf{inr}(e_F)}\ \text{inr}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau_1 + \tau_2 \rightsquigarrow e_F \qquad \Sigma; \Psi; \Gamma, x : \tau_1 \vdash e_1 : \tau \rightsquigarrow e_{F1} \qquad \Sigma; \Psi; \Gamma, y : \tau_2 \vdash e_2 : \tau \rightsquigarrow e_{F2}}{\Sigma; \Psi; \Gamma \vdash \mathsf{case}(e, x.e_1, y.e_2) : \tau \rightsquigarrow \mathsf{case}(e_F, x.e_{F1}, y.e_{F2})}\ \text{case}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{Lb}_{\ell}(e) : (\mathsf{Labeled}\ \ell\ \tau) \rightsquigarrow \mathsf{inl}(e_F)}\ \text{label}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{Labeled}\ \ell\ \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{unlabel}(e) : \mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau \rightsquigarrow \lambda\_.e_F}\ \text{unlabel}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{toLabeled}(e) : \mathbb{SLIO}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(e_F\ ())}\ \text{toLabeled}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{ret}(e) : \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau \rightsquigarrow \lambda\_.\mathsf{inl}(e_F)}\ \text{ret}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \mathbb{SLIO}\ \ell_i\ \ell\ \tau \rightsquigarrow e_{F1} \qquad \Sigma; \Psi; \Gamma, x : \tau \vdash e_2 : \mathbb{SLIO}\ \ell\ \ell_o\ \tau' \rightsquigarrow e_{F2}}{\Sigma; \Psi; \Gamma \vdash \mathsf{bind}(e_1, x.e_2) : \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau' \rightsquigarrow \lambda\_.\mathsf{case}(e_{F1}(), x.e_{F2}(), y.\mathsf{inr}()) } \text{bind}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{Labeled}\ \ell'\ \tau \rightsquigarrow e_F \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash \mathsf{new}\ e : \mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_F))} \text{ref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{ref}\ \ell\ \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash !e : \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(e_F)} \text{deref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \mathsf{ref}\ \ell'\ \tau \rightsquigarrow e_{F1} \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \mathsf{Labeled}\ \ell'\ \tau \rightsquigarrow e_{F2} \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash e_1 := e_2 : \mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit} \rightsquigarrow \lambda\_.\mathsf{inl}(e_{F1} := e_{F2})} \text{assign}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau' \rightsquigarrow e_F \qquad \Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi; \Gamma \vdash e : \tau \rightsquigarrow e_F} \text{sub}$$

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \Lambda e : \forall \alpha.\tau \rightsquigarrow \Lambda e_F} \text{FI}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \forall \alpha.\tau \rightsquigarrow e_F \qquad \mathrm{FV}(\ell) \in \Sigma}{\Sigma; \Psi; \Gamma \vdash e\ [] : \tau[\ell/\alpha] \rightsquigarrow e_F[]} \text{FE}$$

$$\frac{\Sigma; \Psi, c; \Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \nu\ e : c \Rightarrow \tau \rightsquigarrow \nu\ e_F} \text{CI}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : c \Rightarrow \tau \rightsquigarrow e_F \qquad \Sigma; \Psi \vdash c}{\Sigma; \Psi; \Gamma \vdash e \bullet : \tau \rightsquigarrow e_F \bullet} \text{CE}$$

3.1.2 Type preservation for SLIO* to FG translation

Assumption 3.1. $\forall e, \tau, \Sigma, \Psi, \Gamma, \ell_i, \ell_o.$
$\Sigma; \Psi; \Gamma \vdash e : \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau \implies \ell_i \sqsubseteq \ell_o$

Theorem 3.2 (SLIO* $\rightsquigarrow$ FG: Type preservation)**.** $\forall \Sigma, \Psi, \Gamma, e_C, \tau.$
$\Sigma; \Psi; \Gamma \vdash e_C : \tau$ *is a valid typing derivation in SLIO** $\implies$
$\exists e_F.$
$\Sigma; \Psi; \Gamma \vdash e_C : \tau \rightsquigarrow e_F\ \wedge$
$\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top e_F : [\![\tau]\!]$ *is a valid typing derivation in FG*

Proof. Proof by induction on the translation judgment. We show selected cases below.

1. label:

$$\frac{\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top e_F : [\![\tau]\!]}\text{IH}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top \mathsf{inl}(e_F) : ([\![\tau]\!] + \mathsf{unit})^\perp}\text{FG-inl}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top \mathsf{inl}(e_F) : ([\![\tau]\!] + \mathsf{unit})^\ell}\text{FG-sub}$$

2. unlabel:

P1:

$$\frac{\Sigma; \Psi \vdash \ell \sqsubseteq \ell_i \sqcup \ell \qquad \dfrac{}{\Sigma; \Psi \vdash ([\![\tau]\!] + \mathsf{unit}) <: ([\![\tau]\!] + \mathsf{unit})}\text{Lemma 1.1}}{\Sigma; \Psi \vdash ([\![\tau]\!] + \mathsf{unit})^\ell <: ([\![\tau]\!] + \mathsf{unit})^{\ell_i \sqcup \ell}}\text{FGsub-label}$$

Main derivation:

$$\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_\top e_F : ([\![\tau]\!] + \mathsf{unit})^\ell}\text{ IH, Weakening} \qquad \Sigma; \Psi \vdash \ell_i \sqsubseteq \top \qquad P1}{\dfrac{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_i} e_F : ([\![\tau]\!] + \mathsf{unit})^{\ell_i \sqcup \ell}}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_\top \lambda\_.e_F : (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau]\!] + \mathsf{unit})^{\ell_i \sqcup \ell})^\perp}\text{ FG-lam}}\text{ FG-sub}$$

3. toLabeled:

P2:

$$\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_\top e_F : (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau]\!] + \mathsf{unit})^{\ell_o})^\perp}\text{ IH, Weakening} \qquad \Sigma; \Psi \vdash \ell_i \sqsubseteq \top}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_i} e_F : (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau]\!] + \mathsf{unit})^{\ell_o})^\perp}\text{ FG-sub}$$

P1:

$$\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_i} () : \mathsf{unit}} \qquad \begin{array}{c} P2 \\ \Sigma; \Psi \vdash \ell_i \sqcup \perp \sqsubseteq \ell_i \end{array} \qquad \Sigma; \Psi \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell_o} \searrow \perp}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_i} e_F() : ([\![\tau]\!] + \mathsf{unit})^{\ell_o}}\text{ FG-app}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad \Sigma; \Psi \vdash \perp \sqsubseteq \ell_i}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_i} \mathsf{inl}(e_F()) : (([\![\tau]\!] + \mathsf{unit})^{\ell_o} + \mathsf{unit})^{\ell_i}}\text{ FG-inl, FG-sub}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top \lambda\_.\mathsf{inl}(e_F()) : (\mathsf{unit} \xrightarrow{\ell_i} (([\![\tau]\!] + \mathsf{unit})^{\ell_o} + \mathsf{unit})^{\ell_i})^\perp}\text{ FG-lam}$$

4. ret:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_\top e_F : [\![\tau]\!]}\text{ IH, Weakening} \qquad \Sigma; \Psi \vdash \ell_i \sqsubseteq \top}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_i} e_F : [\![\tau]\!]}\text{ FG-sub} \qquad \Sigma; \Psi \vdash \perp \sqsubseteq \ell_i}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_i} \mathsf{inl}(e_F) : ([\![\tau]\!] + \mathsf{unit})^{\ell_i}}\text{ FG-sub, FG-in}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top \lambda\_.\mathsf{inl}(e_F) : (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau]\!] + \mathsf{unit})^{\ell_i})^\perp}$$

5. bind:

P1.1:

$$\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_\top e_{F1} : (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau]\!] + \mathsf{unit})^{\ell})^\perp}\text{ IH1, Weakening} \qquad \Sigma; \Psi \vdash \ell_i \sqsubseteq \top}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_i} e_{F1} : (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau]\!] + \mathsf{unit})^{\ell})^\perp}\text{ FG-sub}$$

P1:

$$\dfrac{\begin{array}{c} P1.1 \\ \Sigma; \Psi \vdash (\ell_i \sqcup \perp) \sqsubseteq \ell_i \end{array} \qquad \begin{array}{c} \dfrac{}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_i} () : \mathsf{unit}}\text{ FG-var} \\ \dfrac{\Sigma; \Psi \vdash \perp \sqsubseteq \ell}{\Sigma; \Psi \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell} \searrow \perp} \end{array}}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_i} e_{F1}() : ([\![\tau]\!] + \mathsf{unit})^{\ell}}\text{ FG-app}$$

P2.1:

$$\dfrac{\dfrac{}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_:\mathsf{unit},x:\llbracket\tau\rrbracket\vdash_{\top}e_{F2}:(\mathsf{unit}\xrightarrow{\ell}(\llbracket\tau'\rrbracket+\mathsf{unit})^{\ell_o})^{\perp}}\text{IH2, Weakening}\qquad \Sigma;\Psi\vdash\ell\sqsubseteq\top}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_:\mathsf{unit},x:\llbracket\tau\rrbracket\vdash_{\ell}e_{F2}:(\mathsf{unit}\xrightarrow{\ell}(\llbracket\tau'\rrbracket+\mathsf{unit})^{\ell_o})^{\perp}}\text{FG-sub}$$

P2:

$$\dfrac{P2.1\qquad \dfrac{}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_:\mathsf{unit},x:\llbracket\tau\rrbracket\vdash_{\ell}():\mathsf{unit}}\text{FG-var}\qquad \Sigma;\Psi\vdash(\ell\sqcup\perp)\sqsubseteq\ell\qquad \dfrac{\Sigma;\Psi\vdash\perp\sqsubseteq\ell_o}{\Sigma;\Psi\vdash(\llbracket\tau'\rrbracket+\mathsf{unit})^{\ell_o}\searrow\perp}}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_:\mathsf{unit},x:\llbracket\tau\rrbracket\vdash_{\ell_i\sqcup\ell}e_{F2}():(\llbracket\tau'\rrbracket+\mathsf{unit})^{\ell_o}}\text{FG-app}$$

P3:

$$\dfrac{\dfrac{}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_:\mathsf{unit},y:\mathsf{unit}\vdash_{\ell}():\mathsf{unit}}\text{FG-var}\qquad \Sigma;\Psi\vdash\perp\sqsubseteq\ell_o}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_:\mathsf{unit},y:\mathsf{unit}\vdash_{\ell}\mathsf{inr}():(\llbracket\tau'\rrbracket+\mathsf{unit})^{\ell_o}}\text{FG-sub, FG-inr}$$

Main derivation:

$$\dfrac{\dfrac{P1\qquad P2\qquad P3\qquad \dfrac{\dfrac{\dfrac{}{\Sigma;\Psi;\Gamma\vdash e_2:\mathbb{SLIO}\;\ell\;\ell_o\;\tau}\text{Given}}{\Sigma;\Psi\vdash\ell\sqsubseteq\ell_o}\text{Assumption 3.1}}{\Sigma;\Psi\vdash(\llbracket\tau'\rrbracket+\mathsf{unit})^{\ell_o}\searrow\ell}}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_:\mathsf{unit}\vdash_{\ell_i}\mathsf{case}(e_{F1}(),x.e_{F2}(),y.\mathsf{inr}()):(\llbracket\tau'\rrbracket+\mathsf{unit})^{\ell_o}}\text{FG-case}}{\Sigma;\Psi;\llbracket\Gamma\rrbracket\vdash_{\top}\lambda\_.\mathsf{case}(e_{F1}(),x.e_{F2}(),y.\mathsf{inr}()):(\mathsf{unit}\xrightarrow{\ell_i}(\llbracket\tau'\rrbracket+\mathsf{unit})^{\ell_o})^{\perp}}\text{FG-lam, weak}$$

6. ref:

P1:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_:\mathsf{unit}\vdash_{\top}e_F:(\llbracket\tau\rrbracket+\mathsf{unit})^{\ell'}}\text{IH, Weakening}\qquad \Sigma;\Psi\vdash\ell\sqsubseteq\top}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_:\mathsf{unit}\vdash_{\ell}e_F:(\llbracket\tau\rrbracket+\mathsf{unit})^{\ell'}}\text{FG-sub}\qquad \dfrac{\Sigma;\Psi\vdash\ell\sqsubseteq\ell'}{\Sigma;\Psi\vdash(\llbracket\tau\rrbracket+\mathsf{unit})^{\ell'}\searrow\ell}}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_:\mathsf{unit}\vdash_{\ell}\mathsf{new}\;e_F:(\mathsf{ref}(\llbracket\tau\rrbracket+\mathsf{unit})^{\ell'})^{\perp}}\text{FG-ref}$$

Main derivation:

$$\dfrac{\dfrac{P1\qquad \Sigma;\Psi\vdash\perp\sqsubseteq\ell}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_:\mathsf{unit}\vdash_{\ell}\mathsf{inl}(\mathsf{new}\;e_F):((\mathsf{ref}(\llbracket\tau\rrbracket+\mathsf{unit})^{\ell'})^{\perp}+\mathsf{unit})^{\ell}}\text{FG-inl, FG-sub}}{\Sigma;\Psi;\llbracket\Gamma\rrbracket\vdash_{\top}\lambda\_.\mathsf{inl}(\mathsf{new}\;e_F):(\mathsf{unit}\xrightarrow{\ell}((\mathsf{ref}(\llbracket\tau\rrbracket+\mathsf{unit})^{\ell'})^{\perp}+\mathsf{unit})^{\ell})^{\perp}}\text{FG-lam}$$

7. deref:

P2:

$$\dfrac{\dfrac{}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_:\mathsf{unit}\vdash_{\top}e_F:(\mathsf{ref}\;(\llbracket\tau\rrbracket+\mathsf{unit})^{\ell})^{\perp}}\text{IH, Weakening}\qquad \Sigma;\Psi\vdash\ell'\sqsubseteq\top}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_:\mathsf{unit}\vdash_{\ell'}e_F:(\mathsf{ref}\;(\llbracket\tau\rrbracket+\mathsf{unit})^{\ell})^{\perp}}\text{FG-sub}$$

P1:

$$\dfrac{P2 \qquad \dfrac{}{\Sigma; \Psi \vdash (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell} <: (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell}}\ \text{Lemma 1.1} \qquad \dfrac{}{\Sigma; \Psi \vdash (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell} \searrow \bot}}{\Sigma; \Psi; \llbracket\Gamma\rrbracket, \_ : \mathsf{unit} \vdash_{\ell'} !e_F : (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell}}\ \text{FG-deref}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad \Sigma; \Psi \vdash \bot \sqsubseteq \ell' \qquad \dfrac{\Sigma; \Psi \vdash \ell \sqsubseteq \ell}{\Sigma; \Psi \vdash (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell} <: (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell}}}{\Sigma; \Psi; \llbracket\Gamma\rrbracket, \_ : \mathsf{unit} \vdash_{\ell'} \mathsf{inl}(!e_F) : ((\llbracket\tau\rrbracket + \mathsf{unit})^{\ell} + \mathsf{unit})^{\ell'}}\ \text{FG-inl, FG-sub}}{\Sigma; \Psi; \llbracket\Gamma\rrbracket \vdash_{\top} \lambda\_.\mathsf{inl}(!e_F) : (\mathsf{unit} \xrightarrow{\ell'} ((\llbracket\tau\rrbracket + \mathsf{unit})^{\ell} + \mathsf{unit})^{\ell'})^{\bot}}\ \text{FG-lam}$$

8. assign:

P3:

$$\dfrac{\dfrac{}{\Sigma; \Psi; \llbracket\Gamma\rrbracket, \_ : \mathsf{unit} \vdash_{\top} e_{F2} : (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell'}}\ \text{IH2, Weakening} \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \top}{\Sigma; \Psi; \llbracket\Gamma\rrbracket, \_ : \mathsf{unit} \vdash_{\ell} e_{F2} : (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell'}}\ \text{FG-sub}$$

P2:

$$\dfrac{\dfrac{}{\Sigma; \Psi; \llbracket\Gamma\rrbracket, \_ : \mathsf{unit} \vdash_{\top} e_{F1} : (\mathsf{ref}(\llbracket\tau\rrbracket + \mathsf{unit})^{\ell'})^{\bot}}\ \text{IH1, Weakening} \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \top}{\Sigma; \Psi; \llbracket\Gamma\rrbracket, \_ : \mathsf{unit} \vdash_{\ell} e_{F1} : (\mathsf{ref}(\llbracket\tau\rrbracket + \mathsf{unit})^{\ell'})^{\bot}}\ \text{FG-sub}$$

P1:

$$\dfrac{P2 \qquad P3 \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash \ell \sqsubseteq \ell'}\ \text{Given}}{\Sigma; \Psi \vdash (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell'} \searrow (\ell \sqcup \bot)}}{\Sigma; \Psi; \llbracket\Gamma\rrbracket, \_ : \mathsf{unit} \vdash_{\ell} e_{F1} := e_{F2} : \mathsf{unit}}\ \text{FG-assign}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad \Sigma; \Psi \vdash \bot \sqsubseteq \ell}{\Sigma; \Psi; \llbracket\Gamma\rrbracket, \_ : \mathsf{unit} \vdash_{\ell} \mathsf{inl}(e_{F1} := e_{F2}) : (\mathsf{unit} + \mathsf{unit})^{\ell}}\ \text{FG-inl, FG-sub}}{\Sigma; \Psi; \llbracket\Gamma\rrbracket \vdash_{\top} \lambda\_.\mathsf{inl}(e_{F1} := e_{F2}) : (\mathsf{unit} \xrightarrow{\ell} (\mathsf{unit} + \mathsf{unit})^{\ell})^{\bot}}\ \text{FG-lam}$$

9. sub:

$$\dfrac{\dfrac{}{\Sigma; \Psi; \llbracket\Gamma\rrbracket \vdash_{\top} e_F : \llbracket\tau'\rrbracket}\ \text{IH} \qquad \Sigma; \Psi \vdash \top \sqsubseteq \top \qquad \dfrac{\Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi \vdash \llbracket\tau'\rrbracket <: \llbracket\tau\rrbracket}\ \text{Lemma 3.3}}{\Sigma; \Psi; \llbracket\Gamma\rrbracket \vdash_{\top} e_F : \llbracket\tau\rrbracket}\ \text{FG-sub}$$

10. FI:

$$\dfrac{\dfrac{}{\Sigma, \alpha; \Psi; \llbracket\Gamma\rrbracket \vdash_{\top} e_F : \llbracket\tau\rrbracket}\ \text{IH}}{\Sigma; \Psi; \llbracket\Gamma\rrbracket \vdash_{\top} \Lambda e_F : (\forall\alpha.(\top, \llbracket\tau\rrbracket))^{\bot}}\ \text{FG-FI}$$

11. FE:

$$\dfrac{\dfrac{\mathrm{FV}(\ell) \in \Sigma \qquad \Sigma; \Psi \vdash \top \sqcup \bot \sqsubseteq \top \qquad \dfrac{}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top e_F : (\forall \alpha.(\top, [\![\tau]\!]))^\bot}\text{ IH} \qquad \Sigma; \Psi \vdash [\![\tau[\ell/\alpha]]\!] \searrow \bot}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top e_F\ [] : [\![\tau]\!][\ell/\alpha]}\text{ FG-FE}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top e_F\ [] : [\![\tau[\ell/\alpha]]\!]}\text{ Lemma 3.6}$$

12. CI:

$$\dfrac{\dfrac{}{\Sigma; \Psi, c; [\![\Gamma]\!] \vdash_\top e_F : [\![\tau]\!]}\text{ IH}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top \nu\ e_F : (c \overset{\top}{\Rightarrow} [\![\tau]\!])^\bot}\text{ FG-CI}$$

13. CE:

$$\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top e_F : (c \overset{\top}{\Rightarrow} [\![\tau]\!])^\bot}\text{ IH} \qquad \Sigma; \Psi \vdash c \qquad \Sigma; \Psi \vdash \top \sqcup \bot \sqsubseteq \top \qquad \Sigma; \Psi \vdash [\![\tau]\!] \searrow \bot}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top e_F \bullet : [\![\tau]\!]}\text{ FG-CE}$$

□

Lemma 3.3 (SLIO* ⇝ FG: Subtyping)**.** *For any SLIO* types τ and τ', Σ, and Ψ, if $\Sigma; \Psi \vdash \tau <: \tau'$, then $\Sigma; \Psi \vdash [\![\tau]\!] <: [\![\tau']\!]$.*

Proof. Proof by induction on SLIO*'s subtyping relation

1. SLIO*sub-base:

$$\dfrac{}{\Sigma; \Psi \vdash [\![\tau]\!] <: [\![\tau]\!]}\text{ Lemma 1.1}$$

2. SLIO*sub-arrow:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_1']\!] <: [\![\tau_1]\!]}\text{ IH1} \qquad \dfrac{}{\Sigma; \Psi \vdash [\![\tau_2]\!] <: [\![\tau_2']\!]}\text{ IH2} \qquad \Sigma; \Psi \vdash \top \sqsubseteq \top}{\Sigma; \Psi \vdash ([\![\tau_1]\!] \overset{\top}{\to} [\![\tau_2]\!])^\bot <: ([\![\tau_1']\!] \overset{\top}{\to} [\![\tau_2']\!])^\bot}\text{ FGsub-arrow}}{\Sigma; \Psi \vdash [\![(\tau_1 \overset{\ell_e}{\to} \tau_2)]\!] <: [\![(\tau_1' \overset{\ell_e'}{\to} \tau_2')]\!]}\text{ Definition of } [\![\cdot]\!]$$

3. SLIO*sub-prod:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_1]\!] <: [\![\tau_1']\!]}\text{ IH1} \qquad \dfrac{}{\Sigma; \Psi \vdash [\![\tau_2]\!] <: [\![\tau_2']\!]}\text{ IH2}}{\Sigma; \Psi \vdash ([\![\tau_1]\!] \times [\![\tau_2]\!])^\bot <: ([\![\tau_1']\!] \times [\![\tau_2']\!])^\bot}\text{ FGsub-arrow}}{\Sigma; \Psi \vdash [\![(\tau_1 \times \tau_2)]\!] <: [\![(\tau_1' \times \tau_2')]\!]}\text{ Definition of } [\![\cdot]\!]$$

4. SLIO*sub-sum:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \llbracket \tau_1 \rrbracket <: \llbracket \tau_1' \rrbracket}\text{ IH1} \qquad \dfrac{}{\Sigma; \Psi \vdash \llbracket \tau_2 \rrbracket <: \llbracket \tau_2' \rrbracket}\text{ IH2}}{\Sigma; \Psi \vdash (\llbracket \tau_1 \rrbracket + \llbracket \tau_2 \rrbracket)^{\perp} <: (\llbracket \tau_1' \rrbracket + \llbracket \tau_2' \rrbracket)^{\perp}}\text{ FGsub-arrow}}{\Sigma; \Psi \vdash \llbracket (\tau_1 + \tau_2) \rrbracket <: \llbracket (\tau_1' + \tau_2') \rrbracket}\text{ Definition of } \llbracket \cdot \rrbracket$$

5. SLIO*sub-labeled:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \llbracket \tau_1 \rrbracket <: \llbracket \tau_1' \rrbracket}\text{ IH1} \qquad \dfrac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}}\text{ FGsub-unit}}{\Sigma; \Psi \vdash (\llbracket \tau_1 \rrbracket + \mathsf{unit}) <: (\llbracket \tau_1' \rrbracket + \mathsf{unit})}\text{ FGsub-sum} \quad \dfrac{\dfrac{}{\mathsf{Labeled}\ \ell_1\ \tau_1 <: \mathsf{Labeled}\ \ell_1'\ \tau_1'}\text{ Given}}{\ell_1 \sqsubseteq \ell_1'}\text{ By inversion}}{\Sigma; \Psi \vdash (\llbracket \tau_1 \rrbracket + \mathsf{unit})^{\ell_1} <: (\llbracket \tau_1' \rrbracket + \mathsf{unit})^{\ell_1'}}\text{ FGsub-arrow}}{\Sigma; \Psi \vdash \llbracket \mathsf{Labeled}\ \ell_1\ \tau_1 \rrbracket <: \llbracket \mathsf{Labeled}\ \ell_1'\ \tau_1' \rrbracket}\text{ Definition of } \llbracket \cdot \rrbracket$$

6. SLIO*sub-monad:

P3:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \llbracket \tau_1 \rrbracket <: \llbracket \tau_1' \rrbracket}\text{ IH} \qquad \dfrac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}}\text{ FGsub-unit}}{\Sigma; \Psi \vdash (\llbracket \tau_1 \rrbracket + \mathsf{unit}) <: (\llbracket \tau_1' \rrbracket + \mathsf{unit})}\text{ FGsub-sum}$$

P2:

$$\dfrac{P3 \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau_1 <: \mathbb{SLIO}\ \ell_i'\ \ell_o'\ \tau_1'}\text{ Given}}{\Sigma; \Psi \vdash \ell_o \sqsubseteq \ell_o'}\text{ By inversion}}{\Sigma; \Psi \vdash (\llbracket \tau_1 \rrbracket + \mathsf{unit})^{\ell_o} <: (\llbracket \tau_1' \rrbracket + \mathsf{unit})^{\ell_o'}}\text{ FGsub-label}$$

P1:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}} \qquad P2 \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau_1 <: \mathbb{SLIO}\ \ell_i'\ \ell_o'\ \tau_1'}\text{ Given}}{\Sigma; \Psi \vdash \ell_i' \sqsubseteq \ell_i}}{\Sigma; \Psi \vdash (\mathsf{unit} \xrightarrow{\ell_i} (\llbracket \tau_1 \rrbracket + \mathsf{unit})^{\ell_o}) <: (\mathsf{unit} \xrightarrow{\ell_i'} (\llbracket \tau_1' \rrbracket + \mathsf{unit})^{\ell_o'})}\text{ FGsub-arrow}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad \dfrac{}{\Sigma; \Psi \vdash \bot \sqsubseteq \bot}}{\Sigma; \Psi \vdash (\mathsf{unit} \xrightarrow{\ell_i} (\llbracket \tau_1 \rrbracket + \mathsf{unit})^{\ell_o})^{\perp} <: (\mathsf{unit} \xrightarrow{\ell_i'} (\llbracket \tau_1' \rrbracket + \mathsf{unit})^{\ell_o'})^{\perp}}\text{ FGsub-label}}{\Sigma; \Psi \vdash \llbracket \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau_1 \rrbracket <: \llbracket \mathbb{SLIO}\ \ell_i'\ \ell_o'\ \tau_1' \rrbracket}\text{ Definition of } \llbracket \cdot \rrbracket$$

7. SLIO*sub-forall:

P1:

$$\dfrac{\dfrac{}{\Sigma, \alpha; \Psi \vdash \llbracket \tau \rrbracket <: \llbracket \tau' \rrbracket}\text{ IH, Weakening} \qquad \dfrac{}{\Sigma, \alpha; \Psi \vdash \top \sqsubseteq \top}}{\Sigma; \Psi \vdash (\forall \alpha.(\top, \llbracket \tau \rrbracket)) <: (\forall \alpha.(\top, \llbracket \tau' \rrbracket))}\text{ FGsub-forall}$$

Main derivation:

$$\dfrac{P1 \qquad \dfrac{}{\Sigma, \alpha; \Psi \vdash \bot \sqsubseteq \bot}}{\dfrac{\Sigma; \Psi \vdash (\forall \alpha.(\top, [\![\tau]\!]))^{\bot} <: (\forall \alpha.(\top, [\![\tau']\!]))^{\bot}}{\Sigma; \Psi \vdash [\![\forall \alpha.\tau]\!] <: [\![\forall \alpha.\tau']\!]}} \text{FGsub-label}$$

8. SLIO*sub-constraint:

   P1:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau]\!] <: [\![\tau']\!]}\text{IH} \qquad \dfrac{}{\Sigma; \Psi \vdash \top \sqsubseteq \top} \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash c \Rightarrow \tau <: c' \Rightarrow \tau'}\text{Given}}{\Sigma; \Psi \vdash c' \implies c}\text{By inversion}}{\Sigma; \Psi \vdash (c \overset{\top}{\Rightarrow} [\![\tau]\!]) <: (c' \overset{\top}{\Rightarrow} [\![\tau']\!])} \text{FGsub-constra}$$

Main derivation:

$$\dfrac{P1 \qquad \dfrac{}{\Sigma, \alpha; \Psi \vdash \bot \sqsubseteq \bot}}{\dfrac{\Sigma; \Psi \vdash (c \overset{\top}{\Rightarrow} [\![\tau]\!])^{\bot} <: (c' \overset{\top}{\Rightarrow} [\![\tau']\!])^{\bot}}{\Sigma; \Psi \vdash [\![c \Rightarrow \tau]\!] <: [\![c' \Rightarrow \tau']\!]}} \text{FGsub-label}$$

□

Lemma 3.4 (SLIO* $\leadsto$ FG: Preservation of well-formedness)**.** $\forall \Sigma, \Psi, \tau.$
$\Sigma; \Psi \vdash \tau \ WF \implies \Sigma; \Psi \vdash [\![\tau]\!] \ WF$

Proof. Proof by induction on the $\tau \ WF$ relation.

1. SLIO*-wff-base:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{b} \ WF}\text{FG-wff-base}}{\Sigma; \Psi \vdash \mathsf{b}^{\bot} \ WF} \text{FG-wff-label}$$

2. SLIO*-wff-unit:

$$\dfrac{}{\Sigma; \Psi \vdash \mathsf{unit} \ WF} \text{FG-wff-unit}$$

3. SLIO*-wff-arrow:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_1]\!] \ WF}\text{IH1} \qquad \dfrac{}{\Sigma; \Psi \vdash [\![\tau_2]\!] \ WF}\text{IH2}}{\Sigma; \Psi \vdash ([\![\tau_1]\!] \overset{\top}{\rightarrow} [\![\tau_2]\!]) \ WF}\text{FG-wff-arrow}}{\Sigma; \Psi \vdash ([\![\tau_1]\!] \overset{\top}{\rightarrow} [\![\tau_2]\!])^{\bot} \ WF} \text{FG-wff-label}$$

4. SLIO*-wff-prod:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_1]\!] \ WF}\text{IH1} \qquad \dfrac{}{\Sigma; \Psi \vdash [\![\tau_2]\!] \ WF}\text{IH2}}{\Sigma; \Psi \vdash [\![(]\!]\tau_1 \times [\![\tau_2]\!]) \ WF}\text{FG-wff-prod}}{\Sigma; \Psi \vdash [\![(]\!]\tau_1 \times [\![\tau_2]\!])^{\bot} \ WF} \text{FG-wff-label}$$

5. SLIO*-wff-sum:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi\vdash\llbracket\tau_1\rrbracket\ WF}\text{IH1}\qquad\dfrac{}{\Sigma;\Psi\vdash\llbracket\tau_2\rrbracket\ WF}\text{IH2}}{\Sigma;\Psi\vdash\llbracket\tau_1\rrbracket+\llbracket\tau_2\rrbracket\ WF}\text{FG-wff-prod}}{\Sigma;\Psi\vdash\llbracket(\rrbracket\tau_1+\llbracket\tau_2\rrbracket)^{\perp}\ WF}\text{FG-wff-label}$$

6. SLIO*-wff-ref:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi\vdash\mathsf{ref}\ \ell\ \tau\ WF}\text{Given}}{\mathrm{FV}(\tau)=\emptyset}\text{By inversion}}{\mathrm{FV}(\llbracket\tau\rrbracket)=\emptyset}\text{Lemma 3.5}\qquad\dfrac{}{\mathrm{FV}(\mathsf{unit})=\emptyset}\qquad\dfrac{\dfrac{}{\Sigma;\Psi\vdash\mathsf{ref}\ \ell\ \tau\ WF}\text{Given}}{\mathrm{FV}(\ell)=\emptyset}\text{By inversion}}{\dfrac{\Sigma;\Psi\vdash\mathrm{FV}((\llbracket\tau\rrbracket+\mathsf{unit})^{\ell})=\emptyset}{\Sigma;\Psi\vdash\mathsf{ref}\ (\llbracket\tau\rrbracket+\mathsf{unit})^{\ell}\ WF}\text{FG-wff-ref}}}{\Sigma;\Psi\vdash(\mathsf{ref}\ (\llbracket\tau\rrbracket+\mathsf{unit})^{\ell})^{\perp}\ WF}\text{FG-wff-label}$$

7. SLIO*-wff-forall:

$$\dfrac{\dfrac{\dfrac{}{\Sigma,\alpha;\Psi\vdash\llbracket\tau\rrbracket\ WF}\text{IH}}{\Sigma;\Psi\vdash(\forall\alpha.(\top,\llbracket\tau\rrbracket))\ WF}\text{FG-wff-forall}}{\Sigma;\Psi\vdash(\forall\alpha.(\top,\llbracket\tau\rrbracket))^{\perp}\ WF}\text{SLIO}^*\text{-wff-label}$$

8. SLIO*-wff-constraint:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi,c\vdash\llbracket\tau\rrbracket\ WF}\text{IH}}{\Sigma;\Psi\vdash(c\overset{\top}{\Rightarrow}\llbracket\tau\rrbracket)\ WF}\text{FG-wff-constraint}}{\Sigma;\Psi\vdash(c\overset{\top}{\Rightarrow}\llbracket\tau\rrbracket)^{\perp}\ WF}\text{SLIO}^*\text{-wff-label}$$

9. SLIO*-wff-labeled:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi\vdash\llbracket\tau\rrbracket\ WF}\text{IH}\qquad\dfrac{}{\Sigma;\Psi\vdash\mathsf{unit}\ WF}\text{FG-wff-unit}}{\Sigma;\Psi\vdash(\llbracket\tau\rrbracket+\mathsf{unit})\ WF}\text{FG-wff-sum}}{\Sigma;\Psi\vdash(\llbracket\tau\rrbracket+\mathsf{unit})^{\ell}\ WF}\text{SLIO}^*\text{-wff-label}$$

10. SLIO*-wff-monad:

P1:

$$\dfrac{\dfrac{}{\Sigma;\Psi\vdash\llbracket\tau\rrbracket\ WF}\text{IH}\qquad\dfrac{}{\Sigma;\Psi\vdash\mathsf{unit}\ WF}\text{FG-wff-unit}}{\Sigma;\Psi\vdash(\llbracket\tau\rrbracket+\mathsf{unit})\ WF}\text{FG-wff-sum}$$

Main derivation:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{unit}\ WF}\ \text{FG-wff-unit} \qquad \dfrac{P1}{\Sigma; \Psi \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell_o}\ WF}\ \text{FG-wff-label}}{\dfrac{\Sigma; \Psi \vdash (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau]\!] + \mathsf{unit})^{\ell_o})\ WF}{\Sigma; \Psi \vdash (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau]\!] + \mathsf{unit})^{\ell_o})^{\perp}\ WF}\ \text{SLIO}^*\text{-wff-label}}\ \text{FG-wff-sum}$$

□

Lemma 3.5 (SLIO* ⇝ FG: Free variable lemma)**.** $\forall \tau.\ FV([\![\tau]\!]) \subseteq FV(\tau)$

Proof. Proof by induciton on the SLIO* types, τ

1. $\tau = \mathsf{b}$:

$$\begin{array}{lll} & \text{FV}([\![\mathsf{b}]\!]) & \\ = & \text{FV}(\mathsf{b}^{\perp}) & \text{Definition of } [\![\cdot]\!] \\ = & \emptyset & \\ = & \text{FV}(\mathsf{b}) & \end{array}$$

2. $\tau = \mathsf{unit}$:

$$\begin{array}{lll} & \text{FV}([\![\mathsf{b}]\!]) & \\ = & \text{FV}(\mathsf{unit}^{\perp}) & \text{Definition of } [\![\cdot]\!] \\ = & \emptyset & \\ = & \text{FV}(\mathsf{unit}) & \end{array}$$

3. $\tau = \tau_1 \to \tau_2$:

$$\begin{array}{lll} & \text{FV}([\![\tau_1 \to \tau_2]\!]) & \\ = & \text{FV}([\![\tau_1]\!] \xrightarrow{\top} [\![\tau_2]\!])^{\perp} & \text{Definition of } [\![\cdot]\!] \\ = & \text{FV}([\![\tau_1]\!]) \cup \text{FV}([\![\tau_2]\!]) & \\ \subseteq & \text{FV}(\tau_1) \cup \text{FV}(\tau_2) & \text{IH on } \tau_1 \text{ and } \tau_2 \\ = & \text{FV}(\tau_1 \to \tau_2) & \end{array}$$

4. $\tau = \tau_1 \times \tau_2$:

$$\begin{array}{lll} & \text{FV}([\![\tau_1 \times \tau_2]\!]) & \\ = & \text{FV}([\![\tau_1]\!] \times [\![\tau_2]\!])^{\perp} & \text{Definition of } [\![\cdot]\!] \\ = & \text{FV}([\![\tau_1]\!]) \cup \text{FV}([\![\tau_2]\!]) & \\ \subseteq & \text{FV}(\tau_1) \cup \text{FV}(\tau_2) & \text{IH on } \tau_1 \text{ and } \tau_2 \\ = & \text{FV}(\tau_1 \times \tau_2) & \end{array}$$

5. $\tau = \tau_1 + \tau_2$:

$$\begin{array}{lll} & \text{FV}([\![\tau_1 + \tau_2]\!]) & \\ = & \text{FV}([\![\tau_1]\!] + [\![\tau_2]\!])^{\perp} & \text{Definition of } [\![\cdot]\!] \\ = & \text{FV}([\![\tau_1]\!]) \cup \text{FV}([\![\tau_2]\!]) & \\ \subseteq & \text{FV}(\tau_1) \cup \text{FV}(\tau_2) & \text{IH on } \tau_1 \text{ and } \tau_2 \\ = & \text{FV}(\tau_1 + \tau_2) & \end{array}$$

6. $\tau = \mathsf{ref}\ \ell_i\ \tau_i$:

$$\begin{array}{lll} & \text{FV}([\![\mathsf{ref}\ \ell_i\ \tau_i]\!]) & \\ = & \text{FV}(\mathsf{ref}\ ([\![\tau_i]\!] + \mathsf{unit})^{\ell_i})^{\perp} & \text{Definition of } [\![\cdot]\!] \\ = & \text{FV}([\![\tau_i]\!]) \cup \text{FV}(\ell_i) & \\ \subseteq & \text{FV}(\tau_i) \cup \text{FV}(\ell_i) & \text{IH} \\ = & \text{FV}(\mathsf{ref}\ \ell_i\ \tau_i) & \end{array}$$

7. $\tau = \forall \alpha.\tau_i$:

$$\begin{array}{lll} & \mathrm{FV}([\![\forall \alpha.\tau_i]\!]) & \\ = & \mathrm{FV}(\forall \alpha.(\top, [\![\tau_i]\!]))^{\perp} & \text{Definition of } [\![\cdot]\!] \\ = & \mathrm{FV}([\![\tau_i]\!]) - \{\alpha\}) & \\ \subseteq & \mathrm{FV}(\tau_i) - \{\alpha\}) & \text{IH} \\ = & \mathrm{FV}(\forall \alpha.\tau_i) & \end{array}$$

8. $\tau = c \Rightarrow \tau_i$:

$$\begin{array}{lll} & \mathrm{FV}([\![c \Rightarrow \tau_i]\!]) & \\ = & \mathrm{FV}(c \overset{\top}{\Rightarrow} [\![\tau_i]\!])^{\perp} & \text{Definition of } [\![\cdot]\!] \\ = & \mathrm{FV}([\![c]\!]) \cup \mathrm{FV}([\![\tau_i]\!]) & \\ \subseteq & \mathrm{FV}([\![c]\!]) \cup \mathrm{FV}(\tau_i) & \text{IH} \\ = & \mathrm{FV}(c \Rightarrow \tau_i) & \end{array}$$

9. $\tau = \mathsf{Labeled}\ \ell_i\ \tau_i$:

$$\begin{array}{lll} & \mathrm{FV}([\![\mathsf{Labeled}\ \ell_i\ \tau_i]\!]) & \\ = & \mathrm{FV}([\![\tau_i]\!] + \mathsf{unit})^{\ell_i} & \text{Definition of } [\![\cdot]\!] \\ = & \mathrm{FV}([\![\tau_i]\!]) \cup \mathrm{FV}(\ell_i) & \\ \subseteq & \mathrm{FV}(\tau_i) \cup \mathrm{FV}(\ell_i) & \text{IH} \\ = & \mathrm{FV}(\mathsf{Labeled}\ \ell_i\ \tau_i) & \end{array}$$

10. $\tau = \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau_i$:

$$\begin{array}{lll} & \mathrm{FV}([\![\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau_i]\!]) & \\ = & \mathrm{FV}(\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau_i]\!] + \mathsf{unit})^{\ell_o})^{\perp} & \text{Definition of } [\![\cdot]\!] \\ = & \mathrm{FV}([\![\tau_i]\!]) \cup \mathrm{FV}(\ell_i) \cup \mathrm{FV}(\ell_o) & \\ \subseteq & \mathrm{FV}(\tau_i) \cup \mathrm{FV}(\ell_i) \cup \mathrm{FV}(\ell_o) & \text{IH} \\ = & \mathrm{FV}(\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau_i) & \end{array}$$

□

Lemma 3.6 (SLIO* ⇝ FG: Substitution lemma)**.** *$\forall \tau.\ s.t \vdash \tau\ WF$ the following holds:* $[\![\tau]\!][\ell/\alpha] = [\![\tau[\ell/\alpha]]\!]$

Proof. Proof by induciton on the SLIO* types, τ

1. $\tau = \mathsf{b}$:

$$\begin{array}{lll} & ([\![\mathsf{b}]\!])[\ell/\alpha] & \\ = & (\mathsf{b}^{\perp})[\ell/\alpha] & \text{Definition of } [\![\cdot]\!] \\ = & (\mathsf{b}^{\perp}) & \\ = & [\![\mathsf{b}]\!] & \\ = & [\![(\mathsf{b}[\ell/\alpha])]\!] & \end{array}$$

2. $\tau = \mathsf{unit}$:

$$\begin{array}{lll} & ([\![\mathsf{unit}]\!])[\ell/\alpha] & \\ = & (\mathsf{unit}^{\perp})[\ell/\alpha] & \text{Definition of } [\![\cdot]\!] \\ = & (\mathsf{unit}^{\perp}) & \\ = & [\![\mathsf{unit}]\!] & \\ = & [\![(\mathsf{unit}[\ell/\alpha])]\!] & \end{array}$$

3. $\tau = \tau_1 \to \tau_2$:

$$
\begin{array}{lll}
& ([\![\tau_1 \to \tau_2]\!])[\ell/\alpha] & \\
= & ([\![\tau_1]\!] \xrightarrow{\top} [\![\tau_2]\!])^{\perp}[\ell/\alpha] & \text{Definition of } [\![\cdot]\!] \\
= & ([\![\tau_1]\!][\ell/\alpha] \xrightarrow{\top} [\![\tau_2]\!][\ell/\alpha])^{\perp} & \\
= & ([\![\tau_1[\ell/\alpha]]\!] \xrightarrow{\top} [\![\tau_2[\ell/\alpha]]\!])^{\perp} & \text{IH on } \tau_1 \text{ and } \tau_2 \\
= & [\![(\tau_1[\ell/\alpha] \to \tau_2[\ell/\alpha])]\!] & \\
= & [\![(\tau_1 \to \tau_2)[\ell/\alpha]]\!] &
\end{array}
$$

4. $\tau = \tau_1 \times \tau_2$:

$$
\begin{array}{lll}
& ([\![\tau_1 \times \tau_2]\!])[\ell/\alpha] & \\
= & ([\![\tau_1]\!] \times [\![\tau_2]\!])^{\perp}[\ell/\alpha] & \text{Definition of } [\![\cdot]\!] \\
= & ([\![\tau_1]\!][\ell/\alpha] \times [\![\tau_2]\!][\ell/\alpha])^{\perp} & \\
= & ([\![\tau_1[\ell/\alpha]]\!] \times [\![\tau_2[\ell/\alpha]]\!])^{\perp} & \text{IH on } \tau_1 \text{ and } \tau_2 \\
= & [\![(\tau_1[\ell/\alpha] \times \tau_2[\ell/\alpha])]\!] & \\
= & [\![(\tau_1 \times \tau_2)[\ell/\alpha]]\!] &
\end{array}
$$

5. $\tau = \tau_1 + \tau_2$:

$$
\begin{array}{lll}
& ([\![\tau_1 + \tau_2]\!])[\ell/\alpha] & \\
= & ([\![\tau_1]\!] + [\![\tau_2]\!])^{\perp}[\ell/\alpha] & \text{Definition of } [\![\cdot]\!] \\
= & ([\![\tau_1]\!][\ell/\alpha] + [\![\tau_2]\!][\ell/\alpha])^{\perp} & \\
= & ([\![\tau_1[\ell/\alpha]]\!] + [\![\tau_2[\ell/\alpha]]\!])^{\perp} & \text{IH on } \tau_1 \text{ and } \tau_2 \\
= & [\![(\tau_1[\ell/\alpha] + \tau_2[\ell/\alpha])]\!] & \\
= & [\![(\tau_1 + \tau_2)[\ell/\alpha]]\!] &
\end{array}
$$

6. $\tau = \mathsf{ref}\ \ell_i\ \tau_i$:

$$
\begin{array}{lll}
& ([\![\mathsf{ref}\ \ell_i\ \tau_i]\!])[\ell/\alpha] & \\
= & (\mathsf{ref}\ ([\![\tau_i]\!] + \mathsf{unit})^{\ell_i})^{\perp}[\ell/\alpha] & \text{Definition of } [\![\cdot]\!] \\
= & (\mathsf{ref}\ ([\![\tau_i]\!] + \mathsf{unit})^{\ell_i})^{\perp} & \text{Lemma 3.4} \\
= & [\![(\mathsf{ref}\ \ell_i\ \tau_i)]\!] & \text{since } \vdash \tau\ WF \\
= & [\![(\mathsf{ref}\ \ell_i\ \tau_i)[\ell/\alpha]]\!] &
\end{array}
$$

7. $\tau = \forall\alpha.\tau_i$:

$$
\begin{array}{lll}
& ([\![\forall\alpha.\tau_i]\!])[\ell/\alpha] & \\
= & (\forall\alpha.(\top, [\![\tau_i]\!]))^{\perp}[\ell/\alpha] & \text{Definition of } [\![\cdot]\!] \\
= & (\forall\alpha.(\top, [\![\tau_i]\!][\ell/\alpha]))^{\perp} & \\
= & (\forall\alpha.(\top, [\![\tau_i[\ell/\alpha]]\!]))^{\perp} & \text{IH} \\
= & (\forall\alpha.\tau_i[\ell/\alpha]) & \\
= & (\forall\alpha.\tau_i)[\ell/\alpha] &
\end{array}
$$

8. $\tau = c \Rightarrow \tau_i$:

$$
\begin{array}{lll}
& ([\![c \Rightarrow \tau_i]\!])[\ell/\alpha] & \\
= & (c \overset{\top}{\Rightarrow} [\![\tau_i]\!])^{\perp}[\ell/\alpha] & \text{Definition of } [\![\cdot]\!] \\
= & (c[\ell/\alpha] \overset{\top}{\Rightarrow} [\![\tau_i]\!][\ell/\alpha])^{\perp} & \\
= & (c[\ell/\alpha] \overset{\top}{\Rightarrow} [\![\tau_i[\ell/\alpha]]\!])^{\perp} & \text{IH} \\
= & (c[\ell/\alpha] \Rightarrow \tau_i[\ell/\alpha]) & \\
= & (c \Rightarrow \tau_i)[\ell/\alpha] &
\end{array}
$$

9. $\tau = \mathsf{Labeled}\ \ell_i\ \tau_i$:

$$
\begin{array}{lll}
 & ([\![\mathsf{Labeled}\ \ell_i\ \tau_i]\!])[\ell/\alpha] & \\
= & ([\![\tau_i]\!] + \mathsf{unit})^{\ell_i}[\ell/\alpha] & \text{Definition of } [\![\cdot]\!] \\
= & ([\![\tau_i]\!][\ell/\alpha] + \mathsf{unit})^{\ell_i[\ell/\alpha]} & \\
= & ([\![\tau_i[\ell/\alpha]]\!] + \mathsf{unit})^{\ell_i[\ell/\alpha]} & \text{IH} \\
= & [\![(\mathsf{Labeled}\ \ell_i[\ell/\alpha]\ \tau_i[\ell/\alpha])]\!] & \\
= & [\![(\mathsf{Labeled}\ \ell_i\ \tau_i)[\ell/\alpha]]\!] &
\end{array}
$$

10. $\tau = \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau_i$:

$$
\begin{array}{lll}
 & ([\![\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau_i]\!])[\ell/\alpha] & \\
= & (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau_i]\!] + \mathsf{unit})^{\ell_o})^{\perp}[\ell/\alpha] & \text{Definition of } [\![\cdot]\!] \\
= & (\mathsf{unit} \xrightarrow{\ell_i[\ell/\alpha]} ([\![\tau_i]\!][\ell/\alpha] + \mathsf{unit})^{\ell_o[\ell/\alpha]})^{\perp} & \\
= & (\mathsf{unit} \xrightarrow{\ell_i[\ell/\alpha]} ([\![\tau_i[\ell/\alpha]]\!] + \mathsf{unit})^{\ell_o[\ell/\alpha]})^{\perp} & \text{IH} \\
= & (\mathbb{SLIO}\ \ell_i[\ell/\alpha]\ \ell_o[\ell/\alpha]\ \tau_i[\ell/\alpha]) & \\
= & (\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau_i)[\ell/\alpha] &
\end{array}
$$

□

3.1.3 Model for SLIO* to FG translation

$W : ((Loc \mapsto Type) \times (Loc \mapsto Type) \times (Loc \leftrightarrow Loc))$

Definition 3.7 (SLIO* ⇝ FG: ${}^s\theta_2$ extends ${}^s\theta_1$)**.** ${}^s\theta_1 \sqsubseteq {}^s\theta_2 \triangleq$
$\forall a \in {}^s\theta_1.{}^s\theta_1(a) = \tau \implies {}^s\theta_2(a) = \tau$

Definition 3.8 (SLIO* ⇝ FG: $\hat{\beta}_2$ extends $\hat{\beta}_1$)**.** $\hat{\beta}_1 \sqsubseteq \hat{\beta}_2 \triangleq$
$\forall (a_1, a_2) \in \hat{\beta}_1.(a_1, a_2) \in \hat{\beta}_2$

Definition 3.9 (SLIO* ⇝ FG: Unary value relation)**.**

$$
\begin{array}{lll}
\lfloor \mathsf{b} \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, {}^s v, {}^t v) \mid {}^s v \in [\![\mathsf{b}]\!] \wedge {}^t v \in [\![\mathsf{b}]\!] \wedge {}^s v = {}^t v\} \\
\lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, {}^s v, {}^t v) \mid {}^s v \in [\![\mathsf{unit}]\!] \wedge {}^t v \in [\![\mathsf{unit}]\!]\} \\
\lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \mid \\
 & & ({}^s\theta, m, {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}} \wedge ({}^s\theta, m, {}^s v_2, {}^t v_2) \in \lfloor \tau_2 \rfloor_V^{\hat{\beta}}\} \\
\lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, \mathsf{inl}\ {}^s v, \mathsf{inl}\ {}^t v) \mid ({}^s\theta, m, {}^s v, {}^t v) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}}\} \cup \\
 & & \{({}^s\theta, m, \mathsf{inr}\ {}^s v, \mathsf{inr}\ {}^t v) \mid ({}^s\theta, m, {}^s v, {}^t v) \in \lfloor \tau_2 \rfloor_V^{\hat{\beta}}\} \\
\lfloor \tau_1 \to \tau_2 \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, \lambda x.e_s, \lambda x.e_t) \mid \forall {}^s\theta' \sqsupseteq {}^s\theta, {}^s v, {}^t v, j < m, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, {}^s v, {}^t v) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}'} \\
 & & \implies ({}^s\theta', j, e_s[{}^s v/x], e_t[{}^t v/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}'}\} \\
\lfloor \forall \alpha.\tau \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, \Lambda e_s, \Lambda e_t) \mid \forall {}^s\theta' \sqsupseteq {}^s\theta, j < m, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, e_s, e_t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}'}\} \\
\lfloor c \Rightarrow \tau \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, \nu e_s, \nu e_t) \mid \mathcal{L} \models c \implies \forall {}^s\theta' \sqsupseteq {}^s\theta, j < m, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, e_s, e_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}'}\} \\
\lfloor \mathsf{ref}\ \ell\ \tau \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, {}^s a, {}^t a) \mid {}^s\theta({}^s a) = \mathsf{Labeled}\ \ell\ \tau \wedge ({}^s a, {}^t a) \in \hat{\beta}\} \\
\lfloor \mathsf{Labeled}\ \ell\ \tau \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, {}^s v, {}^t v) \mid \\
 & & \exists {}^s v', {}^t v'.{}^s v = \mathsf{Lb}_\ell({}^s v') \wedge {}^t v = \mathsf{inl}\ {}^t v' \wedge ({}^s\theta, m, {}^s v', {}^t v') \in \lfloor \tau \rfloor_V^{\hat{\beta}}\} \\
\lfloor \mathbb{SLIO}\ \ell_1\ \ell_2\ \tau \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, {}^s v, {}^t v) \mid \forall {}^s\theta_e \sqsupseteq {}^s\theta, H_s, H_t, i, {}^s v', k \leq m, \hat{\beta} \sqsubseteq \hat{\beta}'. \\
 & & (k, H_s, H_t) \overset{\hat{\beta}'}{\rhd} ({}^s\theta_e) \wedge (H_s, {}^s v) \Downarrow_i^f (H_s', {}^s v') \wedge i < k \implies \\
 & & \exists H_t', {}^t v'.(H_t, {}^t v()) \Downarrow (H_t', {}^t v') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H_s', H_t') \overset{\hat{\beta}''}{\rhd} {}^s\theta' \wedge \\
 & & \exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k - i, {}^s v', {}^t v'') \in \lfloor \tau \rfloor_V^{\hat{\beta}''}\}
\end{array}
$$

Definition 3.10 (SLIO* $\leadsto$ FG: Unary expression relation)**.**

$$\begin{array}{rcl}\lfloor \tau \rfloor_E^{\hat{\beta}} & \triangleq & \{({}^s\theta, n, e_s, e_t) \mid \\ & & \forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.e_s \Downarrow_i {}^s v \implies \\ & & \exists H_t', {}^t v.(H_t, e_t) \Downarrow (H_t', {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta\}\end{array}$$

Definition 3.11 (SLIO* $\leadsto$ FG: Unary heap well formedness)**.**

$$\begin{array}{rcl}(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta & \triangleq & dom({}^s\theta) \subseteq dom(H_S) \wedge \\ & & \hat{\beta} \subseteq (dom({}^s\theta) \times dom(H_t)) \wedge \\ & & \forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}\end{array}$$

Definition 3.12 (SLIO* $\leadsto$ FG: Label substitution)**.** $\sigma : Lvar \mapsto Label$

Definition 3.13 (SLIO* $\leadsto$ FG: Value substitution to values)**.** $\delta^s : Var \mapsto Val$, $\delta^t : Var \mapsto Val$

Definition 3.14 (SLIO* $\leadsto$ FG: Unary interpretation of Γ)**.**

$$\begin{array}{rcl}\lfloor \Gamma \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, n, \delta^s, \delta^t) \mid dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t) \wedge \\ & & \forall x \in dom(\Gamma).({}^s\theta, n, \delta^s(x), \delta^t(x)) \in \lfloor \Gamma(x) \rfloor_V^{\hat{\beta}}\}\end{array}$$

3.1.4 Soundness proof for SLIO* to FG translation

Lemma 3.15 (SLIO* $\leadsto$ FG: Monotonicity)**.** $\forall {}^s\theta, {}^s\theta', n, {}^s v, {}^t v, n', \beta, \beta'$.
$({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n \implies ({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau \rfloor_V^{\hat{\beta}'}$

Proof. Proof by induction on τ

1. Case b:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{b} \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{b} \rfloor_V^{\hat{\beta}'}$

   Since $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{b} \rfloor_V^{\hat{\beta}}$ therefore from Definition 3.9 we know that ${}^s v \in [\![\mathsf{b}]\!] \wedge {}^t v \in [\![\mathsf{b}]\!]$

   Therefore from Definition 3.9 ${}^s v \in [\![\mathsf{b}]\!] \wedge {}^t v \in [\![\mathsf{b}]\!]$ we get the desired

2. Case unit:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}'}$

Since $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}}$ therefore from Definition 3.9 we know that ${}^s v \in [\![\mathsf{unit}]\!] \wedge {}^t v \in [\![\mathsf{unit}]\!]$

Therefore from Definition 3.9 ${}^s v \in [\![\mathsf{unit}]\!] \wedge {}^t v \in [\![\mathsf{unit}]\!]$ we get the desired

3. Case $\tau_1 \times \tau_2$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}'}$

   From Definition 3.9 we know that ${}^s v = ({}^s v_1, {}^s v_2)$ and ${}^t v = ({}^t v_1, {}^t v_2)$.

   We also know that $({}^s\theta, n, {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}}$ and $({}^s\theta, n, {}^s v_2, {}^t v_2) \in \lfloor \tau_2 \rfloor_V^{\hat{\beta}}$

   IH1: $({}^s\theta', n', {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}'}$

   IH2: $({}^s\theta', n', {}^s v_2, {}^t v_2) \in \lfloor \tau_2 \rfloor_V^{\hat{\beta}'}$

   Therefore from Definition 3.9, IH1 and IH2 we get

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}'}$

4. Case $\tau_1 + \tau_2$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}'}$

   From Definition 3.9 two cases arise

   (a) ${}^s v = \mathsf{inl}({}^s v')$ and ${}^t v = \mathsf{inl}({}^t v')$:
   IH: $({}^s\theta', n', {}^s v', {}^t v') \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}'}$
   Therefore from Definition 3.9 and IH we get
   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}'}$

   (b) ${}^s v = \mathsf{inr}({}^s v')$ and ${}^t v = \mathsf{inr}({}^t v')$:
   Symmetric reasosning as in the previous case

5. Case $\tau_1 \to \tau_2$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau_1 \to \tau_2 \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

$({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 \to \tau_2 \rfloor_V^{\hat{\beta}'}$

From Definition 3.9 we know that

$\forall {}^s\theta'' \sqsupseteq {}^s\theta, {}^s v_1, {}^t v_1, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta'', j, {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}} \implies ({}^s\theta'', j, e_s[{}^s v_1/x], e_t[{}^t v_1/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}'}$ (A0)

Similarly from Definition 3.9 we are required to prove

$\forall {}^s\theta'_1 \sqsupseteq {}^s\theta', {}^s v_2, {}^t v_2, j < n', \hat{\beta}' \sqsubseteq \hat{\beta}''.({}^s\theta'_1, j, {}^s v_2, {}^t v_2) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}} \implies ({}^s\theta'_1, j, e_s[{}^s v_2/x], e_t[{}^t v_2/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}''}$

This means we are given some ${}^s\theta'_1 \sqsupseteq {}^s\theta', {}^s v_2, {}^t v_2, j < n', \hat{\beta}' \sqsubseteq \hat{\beta}''$ s.t $({}^s\theta'_1, j, {}^s v_2, {}^t v_2) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}}$ and we are required to prove

$({}^s\theta'_1, j, e_s[{}^s v_2/x], e_t[{}^t v_2/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}'}$

Instantiating (A0) with ${}^s\theta'_1, {}^s v_2, {}^t v_2, j, \hat{\beta}''$ since ${}^s\theta'_1 \sqsupseteq {}^s\theta' \sqsupseteq {}^s\theta$, $j < n' < n$ and $\hat{\beta} \sqsubseteq \hat{\beta}' \sqsubseteq \hat{\beta}''$ therefore we get

$({}^s\theta'_1, j, e_s[{}^s v_2/x], e_t[{}^t v_2/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}''}$

6. Case $\forall \alpha.\tau$:

   <u>Given:</u>

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \forall \alpha.\tau \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   <u>To prove:</u>

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \forall \alpha.\tau \rfloor_V^{\hat{\beta}'}$

   From Definition 3.9 we know that ${}^s v = \Lambda e'_s$ and ${}^t v = \Lambda e'_t$. And

   $\forall {}^s\theta'' \sqsupseteq {}^s\theta, j < n, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}''.({}^s\theta'', j, e'_s, e'_t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}''}$ (F0)

   Similarly from Definition 3.9 we are required to prove

   $\forall {}^s\theta''_1 \sqsupseteq {}^s\theta', j < n', \ell' \in \mathcal{L}, \hat{\beta}' \sqsubseteq \hat{\beta}''_1.({}^s\theta''_1, j, e'_s, e'_t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}''_1}$

   This means we are given some ${}^s\theta''_1 \sqsupseteq {}^s\theta', j < n', \ell'' \in \mathcal{L}, \hat{\beta}' \sqsubseteq \hat{\beta}''_1$

   and we are required to prove

   $({}^s\theta''_1, j, e'_s, e'_t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}''_1}$

   Instantiating (F0) with ${}^s\theta''_1, j, \hat{\beta}''_1$ since ${}^s\theta''_1 \sqsupseteq {}^s\theta' \sqsupseteq {}^s\theta$, $j < n' < n$ and $\hat{\beta} \sqsubseteq \hat{\beta}' \sqsubseteq \hat{\beta}''_1$ therefore we get

   $({}^s\theta''_1, j, e'_s, e'_t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}''_1}$

7. Case $c \Rightarrow \tau$:

   <u>Given:</u>

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor c \Rightarrow \tau \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

To prove:

$({}^s\theta', n', {}^s v, {}^t v) \in \lfloor c \Rightarrow \tau \rfloor_V^{\hat{\beta}'}$

From Definition 3.9 we know that ${}^s v = \nu\ (e'_s)$ and ${}^t v = \nu\ (e'_t)$. And

$\mathcal{L} \models c \implies \forall^s\theta'' \sqsupseteq {}^s\theta, j < n, \hat{\beta}' \sqsubseteq \hat{\beta}''_1.({}^s\theta'', j, e'_s, e'_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}'}$ (C0)

Similarly from Definition 3.9 we are required to prove

$\mathcal{L} \models c \implies \forall^s\theta''_1 \sqsupseteq {}^s\theta', j < n', \hat{\beta}' \sqsubseteq \hat{\beta}''_1.({}^s\theta''_1, j, e'_s, e'_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}''_1}$

This means we are given some $\mathcal{L} \models c, {}^s\theta''_1 \sqsupseteq {}^s\theta', j < n', \hat{\beta}' \sqsubseteq \hat{\beta}''_1$
and we are required to prove

$({}^s\theta''_1, j, e'_s, e'_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}''_1}$

Since $\mathcal{L} \models c$ and instantiating (C0) with ${}^s\theta''_1, j, \hat{\beta}''_1$ since ${}^s\theta''_1 \sqsupseteq {}^s\theta' \sqsupseteq {}^s\theta$, $j < n' < n$ and $\hat{\beta} \sqsubseteq \hat{\beta}' \sqsubseteq \hat{\beta}''_1$ therefore we get

$({}^s\theta''_1, j, e'_s, e'_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}''_1}$

8. Case $\mathsf{ref}\ \ell\ \tau$:

Given:

$({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{ref}\ \ell\ \tau \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

To prove:

$({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{ref}\ \ell\ \tau \rfloor_V^{\hat{\beta}'}$

From Definition 3.9 we know that ${}^s v = {}^s a$ and ${}^t v = {}^t a$. We also know that

${}^s\theta({}^s a) = \mathsf{Labeled}\ \ell\ \tau \wedge ({}^s a, {}^t a) \in \hat{\beta}$

From Definition 3.9, Definition 3.7 and Definition 3.8 we get

$({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{ref}\ \ell\ \tau \rfloor_V^{\hat{\beta}'}$

9. Case $\mathsf{Labeled}\ \ell\ \ \tau$:

Given:

$({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{Labeled}\ \ell\ \ \tau \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

To prove:

$({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{Labeled}\ \ell\ \ \tau \rfloor_V^{\hat{\beta}'}$

From Definition 3.9 it means

$\exists^s v', {}^t v'.{}^s v = \mathsf{Lb}_\ell({}^s v') \wedge {}^t v = \mathsf{inl}\ {}^t v' \wedge ({}^s\theta, n, {}^s v', {}^t v') \in \lfloor \tau \rfloor_V^{\hat{\beta}}$

IH: $({}^s\theta', n', {}^s v', {}^t v') \in \lfloor \tau \rfloor_V^{\hat{\beta}}$

Similarly from Definition 3.9 we need to prove that

$\exists^s v'', {}^t v''. {}^s v = \mathsf{Lb}_\ell({}^s v'') \wedge {}^t v = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', n', {}^s v'', {}^t v'') \in \lfloor \tau \rfloor_V^{\hat\beta}$

We choose ${}^s v''$ as ${}^s v'$ and ${}^t v''$ as ${}^t v'$ and since from IH we know that $({}^s\theta', n', {}^s v', {}^t v') \in \lfloor \tau \rfloor_V^{\hat\beta}$
Therefore from Definition 3.9 we get
$({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{Labeled}\ \ell\ \ \tau \rfloor_V^{\hat\beta'}$

10. Case $\mathbb{SLIO}\ \ell_1\ \ell_2\ \tau$:

Given:

$({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathbb{SLIO}\ \ell_1\ \ell_2\ \tau \rfloor_V^{\hat\beta} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat\beta \sqsubseteq \hat\beta' \wedge n' < n$

To prove:

$({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathbb{SLIO}\ \ell_1\ \ell_2\ \tau \rfloor_V^{\hat\beta'}$

This means from Definition 3.9 we know that
$\forall^s\theta_e \sqsupseteq {}^s\theta, H_s, H_t, i, {}^s v', {}^t v', k \leq n, \hat\beta \sqsubseteq \hat\beta_1.$
$(k, H_s, H_t) \overset{\hat\beta_1}{\triangleright} ({}^s\theta_e) \wedge (H_s, {}^s v) \Downarrow_i^f (H_s', {}^s v') \wedge i < k \implies$
$\exists^t v'.(H_t, {}^t v()) \Downarrow (H_t', {}^t v') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_e, \hat\beta_1 \sqsubseteq \hat\beta_2.(k - i, H_s', H_t') \overset{\hat\beta_2}{\triangleright} {}^s\theta' \wedge$
$\exists^t v''. {}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', {}^t\theta', k - i, {}^s v', {}^t v'') \in \lfloor \tau \rfloor_V^{\hat\beta_2} \wedge$
$(\forall a. H_s(a) \neq H_s'(a) \implies \exists \ell'. {}^s\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom({}^s\theta')/dom({}^s\theta_e). {}^s\theta'(a) \searrow \ell_1)$ (CG0)

Similarly from Definition 3.9 we need to prove
$\forall^s\theta_e' \sqsupseteq {}^s\theta', H_s', H_t', i', {}^s v'', {}^t v'', k' \leq n', \hat\beta' \sqsubseteq \hat\beta_1'.$
$(k', H_s', H_t') \overset{\hat\beta_1'}{\triangleright} ({}^s\theta_e') \wedge (H_s', {}^s v) \Downarrow_i^f (H_s'', {}^s v'') \wedge (H_t', {}^t v()) \Downarrow (H_t'', {}^t v'') \wedge i' < k' \implies$
$\exists^t v''.(H_t', {}^t v()) \Downarrow (H_t'', {}^t v'') \wedge \exists^s\theta'' \sqsupseteq {}^s\theta_e', \hat\beta_1' \sqsubseteq \hat\beta_2'.(k' - i', H_s'', H_t'') \overset{\hat\beta_2'}{\triangleright} {}^s\theta'' \wedge$
$\exists^t v''. {}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k' - i, {}^s v', {}^t v'') \in \lfloor \tau \rfloor_V^{\hat\beta_2'} \wedge$
$(\forall a. H_s(a) \neq H_s'(a) \implies \exists \ell'. {}^s\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom({}^s\theta')/dom({}^s\theta_e). {}^s\theta'(a) \searrow \ell_1)$

This means we are given some ${}^s\theta_e' \sqsupseteq {}^s\theta', H_s', H_t', i', {}^s v'', k' \leq n', \hat\beta' \sqsubseteq \hat\beta_1'$ s.t $(k', H_s', H_t') \triangleright ({}^s\theta_e') \wedge (H_s', {}^s v) \Downarrow_i^f (H_s'', {}^s v'') \wedge i' < k'$

And we need to prove

$\exists^t v''.(H_t', {}^t v()) \Downarrow (H_t'', {}^t v'') \wedge \exists^s\theta'' \sqsupseteq {}^s\theta_e', \hat\beta_1' \sqsubseteq \hat\beta_2'.(k' - i', H_s'', H_t'') \overset{\hat\beta_2'}{\triangleright} {}^s\theta'' \wedge$
$\exists^t v''. {}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta'', k' - i, {}^s v', {}^t v'') \in \lfloor \tau \rfloor_V^{\hat\beta_2'} \wedge$
$(\forall a. H_s(a) \neq H_s'(a) \implies \exists \ell'. {}^s\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom({}^s\theta')/dom({}^s\theta_e). {}^s\theta'(a) \searrow \ell_1)$

Instantiating (CG0) with ${}^s\theta_e' \sqsupseteq {}^s\theta', H_s', H_t', i', {}^s v'', {}^t v'', k' \leq n', \hat\beta' \sqsubseteq \hat\beta_1'$ we get the desired

□

Lemma 3.16 (SLIO* ⇝ FG: Unary monotonicity for Γ)**.** $\forall^s\theta, {}^s\theta', \delta, \Gamma, n, n', \hat\beta, \hat\beta'.$
$({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat\beta} \wedge n' < n \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat\beta \sqsubseteq \hat\beta' \implies ({}^s\theta', n', \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat\beta'}$

Proof. Given: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}} \wedge n' < n \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}'$

To prove: $({}^s\theta', n', \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}'}$

From Definition 3.14 it is given that
$dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t) \wedge \forall x \in dom(\Gamma).({}^s\theta, n, \delta^s(x), \delta^t(x)) \in \lfloor \Gamma(x) \rfloor_V^{\hat{\beta}}$

And again from Definition 3.14 we are required to prove that
$dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t) \wedge \forall x \in dom(\Gamma).({}^s\theta', n', \delta^s(x), \delta^t(x)) \in \lfloor \Gamma(x) \rfloor_V^{\hat{\beta}'}$

- $dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t)$:

  Given

- $\forall x \in dom(\Gamma).({}^s\theta', n', \delta^s(x), \delta^t(x)) \in \lfloor \Gamma(x) \rfloor_V^{\hat{\beta}'}$:

  Since we know that $\forall x \in dom(\Gamma).({}^s\theta, n, \delta^s(x), \delta^t(x)) \in \lfloor \Gamma(x) \rfloor_V^{\hat{\beta}}$ (given)

  Therefore from Lemma 3.15 we get

  $\forall x \in dom(\Gamma).({}^s\theta', n', \delta^s(x), \delta^t(x)) \in \lfloor \Gamma(x) \rfloor_V^{\hat{\beta}'}$

□

Lemma 3.17 (SLIO* ⇝ FG: Unary monotonicity for H)**.** $\forall {}^s\theta, H_s, H_t, n, n', \hat{\beta}, \hat{\beta}'$.
$(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge n' < n \implies (n', H_s, H_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta$

Proof. Given: $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge n' < n$

To prove: $(n', H_s, H_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta$

From Definition 3.11 it is given that
$dom({}^s\theta) \subseteq dom(H_S) \wedge \hat{\beta} \subseteq (dom({}^s\theta) \times dom(H_t)) \wedge \forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$

And again from Definition 3.11 we are required to prove that
$dom({}^s\theta) \subseteq dom(H_S) \wedge \hat{\beta} \subseteq (dom({}^s\theta) \times dom(H_t)) \wedge \forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n'-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$

- $dom({}^s\theta) \subseteq dom(H_S)$:

  Given

- $\hat{\beta} \subseteq (dom({}^s\theta) \times dom(H_t))$:

  Given

- $\forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n'-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$:

  Since we know that $\forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$ (given)

  Therefore from Lemma 3.15 we get

  $\forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n'-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$

□

Theorem 3.18 (SLIO* $\rightsquigarrow$ FG: Fundamental theorem)**.** $\forall \Gamma, \tau, e, \delta^s, \delta^t, \sigma, {}^s\theta, n.$
$\Sigma; \Psi; \Gamma \vdash e_s : \tau \rightsquigarrow e_t \wedge$
$\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$
$\implies$
$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

Proof. Proof by induction on the $\rightsquigarrow$ relation

1. CF-var:

$$\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash x : \tau \rightsquigarrow x}\ \text{CF-var}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \cup \{x \mapsto \tau\}\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, x\ \delta^s, x\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.10 it suffices to prove that

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv.x\ \delta^s \Downarrow_i {}^sv \implies$
$\exists H_t', {}^tv.(H_t, x\ \delta^t) \Downarrow (H_t', {}^tv) \wedge ({}^s\theta, n - i, {}^sv, {}^tv) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^sv$ s.t $x\ \delta^s \Downarrow_i {}^sv$
From SLIO*-Sem-val we know that $i = 0$, ${}^sv = x\ \delta^s$.

And we are required to prove

$\exists H_t', {}^tv.(H_t, x\ \delta^t) \Downarrow (H_t', {}^tv) \wedge ({}^s\theta, n, {}^sv, {}^tv) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-V0)
From fg-val we know that ${}^tv = x\ \delta^t$ and $H_t' = H_t$. So we are left with proving

$({}^s\theta, n, x\ \delta^s, x\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we are given $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \cup \{x \mapsto \tau\ \sigma\}\ \sigma \rfloor_V^{\hat{\beta}}$, therefore from Definition 3.14 we get

$({}^s\theta, n, x\ \delta^s, x\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}}$. And we have $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ in the context. So we are done.

2. CF-lam:

$$\frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash e_s : \tau_2 \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \lambda x.e_s : \tau_1 \to \tau_2 \rightsquigarrow \lambda x.e_t}\ \text{lam}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, (\lambda x.e_s)\ \delta^s, (\lambda x.e_t)\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.10 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv.(\lambda x.e_s)\ \delta^s \Downarrow_i {}^sv \implies$
$\exists H_t', {}^tv.(H_t, (\lambda x.e_t)\ \delta^t) \Downarrow (H_t', {}^tv)({}^s\theta, n - i, {}^sv, {}^tv) \in \lfloor (\tau_1 \to \tau_2)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $(\lambda x.e_s)\ \delta^s \Downarrow_i {}^s v$

From SLIO*-Sem-val and fg-val we know that ${}^s v = (\lambda x.e_s)\ \delta^s$, ${}^t v = (\lambda x.e_t)\ \delta^t$, $H'_t = H_t$ and $i = 0$

It suffices to prove that

$({}^s\theta, n, (\lambda x.e_s)\ \delta^s, (\lambda x.e_t)\ \delta^t) \in \lfloor(\tau_1 \to \tau_2)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

We know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context. So, we are only left to prove

$({}^s\theta, n, (\lambda x.e_s)\ \delta^s, (\lambda x.e_t)\ \delta^t) \in \lfloor(\tau_1 \to \tau_2)\ \sigma\rfloor_V^{\hat{\beta}}$

From Definition 3.9 it suffices to prove

$\forall {}^s\theta' \sqsupseteq {}^s\theta, {}^s v, {}^t v, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, {}^s v, {}^t v) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}'}$
$\implies ({}^s\theta', j, e_s[{}^s v/x], e_t[{}^t v/x]) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}'}$

This means that we are given ${}^s\theta' \sqsupseteq {}^s\theta, {}^s v, {}^t v, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t $({}^s\theta', j, {}^s v, {}^t v) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}'}$
And we need to prove

$({}^s\theta', j, e_s[{}^s v/x]\ \delta^s, e_t[{}^t v/x]\ \delta^t) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}'}$ (F-L0)

Since $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor\Gamma\ \sigma\rfloor_V^{\hat{\beta}}$ therefore from Lemma 3.16 we also have
$({}^s\theta', j, \delta^s, \delta^t) \in \lfloor\Gamma\ \sigma\rfloor_V^{\hat{\beta}'}$
<u>IH:</u>
$({}^s\theta', j, e_s\ \delta^s \cup \{x \mapsto {}^s v_1\}, e_t \cup \{x \mapsto {}^t v_1\}) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}'}$ s.t
$({}^s\theta', j, {}^s v_1, {}^t v_1) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}'}$

We get (F-L0) directly from IH

3. CF-app:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_{s1} : (\tau_1 \to \tau_2) \rightsquigarrow e_{t1} \qquad \Sigma; \Psi; \Gamma \vdash e_{s2} : \tau_1 \rightsquigarrow e_{t2}}{\Sigma; \Psi; \Gamma \vdash e_{s1}\ e_{s2} : \tau_2 \rightsquigarrow e_{t1}\ e_{t2}}\ \text{app}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor\Gamma\ \sigma\rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, (e_{s1}\ e_{s2})\ \delta^s, (e_{t1}\ e_{t2})\ \delta^t) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}}$

This means from Definition 3.10 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(e_{s1}\ e_{s2})\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, (e_{t1}\ e_{t2})\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor\tau_2\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This further means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $(e_{s1}\ e_{s2})\ \delta^s \Downarrow_i {}^s v$

And we need to prove

$\exists H'_t, {}^t v.(H_t, (e_{t1}\ e_{t2})\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$
(F-A0)

<u>IH1:</u>

$({}^s\theta, n, e_{s1}\ \delta^s, e_{t1}\ \delta^t) \in \lfloor (\tau_1 \to \tau_2)\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.10 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_{s1}\ \delta^s \Downarrow_j {}^s v_1 \implies$
$\exists H'_{t1}, {}^t v_1.(H_t, e_{t1}\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 \to \tau_2)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and since we know that $(e_{s1}\ e_{s2})\ \delta^s \Downarrow_i {}^s v$ therefore $\exists j < i < n$ s.t $e_{s1}\ \delta^s \Downarrow_j {}^s v_1$.

And we have

$\exists H'_{t1}, {}^t v_1.(H_t, e_{t1}\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 \to \tau_2)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$
(F-A1)

<u>IH2:</u>

$({}^s\theta, n-j, e_{s2}\ \delta^s, e_{t2}\ \delta^t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.10 it suffices to prove

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall k < n-j, {}^s v_2.e_{s2} \Downarrow_i {}^s v_2 \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t2}) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j-k, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta'_2$

Instantiating with H_s, H'_{t1} and since we know that $(e_{s1}\ e_{s2})\ \delta^s \Downarrow_i {}^s v$ therefore $\exists k < i-j < n-j$ s.t $e_{s2}\ \delta^s \Downarrow_k {}^s v_2$.

And we have

$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t2}) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j-k, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$
(F-A2)

Since from (F-A1) we know that $({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 \to \tau_2)\ \sigma \rfloor_V^{\hat{\beta}}$ where
${}^s v_1 = \lambda x.e'_s$ and ${}^t v_1 = \lambda x.e'_t$

From Definition 3.9 we have
$\forall {}^s\theta'_3 \sqsupseteq {}^s\theta, {}^s v, {}^t v, l < n-j, \hat{\beta}_3 \sqsupseteq \hat{\beta}.({}^s\theta'_3, l, {}^s v, {}^t v) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}_3}$
$\implies ({}^s\theta'_3, l, e'_s[{}^s v/x], e'_t[{}^t v/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}_3}$

Instantiating with ${}^s\theta, {}^s v_2, {}^t v_2, n-j-k, \hat{\beta}$ we get

$({}^s\theta, n-j-k, e'_s[{}^s v_2/x], e'_t[{}^t v_2/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.10 we have

$\forall H_{s4}, H_{t4}.(n-j-k, H_{s4}, H_{t4}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall k' < n-j-k, {}^s v_4.e'_s[{}^s v_2/x] \Downarrow_{k'} {}^s v_4 \implies$
$\exists H'_{t4}, {}^t v_4.(H_{t4}, e'_t[{}^t v_2/x]) \Downarrow (H'_{t4}, {}^t v_4) \wedge ({}^s\theta, n-j-k-k', {}^s v_4, {}^t v_4) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}} \wedge$
$(n-j-k-k', H_{s4}, H'_{t4}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H'_{t2}, from (F-A2) we know that $(n-j-k, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$. Instantiating ${}^s v_4$ wiht ${}^s v$ and since we know that $(e_{s1}\ e_{s2})\ \delta^s \Downarrow_i {}^s v$ therefore $\exists k' < i-j-k < n-j-k$ s.t $e'_s[{}^s v_2/x]\ \delta^s \Downarrow_{k'} {}^s v$. therefore we have

$\exists H'_{t4}, {}^t v_4.(H_{t4}, e'_t[{}^t v_2/x]) \Downarrow (H'_{t4}, {}^t v_4) \wedge ({}^s\theta, n-j-k-k', {}^s v, {}^t v_4) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j-k-k', H_{s4}, H'_{t4}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-A3)

Since from SLIO*-Sem-app we know that $i = j+k+k'$ and $H'_t = H'_{t4}$, ${}^t v = {}^t v_4$ therefore we get (F-A0) from (F-A3) and Lemma 3.15 and Lemma 3.17

4. CF-prod:

$$\frac{\Sigma;\Psi;\Gamma \vdash e_{s1} : \tau_1 \rightsquigarrow e_{t1} \qquad \Sigma;\Psi;\Gamma \vdash e_{s2} : \tau_2 \rightsquigarrow e_{t2}}{\Sigma;\Psi;\Gamma \vdash (e_{s1}, e_{s2}) : (\tau_1 \times \tau_2) \rightsquigarrow (e_{t1}, e_{t2})} \text{ prod}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, (e_{s1}, e_{s2})\ \delta^s, (e_{t1}, e_{t2})\ \delta^t) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.10 it suffices to prove

$\forall H_s, H_t, \hat{\beta}.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(e_{s1}, e_{s2})\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, (e_{t1}, e_{t2})\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that we are given some $H_s, H_t, \hat{\beta}$ s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $(e_{s1}, e_{s2})\ \delta^s \Downarrow_i {}^s v$

And we need to prove

$\exists H'_t, {}^t v.(H_t, (e_{t1}, e_{t2})\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta'$
(F-P0)

<u>IH1:</u>

$({}^s\theta, n, e_{s1}\ \delta^s, e_{t1}\ \delta^t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.10 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n.e_{s1}\ \delta^s \Downarrow_i {}^s v_1 \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and since we know that $(e_{s1}, e_{s2})\ \delta^s \Downarrow_i ({}^s v_1, {}^s v_2)$ therefore $\exists j < i < n$ s.t $e_{s1}\ \delta^s \Downarrow_j {}^s v_1$.

Therefore we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$
(F-P1)

<u>IH2:</u>

$({}^s\theta, n-j, e_{s2}\ \delta^s, e_{t2}\ \delta^t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.10 we have

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall k < n-j.e_{s2}\ \delta^s \Downarrow_k {}^s v_2 \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t2}\ \delta^t) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j-k, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with $H_s, H'_{t1}, \hat{\beta}'_1$ and since we know that $(e_{s1}, e_{s2})\ \delta^s \Downarrow_i ({}^s v_1, {}^s v_2)$ therefore $\exists k < i-j < n-j$ s.t $e_{s2}\ \delta^s \Downarrow_k {}^s v_2$.

Therefore we have

$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t2}\ \delta^t) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j-k, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$
(F-P2)

From SLIO*-Sem-prod we know that $i = j+k+1$, $H'_t = H'_{t2}$ and ${}^t v = ({}^t v_1, {}^t v_2)$ therefore from Definition 3.9 and Lemma 3.15 we get $({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V^{\hat{\beta}}$

And since we have $(n-j-k, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ therefore from Lemma 3.17 we also get

$(n-i, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

5. CF-fst:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \tau_1 \times \tau_2 \leadsto e_t}{\Sigma; \Psi; \Gamma \vdash \mathsf{fst}(e_s) : \tau_1 \leadsto \mathsf{fst}(e_t)}\ \text{fst}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{fst}(e_s)\ \delta^s, \mathsf{fst}(e_t)\ \delta^t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}}$ (F-F0)

This means from Definition 3.10 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{fst}(e_s)\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{fst}(e_t)\ \delta^s) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that we are given some $H_s, H_t, \hat{\beta}$ s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $\mathsf{fst}(e_s)\ \delta^s \Downarrow_i {}^s v$

And we need to prove

$\exists H'_t, {}^t v.(H_t, \mathsf{fst}(e_t)\ \delta^s) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-F0)

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor(\tau_1 \times \tau_2)\ \sigma\rfloor_E^{\hat{\beta}}$

From Definition 3.10 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_s\ \delta^s \Downarrow_j ({}^s v_1, -) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, (e_{t1}, e_{t2})\ \delta^t) \Downarrow (H'_{t1}, ({}^t v_1, -)) \wedge ({}^s\theta, n-j, ({}^s v_1, -), ({}^t v_1, -)) \in \lfloor(\tau_1 \times \tau_2)\ \sigma\rfloor_V^{\hat{\beta}} \wedge$
$(n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and ${}^s v_1$ with ${}^s v$ since we know that $\mathsf{fst}(e_s)\ \delta^s \Downarrow_i {}^s v$ therefore $\exists j < i < n$ s.t $e_s\ \delta^s \Downarrow_j ({}^s v, -)$.

Therefore we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, (e_{t1}, e_{t2})\ \delta^t) \Downarrow (H'_{t1}, ({}^t v_1, -)) \wedge ({}^s\theta, n-j, ({}^s v, -), ({}^t v_1, -)) \in \lfloor(\tau_1 \times \tau_2)\ \sigma\rfloor_V^{\hat{\beta}} \wedge$
$(n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-F1)

From SLIO*-Sem-fst we know that $i = j+1$, $H'_t = H'_{t1}$ and ${}^t v = {}^t v_1$. Since we know $({}^s\theta, n-j, ({}^s v, -), ({}^t v_1, -)) \in \lfloor(\tau_1 \times \tau_2)\ \sigma\rfloor_V^{\hat{\beta}}$ therefore from Definition 3.9 and Lemma 3.15 we get

$({}^s\theta, n-i, {}^s v, {}^t v_1) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}}$

And since from (F-F1) we have $(n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ therefore from Lemma 3.17 we get

$(n-i, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

6. CF-snd:

   Symmetric reasoning as in the CF-fst case

7. CF-inl:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \tau_1 \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \mathsf{inl}(e_s) : (\tau_1 + \tau_2) \rightsquigarrow \mathsf{inl}(e_t)}\ \text{prod}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor\Gamma\ \sigma\rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{inl}(e_s)\ \delta^s, \mathsf{inl}(e_t)\ \delta^t) \in \lfloor(\tau_1 + \tau_2)\ \sigma\rfloor_E^{\hat{\beta}}$

From Definition 3.10 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{inl}(e_s)\ \delta^s \Downarrow_i \mathsf{inl}({}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{inl}(e_t)\ \delta^t) \Downarrow (H'_t, \mathsf{inl}({}^t v)) \wedge ({}^s\theta, n-i, \mathsf{inl}({}^s v), \mathsf{inl}({}^t v)) \in \lfloor(\tau_1 + \tau_2)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that we are given some $H_s, H_t, \hat{\beta}$ s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $\mathsf{inl}(e_s)\ \delta^s \Downarrow_i \mathsf{inl}({}^s v)$

And we need to prove

$\exists H'_t, {}^t v.(H_t, \mathsf{inl}(e_t)\ \delta^t) \Downarrow (H'_t, \mathsf{inl}({}^t v)) \wedge ({}^s\theta, n-i, \mathsf{inl}({}^s v), \mathsf{inl}({}^t v)) \in \lfloor(\tau_1+\tau_2)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-IL0)

IH:

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau_1\ \sigma\rfloor_E^{\hat{\beta}}$

From Definition 3.10 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_s\ \delta^s \Downarrow_j {}^s v_1 \implies \exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v, {}^t v_1) \in \lfloor \tau_1\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and since we know that $\mathsf{inl}(e_s)\ \delta^s \Downarrow_i {}^s v$ therefore $\exists j < i < n$ s.t $e_s\ \delta^s \Downarrow_j {}^s v$.

Therefore we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v, {}^t v_1) \in \lfloor \tau_1\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-IL1)

From SLIO*-Sem-inl we know that $i = j+1$ and $H'_t = H'_{t1}$, ${}^t v = {}^t v_1$. Since we know $({}^s\theta, n-j, {}^s v, {}^t v_1) \in \lfloor \tau_1\ \sigma\rfloor_V^{\hat{\beta}}$ therefore from Definition 3.9 and Lemma 3.15 we get

$({}^s\theta, n-i, \mathsf{inl}({}^s v), \mathsf{inl}({}^t v_1)) \in \lfloor(\tau_1+\tau_2)\ \sigma\rfloor_V^{\hat{\beta}}$

And since from (F-IL1) we have $(n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ therefore from Lemma 3.17 we get

$(n-i, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

8. CF-inr:

   Symmetric reasoning as in the CF-inl case

9. CF-case:

$$\frac{\Sigma;\Psi;\Gamma \vdash e_s : \tau_1+\tau_2 \rightsquigarrow e_t \qquad \Sigma;\Psi;\Gamma, x:\tau_1 \vdash e_{s1} : \tau \rightsquigarrow e_{t1} \qquad \Sigma;\Psi;\Gamma, y:\tau_2 \vdash e_{s2} : \tau \rightsquigarrow e_{t2}}{\Sigma;\Psi;\Gamma \vdash \mathsf{case}(e_s, x.e_{s1}, y.e_{s2}) : \tau \rightsquigarrow \mathsf{case}(e_t, x.e_{t1}, y.e_{t2})}\ \text{case}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma\rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s, \mathsf{case}(e_t, x.e_{t1}, y.e_{t2})\ \delta^t) \in \lfloor \tau\ \sigma\rfloor_E^{\hat{\beta}}$

This means from Definition 3.10 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{case}(e_t, x.e_{t1}, y.e_{t2})\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that we are given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $\mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s \Downarrow_i {}^s v$

And we need to prove

$\exists H'_t, {}^t v.(H_t, \mathsf{case}(e_t, x.e_{t1}, y.e_{t2})\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$
(F-C0)

<u>IH1:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.10 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_s\ \delta^s \Downarrow_j {}^s v_1 \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and since we know that $\mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s \Downarrow_i {}^s v$ therefore $\exists j < i < n$ s.t $e_s\ \delta^s \Downarrow_j {}^s v_1$.

Therefore we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$
(F-C1)

Two cases arise:

(a) ${}^s v_1 = \mathsf{inl}({}^s v'_1)$ and ${}^t v_1 = \mathsf{inl}({}^t v'_1)$:
<u>IH2:</u>
$({}^s\theta, n-j, e_{s1}\ \delta^s \cup \{x \mapsto {}^s v_1\}, e_{t1}\ \delta^t \cup \{x \mapsto {}^t v_1\}) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.10 we have
$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall k < n-j, {}^s v_2.e_{s1}\ \delta^s \cup \{x \mapsto {}^s v_1\} \Downarrow_k {}^s v_2 \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t1}\ \delta^t \cup \{x \mapsto {}^t v_1\}) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j-k, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H'_{t1} and since we know that $\mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s \Downarrow_i {}^s v$ therefore $\exists k < i-j < n-j$ s.t $e_{s1}\ \delta^s \cup \{x \mapsto {}^s v_1\} \Downarrow_k {}^s v$.

Therefore we have
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t1}\ \delta^t \cup \{x \mapsto {}^t v_1\}) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-k, {}^s v, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j-k, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

From SLIO*-Sem-case1 we know that $i = j + k + 1$ and $H'_t = H'_{t2}$, ${}^t v = {}^t v_2$. Since we know $({}^s\theta, n-j-k, {}^s v, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}}$ therefore from Definition 3.9 and Lemma 3.15 we get
$({}^s\theta, n-i, {}^s v, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}}$

And since from (F-C2) we have $(n-j-k, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ therefore from Lemma 3.17 we get $(n-i, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

(b) ${}^{s}v_1 = \mathsf{inr}({}^{s}v_1')$ and ${}^{t}v_1 = \mathsf{inr}({}^{t}v_1')$:
Symmetric reasoning as in the previous case

10. CF-FI:

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash e_s : \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \Lambda e_s : \forall \alpha.\tau \rightsquigarrow \Lambda e_t} \text{ FI}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^{s}\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^{s}\theta, n, \Lambda e_s\ \delta^s, \Lambda e_t\ \delta^t) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.10 we know that

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^{s}\theta \wedge \forall i < n, {}^{s}v.\Lambda e_s \Downarrow_i {}^{s}v \implies$
$\exists H_t', {}^{t}v.(H_t, \Lambda e_t) \Downarrow (H_t', {}^{t}v) \wedge ({}^{s}\theta, n-i, {}^{s}v, {}^{t}v) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^{s}\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^{s}\theta$ and given some $i < n$ s.t $(\Lambda e_s)\ \delta^s \Downarrow_i {}^{s}v$

From SLIO*-Sem-val and fg-val we know that ${}^{s}v = (\Lambda e_s)\ \delta^s$, ${}^{t}v = (\Lambda e_t)\ \delta^t$, $i = 0$ and $H_t' = H_t$

It suffices to prove that

$({}^{s}\theta, n, (\Lambda e_s)\ \delta^s, (\Lambda e_t)\ \delta^t) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^{s}\theta$

We know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^{s}\theta$ from the context. So, we are only left to prove

$({}^{s}\theta, n, (\Lambda e_s)\ \delta^s, (\Lambda e_t)\ \delta^t) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V^{\hat{\beta}}$

From Definition 3.9 it suffices to prove

$\forall {}^{s}\theta' \sqsupseteq {}^{s}\theta, j < n, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^{s}\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}'}$

This means that we are given ${}^{s}\theta' \sqsupseteq {}^{s}\theta, j < n, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}'$
And we need to prove

$({}^{s}\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}'}$ (F-FI0)

Since $({}^{s}\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$ therefore from Lemma 3.16 we also have
$({}^{s}\theta', j, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}'}$
<u>IH:</u>
$({}^{s}\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \cup \{\alpha \mapsto \ell'\} \rfloor_E^{\hat{\beta}'}$

We get (F-FI0) directly from IH

11. CF-FE:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \forall \alpha.\tau \leadsto e_t \qquad \mathrm{FV}(\ell) \in \Sigma}{\Sigma; \Psi; \Gamma \vdash e_s\ [] : \tau[\ell/\alpha] \leadsto e_t[]} \text{ FE}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, e_s\ []\ \delta^s, e_t\ []\ \delta^t) \in \lfloor \tau[\ell/\alpha]\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.10 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.e_s\ [] \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, e_t\ []) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau[\ell/\alpha]\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This further means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $e_s\ []\ \delta^s \Downarrow_i {}^s v$
And we need to prove

$$\exists H'_t, {}^t v.(H_t, e_t\ []) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau[\ell/\alpha]\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \qquad \text{(F-FE0)}$$

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.10 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_s\ \delta^s \Downarrow_j {}^s v_1 \implies$
$\exists H'_{t1}, {}^t v_1.(H_t, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and since we know that $(e_s\ [])\ \delta^s \Downarrow_i {}^s v$ therefore $\exists j < i < n, {}^s v_1$ s.t $e_s\ \delta^s \Downarrow_j {}^s v_1$.

And we have

$\exists H'_{t1}, {}^t v_1.(H_t, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-FE1)

From SLIO*-Sem-FE we know that ${}^s v_1 = \Lambda e'_s$ and ${}^t v_1 = \Lambda e'_t$
Therefore we have
$({}^s\theta, n-j, \Lambda e'_s, \Lambda e'_t) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V^{\hat{\beta}}$

This means from Definition 3.9 we have
$\forall {}^s\theta' \sqsupseteq {}^s\theta, k < n-j, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}_2.({}^s\theta', k, e'_s, e'_t) \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_E^{\hat{\beta}_2}$

Instantiating ${}^s\theta'$ with ${}^s\theta$, k with $n-j-1$, ℓ' with $\ell\ \sigma$ and $\hat{\beta}_2$ with $\hat{\beta}$ and we get
$({}^s\theta, n-j-1, e'_s, e'_t) \in \lfloor \tau[\ell/\alpha]\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.10 we get

$\forall H_{s2}, H_{t2}.(n-j-1, H_{s2}, H_{t2}) \overset{\hat{\beta}_2}{\triangleright} {}^s\theta'_1 \wedge \forall k < n-j-1, {}^s v_2.e'_s \Downarrow_k {}^s v_2 \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e'_t) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-1-k, {}^s v_2, {}^t v_2) \in \lfloor \tau[\ell/\alpha]\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j-1-k, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H'_{t1}. Since from (F-FE1) we know that $(n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ therefore from Lemma 3.17 we get $(n-j-1, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we know that $e_s\ []\ \delta^s \Downarrow_i {}^s v$ and from SLIO*-Sem-FE we know that $i = j+k+1$ (for some k) and $i < n$ therefore we have $k < n-j-1$ s.t $e'_s\ \delta^s \Downarrow_k {}^s v_2$.

Therefore we have
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e'_t) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-1-k, {}^s v_2, {}^t v_2) \in \lfloor \tau[\ell/\alpha]\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j-1-k, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-FE2)

Since $H'_t = H_{t2'}$, ${}^s v = {}^s v_2$ and ${}^t v = {}^t v_2$ therefore we get (F-FE0) directly from (F-FE2)

12. CF-CI:

$$\frac{\Sigma; \Psi, c; \Gamma \vdash e_s : \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \nu\ e_s : c \Rightarrow \tau \rightsquigarrow \nu\ e_t}\ \text{CI}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \nu\ e_s\ \delta^s, \nu e_t\ \delta^t) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.10 we know that
$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n.\nu e_s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, \nu e_t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (c \Rightarrow \tau)\hat{\beta}\ \sigma \rfloor_V^{\wedge} (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some $H_s, H_t, \hat{\beta}$ s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $(\nu e_s)\ \delta^s \Downarrow_i {}^s v$

From SLIO*-Sem-val and fg-val we know that ${}^s v = (\nu e_s)\ \delta^s$, ${}^t v = (\nu e_t)\ \delta^t$, $i = 0$ and $H'_t = H_t$

It suffices to prove that

$({}^s\theta, n, (\nu e_s)\ \delta^s, (\nu e_t)\ \delta^t) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

We know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context. So, we are only left to prove
$({}^s\theta, n, (\nu e_s)\ \delta^s, (\nu e_t)\ \delta^t) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_V^{\hat{\beta}}$

From Definition 3.9 it suffices to prove
$\mathcal{L} \models c\ \sigma \implies \forall {}^s\theta' \sqsupseteq {}^s\theta, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'}$

This means that we are given $\mathcal{L} \models c\ \sigma$ and ${}^s\theta' \sqsupseteq {}^s\theta, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'$

And we need to prove

$({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'}$ (F-CI0)

Since $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$ therefore from Lemma 3.16 we also have

$({}^s\theta', j, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}'}$

And since we know that $\mathcal{L} \models c\ \sigma$ therefore

IH: $({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'}$

We get (F-CI0) directly from IH

13. CF-CE:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : c \Rightarrow \tau \leadsto e_t \qquad \Sigma; \Psi \vdash c}{\Sigma; \Psi; \Gamma \vdash e_s \bullet : \tau \leadsto e_t \bullet} \text{ CE}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, e_s \bullet\ \delta^s, e_t \bullet\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.10 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.e_s \bullet \Downarrow_i {}^s v \implies$
$\exists H_t', {}^t v.(H_t, e_t \bullet) \Downarrow (H_t', {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This further means that given some $H_s, H_t, \hat{\beta}$ s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $e_s\ \bullet\ \delta^s \Downarrow_i {}^s v$

And we need to prove

$\exists H_t', {}^t v.(H_t, e_t \bullet) \Downarrow (H_t', {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-CE0)

IH:

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.10 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_s\ \delta^s \Downarrow_j {}^s v_1 \implies$
$\exists H_{t1}', {}^t v_1.(H_t, e_t\ \delta^t) \Downarrow (H_{t1}', {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H_{t1}') \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and since we know that $(e_s\ \bullet)\ \delta^s \Downarrow_i {}^s v$ therefore $\exists j < i < n$ s.t $e_s\ \delta^s \Downarrow_j {}^s v_1$.

And we have

$\exists H_{t1}', {}^t v_1.(H_t, e_t\ \delta^t) \Downarrow (H_{t1}', {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_s, H_{t1}') \overset{\hat{\beta}}{\triangleright} {}^s\theta$
(F-CE1)

From SLIO*-Sem-CE we know that ${}^s v_1 = \nu e'_s$ and ${}^t v_1 = \nu e'_t$

Therefore we have

$({}^s\theta, n - j, \nu e'_s, \nu e'_t) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_V^{\hat{\beta}}$

This means from Definition 3.9 we have

$\forall {}^s\theta' \sqsupseteq {}^s\theta'_1, k < n - j, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}_2.({}^s\theta', k, e'_s, e'_t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}_2}$

Instantiating ${}^s\theta'$ with ${}^s\theta$, k with $n - j - 1$, ℓ' with $\ell\ \sigma$ and $\hat{\beta}_2$ with $\hat{\beta}$ and we get

$({}^s\theta, n - j - 1, e'_s, e'_t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.10 we get

$\forall H_{s2}, H_{t2}.(n - j - 1, H_{s2}, H_{t2}) \overset{\hat{\beta}_2}{\triangleright} {}^s\theta'_1 \wedge \forall k < n - j - 1.e'_s \Downarrow_k {}^s v_2 \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e'_t) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n - j - 1 - k, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n - i, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H'_{t1}. Since from (F-CE1) we know that $(n - j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ therefore from Lemma 3.17 we get $(n - j - 1, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we know that $e_s\ \bullet\ \delta^s \Downarrow_i {}^s v$ and from SLIO*-Sem-CE we know that $i = j + k + 1$ (for some k) and $i < n$ therefore we have $k < n - j - 1$ s.t $e'_s\ \delta^s \Downarrow_k {}^s v_2$.

Therefore we have

$\exists H'_{t2}, {}^t v_2.(H_{t2}, e'_t) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n - j - 1 - k, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-CE2)

Since $H'_t = H_{t2'}$, ${}^s v = {}^s v_2$ and ${}^t v = {}^t v_2$ therefore we get (F-CE0) directly from (F-CE2)

14. CF-ret:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \mathsf{ret}(e_s) : \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau \rightsquigarrow \lambda\_.\mathsf{inl}(e_t)}\ \text{ret}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{ret}(e_s)\ \delta^s, \lambda\_.\mathsf{inl}(e_t)\ \delta^t) \in \lfloor \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau\ \sigma \rfloor_E^{\hat{\beta}}$

It means from Definition 3.10 that we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{ret}(e_s) \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, \lambda\_.\mathsf{inl}(e_t)) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n - i, {}^s v, {}^t v) \in \lfloor \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some $H_s, H_t, \hat{\beta}$ s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $\mathsf{ret}(e_s)\ \delta^s \Downarrow_i {}^s v$

And we need to prove

$\exists H'_t, {}^t v.(H_t, \lambda\_.\mathsf{inl}(e_t)) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n - i, {}^s v, {}^t v) \in \lfloor \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

From SLIO*-ret and FG-lam we know that $i = 0$, ${}^s v = \mathsf{ret}(e_s)\ \delta^s$, ${}^t v = \lambda\_.\mathsf{inl}(e_t)\ \delta^t$ and $H'_t = H_t$.

So we need to prove

$$({}^s\theta, n, \mathsf{ret}(e_s)\ \delta^s, \lambda\_.\mathsf{inl}(e_t)\ \delta^t) \in \lfloor \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$$

Since we already know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context so we are left with proving

$$({}^s\theta, n, \mathsf{ret}(e_s)\ \delta^s, \lambda\_.\mathsf{inl}(e_t)\ \delta^t) \in \lfloor \mathbb{SLIO}\ \ell_i\ \ell_i\ \tau\ \sigma \rfloor_V^{\hat{\beta}}$$

From Definition 3.9 it means we need to prove
$\forall {}^s\theta_e \sqsupseteq {}^s\theta, H_s, H_t, i, {}^s v', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(k, H_s, H_t) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_s, \mathsf{ret}(e_s)\ \delta^s) \Downarrow_i^f (H'_s, {}^s v') \wedge i < k \implies \exists H'_t, {}^t v'.(H_t, (\lambda\_.\mathsf{inl}(e_t)\ ())\delta^t) \Downarrow$
$(H'_t, {}^t v') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H'_s, H'_t) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k - i, {}^s v', {}^t v'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$

This means we are given some ${}^s\theta_e \sqsupseteq {}^s\theta, H_s, H_t, i, {}^s v', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t
$(k, H_s, H_t) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_s, \mathsf{ret}(e_s)\ \delta^s) \Downarrow_i^f (H'_s, {}^s v') \wedge i < k$. Also from SLIO*-Sem-ret we know that $H'_s = H_s$

And we need to prove

$$\exists H'_t, {}^t v'.(H_t, (\lambda\_.\mathsf{inl}(e_t)\ ())\delta^t) \Downarrow (H'_t, {}^t v') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H_s, H'_t) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$$
$$\exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k - i, {}^s v', {}^t v'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''} \qquad \text{(F-R0)}$$

<u>IH:</u>

$$({}^s\theta_e, k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'}$$

It means from Definition 3.10 that we need to prove

$$\forall H_{s1}, H_{t1}.(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge \forall f < k.e_s\ \delta^s \Downarrow_f {}^s v \implies$$
$$\exists H'_{t1}, {}^t v.(H_{t1}, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v) \wedge ({}^s\theta_e, k - f, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k - f, H_{s1}, H'_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$$

Instantiating H_{s1} with H_s and H_{t1} with H_t. And since we know that $(H_s, \mathsf{ret}(e_s)\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists f < i < k \leq n$ s.t $e_s\ \delta^s \Downarrow_f {}^s v_h$. Therefore we have

$$\exists H'_{t1}, {}^t v.(H_{t1}, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v) \wedge ({}^s\theta_e, k - f, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k - f, H_s, H'_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \qquad \text{(F-R1)}$$

In order to prove (F-R0) we choose H'_t as H'_{t1}, ${}^t v'$ as $\mathsf{inl}({}^t v)$, ${}^s\theta'$ as ${}^s\theta_e$, $\hat{\beta}''$ as $\hat{\beta}'$. Since from SLIO*-Sem-ret we know that $i = f + 1$ therefore from (F-R1) and Lemma 3.17 we know that $(k - i, H_s, H'_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

Next we choose ${}^t v''$ as ${}^t v$ (from F-R1) and from Lemma 3.15 we get $({}^s\theta_e, k - i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$ (we know from SLIO*-Sem-ret that ${}^s v' = {}^s v$)

15. CF-bind:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_{s1} : \mathbb{SLIO}\ \ell_i\ \ell\ \tau \rightsquigarrow e_{t1} \qquad \Sigma; \Psi; \Gamma, x : \tau \vdash e_{s2} : \mathbb{SLIO}\ \ell\ \ell_o\ \tau' \rightsquigarrow e_{t2}}{\Sigma; \Psi; \Gamma \vdash \mathsf{bind}(e_{s1}, x.e_{s2}) : \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau' \rightsquigarrow \lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}())} \text{ bind}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s, \lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}())\ \delta^t) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau')\ \sigma \rfloor_E^{\hat{\beta}}$

It means from Definition 3.10 that we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H_t', {}^t v.(H_t, \lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}())\ \delta^t) \Downarrow (H_t', {}^t v) \wedge$
$({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau')\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $\mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s \Downarrow_i {}^s v$

And we need to prove
$\exists H_t', {}^t v.(H_t, \lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}())\ \delta^t) \Downarrow (H_t', {}^t v) \wedge$
$({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau')\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta$
From SLIO*-Sem-val and fg-val we know that $i = 0$, ${}^s v = \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s$,
${}^t v = \lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}())\ \delta^t$, $H_t' = H_t$

And we need to prove

$({}^s\theta, n, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s, \lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}())\ \delta^t) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau')\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we already know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context so we are left with proving
$({}^s\theta, n, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s, \lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}())\ \delta^t) \in \lfloor (\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau')\ \sigma \rfloor_V^{\hat{\beta}}$

From Definition 3.9 it means we need to prove
$\forall {}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^s v', {}^t v', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s1}, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s) \Downarrow_i^f (H_{s1}', {}^s v') \wedge i < k \implies$
$\exists H_{t1}', {}^t v'.(H_{t1}, (\lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}()))()\ \delta^t) \Downarrow (H_{t1}', {}^t v') \wedge$
$\exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H_{s1}', H_{t1}') \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge \exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k-i, {}^s v', {}^t v'') \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}''}$

This means we are given some ${}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^s v', {}^t v', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge (H_{s1}, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s) \Downarrow_i^f (H_{s1}', {}^s v') \wedge i < k.$

And we need to prove
$\exists H_{t1}', {}^t v'.(H_{t1}, (\lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}()))()\ \delta^t) \Downarrow (H_{t1}', {}^t v') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H_{s1}', H_{t1}') \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge \exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k-i, {}^s v', {}^t v'') \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}''}$ (F-B0)

IH1:

$({}^s\theta, k, e_{s1}\ \delta^s, e_{t1}\ \delta^t) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell\ \tau)\ \sigma\rfloor_E^{\hat{\beta}}$

It means from Definition 3.10 that we need to prove

$\forall H_{s2}, H_{t2}.(k, H_{s2}, H_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_{h1}.e_{s1}\ \delta^s \Downarrow_j {}^s v_{h1} \implies$
$\exists H'_{t2}, {}^t v_{h1}.(H_{t2}, e_{t1}\ \delta^t) \Downarrow (H'_{t2}, {}^t v_{h1}) \wedge ({}^s\theta, k-j, {}^s v_{h1}, {}^t v_{h1}) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell\ \tau)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (k - j, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating H_{s2} with H_{s1} and H_{t2} with H_{t1}. And since we know that $(H_{s1}, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists j < i < k \leq n$ s.t $e_{s1}\ \delta^s \Downarrow_j {}^s v_{h1}$.
Therefore we have
$\exists H'_{t2}, {}^t v_{h1}.(H_{t2}, e_{t1}\ \delta^t) \Downarrow (H'_{t2}, {}^t v_{h1}) \wedge ({}^s\theta, k-j, {}^s v_{h1}, {}^t v_{h1}) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell\ \tau)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (k - j, H_{s1}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-B1.1)

From Definition 3.9 we know have
$\forall {}^s\theta_e \sqsupseteq {}^s\theta, H_{s3}, H_{t3}, b, {}^s v'_{h1}, {}^t v'_{h1}, m \leq k-j, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(m, H_{s3}, H_{t3}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s3}, {}^s v_{h1}) \Downarrow_b^f (H'_{s3}, {}^s v'_{h1}) \wedge b < m \implies$
$\exists H'_{t3}, {}^t v'_{h1}.(H_{t3}, {}^t v_{h1}()) \Downarrow (H'_{t3}, {}^t v'_{h1}) \wedge \exists {}^s\theta'' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(m-b, H'_{s3}, H'_{t3}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta'' \wedge$
$\exists {}^t v''_{h1}.{}^t v'_{h1} = \mathsf{inl}\ {}^t v''_{h1} \wedge ({}^s\theta'', m-b, {}^s v'_{h1}, {}^t v''_{h1}) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}''}$

Instantiating ${}^s\theta_e$ with ${}^s\theta$, H_{s3} with H_{s1}, H_{t3} with H'_{t2}, m with $k-j$ and $\hat{\beta}'$ with $\hat{\beta}$. Since we know that $(H_{s1}, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists b < i-j < k-j$ s.t $(H_{s1}, {}^s v_{h1})\ \delta^s \Downarrow_b (H'_{s3}, {}^s v'_{h1})$.

Therefore we have

$\exists H'_{t3}, {}^t v'_{h1}.(H_{t3}, {}^t v_{h1}()) \Downarrow (H'_{t3}, {}^t v'_{h1}) \wedge \exists {}^s\theta'' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-j-b, H'_{s3}, H'_{t3}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta'' \wedge$
$\exists {}^t v''.{}^t v'_{h1} = \mathsf{inl}\ {}^t v''_{h1} \wedge ({}^s\theta'', k-j-b, {}^s v'_{h1}, {}^t v''_{h1}) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}''}$ (F-B1)

IH2:

$({}^s\theta'', k-j-b, e_{s2}\ \delta^s \cup \{x \mapsto {}^s v'_{h1}\}, e_{t2}\ \delta^t \cup \{x \mapsto {}^t v''_{h1}\}) \in \lfloor(\mathbb{SLIO}\ \ell\ \ell_o\ \tau')\ \sigma\rfloor_E^{\hat{\beta}''}$

It means from Definition 3.10 that we need to prove

$\forall H_{s4}, H_{t4}.(k, H_{s4}, H_{t4}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta \wedge \forall c < (k-j-b), {}^s v_{h2}.e_{s2}\ \delta^s \Downarrow_j {}^s v_{h2} \implies$
$\exists H'_{t4}, {}^t v_{h2}.(H_{t4}, e_{t2}\ \delta^t) \Downarrow (H'_{t4}, {}^t v_{h2}) \wedge ({}^s\theta'', k-j-b-c, {}^s v_{h2}, {}^t v_{h2}) \in \lfloor(\mathbb{SLIO}\ \ell\ \ell_o\ \tau')\ \sigma\rfloor_V^{\hat{\beta}''} \wedge$
$(k-j-b-c, H_{s4}, H'_{t4}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta''$

Instantiating H_{s4} with H'_{s3} and H_{t4} with H'_{t3}. And since we know that $(H_{s1}, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists c < i-j-b < k-j-b$ s.t $e_{s2}\ \delta^s \Downarrow_c {}^s v_{h2}$.
Therefore we have
$\exists H'_{t4}, {}^t v_{h2}.(H_{t4}, e_{t2}\ \delta^t) \Downarrow (H'_{t4}, {}^t v_{h2}) \wedge ({}^s\theta'', k-j-b-c, {}^s v_{h2}, {}^t v_{h2}) \in \lfloor(\mathbb{SLIO}\ \ell\ \ell_o\ \tau')\ \sigma\rfloor_V^{\hat{\beta}''} \wedge$
$(k-j-b-c, H_{s4}, H'_{t4}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta''$ (F-B2.1)

From Definition 3.9 we know have

$\forall^s\theta_e \sqsupseteq {}^s\theta'', H_{s5}, H_{t5}, d, {}^s v'_{h2}, {}^t v'_{h2}, m \le k-j-b-c, \hat{\beta}'' \sqsubseteq \hat{\beta}''_1.$

$(m, H_{s5}, H_{t5}) \overset{\hat{\beta}''_1}{\triangleright} ({}^s\theta_e) \wedge (H_{s5}, {}^s v_{h2}) \Downarrow^f_d (H'_{s5}, {}^s v'_{h2}) \wedge d < m \implies$

$\exists H'_{t5}, {}^t v'_{h2}.(H_{t5}, {}^t v_{h2}()) \Downarrow (H'_{t5}, {}^t v'_{h2}) \wedge \exists^s\theta''' \sqsupseteq {}^s\theta_e, \hat{\beta}''_1 \sqsubseteq \hat{\beta}''_2.(m-d, H'_{s5}, H'_{t5}) \overset{\hat{\beta}''_2}{\triangleright} {}^s\theta''' \wedge$

$\exists^t v''_{h2}.{}^t v'_{h2} = \mathsf{inl}\ {}^t v''_{h2} \wedge ({}^s\theta''', m-d, {}^s v'_{h2}, {}^t v''_{h2}) \in \lfloor \tau'\ \sigma \rfloor^{\hat{\beta}''_2}_V$

Instantiating ${}^s\theta_e$ with ${}^s\theta''$, H_{s5} with H'_{s3}, H_{t5} with H'_{t3}, m with $k-j-b-c$ and $\hat{\beta}''_1$ with $\hat{\beta}''$. Since we know that $(H_{s1}, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s) \Downarrow^f_i (H'_s, {}^s v')$ therefore $\exists d < i-j-b-c < k-j-b-c$ s.t $(H'_{s3}, {}^s v_{h2})\ \delta^s \Downarrow_d (H'_{s5}, {}^s v'_{h2})$.

Therefore we have

$\exists H'_{t5}, {}^t v'_{h2}.(H_{t5}, {}^t v_{h2}()) \Downarrow (H'_{t5}, {}^t v'_{h2}) \wedge \exists^s\theta''' \sqsupseteq {}^s\theta_e, \hat{\beta}''_1 \sqsubseteq \hat{\beta}''_2.(k-j-b-c-d, H'_{s5}, H'_{t5}) \overset{\hat{\beta}''_2}{\triangleright} {}^s\theta''' \wedge$
$\exists^t v''.{}^t v'_{h2} = \mathsf{inl}\ {}^t v''_{h2} \wedge ({}^s\theta''', k-j-b-c-d, {}^s v'_{h2}, {}^t v''_{h2}) \in \lfloor \tau'\ \sigma \rfloor^{\hat{\beta}''_2}_V$ (F-B2)

In order to prove (F-B0) we choose H'_{t1} as H'_{t5} and ${}^t v'$ as ${}^t v'_{h2}$. Next we choose ${}^s\theta'$ as ${}^s\theta'''$ and $\hat{\beta}''$ as $\hat{\beta}''_2$ (both chosen from (F-B2)). Also from SLIO*-Sem-bind we know that in (F-B0) H'_{s1} will be H'_{s5}.

Since $(k-j-b-c-d, H'_{s5}, H'_{t5}) \overset{\hat{\beta}''_2}{\triangleright} {}^s\theta'''$ therefore Lemma 3.15 we get $(k-i, H'_{s5}, H'_{t5}) \overset{\hat{\beta}''_2}{\triangleright} {}^s\theta'''$
Also since from (F-B2) we have $\exists^t v''.{}^t v'_{h2} = \mathsf{inl}\ {}^t v''_{h2} \wedge ({}^s\theta''', k-j-b-c-d, {}^s v'_{h2}, {}^t v''_{h2}) \in \lfloor \tau'\ \sigma \rfloor^{\hat{\beta}''_2}_V$
Sicne $i = j+b+c+d+1$ therefore from Lemma 3.15 we get

$\exists^t v''.{}^t v'_{h2} = \mathsf{inl}\ {}^t v''_{h2} \wedge ({}^s\theta''', k-i, {}^s v'_{h2}, {}^t v''_{h2}) \in \lfloor \tau'\ \sigma \rfloor^{\hat{\beta}''_2}_V$

16. CF-label:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \mathsf{Lb}_\ell(e_s) : (\mathsf{Labeled}\ \ell\ \tau) \rightsquigarrow \mathsf{inl}(e_t)}\ \text{label}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor^{\hat{\beta}}_V$

To prove: $({}^s\theta, n, \mathsf{Lb}_\ell(e_s)\ \delta^s, \mathsf{inl}(e_t)\ \delta^t) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor^{\hat{\beta}}_E$

From Definition 3.10 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{Lb}_\ell(e_s)\ \delta^s \Downarrow_i \mathsf{Lb}_\ell({}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{inl}(e_t)\ \delta^t) \Downarrow (H'_t, \mathsf{inl}({}^t v)) \wedge ({}^s\theta, n-i, \mathsf{Lb}_\ell({}^s v), \mathsf{inl}({}^t v)) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor^{\hat{\beta}}_V \wedge$
$(n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that we are given some $H_s, H_t, \hat{\beta}$ s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $\mathsf{Lb}_\ell(e_s)\ \delta^s \Downarrow_i \mathsf{Lb}_\ell({}^s v)$.

And we need to prove

$\exists H'_t, {}^t v.(H_t, \mathsf{inl}(e_t)\ \delta^t) \Downarrow (H'_t, \mathsf{inl}({}^t v)) \wedge ({}^s\theta, n-i, \mathsf{Lb}_\ell({}^s v), \mathsf{inl}({}^t v)) \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_V^{\hat{\beta}} \wedge$
$(n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-LB0)

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.10 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_s\ \delta^s \Downarrow_j {}^s v_1 \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and since we know that $\mathsf{Lb}_\ell(e_s)\ \delta^s \Downarrow_i \mathsf{Lb}_\ell({}^s v)$ therefore $\exists j < i < n$ s.t $e_s\ \delta^s \Downarrow_j {}^s v$.

Therefore we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v, {}^t v) \in \lfloor (\tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-LB1)

Since from (F-LB0) we are required to prove $({}^s\theta, n-i, \mathsf{Lb}_\ell({}^s v), \mathsf{inl}({}^t v)) \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_V^{\hat{\beta}}$. Since from SLIO*-Sem-label we know that $i = j+1$, ${}^s v = {}^s v_1$ and ${}^t v = {}^t v_1$. Therefore we get this from Definition 3.9, (F-LB1) and Lemma 3.15.

From Lemma 3.15 we get $(n-i, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

17. CF-toLabeled:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \mathbb{SLIO}\ \ell_i\ \ell_o\ \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \mathsf{toLabeled}(e_s) : \mathbb{SLIO}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(e_t\ ())}\ \text{toLabeled}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{toLabeled}(e_s)\ \delta^s, (\lambda\_.\mathsf{inl}\ e_t())\ \delta^t) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau))\ \sigma\rfloor_E^{\hat{\beta}}$

It means from Definition 3.10 that we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{toLabeled}(e_s)\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, (\lambda\_.\mathsf{inl}\ e_t())\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau))\ \sigma\rfloor_V^{\hat{\beta}} \wedge$
$(n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $\mathsf{toLabeled}(e_s)\ \delta^s \Downarrow_i {}^s v$

And we need to prove

$\exists H'_t, {}^t v.(H_t, (\lambda\_.\mathsf{inl}\ e_t())\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau))\ \sigma\rfloor_V^{\hat{\beta}} \wedge$
$(n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

From SLIO*-Sem-val and fg-val we know that $i = 0$, ${}^s v = \mathsf{toLabeled}(e_s)\ \delta^s$,
${}^t v = (\lambda\_.\mathsf{inl}\ e_t())\ \delta^t$, $H'_t = H_t$

And we need to prove

$$({}^s\theta, n, \mathsf{toLabeled}(e_s)\ \delta^s, (\lambda\_.\mathsf{inl}\ e_t())\ \delta^t) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau))\ \sigma\rfloor_V^{\hat\beta} \wedge (n, H_s, H_t) \overset{\hat\beta}{\triangleright} {}^s\theta$$

Since we already know $(n, H_s, H_t) \overset{\hat\beta}{\triangleright} {}^s\theta$ from the context so we are left with proving
$({}^s\theta, n, \mathsf{toLabeled}(e_s)\ \delta^s, (\lambda\_.\mathsf{inl}\ e_t())\ \delta^t) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau))\ \sigma\rfloor_V^{\hat\beta}$

From Definition 3.9 it means we need to prove
$\forall {}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^s v', {}^t v', k \leq n, \hat\beta \sqsubseteq \hat\beta'$.
$(k, H_{s1}, H_{t1}) \overset{\hat\beta'}{\triangleright} ({}^s\theta_e) \wedge (H_{s1}, \mathsf{toLabeled}(e_s)\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^s v') \wedge i < k \implies$
$\exists H'_{t1}, {}^t v'.(H_{t1}, (\lambda\_.\mathsf{inl}\ e_t())()\ \delta^t) \Downarrow (H'_{t1}, {}^t v') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat\beta' \sqsubseteq \hat\beta''.(k-i, H'_{s1}, H'_{t1}) \overset{\hat\beta''}{\triangleright} {}^s\theta' \wedge$
$\exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k-i, {}^s v', {}^t v'') \in \lfloor(\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rfloor_V^{\hat\beta''}$

This means we are given some ${}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^s v', {}^t v', k \leq n, \hat\beta \sqsubseteq \hat\beta'$ s.t
$(k, H_{s1}, H_{t1}) \overset{\hat\beta'}{\triangleright} {}^s\theta_e \wedge (H_{s1}, \mathsf{toLabeled}(e_s)\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^s v') \wedge i < k$.

And we need to prove

$\exists H'_{t1}, {}^t v'.(H_{t1}, (\lambda\_.\mathsf{inl}\ e_t())()\ \delta^t) \Downarrow (H'_{t1}, {}^t v') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat\beta' \sqsubseteq \hat\beta''.(k-i, H'_{s1}, H'_{t1}) \overset{\hat\beta''}{\triangleright} {}^s\theta' \wedge$
$\exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k-i, {}^s v', {}^t v'') \in \lfloor(\mathsf{Labeled}\ \ell_o\ \tau)\ \sigma\rfloor_V^{\hat\beta''}$ (F-TL0)

<u>IH:</u>

$({}^s\theta, k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau)\ \sigma\rfloor_E^{\hat\beta}$

It means from Definition 3.10 that we need to prove

$\forall H_{s2}, H_{t2}.(k, H_{s2}, H_{t2}) \overset{\hat\beta}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_{h1}.e_s\ \delta^s \Downarrow_j {}^s v_{h1} \implies$
$\exists H'_{t2}, {}^t v_{h1}.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^t v_{h1}) \wedge ({}^s\theta, k-j, {}^s v_{h1}, {}^t v_{h1}) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau)\ \sigma\rfloor_V^{\hat\beta} \wedge (k-j, H_{s2}, H'_{t2}) \overset{\hat\beta}{\triangleright} {}^s\theta$

Instantiating H_{s2} with H_{s1} and H_{t2} with H_{t1}. And since we know that $(H_{s1}, \mathsf{toLabeled}(e_s)\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists j < i < k \leq n$ s.t $e_s\ \delta^s \Downarrow_j {}^s v_{h1}$.
Therefore we have
$\exists H'_{t2}, {}^t v_{h1}.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^t v_{h1}) \wedge ({}^s\theta, k-j, {}^s v_{h1}, {}^t v_{h1}) \in \lfloor(\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau)\ \sigma\rfloor_V^{\hat\beta} \wedge (k-j, H_{s1}, H'_{t2}) \overset{\hat\beta}{\triangleright} {}^s\theta$ (F-TL1.1)

From Definition 3.9 we know have
$\forall {}^s\theta_e \sqsupseteq {}^s\theta, H_{s3}, H_{t3}, b, {}^s v'_{h1}, {}^t v'_{h1}, m \leq k-j, \hat\beta \sqsubseteq \hat\beta'$.
$(m, H_{s3}, H_{t3}) \overset{\hat\beta'}{\triangleright} ({}^s\theta_e) \wedge (H_{s3}, {}^s v_{h1}) \Downarrow_b^f (H'_{s3}, {}^s v'_{h1}) \wedge b < m \implies$

$\exists H'_{t3}, {}^t v'_{h1}.(H_{t3}, {}^t v_{h1}\ ()) \Downarrow (H'_{t3}, {}^t v'_{h1}) \wedge \exists^s\theta'' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(m-b, H'_{s3}, H'_{t3}) \overset{\hat{\beta}''}{\rhd} {}^s\theta'' \wedge$
$\exists^t v''_{h1}.{}^t v'_{h1} = \mathsf{inl}\ {}^t v''_{h1} \wedge ({}^s\theta'', m-b, {}^s v'_{h1}, {}^t v''_{h1}) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$

Instantiating ${}^s\theta_e$ with ${}^s\theta$, H_{s3} with H_{s1}, H_{t3} with H'_{t2}, m with $k-j$ and $\hat{\beta}'$ with $\hat{\beta}$. Since we know that $(H_{s1}, \mathsf{toLabeled}(e_s)\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists b < i-j < k-j$ s.t $(H_{s1}, {}^s v_{h1})\ \delta^s \Downarrow_b (H'_{s3}, {}^s v'_{h1})$.

Therefore we have

$\exists H'_{t3}, {}^t v'_{h1}.(H_{t3}, {}^t v_{h1}\ ()) \Downarrow (H'_{t3}, {}^t v'_{h1}) \wedge \exists^s\theta'' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-j-b, H'_{s3}, H'_{t3}) \overset{\hat{\beta}''}{\rhd} {}^s\theta'' \wedge$
$\exists^t v''.{}^t v'_{h1} = \mathsf{inl}\ {}^t v''_{h1} \wedge ({}^s\theta'', k-j-b, {}^s v'_{h1}, {}^t v''_{h1}) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$ (F-TL1)

In order to prove (F-TL0) we choose ${}^s\theta'$ as ${}^s\theta''$ and $\hat{\beta}'$ as $\hat{\beta}''$ (both chosen from (F-TL2))
Also from SLIO*-Sem-toLabeled and fg-inl, fg-app we know that $H'_s = H'_{s3}$ and $H'_t = H'_{t3}$, and ${}^s v' = {}^s v'_{h1}$, ${}^t v' = {}^t v'_{h1}$
Therefore we get the desired from (F-TL1) and Lemma 3.15

18. CF-unlabel:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \mathsf{Labeled}\ \ell\ \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \mathsf{unlabel}(e_s) : \mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau \rightsquigarrow \lambda\_.e_t}\ \text{unlabel}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{unlabel}(e_s)\ \delta^s, \lambda\_.e_t\ \delta^t \in \lfloor \mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau\ \sigma \rfloor_E^{\hat{\beta}}$

It means from Definition 3.10 that we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{unlabel}(e_s)\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, \lambda\_.e_t\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\rhd} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta$ and given some $i < n, {}^s v$ s.t $\mathsf{unlabel}(e_s)\ \delta^s \Downarrow_i {}^s v$

And we need to prove

$\exists H'_t, {}^t v.(H_t, \lambda\_.e_t\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\rhd} {}^s\theta$
From SLIO*-Sem-val and fg-val we know that $i = 0$, ${}^s v = \mathsf{unlabel}(e_s)\ \delta^s$, ${}^t v = \lambda\_.e_t\ \delta^t$, $H'_t = H_t$

And we need to prove

$({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta$

Since we already know $(n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta$ from the context so we are left with proving
$({}^s\theta, n, \mathsf{unlabel}(e_s)\ \delta^s, \lambda\_.e_t\ \delta^t) \in \lfloor \mathbb{SLIO}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau\ \sigma \rfloor_V^{\hat{\beta}}$

From Definition 3.9 it means we need to prove

$\forall^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^s v', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s1}, \mathsf{unlabel}(e_s)\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^s v') \wedge i < k \implies$
$\exists H'_{t1}, {}^t v'.(H_{t1}, (\lambda\_.e_t)()\ \delta^t) \Downarrow (H'_{t1}, {}^t v') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k - i, {}^s v', {}^t v'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$

This means we are given some ${}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^s v', {}^t v', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t

$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge (H_{s1}, \mathsf{unlabel}(e_s)\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^s v') \wedge i < k.$

And we need to prove

$\exists H'_{t1}, {}^t v'.(H_{t1}, (\lambda\_.e_t)()\ \delta^t) \Downarrow (H'_{t1}, {}^t v') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k - i, {}^s v', {}^t v'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$ (F-U0)

<u>IH:</u>

$({}^s\theta_e, k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_E^{\hat{\beta}'}$

It means from Definition 3.10 that we need to prove

$\forall H_{s2}, H_{t2}.(k, H_{s2}, H_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge \forall f < k, {}^s v_h.e_s\ \delta^s \Downarrow_f {}^s v_h \implies$
$\exists H'_{t2}, {}^t v_h.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^t v_h) \wedge ({}^s\theta_e, k - f, {}^s v_h, {}^t v_h) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k - f, H_{s2}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

Instantiating H_{s2} with H_{s1} and H_{t2} with H_{t1}. And since we know that $(H_{s1}, \mathsf{unlabel}(e_s)\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists f < i < k \leq n$ s.t $e_s\ \delta^s \Downarrow_f {}^s v_h$.
Therefore we have
$\exists H'_{t2}, {}^t v_h.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^t v_h) \wedge ({}^s\theta_e, k - f, {}^s v_h, {}^t v_h) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k - f, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$ (F-U1)

In order to prove (F-U0) we choose H'_{t1} as H'_{t2}, ${}^t v'$ as ${}^t v_h$, ${}^s\theta'$ as ${}^s\theta_e$ and $\hat{\beta}''$ as $\hat{\beta}'$
From SLIO*-Sem-unlabel and fg-app we also know that $H'_{s1} = H_{s1}$ and $H'_{t1} = H'_{t2}$
We need to prove

(a) $(k - i, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$:

Since from (F-U1) we know that $(k - f, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

Therefore from Lemma 3.17 we also get $(k - i, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

(b) $\exists^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta_e, k - i, {}^s v', {}^t v'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$:
Since from (F-U1) we have
$({}^s\theta_e, k - f, {}^s v_h, {}^t v_h) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'}$

This means from Definition 3.9 we know that
$\exists^s v_i, {}^t v_i.{}^s v_h = \mathsf{Lb}_\ell({}^s v_i) \wedge {}^t v_h = \mathsf{inl}\ {}^t v_i \wedge ({}^s\theta_e, k - f - 1, {}^s v_i, {}^t v_i) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-U2)

Since we know that ${}^t v' = {}^t v_h$ and since from (F-U2) we have ${}^t v_h = \mathsf{inl}\ {}^t v_i$. Therefore from we choose ${}^t v''$ as ${}^t v_i$ to get the first conjunct
From SLIO*-Sem-unlabel we know that ${}^s v = {}^s v_i$ and since we know that $({}^s\theta_e, k - f - 1, {}^s v_i, {}^t v_i) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$
Therefore from Lemma 3.15 we also get $({}^s\theta_e, k - i, {}^s v_i, {}^t v_i) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$

19. CF-ref:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \mathsf{Labeled}\ \ell'\ \tau \rightsquigarrow e_t \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash \mathsf{new}\ e_s : \mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_t))}\ \text{ref}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{new}\ e_s\ \delta^s, \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_t))\ \delta^t \in \lfloor \mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_E^{\hat{\beta}}$

It means from Definition 3.10 that we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{new}\ e_s\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H_t', {}^t v.(H_t, \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_t))\ \delta^t) \Downarrow (H_t', {}^t v) \wedge ({}^s\theta, n - i, {}^s v, {}^t v) \in \lfloor \mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge$
$(n - i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t
$\mathsf{new}\ e_s\ \delta^s \Downarrow_i {}^s v$

From SLIO*-Sem-val and fg-val we know that $i = 0$, ${}^s v = \mathsf{new}\ e_s\ \delta^s$, ${}^t v = \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_t))\ \delta^t$, $H_t' = H_t$

And we need to prove

$({}^s\theta, n, \mathsf{new}\ e_s\ \delta^s, \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_t))\ \delta^t) \in \lfloor \mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we already know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context so we are left with proving
$({}^s\theta, n, \mathsf{new}\ e_s\ \delta^s, \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_t))\ \delta^t) \in \lfloor \mathbb{SLIO}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat{\beta}}$

From Definition 3.9 it means we need to prove
$\forall {}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^s v', k \le n, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s1}, \mathsf{new}\ e_s\ \delta^s) \Downarrow_i^f (H_{s1}', {}^s v') \wedge i < k \implies$
$\exists H_{t1}', {}^t v'.(H_{t1}, (\lambda\_.\mathsf{inl}(\mathsf{new}\ e_t))()\ \delta^t) \Downarrow (H_{t1}', {}^t v') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H_{s1}', H_{t1}') \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k - i, {}^s v', {}^t v'') \in \lfloor (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat{\beta}''}$

This means we are given some ${}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^s v', {}^t v', k \le n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge (H_{s1}, \mathsf{new}\ (e_s)\ \delta^s) \Downarrow_i^f (H_{s1}', {}^s v') \wedge i < k.$

And we need to prove

$\exists H'_{t1}, {}^t v'.(H_{t1}, (\lambda\_.\mathsf{inl}(\mathsf{new}\ e_t))()\ \delta^t) \Downarrow (H'_{t1}, {}^t v') \wedge \exists^s \theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k-i, {}^s v', {}^t v'') \in \lfloor (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat{\beta}''}$ (F-N0)

From SLIO*-Sem-ref we know that ${}^s v' = a_s$ and from fg-ref, fg-inl we know that ${}^t v' = \mathsf{inl}\ a_t$.

<u>IH:</u>

$({}^s\theta_e, k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_E^{\hat{\beta}'}$

It means from Definition 3.10 that we need to prove

$\forall H_{s2}, H_{t2}.(k, H_{s2}, H_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge \forall f < k, {}^s v_h.e_s\ \delta^s \Downarrow_f {}^s v_h \implies$
$\exists H'_{t2}, {}^t v_h.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^t v_h) \wedge ({}^s\theta_e, k-f, {}^s v_h, {}^t v_h) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k-f, H_{s2}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

Instantiating H_{s2} with H_{s1} and H_{t2} with H_{t1}. And since we know that $(H_{s1}, \mathsf{new}\ (e_s)\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists f < i < k \leq n$ s.t $e_s\ \delta^s \Downarrow_f {}^s v_h$.

Therefore we have

$\exists H'_{t2}, {}^t v_h.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^t v_h) \wedge ({}^s\theta_e, k-f, {}^s v_h, {}^t v_h) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k-f, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$ (F-N1)

In order to prove (F-N0) we choose H'_{t1} as $H'_{t2} \cup \{a_t \mapsto {}^t v_h\}$, ${}^t v$ as a_t, ${}^s\theta'$ as ${}^s\theta_n$ where ${}^s\theta_n = {}^s\theta_e \cup \{a_s \mapsto (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma\}$

And we choose $\hat{\beta}''$ as $\hat{\beta}_n$ where $\hat{\beta}_n = \hat{\beta}' \cup \{(a_s, a_t)\}$

From SLIO*-Sem-ref and fg-ref we also know that $H'_{s1} = H_{s1} \cup \{a_s \mapsto {}^s v_h\}$

We need to prove

(a) $(k-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}_n}{\triangleright} {}^s\theta_n$:

From Definition 3.11 it suffices to prove that

- $dom({}^s\theta_n) \subseteq dom(H'_{s1})$:

  Since $dom({}^s\theta_e) \subseteq dom(H_{s1})$ (given that we have $(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$)

  And since we know that
  ${}^s\theta_n = {}^s\theta_e \cup \{a_s \mapsto (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma\}$ and $H'_{s1} = H_{s1} \cup \{a_s \mapsto {}^s v_h\}$
  Therefore we get $dom({}^s\theta_n) \subseteq dom(H'_{s1})$
- $\hat{\beta}_n \subseteq (dom({}^s\theta_n) \times dom(H'_{t1}))$:

  Since $\hat{\beta}' \subseteq (dom({}^s\theta_e) \times dom(H_{t1}))$ (given that we have $(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$)

  And since we know that
  ${}^s\theta_n = {}^s\theta_e \cup \{a_s \mapsto (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma\}$, $H'_{t1} = H_{t1} \cup \{a_t \mapsto {}^t v_h\}$ and $\hat{\beta}_n = \hat{\beta}' \cup \{(a_s, a_t)\}$

  Therefore we get $\hat{\beta}_n \subseteq (dom({}^s\theta_n) \times dom(H'_{t1}))$
- $\forall (a_1, a_2) \in \hat{\beta}_n.({}^s\theta_n, k-i-1, H'_{s1}(a_1), H'_{t1}(a_2)) \in \lfloor {}^s\theta_n(a) \rfloor_V^{\hat{\beta}_n}$:
  $\forall (a_1, a_2) \in \hat{\beta}_n$

- $(a_1, a_2) = (a_s, a_t)$:
  Since from (F-N1) we know that $({}^s\theta_e, k - f, {}^s v_h, {}^t v_h) \in \lfloor(\mathsf{Labeled}\ \ell'\ \tau)\ \sigma\rfloor_V^{\hat{\beta}'}$
  From Lemma 3.15 we get $({}^s\theta_n, k - i - 1, {}^s v_h, {}^t v_h) \in \lfloor(\mathsf{Labeled}\ \ell'\ \tau)\ \sigma\rfloor_V^{\hat{\beta}_n}$
- $(a_1, a_2) \neq (a_s, a_t)$:
  Since we have $(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$ therefore
  from Definition 3.11 we get
  $({}^s\theta_e, k - 1, H_{s1}(a_1), H_{t1}(a_2)) \in \lfloor {}^s\theta_e(a_1)\rfloor_V^{\hat{\beta}'}$
  From Lemma 3.15 we get
  $({}^s\theta_n, k - i - 1, H_{s1}(a_1), H_{t1}(a_2)) \in \lfloor {}^s\theta_n(a_1)\rfloor_V^{\hat{\beta}'}$

(b) $\exists^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta_n, k - i, {}^s v', {}^t v'') \in \lfloor(\mathsf{ref}\ \ell'\ \tau)\ \sigma\rfloor_V^{\hat{\beta}_n}$:
We choose ${}^t v''$ as ${}^t v_h$ from (F-N1), fg-inl and fg-ref we know that ${}^t v' = \mathsf{inl}\ {}^t v_h$

In order to prove $({}^s\theta_n, k - i, {}^s v', {}^t v'') \in \lfloor(\mathsf{ref}\ \ell'\ \tau)\ \sigma\rfloor_V^{\hat{\beta}_n}$, from Definition 3.9 it suffices to prove that
${}^s\theta_n(a_s) = (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \wedge (a_s, a_t) \in \hat{\beta}_n$

We get this by construction of ${}^s\theta_n$ and $\hat{\beta}_n$

20. CF-deref:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \mathsf{ref}\ \ell\ \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash !e_s : \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(e_t)}\ \text{deref}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma\rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, !e_s\ \delta^s, \lambda\_.\mathsf{inl}(e_t)\ \delta^t \in \lfloor \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_E^{\hat{\beta}}$

It means from Definition 3.10 that we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.!e_s\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H_t', {}^t v.(H_t, \lambda\_.\mathsf{inl}(e_t)\ \delta^t) \Downarrow (H_t', {}^t v) \wedge ({}^s\theta, n - i, {}^s v, {}^t v) \in \lfloor \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_V^{\hat{\beta}} \wedge$
$(n - i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t
$!e_s\ \delta^s \Downarrow_i {}^s v$

And we need to prove
$\exists H_t', {}^t v.(H_t, \lambda\_.\mathsf{inl}(e_t)\ \delta^t) \Downarrow (H_t', {}^t v) \wedge ({}^s\theta, n - i, {}^s v, {}^t v) \in \lfloor \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_V^{\hat{\beta}} \wedge$
$(n - i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta$
From SLIO*-Sem-val and fg-val we know that $i = 0$, ${}^s v = !e_s\ \delta^s$, ${}^t v = \lambda\_.\mathsf{inl}(e_t)\ \delta^t$, $H_t' = H_t$

And we need to prove
$({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we already know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context so we are left with proving

$({}^s\theta, n, !e_s\ \delta^s, \lambda\_.\mathsf{inl}(e_t)\ \delta^t) \in \lfloor \mathbb{SLIO}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat\beta}$

From Definition 3.9 it means we need to prove
$\forall {}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^sv', {}^tv', k \leq n, \hat\beta \sqsubseteq \hat\beta'.$
$(k, H_{s1}, H_{t1}) \overset{\hat\beta'}{\triangleright} ({}^s\theta_e) \wedge (H_{s1}, !e_s\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^sv') \wedge i < k \implies$
$\exists H'_{t1}, {}^tv'.(H_{t1}, (\lambda\_.\mathsf{inl}(e_t))()\ \delta^t) \Downarrow (H'_{t1}, {}^tv') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat\beta' \sqsubseteq \hat\beta''.(k-i, H'_{s1}, H'_{t1}) \overset{\hat\beta''}{\triangleright} {}^s\theta' \wedge$
$\exists {}^tv''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', k-i, {}^sv', {}^tv'') \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat\beta''}$

This means we are given some ${}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^sv', {}^tv', k \leq n, \hat\beta \sqsubseteq \hat\beta'$ s.t

$(k, H_{s1}, H_{t1}) \overset{\hat\beta'}{\triangleright} {}^s\theta_e \wedge (H_{s1}, !(e_s)\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^sv') \wedge i < k.$

And we need to prove

$\exists H'_{t1}, {}^tv'.(H_{t1}, (\lambda\_.\mathsf{inl}(e_t))()\ \delta^t) \Downarrow (H'_{t1}, {}^tv') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat\beta' \sqsubseteq \hat\beta''.(k-i, H'_{s1}, H'_{t1}) \overset{\hat\beta''}{\triangleright} {}^s\theta' \wedge$
$\exists {}^tv''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', k-i, {}^sv', {}^tv'') \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat\beta''}$ (F-D0)

<u>IH:</u>

$({}^s\theta_e, k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\mathsf{ref}\ \ell\ \tau)\ \sigma \rfloor_E^{\hat\beta'}$

It means from Definition 3.10 that we need to prove

$\forall H_{s2}, H_{t2}.(k, H_{s2}, H_{t2}) \overset{\hat\beta'}{\triangleright} {}^s\theta_e \wedge \forall f < k, {}^sv_h.e_s\ \delta^s \Downarrow_f {}^sv_h \implies$
$\exists H'_{t2}, {}^tv_h.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^tv_h) \wedge ({}^s\theta_e, k-f, {}^sv_h, {}^tv_h) \in \lfloor (\mathsf{ref}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat\beta'} \wedge (k-f, H_{s2}, H'_{t2}) \overset{\hat\beta'}{\triangleright} {}^s\theta_e$

Instantiating H_{s2} with H_{s1} and H_{t2} with H_{t1}. And since we know that $(H_{s1}, !e_s\ \delta^s) \Downarrow_i^f (H'_s, {}^sv')$ therefore $\exists f < i < k \leq n$ s.t $e_s\ \delta^s \Downarrow_f {}^sv_h$.
Therefore we have

$\exists H'_{t2}, {}^tv_h.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^tv_h) \wedge ({}^s\theta_e, k-f, {}^sv_h, {}^tv_h) \in \lfloor (\mathsf{ref}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat\beta'} \wedge (k-f, H_{s1}, H'_{t2}) \overset{\hat\beta'}{\triangleright} {}^s\theta_e$
(F-D1)

In order to prove (F-D0) we choose H'_{t1} as H'_{t2}, ${}^tv'_1$ as $H'_{t2}(a)$ (where ${}^tv_h = a_t$ from fg-deref), ${}^s\theta'$ as ${}^s\theta_e$ and we choose $\hat\beta''$ as $\hat\beta'$.
From SLIO*-Sem-deref we also know that $H'_{s1} = H_{s1}$
We need to prove

(a) $(k-i, H_{s1}, H'_{t2}) \overset{\hat\beta'}{\triangleright} {}^s\theta_e$:
Since from (F-D1) we have $(k-f, H_{s1}, H'_{t2}) \overset{\hat\beta'}{\triangleright} {}^s\theta_e$ and since $f < i$ threfore from Lemma 3.17 we get $(k-i, H_{s1}, H'_{t2}) \overset{\hat\beta'}{\triangleright} {}^s\theta_e$

(b) $\exists {}^tv''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta_e, k-i, {}^sv', {}^tv'') \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat\beta'}$:
Since from SLIO*-Sem-deref and fg-deref we know that ${}^sv_h = a_s$ and ${}^tv_h = a_t$.
Therefore from (F-D1) and from Definition 3.9 we know that
${}^s\theta_e(a_s) = (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \wedge (a_s, a_t) \in \hat\beta'$

Since from (F-D1) we know that $(k - f, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$ which means from Definition 3.11 we know that
$({}^s\theta, k - f - 1, H_{s1}(a_s), H'_{t2}(a_t)) \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_V^{\hat{\beta}'}$ (F-D2)

This means from Definition 3.9 we know that
$\exists^s v_i, {}^t v_i.H_{s1}(a_s) = \mathsf{Lb}_\ell({}^s v_i) \wedge H'_{t2}(a_t) = \mathsf{inl}\ {}^t v_i \wedge ({}^s\theta_e, k - f - 1, {}^s v_i, {}^t v_i) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}'}$

We choose ${}^t v''$ as ${}^t v_i$ and we know that ${}^t v' = H'_{t2}(a_t) = \mathsf{inl}\ {}^t v_i$. This proves the first conjunct.

Since from (F-D2) we have $({}^s\theta, k - f - 1, H_{s1}(a_s), H'_{t2}(a_t)) \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_V^{\hat{\beta}'}$ therefore from Lemma 3.15 we get
$({}^s\theta, k - i - 1, H_{s1}(a_s), H'_{t2}(a_t)) \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_V^{\hat{\beta}'}$
This proves the second conjunct.

21. CF-assign:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_{s1} : \mathsf{ref}\ \ell'\ \tau \rightsquigarrow e_{t1} \qquad \Sigma; \Psi; \Gamma \vdash e_{s2} : \mathsf{Labeled}\ \ell'\ \tau \rightsquigarrow e_{t2} \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash e_{s1} := e_{s2} : \mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit} \rightsquigarrow \lambda\_.\mathsf{inl}(e_{t1} := e_{t2})}\ \text{assign}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor\Gamma\ \sigma\rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, (e_{s1} := e_{s2})\ \delta^s, \lambda\_.\mathsf{inl}(e_{t1} := e_{t2})\ \delta^t \in \lfloor\mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit}\ \sigma\rfloor_E^{\hat{\beta}}$

It means from Definition 3.10 that we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(e_{s1} := e_{s2})\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, \lambda\_.\mathsf{inl}(e_{t1} := e_{t2})\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n - i, {}^s v, {}^t v) \in \lfloor\mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit}\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $(e_{s1} := e_{s2})\ \delta^s \Downarrow_i {}^s v$

And we need to prove
$\exists H'_t, {}^t v.(H_t, \lambda\_.\mathsf{inl}(e_{t1} := e_{t2})\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n - i, {}^s v, {}^t v) \in \lfloor\mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit}\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

From SLIO*-Sem-val and fg-val we know that $i = 0$, ${}^s v = (e_{s1} := e_{s2})\ \delta^s$, ${}^t v = \lambda\_.\mathsf{inl}(e_{t1} := e_{t2})\ \delta^t$, $H'_t = H_t$

And we need to prove

$({}^s\theta, n, (e_{s1} := e_{s2})\ \delta^s, \lambda\_.\mathsf{inl}(e_{t1} := e_{t2})\ \delta^t) \in \lfloor\mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit}\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we already know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context so we are left with proving
$({}^s\theta, n, (e_{s1} := e_{s2})\ \delta^s, \lambda\_.\mathsf{inl}(e_{t1} := e_{t2})\ \delta^t) \in \lfloor\mathbb{SLIO}\ \ell\ \ell\ \mathsf{unit}\ \sigma\rfloor_V^{\hat{\beta}}$

From Definition 3.9 it means we need to prove
$\forall^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^sv', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s1}, (e_{s1} := e_{s2})\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^sv') \wedge i < k \implies$
$\exists H'_{t1}, {}^tv'.(H_{t1}, (\lambda\_.\mathsf{inl}(e_{t1} := e_{t2})()\ \delta^t)) \Downarrow (H'_{t1}, {}^tv') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright}$
${}^s\theta' \wedge \exists^t v''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', k-i, {}^sv', {}^tv'') \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}''}$

This means we are given some ${}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^sv', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t

$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge (H_{s1}, (e_{s1} := e_{s2})\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^sv') \wedge i < k.$

And we need to prove
$\exists H'_{t1}, {}^tv'.(H_{t1}, (\lambda\_.\mathsf{inl}(e_{t1} := e_{t2})()\ \delta^t)) \Downarrow (H'_{t1}, {}^tv') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.$
$(k-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge \exists^t v''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', k-i, {}^sv', {}^tv'') \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}''}$ (F-S0)

<u>IH1:</u>

$({}^s\theta_e, k, e_{s1}\ \delta^s, e_{t1}\ \delta^t) \in \lfloor (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_E^{\hat{\beta}'}$

It means from Definition 3.10 that we need to prove

$\forall H_{s2}, H_{t2}.(k, H_{s2}, H_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge \forall f < k, {}^sv_{h1}.e_{s1}\ \delta^s \Downarrow_f {}^sv_{h1} \implies$
$\exists H'_{t2}, {}^tv_{h1}.(H_{t2}, e_{t1}\ \delta^t) \Downarrow (H'_{t2}, {}^tv_{h1}) \wedge ({}^s\theta_e, k-f, {}^sv_{h1}, {}^tv_{h1}) \in \lfloor (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k-f, H_{s2}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

Instantiating H_{s2} with H_{s1} and H_{t2} with H_{t1}. And since we know that $(H_{s1}, e_{s1} := e_{s2}\ \delta^s) \Downarrow_i^f (H'_s, {}^sv')$ therefore $\exists f < i < k \leq n$ s.t $e_s\ \delta^s \Downarrow_f {}^sv_{h1}$.
Therefore we have
$\exists H'_{t2}, {}^tv_{h1}.(H_{t2}, e_{t1}\ \delta^t) \Downarrow (H'_{t2}, {}^tv_{h1}) \wedge ({}^s\theta_e, k-f, {}^sv_{h1}, {}^tv_{h1}) \in \lfloor (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k-f, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$ (F-S1)

<u>IH2:</u>

$({}^s\theta_e, k-f, e_{s2}\ \delta^s, e_{t2}\ \delta^t) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_E^{\hat{\beta}'}$

It means from Definition 3.10 that we need to prove

$\forall H_{s3}, H_{t3}.(k, H_{s3}, H_{t3}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge \forall l < k-f, {}^sv_{h2}.e_{s2}\ \delta^s \Downarrow_l {}^sv_{h2} \implies$
$\exists H'_{t3}, {}^tv_{h2}.(H_{t3}, e_{t2}\ \delta^t) \Downarrow (H'_{t3}, {}^tv_{h2}) \wedge ({}^s\theta_e, k-f-l, {}^sv_{h2}, {}^tv_{h2}) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k-f-l, H_{s3}, H'_{t3}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

Instantiating H_{s3} with H_{s1} and H_{t3} with H'_{t2}. And since we know that $(H_{s1}, e_{s1} := e_{s2}\ \delta^s) \Downarrow_i^f (H'_s, {}^sv')$ therefore $\exists l < i-f < k-f$ s.t $e_{s2}\ \delta^s \Downarrow_l {}^sv_{h2}$.
Therefore we have
$\exists H'_{t3}, {}^tv_{h2}.(H_{t3}, e_{t2}\ \delta^t) \Downarrow (H'_{t3}, {}^tv_{h2}) \wedge ({}^s\theta_e, k-f-l, {}^sv_{h2}, {}^tv_{h2}) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k-f-l, H_{s1}, H'_{t3}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$ (F-S2)

In order to prove (F-S0) we choose H'_{t1} as $H'_{t3}[a_t \mapsto {}^t v_{h3}]$, ${}^t v'$ as (), ${}^s\theta'$ as ${}^s\theta_e$ and $\hat{\beta}''$ as $\hat{\beta}'$
From SLIO*-Sem-assign and fg-assign we also know that ${}^s v_{h2} = a_s$, ${}^t v_{h2} = a_t$, $H'_{s1} = H_{s1}[a_s \mapsto {}^s v_{h3}]$ and $H'_{t1} = H'_{t3}[a_t \mapsto {}^t v_{h3}]$
We need to prove

(a) $(k-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$:
From Definition 3.11 it suffices to prove that

- $dom({}^s\theta_e) \subseteq dom(H'_{s1})$:

  Since $dom({}^s\theta_e) \subseteq dom(H_{s1})$ (given that we have $(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$)

  And since $dom(H_{s1}) = dom(H'_{s1})$ therefore we also get
  $dom({}^s\theta_e) \subseteq dom(H'_{s1})$
- $\hat{\beta}' \subseteq (dom({}^s\theta_e) \times dom(H'_{t1}))$:

  Since $\hat{\beta}' \subseteq (dom({}^s\theta_e) \times dom(H_{t1}))$ (given that we have $(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$)

  And since $dom(H_{t1}) \subseteq dom(H'_{t1})$ therefore we also have $\hat{\beta}' \subseteq (dom({}^s\theta_e) \times dom(H'_{t1}))$
- $\forall(a_1, a_2) \in \hat{\beta}'.({}^s\theta_e, k-i-1, H'_{s1}(a_1), H'_{t1}(a_2)) \in \lfloor {}^s\theta_e(a_1) \rfloor_V^{\hat{\beta}'}$:
  $\forall(a_1, a_2) \in \hat{\beta}_n$
  - $(a_1, a_2) = (a_s, a_t)$:
    Since from (F-S2) we know that $({}^s\theta_e, k-f-l, {}^s v_{h2}, {}^t v_{h2}) \in \lfloor(\mathsf{Labeled}\ \ell'\ \tau)\ \sigma\rfloor_V^{\hat{\beta}'}$
    From Lemma 3.15 we get $({}^s\theta_e, k-i-1, {}^s v_{h2}, {}^t v_{h2}) \in \lfloor(\mathsf{Labeled}\ \ell'\ \tau)\ \sigma\rfloor_V^{\hat{\beta}'}$
  - $(a_1, a_2) \neq (a_s, a_t)$:

    Since we have $(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$ therefore
    from Definition 3.11 we get
    $({}^s\theta_e, k-1, H_{s1}(a_1), H_{t1}(a_2)) \in \lfloor {}^s\theta_e(a_1)\rfloor_V^{\hat{\beta}'}$
    From Lemma 3.15 we get
    $({}^s\theta_n, k-i-1, H_{s1}(a_1), H_{t1}(a_2)) \in \lfloor {}^s\theta_e(a_1)\rfloor_V^{\hat{\beta}'}$

(b) $\exists^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta_e, k-i, {}^s v', {}^t v'') \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}_n}$:
We choose ${}^t v''$ as () from (F-S1), fg-inl and fg-assign we know that ${}^t v' = \mathsf{inl}\ ()$

<u>To prove:</u> $({}^s\theta_n, k-i, (), ()) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}_n}$,
We get this directly from Definition 3.9

□

Lemma 3.19 (SLIO* $\rightsquigarrow$ FG: Subtyping)**.** *The following holds:*
$\forall \Sigma, \Psi, \sigma, \tau, \tau'$.

1. $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor(\tau\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor(\tau'\ \sigma)\rfloor_V^{\hat{\beta}}$

2. $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor(\tau\ \sigma)\rfloor_E^{\hat{\beta}} \subseteq \lfloor(\tau'\ \sigma)\rfloor_E^{\hat{\beta}}$

Proof. <u>Proof of Statement (1)</u>
Proof by induction on $\tau <: \tau'$

1. SLIO*sub-arrow:

   Given:

$$\frac{\Sigma;\Psi \vdash \tau_1' <: \tau_1 \qquad \Sigma;\Psi \vdash \tau_2 <: \tau_2'}{\Sigma;\Psi \vdash \tau_1 \to \tau_2 <: \tau_1' \to \tau_2'}$$

   To prove: $\lfloor((\tau_1 \to \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor((\tau_1' \to \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

   It suffices to prove: $\forall ({}^s\theta, n, \lambda x.e_i) \in \lfloor((\tau_1 \to \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, \lambda x.e_i) \in \lfloor((\tau_1' \to \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

   This means that given some ${}^s\theta, n$ and $\lambda x.e_i$ s.t $({}^s\theta, n, \lambda x.e_i) \in \lfloor((\tau_1 \to \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}}$
   Therefore from Definition 3.9 we are given:
   $\forall {}^s\theta' \sqsupseteq {}^s\theta, {}^s v, {}^t v, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.$
   $({}^s\theta', j, {}^s v, {}^t v) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}'} \implies ({}^s\theta', j, e_s[{}^s v/x], e_t[{}^t v/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}'}$ (S-A0)

   And it suffices to prove: $({}^s\theta, n, \lambda x.e_i) \in \lfloor((\tau_1' \to \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

   Again from Definition 3.9 it suffices to prove:
   $\forall {}^s\theta_1' \sqsupseteq {}^s\theta, {}^s v_1, {}^t v_1, k < n, \hat{\beta} \sqsubseteq \hat{\beta}_1'.$
   $({}^s\theta_1', k, {}^s v_1, {}^t v_1) \in \lfloor \tau_1' \rfloor_V^{\hat{\beta}_1'} \implies ({}^s\theta_1', k, e_s[{}^s v_1/x], e_t[{}^t v_1/x]) \in \lfloor \tau_2' \rfloor_E^{\hat{\beta}_1'}$

   This means that given some ${}^s\theta_1' \sqsubseteq {}^s\theta, {}^s v_1, {}^t v_1, k < n, \hat{\beta} \sqsubseteq \hat{\beta}_1'$ s.t $({}^s\theta_1', k, {}^s v_1, {}^t v_1) \in \lfloor \tau_1' \rfloor_V^{\hat{\beta}'}$

   And we are required to prove: $({}^s\theta_1', k, e_s[{}^s v_1/x], e_t[{}^t v_1/x]) \in \lfloor \tau_2' \rfloor_E^{\hat{\beta}_1'}$

   IH: $\lfloor(\tau_1'\ \sigma)\rfloor_V^{\hat{\beta}_1'} \subseteq \lfloor(\tau_1\ \sigma)\rfloor_V^{\hat{\beta}_1'}$ (Statement (1))
   $\lfloor(\tau_2\ \sigma)\rfloor_E^{\hat{\beta}_1'} \subseteq \lfloor(\tau_2'\ \sigma)\rfloor_E^{\hat{\beta}_1'}$ (Sub-A0, From Statement (2))

   Instantiating (S-A0) with ${}^s\theta_1', {}^s v_1, {}^t v_1, k, \hat{\beta}_1'$
   Since $({}^s\theta_1', k, {}^s v_1, {}^t v_1) \in \lfloor \tau_1'\ \sigma \rfloor_V^{\hat{\beta}}$ therefore from IH1 we know that $({}^s\theta_1', k, {}^s v_1, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}}$
   As a result we get
   $({}^s\theta_1', k, e_s[{}^s v_1/x], e_t[{}^t v_1/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}_1'}$
   From (Sub-A0), we know that
   $({}^s\theta_1', k, e_s[{}^s v_1/x], e_t[{}^t v_1/x]) \in \lfloor \tau_2'\ \sigma \rfloor_E^{\hat{\beta}_1'}$

2. SLIO*sub-prod:

   Given:

$$\frac{\Sigma;\Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma;\Psi \vdash \tau_2 <: \tau_2'}{\Sigma;\Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}$$

   To prove: $\lfloor((\tau_1 \times \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor((\tau_1' \times \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

   IH1: $\lfloor(\tau_1\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor(\tau_1'\ \sigma)\rfloor_V^{\hat{\beta}}$ (Statement (1))

IH2: $\lfloor(\tau_2\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor(\tau_2'\ \sigma)\rfloor_V^{\hat{\beta}}$ (Statement (1))

It suffices to prove:

$\forall({}^s\theta, n, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \in \lfloor((\tau_1 \times \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \in \lfloor((\tau_1' \times \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

This means that given $({}^s\theta, n, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \in \lfloor((\tau_1 \times \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}}$

Therefore from Definition 3.9 we are given:

$({}^s\theta, n, {}^s v_1, {}^t v_1) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}} \wedge ({}^s\theta, n, {}^s v_2, {}^t v_2) \in \lfloor\tau_2\ \sigma\rfloor_V^{\hat{\beta}}$ (S-P0)

And it suffices to prove: $({}^s\theta, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \in \lfloor((\tau_1' \times \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

Again from Definition 3.9, it suffices to prove:

$({}^s\theta, n, {}^s v_1, {}^t v_1) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}} \wedge ({}^s\theta, n, {}^s v_2, {}^t v_2) \in \lfloor\tau_2\ \sigma\rfloor_V^{\hat{\beta}}$

Since from (S-P0) we know that $({}^s\theta, n, {}^s v_1, {}^t v_1) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}}$ therefore from IH1 we have $({}^s\theta, n, {}^s v_1, {}^t v_1) \in \lfloor\tau_1'\ \sigma\rfloor_V^{\hat{\beta}}$

Similarly since from (S-P0) we have $({}^s\theta, n, {}^s v_2, {}^t v_2) \in \lfloor\tau_2\ \sigma\rfloor_V^{\hat{\beta}}$ therefore from IH2 we get $({}^s\theta, n, {}^s v_2, {}^t v_2) \in \lfloor\tau_2'\ \sigma\rfloor_V^{\hat{\beta}}$

3. SLIO*sub-sum:

   Given:

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'}$$

   To prove: $\lfloor((\tau_1 + \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor((\tau_1' + \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

   IH1: $\lfloor(\tau_1\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor(\tau_1'\ \sigma)\rfloor_V^{\hat{\beta}}$ (Statement (1))

   IH2: $\lfloor(\tau_2\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor(\tau_2'\ \sigma)\rfloor_V^{\hat{\beta}}$ (Statement (1))

   It suffices to prove: $\forall({}^s\theta, n, {}^s v, {}^t v) \in \lfloor((\tau_1 + \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, {}^s v, {}^t v) \in \lfloor((\tau_1' + \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

   This means that given: $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor((\tau_1 + \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}}$

   And it suffices to prove: $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor((\tau_1' + \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

   2 cases arise

   (a) ${}^s v = \mathsf{inl}\ {}^s v_i$ and ${}^t v = \mathsf{inl}\ {}^t v_i$:
   From Definition 3.9 we are given:
   $({}^s\theta, n, {}^s v_i, {}^t v_i) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}}$ (S-S0)
   And we are required to prove that:
   $({}^s\theta, n, {}^s v_i, {}^t v_i) \in \lfloor\tau_1'\ \sigma\rfloor_V^{\hat{\beta}}$
   From (S-S0) and IH1 we get
   $({}^s\theta, n, {}^s v_i, {}^t v_i) \in \lfloor\tau_1'\ \sigma\rfloor_V^{\hat{\beta}}$

(b) ${}^s v = \mathsf{inr}\ {}^s v_i$ and ${}^t v = \mathsf{inr}\ {}^t v_i$:
Symmetric reasoning

4. SLIO*sub-forall:
Given:

$$\frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash \forall \alpha.\tau_1 <: \forall \alpha.\tau_2}$$

To prove: $\lfloor ((\forall \alpha.\tau_1)\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\forall \alpha.\tau_2)\ \sigma \rfloor_V^{\hat{\beta}}$

It suffices to prove: $\forall ({}^s\theta, n, \Lambda e_s, \Lambda e_t) \in \lfloor ((\forall \alpha.\tau_1)\ \sigma) \rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, \Lambda e_s, \Lambda e_t) \in \lfloor ((\forall \alpha.\tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

This means that given: $({}^s\theta, n, \Lambda e_s, \Lambda e_t) \in \lfloor ((\forall \alpha.\tau_1)\ \sigma) \rfloor_V^{\hat{\beta}}$
Therefore from Definition 3.9 we are given:
$\forall {}^s\theta' \sqsupseteq {}^s\theta, j < n, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, e_s, e_t) \in \lfloor \tau_1[\ell'/\alpha]\ \sigma \rfloor_E^{\hat{\beta}'}$ (S-F0)

And it suffices to prove: $({}^s\theta, n, \Lambda e_s, \Lambda e_t) \in \lfloor ((\forall \alpha.\tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

Again from Definition 3.9, it suffices to prove:
$\forall {}^s\theta'_1 \sqsupseteq {}^s\theta, k < n, \ell'_1 \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}'_1.({}^s\theta'_1, k, e_s, e_t) \in \lfloor \tau_2[\ell'_1/\alpha]\ \sigma \rfloor_E^{\hat{\beta}'_1}$

This means that given ${}^s\theta_1 \sqsupseteq {}^s\theta, k < n, \ell'_1 \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}'_1$
And we are required to prove: $({}^s\theta'_1, k, e_s, e_t) \in \lfloor \tau_2[\ell'_1/\alpha]\ \sigma \rfloor_E^{\hat{\beta}'_1}$

Instantiating (S-F0) with ${}^s\theta_1, k, \ell'_1, \hat{\beta}'_1$ we get
$({}^s\theta'_1, k, e_s, e_t) \in \lfloor \tau_1[\ell'_1/\alpha]\ \sigma \rfloor_E^{\hat{\beta}'_1}$

$\lfloor (\tau_1\ (\sigma \cup [\alpha \mapsto \ell'])) \rfloor_E^{\hat{\beta}'_1} \subseteq \lfloor (\tau_2\ (\sigma \cup [\alpha \mapsto \ell'])) \rfloor_E^{\hat{\beta}'_1}$ (Sub-F0, Statement (2))

From (Sub-F0), we know that
$({}^s\theta'_1, k, e_s, e_t) \in \lfloor \tau_2[\ell'_1/\alpha]\ \sigma \rfloor_E^{\hat{\beta}'_1}$

5. SLIO*sub-constraint:
Given:

$$\frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash c_1 \Rightarrow \tau_1 <: c_2 \Rightarrow \tau_2}$$

To prove: $\lfloor ((c_1 \Rightarrow \tau_1)\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor ((c_2 \Rightarrow \tau_2))\ \sigma \rfloor_V^{\hat{\beta}}$

It suffices to prove: $\forall ({}^s\theta, n, \nu e_s, \nu e_t) \in \lfloor ((c_1 \Rightarrow \tau_1)\ \sigma) \rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, \nu e_s, \nu e_t) \in \lfloor ((c_2 \Rightarrow \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

This means that given: $({}^s\theta, n, \nu e_s, \nu e_t) \in \lfloor ((c_1 \Rightarrow \tau_1)\ \sigma) \rfloor_V^{\hat{\beta}}$
Therefore from Definition 3.9 we are given:

$$\mathcal{L} \models c_1\ \sigma \implies \forall^s\theta' \sqsupseteq {}^s\theta, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, e_s, e_t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}'} \qquad \text{(S-C0)}$$

And it suffices to prove: $({}^s\theta, n, \nu e_s, \nu e_t) \in \lfloor ((c_2 \Rightarrow \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

Again from Definition 3.9, it suffices to prove:

$\mathcal{L} \models c_2\ \sigma \implies \forall^s\theta'_1 \sqsupseteq {}^s\theta, k < n, \hat{\beta} \sqsubseteq \hat{\beta}'_1.({}^s\theta'_1, k, e_s, e_t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}'_1}$

This means that given $\mathcal{L} \models c_2, {}^s\theta'_1 \sqsupseteq {}^s\theta, k < n, \hat{\beta} \sqsubseteq \hat{\beta}'_1$

And we are required to prove:

$({}^s\theta'_1, k, e_s, e_t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}'_1}$

since we know that $c_2 \implies c_1$ and since $\mathcal{L} \models c_2\ \sigma$ therefore $\mathcal{L} \models c_1\ \sigma$. Next we instantiate (S-C0) with ${}^s\theta'_1, k, \hat{\beta}'_1$ to get

$({}^s\theta'_1, k, e_s, e_t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}'_1}$

$\lfloor (\tau_1\ \sigma) \rfloor_E^{\hat{\beta}'_1} \subseteq \lfloor (\tau_2\ \sigma) \rfloor_E^{\hat{\beta}} \hat{\beta}'_1$ (Sub-C0, Statement (2))

Therefore from (Sub-C0), we get

$({}^s\theta'_1, k, e_s, e_t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}'_1}$

6. SLIO*sub-label:

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi \vdash \mathsf{Labeled}\ \ell\ \tau <: \mathsf{Labeled}\ \ell'\ \tau'}$$

To prove: $\lfloor ((\mathsf{Labeled}\ \ell\ \tau)\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor ((\mathsf{Labeled}\ \ell\ '\tau')\ \sigma) \rfloor_V^{\hat{\beta}}$

IH: $\lfloor (\tau\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau'\ \sigma) \rfloor_V^{\hat{\beta}}$ (Statement (1))

It suffices to prove:

$\forall ({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathsf{Labeled}\ \ell\ \tau)\ \sigma) \rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathsf{Labeled}\ \ell'\ \tau')\ \sigma) \rfloor_V^{\hat{\beta}}$

This means that given some $({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathsf{Labeled}\ \ell\ \tau)\ \sigma) \rfloor_V^{\hat{\beta}}$
Therefore from Definition 3.9 we are given:

$$\exists^s v', {}^tv'.{}^sv = \mathsf{Lb}_\ell({}^sv') \wedge {}^tv = \mathsf{inl}\ {}^tv' \wedge ({}^s\theta, m, {}^sv', {}^tv') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \qquad \text{(S-L0)}$$

And we are required to prove that

$({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathsf{Labeled}\ \ell'\ \tau')\ \sigma) \rfloor_V^{\hat{\beta}}$
From Definition 3.9 it suffices to prove

$\exists^s v', {}^tv'.{}^sv = \mathsf{Lb}_\ell({}^sv') \wedge {}^tv = \mathsf{inl}\ {}^tv' \wedge ({}^s\theta, m, {}^sv', {}^tv') \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}}$

We get this directly from (S-L0) and IH

7. SLIO*sub-CG:

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell_1' \sqsubseteq \ell_1 \qquad \Sigma; \Psi \vdash \ell_2 \sqsubseteq \ell_2'}{\Sigma; \Psi \vdash \mathbb{SLIO}\ \ell_1\ \ell_2\ \tau <: \mathbb{SLIO}\ \ell_1'\ \ell_2'\ \tau'}$$

To prove: $\lfloor ((\mathbb{SLIO}\ \ell_i\ \ell_2\ \tau)\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor ((\mathbb{SLIO}\ \ell_1'\ \ell_2'\ \tau')\ \sigma) \rfloor_V^{\hat{\beta}}$

It suffices to prove:

$\forall ({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathbb{SLIO}\ \ell_1\ \ell_2\ \tau)\ \sigma) \rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathbb{SLIO}\ \ell_1'\ \ell_2'\ \tau')\ \sigma) \rfloor_V^{\hat{\beta}}$

This means that given $({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathbb{SLIO}\ \ell_1\ \ell_2\ \tau)\ \sigma) \rfloor_V^{\hat{\beta}}$
Therefore from Definition 3.9 we are given:
$\forall {}^s\theta_e \sqsupseteq {}^s\theta, H_s, H_t, i, {}^sv', k \leq m, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(k, H_s, H_t) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_s, {}^sv) \Downarrow_i^f (H_s', {}^sv') \wedge i < k \implies$
$\exists H_t', {}^tv'.(H_t, {}^tv()) \Downarrow (H_t', {}^tv') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H_s', H_t') \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists {}^tv''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', k - i, {}^sv', {}^tv'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$ (S-M0)

And we are required to prove

$({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathbb{SLIO}\ \ell_1'\ \ell_2'\ \tau')\ \sigma) \rfloor_V^{\hat{\beta}}$

So again from Definition 3.9 we need to prove
$\forall {}^s\theta_{e1} \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i_1, {}^sv_1', k_1 \leq n, \hat{\beta} \sqsubseteq \hat{\beta}_1'.$
$(k_1, H_{s1}, H_{t1}) \overset{\hat{\beta}_1'}{\triangleright} ({}^s\theta_{e1}) \wedge (H_{s1}, {}^sv) \Downarrow_{i_1}^f (H_{s1}', {}^sv_1') \wedge i_1 < k_1 \implies$
$\exists H_{t1}', {}^tv_1'.(H_{t1}, {}^tv()) \Downarrow (H_{t1}', {}^tv_1') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_{e1}, \hat{\beta}_1' \sqsubseteq \hat{\beta}_1''.(k_1 - i_1, H_{s1}', H_{t1}') \overset{\hat{\beta}_1''}{\triangleright} {}^s\theta' \wedge$
$\exists {}^tv_1''.{}^tv_1' = \mathsf{inl}\ {}^tv_1'' \wedge ({}^s\theta', k_1 - i_1, {}^sv_1', {}^tv_1'') \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}_1''}$

This means we are given some ${}^s\theta_{e1} \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i_1, {}^sv_1', k_1 \leq n, \hat{\beta} \sqsubseteq \hat{\beta}_1'$ s.t $(k_1, H_{s1}, H_{t1}) \overset{\hat{\beta}_1'}{\triangleright}$ $({}^s\theta_{e1}) \wedge (H_{s1}, {}^sv_1) \Downarrow_{i_1}^f (H_{s1}', {}^sv_1') \wedge i_1 < k_1$

And we need to prove

$\exists H_{t1}', {}^tv_1'.(H_{t1}, {}^tv_1()) \Downarrow (H_{t1}', {}^tv_1') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_{e1}, \hat{\beta}_1' \sqsubseteq \hat{\beta}_1''.(k_1 - i_1, H_{s1}', H_{t1}') \overset{\hat{\beta}_1''}{\triangleright} {}^s\theta' \wedge$
$\exists {}^tv_1''.{}^tv_1' = \mathsf{inl}\ {}^tv_1'' \wedge ({}^s\theta', k_1 - i_1, {}^sv_1', {}^tv_1'') \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}_1''}$

We instantiate (S-M0) with ${}^s\theta_{e1}, H_{s1}, H_{t1}, i_1, {}^sv_1', k_1, \hat{\beta}_1'$ we get

$\exists H_t', {}^tv'.(H_t, {}^tv()) \Downarrow (H_t', {}^tv') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_{e1}, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H_s', H_t') \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists {}^tv''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', k - i, {}^sv', {}^tv'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$

IH: $\lfloor (\tau\ \sigma) \rfloor_V^{\hat{\beta}''} \subseteq \lfloor (\tau'\ \sigma) \rfloor_V^{\hat{\beta}} \hat{\beta}''$ (Statement (1))

Since we have $({}^s\theta', k - i, {}^sv', {}^tv'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$ therefore from IH we get $({}^s\theta', k - i, {}^sv', {}^tv'') \in$ $\lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}''}$

8. SLIO*sub-base:

   Trivial

Proof of Statement(2)

It suffice to prove that

$\forall({}^s\theta, n, e_s, e_t) \in \lfloor(\tau\ \sigma)\rfloor_E^{\hat{\beta}}.\ ({}^s\theta, n, e_s, e_t) \in \lfloor(\tau'\ \sigma)\rfloor_E^{\hat{\beta}}$

This means that we are given $({}^s\theta, n, e_s, e_t) \in \lfloor(\tau\ \sigma)\rfloor_E^{\hat{\beta}}$

From Definition 3.10 it means we have

$$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv.e_s \Downarrow_i {}^sv \implies$$
$$\exists H_t', {}^tv.(H_t, e_t) \Downarrow (H_t', {}^tv) \wedge ({}^s\theta, n-i, {}^sv, {}^tv) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta \qquad \text{(Sub-E0)}$$

And we need to prove

$({}^s\theta, n, e_s, e_t) \in \lfloor(\tau'\ \sigma)\rfloor_E^{\hat{\beta}}$

From Definition 3.10 we need to prove

$$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^sv_1.e_s \Downarrow_j {}^sv_1 \implies$$
$$\exists H_{t1}', {}^tv_1.(H_{t1}, e_t) \Downarrow (H_{t1}', {}^tv_1) \wedge ({}^s\theta, n-j, {}^sv_1, {}^tv_1) \in \lfloor\tau'\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H_{t1}') \overset{\hat{\beta}}{\triangleright} {}^s\theta$$

This further means that given H_{s1}, H_{t1} s.t $(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $j < n, {}^sv_1$ s.t $e_s \Downarrow_j {}^sv_1$

And it suffices to prove that

$\exists H_{t1}', {}^tv_1.(H_{t1}, e_t) \Downarrow (H_{t1}', {}^tv_1) \wedge ({}^s\theta, n-j, {}^sv_1, {}^tv_1) \in \lfloor\tau'\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H_{t1}') \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating (Sub-E0) with the given H_{s1}, H_{t1} and $j < n, {}^sv_1$. We get

$\exists H_t', {}^tv.(H_{t1}, e_t) \Downarrow (H_t', {}^tv) \wedge ({}^s\theta, n-j, {}^sv_1, {}^tv) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we have $({}^s\theta, n-j, {}^sv_1, {}^tv) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}}$ therefore from Statement(1) we get $({}^s\theta, n-j, {}^sv_1, {}^tv) \in \lfloor\tau'\ \sigma\rfloor_V^{\hat{\beta}}$

□

Theorem 3.20 (SLIO* $\rightsquigarrow$ FG: Deriving CG NI via compilation)**.** $\forall e_s, {}^sv_1, {}^sv_2, {}^sv_1', {}^sv_2', n_1, n_2, H_{s1}', H_{s2}'$.

let $\mathsf{bool} = (\mathsf{unit} + \mathsf{unit})$.

$\emptyset, \emptyset, x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e_s : \mathbb{SLIO}\ \bot\ \bot\ \mathsf{bool}\ \wedge$

$\emptyset, \emptyset, \emptyset \vdash {}^sv_1 : \mathsf{Labeled}\ \top\ \mathsf{bool} \wedge \emptyset, \emptyset, \emptyset \vdash {}^sv_2 : \mathsf{Labeled}\ \top\ \mathsf{bool}\ \wedge$

$(\emptyset, e_s[{}^sv_1/x]) \Downarrow_{n_1}^f (H_{s1}', {}^sv_1')\ \wedge$

$(\emptyset, e_s[{}^sv_2/x]) \Downarrow_{n_2}^f (H_{s2}', {}^sv_2')$

$\implies$

${}^sv_1' = {}^sv_2'$

Proof. From the CG to FG translation we know that $\exists e_t$ s.t

$\emptyset, \emptyset, x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e_s : \mathbb{SLIO}\ \bot\ \bot\ \mathsf{bool} \rightsquigarrow e_t$

Similarly we also know that $\exists {}^tv_1, , {}^tv_2$ s.t

$$\emptyset, \emptyset, \emptyset \vdash {}^sv_1 : \mathsf{Labeled}\ \top\ \mathsf{bool} \rightsquigarrow {}^tv_1 \text{ and } \emptyset, \emptyset, \emptyset \vdash {}^sv_2 : \mathsf{Labeled}\ \top\ \mathsf{bool} \rightsquigarrow {}^tv_2 \qquad \text{(NI-0)}$$

From type preservation theorem we know that

$\emptyset, \emptyset, x : ((\mathsf{unit} + \mathsf{unit})^\bot + \mathsf{unit})^\top \vdash_\top e_t : (\mathsf{unit} \overset{\bot}{\rightarrow} ((\mathsf{unit} + \mathsf{unit})^\bot + \mathsf{unit})^\bot)^\bot$

$\emptyset, \emptyset, \emptyset \vdash_\top {}^t v_1 : ((\mathsf{unit} + \mathsf{unit})^\perp + \mathsf{unit})^\top$
$\emptyset, \emptyset, \emptyset \vdash_\top {}^t v_2 : ((\mathsf{unit} + \mathsf{unit})^\perp + \mathsf{unit})^\top$ (NI-1)

Since we have $\emptyset, \emptyset, \emptyset \vdash {}^s v_1 : \mathsf{Labeled}\ \top\ \mathsf{bool} \rightsquigarrow {}^t v_1$
And since ${}^s v_1$ and ${}^t v_1$ are closed terms (from given and NI-1)
Therefore from Theorem 3.18 we have (we choose n s.t $n > n_1$ and $n > n_2$)
$(\emptyset, n, {}^s v_1, {}^t v_1) \in \lfloor \mathsf{Labeled}\ \top\ \mathsf{bool} \rfloor_E^{\emptyset}$ (NI-2)
And therefore from Definition 3.14 and (NI-2) we have
$(\emptyset, n, (x \mapsto {}^s v_1), (x \mapsto {}^t v_1)) \in \lfloor x \mapsto \mathsf{Labeled}\ \top\ \mathsf{bool} \rfloor_V^{\emptyset}$

From (NI-0) we know that $\emptyset, \emptyset, x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e_s : \mathbb{SLIO}\ \perp\ \perp\ \mathsf{bool} \rightsquigarrow e_t$
Therefore we can apply Theorem 3.18 to get
$(\emptyset, n, e_s[{}^s v_1/x], e_t[{}^t v_1/x]) \in \lfloor \mathbb{SLIO}\ \perp\ \perp\ \mathsf{bool} \rfloor_E^{\emptyset}$ (NI-3.1)
Applying Definition 3.10 on (NI-3.1) we get

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}}{\triangleright} \emptyset \wedge \forall i < n. e_s[{}^s v_1/x] \Downarrow_i {}^s v \implies$
$\exists H'_{t2}, {}^t v.(H_{t2}, e_t[{}^t v_1/x]) \Downarrow (H'_{t2}, {}^t v) \wedge (\emptyset, n-i, {}^s v, {}^t v) \in \lfloor \mathbb{SLIO}\ \perp\ \perp\ \mathsf{bool} \rfloor_V^{\hat{\beta}} \wedge (n-i, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} \emptyset$

Instantiating with $\emptyset, \emptyset$. From SLIO*-Sem-val we know that $i = 0$ and ${}^s v = e_s[{}^s v_1/x]$.

Therefore we have
$\exists H'_{t2}, {}^t v.(H_{t2}, e_t[{}^t v_1/x]) \Downarrow (H'_{t2}, {}^t v) \wedge (\emptyset, n, {}^s v, {}^t v) \in \lfloor \mathbb{SLIO}\ \perp\ \perp\ \mathsf{bool} \rfloor_V^{\hat{\beta}} \wedge (n, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} \emptyset$

From translation and from (NI-1) we know that ${}^t v = e_t[{}^t v_1/x] = \lambda\_.e_{b1}$ and therefore from fg-val we have $H'_{t2} = \emptyset$

Therefore we have
$(\emptyset, n, e_s[{}^s v_1/x], \lambda\_.e_{b1}) \in \lfloor \mathbb{SLIO}\ \perp\ \perp\ \mathsf{bool} \rfloor_V^{\emptyset}$

Expanding $(\emptyset, n, e_s[{}^s v_1/x], \lambda\_.e_{b1}) \in \lfloor \mathbb{SLIO}\ \perp\ \perp\ \mathsf{bool} \rfloor_V^{\emptyset}$ using Definition 3.9 we get

$\forall {}^s\theta_e \sqsupseteq \emptyset, H_{s3}, H_{t3}, i, {}^s v'', k \leq n, \emptyset \sqsubseteq \hat{\beta}'.$
$(k, H_{s3}, H_{t3}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s3}, e_s[{}^s v_1/x]) \Downarrow_i^f (H'_{s1}, {}^s v''_1) \wedge i < k \implies$
$\exists H''_{t1}, {}^t v'', (H_{t3}, (\lambda\_.e_{b1})()) \Downarrow (H''_{t1}, {}^t v''_1) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H'_{s1}, H''_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge \exists {}^t v'''_1. {}^t v''_1 = \mathsf{inl}\ {}^t v'''_1 \wedge ({}^s\theta', k-i, {}^s v''_1, {}^t v'''_1) \in \lfloor \mathsf{bool} \rfloor_V^{\hat{\beta}''}$

Instantiating with $\emptyset, \emptyset, \emptyset, n_1, {}^s v'_1, n, \emptyset$ we get

$\exists H''_{t1}, {}^t v''.(\emptyset, (\lambda\_.e_{b1})()) \Downarrow (H''_{t1}, {}^t v''_1) \wedge \exists {}^s\theta' \sqsupseteq \emptyset, \emptyset \sqsubseteq \hat{\beta}''.(n-n_1, H'_{s1}, H''_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge \exists {}^t v'''_1. {}^t v''_1 = \mathsf{inl}\ {}^t v'''_1 \wedge ({}^s\theta', n-n_1, {}^s v'_1, {}^t v'''_1) \in \lfloor \mathsf{bool} \rfloor_V^{\hat{\beta}''}$ (NI-3.2)

Since we have $\exists {}^t v'''_1. {}^t v''_1 = \mathsf{inl}\ {}^t v'''_1 \wedge ({}^s\theta', n-n_1, {}^s v'_1, {}^t v'''_1) \in \lfloor (\mathsf{unit} + \mathsf{unit}) \rfloor_V^{\hat{\beta}''}$, therefore from Definition 3.9 we know that 2 cases arise

- ${}^s v'_1 = \mathsf{inl}^s v'_{i1}$ and ${}^t v'''_1 = \mathsf{inl}^t v'_{i1}$:
  And from Definition 3.9 we know that
  $({}^s\theta', n-n_1, {}^s v'_{i1}, {}^t v'_{i1}) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}''}$
  which means ${}^s v'_{i1} = {}^t v'_{i1} = ()$
- ${}^s v'_1 = \mathsf{inr}^s v'_{i1}$ and ${}^t v'''_1 = \mathsf{inr}^t v'_{i1}$:
  Same reasoning as in the previous case

Thus no matter which case occurs we have ${}^s v_1' = {}^t v_1'''$ (NI-3.3)

Similarly we can apply Theorem 3.18 with the other substitution to get
$(\emptyset, n, e_s[{}^s v_2/x], e_t[{}^t v_2/x]) \in \lfloor \mathbb{SLIO} \perp \perp \mathsf{bool} \rfloor_E^{\emptyset}$ (NI-4.1)

Applying Definition 3.10 on (NI-4.1) we get

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}}{\triangleright} \emptyset \wedge \forall i < n, {}^s v_s.e_s[{}^s v_2/x] \Downarrow_i {}^s v_s \implies \exists H'_{t2}, {}^t v_s.(H_{t2}, e_t[{}^t v_2/x]) \Downarrow (H'_{t2}, {}^t v_s) \wedge (\emptyset, n-i, {}^s v_s, {}^t v_s) \in \lfloor \mathbb{SLIO} \perp \perp \mathsf{bool} \rfloor_V^{\hat{\beta}} \wedge (n-i, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} \emptyset$

Instantiating with $\emptyset, \emptyset$. From SLIO*-Sem-val we know that $i = 0$ and ${}^s v_s = e_s[{}^s v_2/x]$.

Therefore we have

$\exists H'_{t2}, {}^t v_s.(H_{t2}, e_t[{}^t v_2/x]) \Downarrow (H'_{t2}, {}^t v_s) \wedge (\emptyset, n, {}^s v_s, {}^t v_s) \in \lfloor \mathbb{SLIO} \perp \perp \mathsf{bool} \rfloor_V^{\hat{\beta}} \wedge (n, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} \emptyset$

Also from (NI-1) and from translation we know that ${}^t v = e_t[{}^t v_2/x] = \lambda\_.e_{b2}$ and therefore from fg-val we know that $H'_{t2} = \emptyset$

Therefore we have
$(\emptyset, n, e_s[{}^s v_2/x], \lambda\_.e_{b2}) \in \lfloor \mathbb{SLIO} \perp \perp \mathsf{bool} \rfloor_V^{\emptyset}$

Expanding $(\emptyset, n, e_s[{}^s v_2/x], \lambda x.e_{b2}) \in \lfloor \mathbb{SLIO} \perp \perp \mathsf{bool} \rfloor_V^{\emptyset}$ using Definition 3.9 we get

$\forall {}^s\theta_e \sqsupseteq \emptyset, H_{s3}, H_{t3}, i, {}^s v'', k \leq n, \emptyset \sqsubseteq \hat{\beta}'.$
$(k, H_{s3}, H_{t3}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s3}, e_s[{}^s v_2/x]) \Downarrow_i^f (H'_{s2}, {}^s v_2'') \wedge i < k \implies$
$\exists H''_{t2}, {}^t v'', (H_{t3}, (\lambda\_.e_{b2})()) \Downarrow (H''_{t2}, {}^t v_2'') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H'_{s2}, H''_{t2}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge \exists {}^t v_2'''.{}^t v_2'' = \mathsf{inl}\ {}^t v_2''' \wedge ({}^s\theta', k-i, {}^s v_1'', {}^t v_2''') \in \lfloor \mathsf{bool} \rfloor_V^{\hat{\beta}''}$

Instantiating with $\emptyset, \emptyset, \emptyset, n_2, {}^s v_2', n, \emptyset$ we get

$\exists H''_{t2}, {}^t v''.(\emptyset, (\lambda\_.e_{b2})()) \Downarrow (H''_{t2}, {}^t v_2'') \wedge \exists {}^s\theta' \sqsupseteq \emptyset, \emptyset \sqsubseteq \hat{\beta}''.(n-n_1, H'_{s2}, H''_{t2}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge \exists {}^t v_2'''.{}^t v_2'' = \mathsf{inl}\ {}^t v_2''' \wedge ({}^s\theta', n-n_1, {}^s v_1', {}^t v_2''') \in \lfloor \mathsf{bool} \rfloor_V^{\hat{\beta}''}$ (NI-4.2)

Since we have $\exists {}^t v_2'''.{}^t v_2'' = \mathsf{inl}\ {}^t v_2''' \wedge ({}^s\theta', n-n_1, {}^s v_2', {}^t v_2''') \in \lfloor \mathsf{bool} \rfloor_V^{\hat{\beta}''}$, therefore from Definition 3.9 2 cases arise

- ${}^s v_2' = \mathsf{inl}^s v_{i2}'$ and ${}^t v_2''' = \mathsf{inl}^t v_{i2}'$:
  And from Definition 3.9 we know that
  $({}^s\theta', n-n_1, {}^s v_{i2}', {}^t v_{i2}') \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}''}$
  which means ${}^s v_{i2}' = {}^t v_{i2}' = ()$
- ${}^s v_2' = \mathsf{inr}^s v_{i2}'$ and ${}^t v_2''' = \mathsf{inr}^t v_{i2}'$:
  Same reasoning as in the previous case

Thus no matter which case occurs we have ${}^s v_2' = {}^t v_2'''$ (NI-4.3)

From SLIO* to FG translation we know that $\exists {}^t v_{i1}.{}^t v_1 = \mathsf{inl}\ {}^t v_{i1}$ and similarly $\exists {}^t v_{i2}.{}^t v_2 = \mathsf{inl}\ {}^t v_{i2}$

From (NI-1) since $\emptyset, \emptyset, \emptyset \vdash_\top {}^t v_1 : (\mathsf{bool}^\perp + \mathsf{unit})^\top$ therefore from SLIO*-inl we know that $\emptyset, \emptyset, \emptyset \vdash_\top {}^t v_{i1} : \mathsf{bool}^\perp$

And from SLIO*sub-sum we know that $\emptyset, \emptyset, \emptyset \vdash_\top {}^t v_{i1} : \mathsf{bool}^\top$
Therefore we also have $\emptyset, \emptyset, \emptyset \vdash_\bot {}^t v_{i1} : \mathsf{bool}^\top$ (NI-5.1)

Similarly we also have $\emptyset, \emptyset, \emptyset \vdash_\bot {}^t v_{i2} : \mathsf{bool}^\top$ (NI-5.2)

Next, let $e_T = (\lambda x : (\mathsf{bool}^\bot + \mathsf{unit})^\top.\mathsf{case}(e_t(), y.y, z.{}^t v_b))\ (\mathsf{case}(u, -.\mathsf{inl}\ true, -.\mathsf{inl}\ false)) : \mathsf{bool}^\bot$
where $true = \mathsf{inl}\ ()$ and $false = \mathsf{inr}\ ()$

We claim $\emptyset, \emptyset, u : \mathsf{bool}^\top \vdash_\bot e_T : \mathsf{bool}^\bot$

To show this we give its typing derivation
P2.3:

$$\dfrac{\dfrac{\dfrac{}{\emptyset, \emptyset, u : \mathsf{bool}^\top, - \vdash_\bot false : \mathsf{bool}^\bot}\text{FG-inl}}{\emptyset, \emptyset, u : \mathsf{bool}^\top, - \vdash_\bot \mathsf{inl}\ false : (\mathsf{bool}^\bot + \mathsf{unit})^\bot}\text{FG-inl}}{\emptyset, \emptyset, u : \mathsf{bool}^\top, - \vdash_\bot \mathsf{inl}\ false : (\mathsf{bool}^\bot + \mathsf{unit})^\top}\text{FGSub-base}$$

P2.2:

$$\dfrac{\dfrac{\dfrac{}{\emptyset, \emptyset, u : \mathsf{bool}^\top, - \vdash_\bot true : \mathsf{bool}^\bot}\text{FG-inl}}{\emptyset, \emptyset, u : \mathsf{bool}^\top, - \vdash_\bot \mathsf{inl}\ true : (\mathsf{bool}^\bot + \mathsf{unit})^\bot}\text{FG-inl}}{\emptyset, \emptyset, u : \mathsf{bool}^\top, - \vdash_\bot \mathsf{inl}\ true : (\mathsf{bool}^\bot + \mathsf{unit})^\top}\text{FGSub-base}$$

P2.1:

$$\dfrac{}{\emptyset, \emptyset, u : \mathsf{bool}^\top \vdash_\bot u : \mathsf{bool}^\top}$$

P2:

$$\dfrac{P2.1 \qquad P2.2 \qquad P2.3 \qquad \dfrac{}{\emptyset, \emptyset \models (\mathsf{bool}^\bot + \mathsf{unit})^\top \searrow \bot}}{\emptyset, \emptyset, u : \mathsf{bool}^\top \vdash_\bot (\mathsf{case}(u, -.\mathsf{inl}\ true, -.\mathsf{inl}\ false)) : (\mathsf{bool}^\bot + \mathsf{unit})^\top}$$

P1.2:

$$\dfrac{\dfrac{}{\emptyset, \emptyset, u : \mathsf{bool}^\top, x : (\mathsf{bool}^\bot + \mathsf{unit})^\top \vdash_\bot e_t : (\mathsf{unit} \xrightarrow{\bot} (\mathsf{bool}^\bot + \mathsf{unit})^\bot)^\bot}\text{NI-1} \quad \dfrac{}{\emptyset, \emptyset, u : \mathsf{bool}^\top, x : (\mathsf{bool}^\bot + \mathsf{unit})^\top \vdash_\bot () : \mathsf{unit}}\text{FG-unit} \quad \dfrac{}{\emptyset, \emptyset \models \bot \sqcup \bot \sqsubseteq \bot} \quad \dfrac{}{\emptyset, \emptyset \models (\mathsf{bool}^\bot + \mathsf{unit})^\bot \searrow \bot}}{\emptyset, \emptyset, u : \mathsf{bool}^\top, x : (\mathsf{bool}^\bot + \mathsf{unit})^\top \vdash_\bot e_t() : (\mathsf{bool}^\bot + \mathsf{unit})^\bot}\text{FG-app}$$

P1.1:

$$\dfrac{P1.2 \quad \dfrac{}{\emptyset, \emptyset, u : \mathsf{bool}^\top, x : (\mathsf{bool}^\bot + \mathsf{unit})^\top, y : \mathsf{bool}^\bot \vdash_\bot y : \mathsf{bool}^\bot}\text{FG-var} \quad \dfrac{}{\emptyset, \emptyset, u : \mathsf{bool}^\top, x : (\mathsf{bool}^\bot + \mathsf{unit})^\top, z : \mathsf{unit} \vdash_\bot false : \mathsf{bool}^\bot}\text{FG-var} \quad \dfrac{}{\emptyset, \emptyset \models \mathsf{bool}^\bot \searrow \bot}}{\emptyset, \emptyset, u : \mathsf{bool}^\top, x : (\mathsf{bool}^\bot + \mathsf{unit})^\top \vdash_\bot \mathsf{case}(e_t(), y.y, z.{}^t v_b) : \mathsf{bool}^\bot}\text{FG-case}$$

P1:

$$\dfrac{\dfrac{P1.1}{\emptyset, \emptyset, u : \mathsf{bool}^\top, x : (\mathsf{bool}^\bot + \mathsf{unit})^\top \vdash_\bot \mathsf{case}(e_t(), y.y, z.{}^t v_b) : \mathsf{bool}^\bot}}{\emptyset, \emptyset, u : \mathsf{bool}^\top \vdash_\bot (\lambda x : (\mathsf{bool}^\bot + \mathsf{unit})^\top.\mathsf{case}(e_t(), y.y, z.{}^t v_b)) : ((\mathsf{bool}^\bot + \mathsf{unit})^\top \xrightarrow{\bot} \mathsf{bool}^\bot)^\bot}$$

Main derivation:

$$\dfrac{P1 \qquad P2 \qquad \dfrac{}{\emptyset, \emptyset \models \bot \sqcup \bot \sqsubseteq \bot} \qquad \dfrac{}{\emptyset, \emptyset \models \mathsf{bool}^{\bot} \searrow \bot}}{\emptyset, \emptyset, u : \mathsf{bool}^{\top} \vdash_{\bot} (\lambda x : (\mathsf{bool}^{\bot} + \mathsf{unit})^{\top}.\mathsf{case}(e_t(), y.y, z.{}^{t}v_b))\ (\mathsf{case}(u, -.\mathsf{inl}\ true, -.\mathsf{inl}\ false)) : \mathsf{bool}^{\bot}} \text{ FG-app}$$

Assuming $e_{b1}()$ reduces in n_{t1} steps in (NI-3.2) and $e_{b2}()$ reduces in n_{t2} steps in (NI-4.2).

We instantiate Theorem 1.29 with $e_T, {}^{t}v_{i1}, {}^{t}v_{i2}$, $n_{t1}+2, n_{t2}+2$, H''_{t1}, H''_{t2} and $\bot$ and therefore from (NI-3.3) and (NI-4.3) we get ${}^{t}v'''_1 = {}^{t}v'''_2$ and thus ${}^{s}v'_1 = {}^{s}v'_2$

□

3.2 Translation from FG to FG$^-$

3.2.1 FG$^-$ typesystem

Lemma 3.21 (FG$^-$: Reflexivity of subtyping)**.** *The following hold:*

1. *For all* Σ, Ψ, τ*:* $\Sigma; \Psi \vdash \tau <: \tau$
2. *For all* Σ, Ψ, A*:* $\Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}$

Proof. Proof by simultaneous induction on τ and A.

Proof of statement (1)

Let $\tau = \mathsf{A}^\ell$. Then, we have:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}}\text{IH(2)} \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell}{\Sigma; \Psi \vdash \mathsf{A}^\ell <: \mathsf{A}^\ell}\text{FGsub-label}$$

Proof of statement (2)

We proceed by cases on A.

1. $\mathsf{A} = \mathsf{b}$:

$$\dfrac{}{\Sigma; \Psi \vdash \mathsf{b} <: \mathsf{b}}\text{FGsub-base}$$

2. $\mathsf{A} = \mathsf{ref}\ \tau$:

$$\dfrac{}{\Sigma; \Psi \vdash \mathsf{ref}\ \tau <: \mathsf{ref}\ \tau}\text{FGsub-ref}$$

3. $\mathsf{A} = \tau_1 \times \tau_2$:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\text{IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\text{IH(1) on } \tau_2}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1 \times \tau_2}$$

4. $\mathsf{A} = \tau_1 + \tau_2$:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\text{IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\text{IH(1) on } \tau_2}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1 + \tau_2}$$

5. $\mathsf{A} = \tau_1 \xrightarrow{\ell_e} \tau_2$:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\text{IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash \tau_2 <: \tau_2}\text{IH(2) on } \tau_2 \qquad \dfrac{}{\Sigma; \Psi \vdash \ell_e \sqsubseteq \ell_e}}{\Sigma; \Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1 \xrightarrow{\ell_e} \tau_2}$$

6. $\mathsf{A} = \mathsf{unit}$:

$$\dfrac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}}$$

Type system: $\boxed{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau}$

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \tau' \searrow pc}{\Sigma; \Psi; \Gamma, x : \tau \vdash_{pc} x : \tau'} \text{ FG}^{-}\text{-var} \qquad \frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{\ell_e} e : \tau_2}{\Sigma; \Psi; \Gamma \vdash_{pc} \lambda x.e : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{pc}} \text{ FG}^{-}\text{-lam}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 \searrow \ell \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1\ e_2 : \tau_2} \text{ FG}^{-}\text{-app}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : \tau_1 \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_2}{\Sigma; \Psi; \Gamma \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^{pc}} \text{ FG}^{-}\text{-prod}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^{\ell} \qquad \Sigma; \Psi \vdash \tau_1 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{fst}(e) : \tau_1} \text{ FG}^{-}\text{-fst} \qquad \frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau_1}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inl}(e) : (\tau_1 + \tau_2)^{pc}} \text{ FG}^{-}\text{-inl}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 + \tau_2)^{\ell} \qquad \Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_1 : \tau \qquad \Sigma; \Psi; \Gamma, y : \tau_2 \vdash_{pc \sqcup \ell} e_2 : \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{case}(e, x.e_1, y.e_2) : \tau} \text{ FG}^{-}\text{-case}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc'} e : \tau' \qquad \Sigma; \Psi \vdash pc \sqsubseteq pc' \qquad \Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau} \text{ FG}^{-}\text{-sub}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau \qquad \Sigma; \Psi \vdash \tau \searrow pc}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{new}\ e : (\mathsf{ref}\ \tau)^{pc}} \text{ FG}^{-}\text{-ref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\mathsf{ref}\ \tau)^{\ell} \qquad \Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \tau' \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} !e : \tau'} \text{ FG}^{-}\text{-deref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\mathsf{ref}\ \tau)^{\ell} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau \qquad \Sigma; \Psi \vdash \tau \searrow (pc \sqcup \ell)}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 := e_2 : \mathsf{unit}^{pc}} \text{ FG}^{-}\text{-assign}$$

$$\frac{}{\Sigma; \Psi; \Gamma \vdash_{pc} () : \mathsf{unit}^{pc}} \text{ FG}^{-}\text{-unitI} \qquad \frac{\Sigma, \alpha; \Psi; \Gamma \vdash_{\ell_e} e : \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} \Lambda e : (\forall \alpha.(\ell_e, \tau))^{pc}} \text{ FG}^{-}\text{-FI}$$

$$\frac{\begin{array}{c} \Sigma; \Psi; \Gamma \vdash_{pc} e : (\forall \alpha.(\ell_e, \tau))^{\ell} \\ FV(\ell') \subseteq \Sigma \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e[\ell'/\alpha] \qquad \Sigma; \Psi \vdash \tau[\ell'/\alpha] \searrow \ell \end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} e\ [] : \tau[\ell'/\alpha]} \text{ FG}^{-}\text{-FE}$$

$$\frac{\Sigma; \Psi, c; \Gamma \vdash_{\ell_e} e : \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} \nu\ e : (c \overset{\ell_e}{\Rightarrow} \tau)^{pc}} \text{ FG}^{-}\text{-CI}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell} \qquad \Sigma; \Psi \vdash c \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e \qquad \Sigma; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e \bullet : \tau} \text{ FG}^{-}\text{-CE}$$

Figure 8: Type system for FG^{-}

$$\frac{\Sigma; \Psi \vdash \ell \sqsubseteq \ell' \qquad \Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}'}{\Sigma; \Psi \vdash \mathsf{A}^{\ell} <: \mathsf{A}'^{\ell'}} \text{ FG}^{-}\text{sub-label} \qquad \frac{}{\Sigma; \Psi \vdash \mathsf{b} <: \mathsf{b}} \text{ FG}^{-}\text{sub-base}$$

$$\frac{}{\Sigma; \Psi \vdash \mathsf{ref}\ \tau <: \mathsf{ref}\ \tau} \text{ FG}^{-}\text{sub-ref} \qquad \frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'} \text{ FG}^{-}\text{sub-prod}$$

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'} \text{ FG}^{-}\text{sub-sum}$$

$$\frac{\Sigma; \Psi \vdash \tau_1' <: \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2' \qquad \Sigma; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'} \text{ FG}^{-}\text{sub-arrow}$$

$$\frac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}} \text{ FG}^{-}\text{sub-unit} \qquad \frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash \forall \alpha.\tau_1 <: \forall \alpha.\tau_2} \text{ FG}^{-}\text{sub-forall}$$

$$\frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi, c_2 \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash c_1 \Rightarrow \tau_1 <: c_2 \Rightarrow \tau_2} \text{ FG}^{-}\text{sub-constraint}$$

Figure 9: FG^{-} subtyping

7. $\mathsf{A} = \forall \alpha.\tau_i$:

$$\frac{\overline{\Sigma, \alpha; \Psi \vdash \tau_i <: \tau_i} \text{ IH(1) on } \tau_i}{\Sigma; \Psi \vdash \forall \alpha.\tau_i <: \forall \alpha.\tau_i}$$

8. $\mathsf{A} = c \Rightarrow \tau_i$:

$$\frac{\overline{\Sigma; \Psi \vdash c \implies c} \qquad \overline{\Sigma; \Psi, c \vdash \tau_i <: \tau_i} \text{ IH(1) on } \tau_i}{\Sigma; \Psi \vdash c \Rightarrow \tau <: c \Rightarrow \tau_i}$$

□

3.2.2 Type translation

We define a translation of types, indexed by a label ℓ (which represents a *pc* joined with all outer labels) below. This is written $[\![\tau]\!]_{\ell}$.

Definition 3.22 (FG $\rightsquigarrow$ FG$^-$: Type translation)**.**

$$
\begin{array}{lcl}
[\![\mathsf{b}]\!]_\ell & = & \mathsf{b} \\
[\![\tau_1 \xrightarrow{\ell_e} \tau_2]\!]_\ell & = & \forall\alpha.\alpha, (\forall\beta.\alpha, ((\ell \sqsubseteq \alpha \sqsubseteq \ell_e \wedge \beta \sqsubseteq \alpha) \overset{\alpha}{\Rightarrow} ([\![\tau_1]\!]_\beta \overset{\alpha}{\to} [\![\tau_2]\!]_\alpha)^\alpha)^\alpha)^\alpha \\
[\![\tau_1 \times \tau_2]\!]_\ell & = & [\![\tau_1]\!]_\ell \times [\![\tau_2]\!]_\ell \\
[\![\tau_1 + \tau_2]\!]_\ell & = & [\![\tau_1]\!]_\ell + [\![\tau_2]\!]_\ell \\
[\![\mathsf{ref}\ \tau]\!]_\ell & = & \mathsf{ref}\ [\![\tau]\!]_\bot \\
[\![\mathsf{unit}]\!]_\ell & = & \mathsf{unit} \\
[\![\forall\gamma.(\ell_e, \tau)]\!]_\ell & = & \forall\alpha.\alpha, ((\ell \sqsubseteq \alpha \sqsubseteq \ell_e) \overset{\alpha}{\Rightarrow} (\forall\gamma.\alpha, [\![\tau]\!]_\alpha)^\alpha)^\alpha \\
[\![c \overset{\ell_e}{\Rightarrow} \tau]\!]_\ell & = & \forall\alpha.\alpha, (((c \wedge \ell \sqsubseteq \alpha \sqsubseteq \ell_e) \overset{\alpha}{\Rightarrow} [\![\tau]\!]_\alpha)^\alpha)^\alpha \\
 & & \\
[\![\mathsf{A}^{\ell'}]\!]_\ell & = & ([\![\mathsf{A}]\!]_{\ell \sqcup \ell'})^{\ell \sqcup \ell'}
\end{array}
$$

Translation judgement:

$\boxed{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau \rightsquigarrow \Sigma; \Psi; \Gamma' \vdash_{pc'} e_M : [\![\tau]\!]_{pc'}}$ where

$pc' \sqsubseteq pc$ and $\forall i \in 1 \ldots n.\ell_i \sqsubseteq pc'$

$\Gamma = x_1 : \tau_1, \ldots, x_n : \tau_n$

$\Gamma' = x_1 : [\![\tau_1]\!]_{\ell_1}, \ldots, x_n : [\![\tau_n]\!]_{\ell_n}$

3.2.3 Type preservation: FG to FG$^-$

Theorem 3.23 (FG $\rightsquigarrow$ FG$^-$: Type preservation)**.** *Suppose (1) $\Gamma = x_1 : \tau_1, \ldots, x_n : \tau_n$ and (2) $\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau$ in FG. Suppose $\ell_1, \ldots, \ell_n$ and pc' are arbitrary labels with free variables in Σ such that (3) $\Sigma; \Psi \vdash pc' \sqsubseteq pc$ and (4) For each $i \in [1, n]$, $\Sigma; \Psi \vdash \ell_i \sqsubseteq pc'$.*

Let Γ' be the FG$^-$ context $x_1 : [\![\tau_1]\!]_{\ell_1}, \ldots, x_n : [\![\tau_n]\!]_{\ell_n}$. Then, $\Sigma; \Psi; \Gamma' \vdash_{pc'} e : [\![\tau]\!]_{pc'}$ in FG$^-$.

Proof. Proof by induction on the $\rightsquigarrow$ relation

1. var:

$$\frac{}{\Sigma; \Psi; \Gamma \vdash_{pc} x : \tau \rightsquigarrow \Sigma; \Psi; \Gamma' \vdash_{pc'} x : [\![\tau]\!]_{pc'}}\ \text{var}$$

$$\frac{[\![\tau]\!]_{\ell_n} <: [\![\tau]\!]_{pc'}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} x : [\![\tau]\!]_{pc'}}$$

2. lam:

$$\frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{\ell_e} e : \tau_2 \rightsquigarrow \Sigma; \Psi; \Gamma, x : [\![\tau_1]\!]_{\ell_{n+1}} \vdash_{\ell'_e} e_m : [\![\tau_2]\!]_{\ell'_e} \qquad \ell_{n+1} \sqsubseteq \ell'_e \sqsubseteq \ell_e}{\Sigma; \Psi; \Gamma \vdash_{pc} \lambda x.e : (\tau_1 \xrightarrow{\ell_e} \tau_2)^\bot \rightsquigarrow \Sigma; \Psi; \Gamma' \vdash_{pc'} e_M : T_1}\ \text{lam}$$

$T_1 = (\forall\alpha.\alpha, (\forall\beta.\alpha, ((pc' \sqsubseteq \alpha \sqsubseteq \ell_e \wedge \beta \sqsubseteq \alpha) \overset{\alpha}{\Rightarrow} ([\![\tau_1]\!]_\beta \overset{\alpha}{\to} [\![\tau_2]\!]_\alpha)^\alpha)^\alpha)^\alpha)^{pc'}$

$T_{1.1} = (\forall\beta.\alpha, ((pc' \sqsubseteq \alpha \sqsubseteq \ell_e \wedge \beta \sqsubseteq \alpha) \overset{\alpha}{\Rightarrow} ([\![\tau_1]\!]_\beta \overset{\alpha}{\to} [\![\tau_2]\!]_\alpha)^\alpha)^\alpha)^\alpha$

$T_{1.2} = ((pc' \sqsubseteq \alpha \sqsubseteq \ell_e \wedge \beta \sqsubseteq \alpha) \overset{\alpha}{\Rightarrow} ([\![\tau_1]\!]_\beta \overset{\alpha}{\to} [\![\tau_2]\!]_\alpha)^\alpha)^\alpha$

$T_{1.3} = ([\![\tau_1]\!]_\beta \overset{\alpha}{\to} [\![\tau_2]\!]_\alpha)^\alpha$

$c_1 = (pc' \sqsubseteq \alpha \sqsubseteq \ell_e \wedge \beta \sqsubseteq \alpha)$

P1:

$$\dfrac{\dfrac{\overline{\Sigma;\Psi;\Gamma,x:\tau_1 \vdash_{\ell_e} e:\tau_2}\text{ Given}}{\Sigma,\alpha,\beta;\Psi,c_1;\Gamma,x:\tau_1 \vdash_{\ell_e} e:\tau_2}\text{ Weakening}}{\Sigma,\alpha,\beta;\Psi,c_1;\Gamma',x:[\![\tau_1]\!]_\beta \vdash_\alpha e_m:[\![\tau_2]\!]_\alpha}\text{ IH}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{P1}{\Sigma,\alpha,\beta;\Psi,c_1;\Gamma' \vdash_\alpha \lambda x.e_m : T_{1.3}}\text{ FG}^-\text{-lam}}{\Sigma,\alpha,\beta;\Psi;\Gamma' \vdash_\alpha \nu(\lambda x.e_m)) : T_{1.2}}\text{ FG}^-\text{-CI}}{\Sigma,\alpha;\Psi;\Gamma' \vdash_\alpha \Lambda(\nu(\lambda x.e_m)) : T_{1.1}}\text{ FG}^-\text{-FI}}{\Sigma;\Psi;\Gamma' \vdash_{pc'} \Lambda(\Lambda(\nu(\lambda x.e_m))) : T_1}\text{ FG}^-\text{-FI}$$

3. app:

$$\dfrac{\begin{array}{c}\Sigma;\Psi;\Gamma \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\ell_e} \tau_2)^\ell \rightsquigarrow \Sigma;\Psi;\Gamma' \vdash_{pc'} e_{m1} : T_1 \\ \Sigma;\Psi;\Gamma \vdash_{pc} e_2 : \tau_1 \rightsquigarrow \Sigma;\Psi;\Gamma' \vdash_{pc'} e_{m2} : [\![\tau_1]\!]_{pc'}\end{array}}{\Sigma;\Psi;\Gamma \vdash_{pc} e_1\ e_2 : \tau_2 \rightsquigarrow \Sigma;\Psi;\Gamma' \vdash_{pc'} e_M : [\![\tau_2]\!]_{pc'}}\text{ app}$$

$T_1 = (\forall\alpha.\alpha, (\forall\beta.\alpha, (((pc' \sqcup \ell) \sqsubseteq \alpha \sqsubseteq \ell_e \wedge \beta \sqsubseteq \alpha) \overset{\alpha}{\Rightarrow} ([\![\tau_1]\!]_\beta \xrightarrow{\alpha} [\![\tau_2]\!]_\alpha)^\alpha)^\alpha)^\alpha)^{pc' \sqcup \ell}$

$T_{1.1} = (\forall\beta.(pc' \sqcup \ell), (((pc' \sqcup \ell) \sqsubseteq (pc' \sqcup \ell) \sqsubseteq \ell_e \wedge \beta \sqsubseteq (pc' \sqcup \ell)) \overset{(pc' \sqcup \ell)}{\Rightarrow} ([\![\tau_1]\!]_\beta \xrightarrow{(pc' \sqcup \ell)} [\![\tau_2]\!]_{(pc' \sqcup \ell)})^{(pc' \sqcup \ell)})^{(pc' \sqcup \ell)})^{(pc' \sqcup \ell)}$

$T_{1.2} = (((pc' \sqcup \ell) \sqsubseteq (pc' \sqcup \ell) \sqsubseteq \ell_e \wedge (pc' \sqcup \ell) \sqsubseteq (pc' \sqcup \ell)) \overset{(pc' \sqcup \ell)}{\Rightarrow} ([\![\tau_1]\!]_{(pc' \sqcup \ell)} \xrightarrow{(pc' \sqcup \ell)} [\![\tau_2]\!]_{(pc' \sqcup \ell)})^{(pc' \sqcup \ell)})^{(pc' \sqcup \ell)}$

$c_1 = ((pc' \sqcup \ell) \sqsubseteq (pc' \sqcup \ell) \sqsubseteq \ell_e \wedge (pc' \sqcup \ell) \sqsubseteq (pc' \sqcup \ell))$

$T_{1.3} = ([\![\tau_1]\!]_{(pc' \sqcup \ell)} \xrightarrow{(pc' \sqcup \ell)} [\![\tau_2]\!]_{(pc' \sqcup \ell)})^{(pc' \sqcup \ell)}$

$T_{1.4} = ([\![\tau_1]\!]_{(pc')} \xrightarrow{(pc' \sqcup \ell)} [\![\tau_2]\!]_{(pc' \sqcup \ell)})^{(pc' \sqcup \ell)}$

P7:

$$\overline{pc' \sqcup \ell \sqsubseteq pc' \sqcup \ell}$$

P6:

$$\overline{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_{m2} : [\![\tau_1]\!]_{pc'}}\text{ IH2}$$

P5:

$$\overline{\Sigma;\Psi \vdash T_{1.3} \searrow pc' \sqcup \ell}\text{ Definition of } [\![\cdot]\!]$$

P4:

$$\overline{\Sigma;\Psi \vdash T_{1.2} \searrow pc' \sqcup \ell}\text{ Definition of } [\![\cdot]\!]$$

P3:

$$\overline{\Sigma;\Psi \vdash T_{1.1} \searrow pc' \sqcup \ell}\text{ Definition of } [\![\cdot]\!]$$

P2:

$$\frac{}{pc' \sqcup pc' \sqcup \ell \sqsubseteq pc' \sqcup \ell}$$

P1:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi; \Gamma' \vdash_{pc'} e_{m1} : T_1}\text{ IH1} \qquad P2 \qquad P3}{\Sigma; \Psi; \Gamma' \vdash_{pc'} e_{m1}[] : T_{1.1}}\text{ FG}^{-}\text{-FE} \qquad P2 \qquad P4}{\Sigma; \Psi; \Gamma' \vdash_{pc'} e_{m1}[][] : T_{1.2}}\text{ FG}^{-}\text{-FE}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{P1 \qquad \dfrac{}{\Sigma; \Psi \vdash c_1} \qquad P2 \qquad P5}{\Sigma; \Psi; \Gamma' \vdash_{pc'} (e_{m1}[][]\bullet) : T_{1.3}}\text{ FG}^{-}\text{-CE}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} (e_{m1}[][]\bullet) : T_{1.4}}\text{ FG}^{-}\text{-sub} \qquad P6 \qquad P7}{\Sigma; \Psi; \Gamma' \vdash_{pc'} (e_{m1}[][]\bullet)\ e_{m_2} : [\![\tau_2]\!]_{pc' \sqcup \ell}}\text{ FG}^{-}\text{-app}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} (e_{m1}[][]\bullet)\ e_{m_2} : [\![\tau_2]\!]_{pc'}}\text{ Lemma 3.26}$$

4. prod:

$$\dfrac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : \tau_1 \rightsquigarrow \Sigma; \Psi; \Gamma' \vdash_{pc'} e_{m1} : [\![\tau_1]\!]_{pc'} \\ \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_2 \rightsquigarrow \Sigma; \Psi; \Gamma' \vdash_{pc'} e_{m2} : [\![\tau_2]\!]_{pc'}\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^{\perp} \rightsquigarrow \Sigma; \Psi; \Gamma' \vdash_{pc'} (e_{m1}, e_{m2}) : ([\![\tau_1]\!]_{pc'} \times [\![\tau_2]\!]_{pc'})^{pc'}}\text{ prod}$$

$$\dfrac{\dfrac{}{\Sigma; \Psi; \Gamma' \vdash_{pc'} e_{m1} : [\![\tau_1]\!]_{pc'}}\text{ IH1} \qquad \dfrac{}{\Sigma; \Psi; \Gamma' \vdash_{pc'} e_{m2} : [\![\tau_2]\!]_{pc'}}\text{ IH2}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} (e_{m1}, e_{m2}) : ([\![\tau_1]\!]_{pc'} \times [\![\tau_2]\!]_{pc'})^{pc'}}\text{ FG}^{-}\text{-prod}$$

5. fst:

$$\dfrac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^{\ell} \rightsquigarrow \Sigma; \Psi; \Gamma' \vdash_{pc'} e_m : ([\![\tau_1]\!]_{\ell \sqcup pc'} \times [\![\tau_2]\!]_{\ell \sqcup pc'})^{\ell \sqcup pc'} \qquad \Sigma; \Psi \vdash \tau_1 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{fst}(e) : \tau_1 \rightsquigarrow \Sigma; \Psi; \Gamma' \vdash_{pc'} \mathsf{fst}(e_m) : [\![\tau_1]\!]_{pc'}}\text{ fst}$$

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi; \Gamma' \vdash_{pc'} e_m : ([\![\tau_1]\!]_{\ell \sqcup pc'} \times [\![\tau_2]\!]_{\ell \sqcup pc'})^{\ell \sqcup pc'}}\text{ IH}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} \mathsf{fst}(e_m) : [\![\tau_1]\!]_{\ell \sqcup pc'}}\text{ FG}^{-}\text{-fst}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} \mathsf{fst}(e_m) : [\![\tau_1]\!]_{pc'}}\text{ Lemma 3.26}$$

6. snd:

$$\dfrac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^{\ell} \rightsquigarrow \Sigma; \Psi; \Gamma' \vdash_{pc'} e_m : ([\![\tau_1]\!]_{\ell \sqcup pc'} \times [\![\tau_2]\!]_{\ell \sqcup pc'})^{\ell \sqcup pc'} \qquad \Sigma; \Psi \vdash \tau_2 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{snd}(e) : \tau_2 \rightsquigarrow \Sigma; \Psi; \Gamma' \vdash_{pc'} \mathsf{snd}(e_m) : [\![\tau_2]\!]_{pc'}}\text{ snd}$$

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi; \Gamma' \vdash_{pc'} e_m : ([\![\tau_1]\!]_{\ell \sqcup pc'} \times [\![\tau_2]\!]_{\ell \sqcup pc'})^{\ell \sqcup pc'}}\text{ IH}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} \mathsf{snd}(e_m) : [\![\tau_2]\!]_{\ell \sqcup pc'}}\text{ FG}^{-}\text{-snd}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} \mathsf{snd}(e_m) : [\![\tau_2]\!]_{pc'}}\text{ Lemma 3.26}$$

7. inl:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau_1 \leadsto \Sigma; \Psi; \Gamma' \vdash_{pc'} e_m : [\![\tau_1]\!]_{pc'}}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inl}(e) : (\tau_1 + \tau_2)^{\perp} \leadsto \Sigma; \Psi; \Gamma' \vdash_{pc'} \mathsf{inl}(e_m) : ([\![\tau_1]\!]_{pc'} + [\![\tau_2]\!]_{pc'})^{pc'}} \text{ inl}$$

$$\frac{\overline{\Sigma; \Psi; \Gamma' \vdash_{pc'} e_m : [\![\tau_1]\!]_{pc'}} \text{ IH}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} \mathsf{inl}(e_m) : ([\![\tau_1]\!]_{pc'} + [\![\tau_2]\!]_{pc'})^{pc'}} \text{ FG}^{-}\text{-inl}$$

8. inr:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau_2 \leadsto \Sigma; \Psi; \Gamma' \vdash_{pc'} e_m : [\![\tau_2]\!]_{pc'}}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inr}(e) : (\tau_1 + \tau_2)^{\perp} \leadsto \Sigma; \Psi; \Gamma' \vdash_{pc'} e_M : ([\![\tau_1]\!]_{pc'} + [\![\tau_2]\!]_{pc'})^{pc'}} \text{ inr}$$

$$\frac{\overline{\Sigma; \Psi; \Gamma' \vdash_{pc'} e_m : [\![\tau_2]\!]_{pc'}} \text{ IH}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} \mathsf{inr}(e_m) : ([\![\tau_1]\!]_{pc'} + [\![\tau_2]\!]_{pc'})^{pc'}} \text{ FG}^{-}\text{-inr}$$

9. case:

$$\frac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 + \tau_2)^{\ell} \leadsto \Sigma; \Psi; \Gamma' \vdash_{pc'} e_m : ([\![\tau_1]\!]_{pc' \sqcup \ell} + [\![\tau_1]\!]_{pc' \sqcup \ell})^{pc' \sqcup \ell} \\ \Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_1 : \tau \leadsto \Sigma; \Psi; \Gamma', x : [\![\tau_1]\!]_{\ell_{n+1}} \vdash_{pc' \sqcup \ell} e_{m1} : [\![\tau]\!]_{pc' \sqcup \ell} \\ \Sigma; \Psi; \Gamma, y : \tau_2 \vdash_{pc \sqcup \ell} e_2 : \tau \leadsto \Sigma; \Psi; \Gamma', y : [\![\tau_2]\!]_{\ell_{n+2}} \vdash_{pc' \sqcup \ell} e_{m2} : [\![\tau]\!]_{pc' \sqcup \ell}\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{case}(e, x.e_1, y.e_2) : \tau \leadsto \Sigma; \Psi; \Gamma' \vdash_{pc'} \mathsf{case}(e_m, x.e_{m1}, x.e_{m2}) : [\![\tau]\!]_{pc'}} \text{ case}$$

P2:

$$\frac{}{\Sigma; \Psi; \Gamma', y : [\![\tau_2]\!]_{pc' \sqcup \ell} \vdash_{pc' \sqcup \ell} e_{m2} : [\![\tau]\!]_{pc' \sqcup \ell}} \text{ IH3 @ } pc' \sqcup \ell$$

P1:

$$\frac{}{\Sigma; \Psi; \Gamma', x : [\![\tau_1]\!]_{pc' \sqcup \ell} \vdash_{pc' \sqcup \ell} e_{m1} : [\![\tau]\!]_{pc' \sqcup \ell}} \text{ IH2 @ } pc' \sqcup \ell$$

Main derivation:

$$\frac{\dfrac{\overline{\Sigma; \Psi; \Gamma' \vdash_{pc'} e_m : ([\![\tau_1]\!]_{pc' \sqcup \ell} + [\![\tau_1]\!]_{pc' \sqcup \ell})^{pc' \sqcup \ell}} \text{ IH1} \qquad P1 \qquad P2}{\Sigma; \Psi; \Gamma' \vdash_{pc'} \mathsf{case}(e_m, x.e_{m1}, x.e_{m2}) : [\![\tau]\!]_{pc' \sqcup \ell}} \text{ FG}^{-}\text{-case}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} \mathsf{case}(e_m, x.e_{m1}, x.e_{m2}) : [\![\tau]\!]_{pc'}} \text{ Lemma 3.26}$$

10. sub:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc''} e : \tau' \leadsto \Sigma; \Psi; \Gamma' \vdash_{pc'} e_m : [\![\tau']\!]_{pc'} \qquad \Sigma; \Psi \vdash pc \sqsubseteq pc'' \qquad \Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau \leadsto \Sigma; \Psi; \Gamma' \vdash_{pc'} e_m : [\![\tau]\!]_{pc'}} \text{ sub}$$

$$\frac{\dfrac{\overline{pc' \sqsubseteq pc \sqsubseteq pc''}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} e_m : [\![\tau']\!]_{pc'}} \text{ IH} \qquad \dfrac{\tau' <: \tau}{[\![\tau']\!]_{pc'} <: [\![\tau]\!]_{pc'}} \text{ Lemma 3.24}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} e_m : [\![\tau]\!]_{pc'}}$$

11. ref:

$$\dfrac{\Sigma;\Psi;\Gamma \vdash_{pc} e : \tau \rightsquigarrow \Sigma;\Psi;\Gamma' \vdash_{pc'} e_m : [\![\tau]\!]_{pc'} \qquad \Sigma;\Psi \vdash \tau \searrow pc}{\Sigma;\Psi;\Gamma \vdash_{pc} \mathsf{new}\ e : (\mathsf{ref}\ \tau)^{\perp} \rightsquigarrow \Sigma;\Psi;\Gamma' \vdash_{pc'} \mathsf{new}\ \ e_m : (\mathsf{ref}\ [\![\tau]\!]_{\perp})^{pc'}}\ \text{ref}$$

P1:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi \vdash \tau \searrow pc}\ \text{Given} \qquad \Sigma;\Psi \vdash pc' \sqsubseteq pc}{\Sigma;\Psi \vdash \tau \searrow pc'}}{\Sigma;\Psi \vdash [\![\tau]\!]_{\perp} \searrow pc'}\ \text{Lemma 3.29}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_m : [\![\tau]\!]_{pc'}}\ \text{IH}}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_m : [\![\tau]\!]_{\perp}}\ \text{Lemma 3.26} \qquad P1}{\Sigma;\Psi;\Gamma' \vdash_{pc'} \mathsf{new}\ e_m : (\mathsf{ref}\ [\![\tau]\!]_{\perp})^{pc'}}\ \text{FG}^{-}\text{-new}$$

12. deref:

$$\dfrac{\begin{array}{c}\Sigma;\Psi;\Gamma \vdash_{pc} e : (\mathsf{ref}\ \tau)^{\ell} \rightsquigarrow \Sigma;\Psi;\Gamma' \vdash_{pc'} e_m : (\mathsf{ref}[\![\tau]\!]_{\perp})^{\ell \sqcup pc'} \\ \Sigma;\Psi \vdash \tau <: \tau' \qquad \Sigma;\Psi \vdash \tau' \searrow \ell\end{array}}{\Sigma;\Psi;\Gamma \vdash_{pc} !e : \tau' \rightsquigarrow \Sigma;\Psi;\Gamma' \vdash_{pc'} !e_m : [\![\tau']\!]_{pc'}}\ \text{deref}$$

$$\dfrac{\dfrac{\dfrac{\tau <: \tau'}{\Sigma;\Psi \vdash [\![\tau]\!]_{\perp} <: [\![\tau']\!]_{pc' \sqcup \ell}}\ \text{Lemma 3.24} \qquad \dfrac{\dfrac{}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_m : (\mathsf{ref}[\![\tau]\!]_{\perp})^{\ell \sqcup pc'}}\ \text{IH1}}{\Sigma;\Psi \vdash [\![\tau']\!]_{pc' \sqcup \ell} \searrow \ell \sqcup pc'}\ \text{Definition of } \searrow}{\Sigma;\Psi;\Gamma' \vdash_{pc'} !e_m : [\![\tau']\!]_{pc' \sqcup \ell}}}{\Sigma;\Psi;\Gamma' \vdash_{pc'} !e_m : [\![\tau']\!]_{pc'}}\ \text{Lemma 3.26}$$

13. assign:

$$\dfrac{\begin{array}{c}\Sigma;\Psi;\Gamma \vdash_{pc} e_1 : (\mathsf{ref}\ \tau)^{\ell} \rightsquigarrow \Sigma;\Psi;\Gamma' \vdash_{pc'} e_{m1} : (\mathsf{ref}\ [\![\tau]\!]_{\perp})^{\ell \sqcup pc'} \\ \Sigma;\Psi;\Gamma \vdash_{pc} e_2 : \tau \rightsquigarrow \Sigma;\Psi;\Gamma' \vdash_{pc'} e_{m2} : [\![\tau]\!]_{pc'} \qquad \Sigma;\Psi \vdash \tau \searrow (pc \sqcup \ell)\end{array}}{\Sigma;\Psi;\Gamma \vdash_{pc} e_1 := e_2 : \mathsf{unit}^{\perp} \rightsquigarrow \Sigma;\Psi;\Gamma' \vdash_{pc'} e_{m1} := e_{m2} : \mathsf{unit}^{pc'}}\ \text{assign}$$

P1:

$$\dfrac{\dfrac{}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_{m2} : [\![\tau]\!]_{pc'}}\ \text{IH2} \qquad \dfrac{\dfrac{}{\tau \searrow pc}\ \text{Given}}{\tau \searrow pc'}}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_{m2} : [\![\tau]\!]_{\perp}}\ \text{Lemma 3.26}$$

Main derivation:

$$\dfrac{\dfrac{}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_{m1} : (\mathsf{ref}\ [\![\tau]\!]_{\perp})^{\ell \sqcup pc'}}\ \text{IH1} \qquad P1 \qquad \dfrac{\tau \searrow (\ell \sqcup pc)}{[\![\tau]\!]_{\perp} \searrow \ell \sqcup pc'}\ \text{Lemma 3.29}}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_{m1} := e_{m2} : \mathsf{unit}^{pc'}}\ \text{FG}^{-}\text{-assign}$$

14. unitI:

$$\frac{}{\Sigma; \Psi; \Gamma \vdash_{pc} () : \mathsf{unit}^{\bot} \rightsquigarrow \Sigma; \Psi; \Gamma' \vdash_{pc'} () : \mathsf{unit}^{pc'}} \text{ unitI}$$

$$\frac{}{\Sigma; \Psi; \Gamma' \vdash_{pc'} () : \mathsf{unit}^{pc'}} \text{ FG}^{-}\text{-unitI}$$

15. FI:

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash_{\ell_e} e : \tau \rightsquigarrow \Sigma, \alpha; \Psi; \Gamma' \vdash_{\ell'_e} e_m : [\![\tau]\!]_{\ell'_e} \qquad \ell'_e \sqsubseteq \ell_e}{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\forall \alpha.(\ell_e, \tau))^{\bot} \rightsquigarrow \Sigma; \Psi; \Gamma' \vdash_{pc'} \Lambda((\nu(\Lambda\ e_m))) : T_1} \text{ FI}$$

$T_1 = (\forall \alpha.\alpha, ((pc' \sqsubseteq \alpha \sqsubseteq \ell_e) \overset{\alpha}{\Rightarrow} (\forall \gamma.\alpha, [\![\tau]\!]_{\alpha})^{\alpha})^{\alpha})^{pc'}$

$T_{1.1} = ((pc' \sqsubseteq \alpha \sqsubseteq \ell_e) \overset{\alpha}{\Rightarrow} (\forall \gamma.\alpha, [\![\tau]\!]_{\alpha})^{\alpha})^{\alpha}$

$T_{1.2} = (\forall \gamma.\alpha, [\![\tau]\!]_{\alpha})^{\alpha}$

$c_1 = (pc' \sqsubseteq \alpha \sqsubseteq \ell_e)$

$T_{1.3} = [\![\tau]\!]_{\alpha}$

P1:

$$\frac{\dfrac{}{\Sigma, \alpha, \gamma; \Psi, c_1; \Gamma' \vdash_{\alpha} e_m : T_{1.3}} \text{ IH with } \ell'_e \text{ as } \alpha}{\Sigma, \alpha, \gamma; \Psi, c_1; \Gamma' \vdash_{\alpha} \Lambda\ e_m : T_{1.2}} \text{ FG}^{-}\text{-FI}$$

Main derivation:

$$\frac{\dfrac{P1}{\Sigma, \alpha; \Psi; \Gamma' \vdash_{\alpha} \nu(\Lambda\ e_m) : T_{1.1}} \text{ FG}^{-}\text{-CI}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} \Lambda((\nu(\Lambda\ e_m))) : T_1} \text{ FG}^{-}\text{-FI}$$

16. CI:

$$\frac{\Sigma; \Psi, c; \Gamma \vdash_{\ell_e} e : \tau \rightsquigarrow \Sigma; \Psi, c; \Gamma' \vdash_{\ell'_e} e_m : [\![\tau]\!]_{\ell'_e} \qquad \ell'_e \sqsubseteq \ell_e}{\Sigma; \Psi; \Gamma \vdash_{pc} e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\bot} \rightsquigarrow \Sigma; \Psi; \Gamma' \vdash_{pc'} \Lambda(\nu\ e_m) : T_1} \text{ CI}$$

$T_1 = (\forall \alpha.\alpha, ((pc' \sqsubseteq \alpha \sqsubseteq \ell_e) \overset{\alpha}{\Rightarrow} [\![\tau]\!]_{\alpha})^{\alpha})^{pc'}$

$T_{1.1} = ((pc' \sqsubseteq \alpha \sqsubseteq \ell_e) \overset{\alpha}{\Rightarrow} [\![\tau]\!]_{\alpha})^{\alpha}$

$T_{1.2} = [\![\tau]\!]_{\alpha}$

$c_1 = (pc' \sqsubseteq \alpha \sqsubseteq \ell_e)$

$$\frac{\dfrac{\dfrac{}{\Sigma, \alpha; \Psi, c_1; \Gamma' \vdash_{\alpha} e_m : T_{1.2}} \text{ IH with } \ell'_e \text{ as } \alpha}{\Sigma, \alpha; \Psi; \Gamma' \vdash_{\alpha} \nu\ e_m : T_{1.1}} \text{ FG}^{-}\text{-CI}}{\Sigma; \Psi; \Gamma' \vdash_{pc'} \Lambda(\nu\ e_m) : T_1} \text{ FG}^{-}\text{-FI}$$

17. FE:

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e : (\forall\gamma.(\ell_e,\tau))^{\ell} \rightsquigarrow \Sigma;\Psi;\Gamma' \vdash_{pc'} e_m : T_1 \quad \mathrm{FV}(\ell') \in \Sigma \qquad \Sigma;\Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e[\ell'/\gamma] \qquad \Sigma;\Psi \vdash \tau[\ell'/\gamma] \searrow \ell}{\Sigma;\Psi;\Gamma \vdash_{pc} e : \tau[\ell'/\gamma] \rightsquigarrow \Sigma;\Psi;\Gamma' \vdash_{pc'} e_m[] \bullet [] : \llbracket \tau[\ell'/\gamma] \rrbracket_{pc'}} \text{FE}$$

$T_1 = (\forall\alpha.\alpha, (((pc' \sqcup \ell) \sqsubseteq \alpha \sqsubseteq \ell_e) \overset{\alpha}{\Rightarrow} (\forall\gamma.\alpha, \llbracket\tau\rrbracket_{\alpha})^{\alpha})^{\alpha})^{pc' \sqcup \ell}$

$T_{1.1} = (((pc' \sqcup \ell) \sqsubseteq (pc' \sqcup \ell) \sqsubseteq \ell_e) \overset{(pc' \sqcup \ell)}{\Rightarrow} (\forall\gamma.(pc' \sqcup \ell), \llbracket\tau\rrbracket_{(pc' \sqcup \ell)})^{(pc' \sqcup \ell)})^{(pc' \sqcup \ell)}$

$T_{1.2} = (\forall\gamma.(pc' \sqcup \ell), \llbracket\tau\rrbracket_{(pc' \sqcup \ell)})^{(pc' \sqcup \ell)}$

$c_1 = ((pc' \sqcup \ell) \sqsubseteq (pc' \sqcup \ell) \sqsubseteq \ell_e)$

$T_{1.3} = \llbracket\tau\rrbracket_{(pc' \sqcup \ell)}[\ell'/\gamma]$

$T_{1.31} = \llbracket\tau[\ell'/\gamma]\rrbracket_{(pc' \sqcup \ell)}$

$T_{1.4} = \llbracket\tau[\ell'/\gamma]\rrbracket_{pc'}$

P5:

$$\frac{}{T_{1.2} \searrow (pc' \sqcup \ell)} \text{Definition of } \llbracket\cdot\rrbracket$$

P4:

$$\frac{}{T_{1.1} \searrow (pc' \sqcup \ell)} \text{Definition of } \llbracket\cdot\rrbracket$$

P3:

$$\frac{}{(pc' \sqcup \ell) \sqsubseteq (pc \sqcup \ell) \sqsubseteq \ell_e} \text{Given}$$

P2:

$$\frac{\dfrac{}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_m : T_1}\text{IH} \qquad P4}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_m[] : T_{1.1}} \text{FG}^{-}\text{-FE}$$

P1:

$$\frac{P2 \qquad P3 \qquad P5}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_m[]\bullet : T_{1.2}} \text{FG}^{-}\text{-CE}$$

P0:

$$\frac{\dfrac{P1 \qquad \dfrac{}{\Sigma;\Psi \vdash T_{1.3} \searrow (pc' \sqcup \ell)}\text{Definition of } \llbracket\cdot\rrbracket \qquad P2}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_m[] \bullet [] : T_{1.3}} \text{FG}^{-}\text{-FE}}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_m[] \bullet [] : T_{1.31}} \text{Lemma 3.28}$$

Main derivation:

$$\frac{P0 \qquad \dfrac{}{\Sigma;\Psi \vdash \tau[\ell'/\alpha] \searrow \ell}}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_m[] \bullet [] : T_{1.4}} \text{Lemma 3.26}$$

18. CE:

$$\dfrac{\begin{array}{c}\Sigma;\Psi;\Gamma \vdash_{pc} e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell} \rightsquigarrow \Sigma;\Psi;\Gamma' \vdash_{pc'} e_m : T_1 \\ \Sigma;\Psi \vdash c \qquad \Sigma;\Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e \qquad \Sigma;\Psi \vdash \tau \searrow \ell\end{array}}{\Sigma;\Psi;\Gamma \vdash_{pc} e : \tau \rightsquigarrow \Sigma;\Psi;\Gamma' \vdash_{pc'} e_m[]\bullet : [\![\tau]\!]_{pc'}} \text{ CE}$$

$T_1 = (\forall\alpha.\alpha, ((c \wedge (pc' \sqcup \ell) \sqsubseteq \alpha \sqsubseteq \ell_e) \overset{\alpha}{\Rightarrow} [\![\tau]\!]_{\alpha})^{\alpha})^{pc' \sqcup \ell}$

$T_{1.1} = ((c \wedge (pc' \sqcup \ell) \sqsubseteq (pc' \sqcup \ell) \sqsubseteq \ell_e) \overset{(pc' \sqcup \ell)}{\Rightarrow} [\![\tau]\!]_{(pc' \sqcup \ell)})^{(pc' \sqcup \ell)}$

$T_{1.2} = [\![\tau]\!]_{(pc' \sqcup \ell)}$

$T_{1.3} = [\![\tau]\!]_{pc'}$

$c_1 = (c \wedge (pc' \sqcup \ell) \sqsubseteq (pc' \sqcup \ell) \sqsubseteq \ell_e)$

P3:

$$\dfrac{\dfrac{}{\Sigma;\Psi \vdash (pc \sqcup \ell) \sqsubseteq \ell_e} \text{ Given}}{\Sigma;\Psi \vdash (pc' \sqcup \ell) \sqsubseteq \ell_e}$$

P2:

$$\dfrac{}{\Sigma;\Psi \vdash T_{1.2} \searrow (pc' \sqcup \ell)} \text{ Definition of } [\![\cdot]\!]$$

P1:

$$\dfrac{}{\Sigma;\Psi \vdash T_{1.1} \searrow (pc' \sqcup \ell)} \text{ Definition of } [\![\cdot]\!]$$

P0:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_m : T_1} \text{ IH} \qquad P1}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_m[] : T_{1.1}} \text{ FG}^{-}\text{-FE} \qquad \dfrac{\dfrac{}{\Sigma;\Psi \vdash c} \text{ Given, Weakening} \qquad P3}{\Sigma;\Psi \vdash c_1} \qquad P2}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_m[]\bullet : T_{1.2}} \text{ FG}^{-}\text{-CE}$$

Main derivation:

$$\dfrac{P0.1 \qquad \dfrac{}{\tau \searrow \ell} \text{ Given}}{\Sigma;\Psi;\Gamma' \vdash_{pc'} e_m[]\bullet : T_{1.3}} \text{ Lemma 3.26}$$

□

Lemma 3.24 (FG $\rightsquigarrow$ FG$^-$: Subtyping)**.** $\forall \Sigma, \Psi, \ell, \ell'.\ \Sigma;\Psi \vdash \ell \sqsubseteq \ell'$ *and the following holds:*

1. $\forall \tau, \tau'$.
   $\Sigma;\Psi \vdash \tau <: \tau' \implies [\![\tau]\!]_{\ell} <: [\![\tau']\!]_{\ell'}$

2. $\forall \mathsf{A}, \mathsf{A}'$.
   $\Sigma;\Psi \vdash \mathsf{A} <: \mathsf{A}' \implies \Sigma;\Psi \vdash [\![\mathsf{A}]\!]_{\ell} <: [\![\mathsf{A}']\!]_{\ell'}$

Proof. Proof by simultaneous induction on $\tau <: \tau$ and $\mathsf{A} <: \mathsf{A}$

Proof of statement (1)

Let $\tau = \mathsf{A}_1^{\ell_1}$ and $\tau' = \mathsf{A}_2^{\ell_2}$

P2:

$$\dfrac{\dfrac{\dfrac{}{\mathsf{A}_1^{\ell_1} <: \mathsf{A}_2^{\ell_2}}\text{ Given}}{\Sigma; \Psi \vdash \mathsf{A}_1 <: \mathsf{A}_2}\text{ By inversion} \qquad P1}{\Sigma; \Psi \vdash ([\![\mathsf{A}_1]\!]_{\ell \sqcup \ell_1}) <: ([\![\mathsf{A}_2]\!]_{\ell' \sqcup \ell_2})}\text{ IH(2) on } \mathsf{A}_1 <: \mathsf{A}_2$$

P1:

$$\dfrac{\dfrac{\dfrac{}{\mathsf{A}_1^{\ell_1} <: \mathsf{A}_2^{\ell_2}}\text{ Given}}{\Sigma; \Psi \vdash \ell_1 \sqsubseteq \ell_2}\text{ By inversion} \qquad \dfrac{}{\Sigma; \Psi \vdash \ell \sqsubseteq \ell'}\text{ Given}}{\Sigma; \Psi \vdash \ell \sqcup \ell_1 \sqsubseteq \ell' \sqcup \ell_2}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad P2}{\Sigma; \Psi \vdash ([\![\mathsf{A}_1]\!]_{\ell \sqcup \ell_1})^{\ell \sqcup \ell_1} <: ([\![\mathsf{A}_2]\!]_{\ell \sqcup \ell_2})^{\ell' \sqcup \ell_2}}}{\Sigma; \Psi \vdash \left[\!\!\left[\mathsf{A}_1^{\ell_1}\right]\!\!\right]_{\ell} <: \left[\!\!\left[\mathsf{A}_2^{\ell_2}\right]\!\!\right]_{\ell'}}$$

Proof of statement (2)

We proceed by cases on $\mathsf{A} <: \mathsf{A}$

1. FGsub-base:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{b} <: \mathsf{b}}\text{ FG}^{-}\text{sub-base}}{\Sigma; \Psi \vdash [\![\mathsf{b}]\!]_{\ell} <: [\![\mathsf{b}]\!]_{\ell'}}\text{ Definition of } [\![.]\!]$$

2. FGsub-ref:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{ref}\ [\![\tau_i]\!]_{\perp} <: \mathsf{ref}\ [\![\tau_i]\!]_{\perp}}\text{ FG}^{-}\text{sub-ref}}{\Sigma; \Psi \vdash [\![\mathsf{ref}\ \tau_i]\!]_{\ell} <: [\![\mathsf{ref}\ \tau_i]\!]_{\ell'}}\text{ Definition of } [\![.]\!]$$

3. FGsub-prod:

P1:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}\text{ Given}}{\Sigma; \Psi \vdash \tau_1 <: \tau_1'}\text{ By inversion}}{\Sigma; \Psi \vdash [\![\tau_1]\!]_{\ell} <: [\![\tau_1']\!]_{\ell'}}\text{ IH(1) on } \tau_1 <: \tau_1'$$

P2:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}\text{ Given}}{\Sigma; \Psi \vdash \tau_2 <: \tau_2'}\text{ By inversion}}{\Sigma; \Psi \vdash [\![\tau_2]\!]_{\ell} <: [\![\tau_2']\!]_{\ell'}}\text{ IH(1) on } \tau_2 <: \tau_2'$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad P2}{\Sigma; \Psi \vdash [\![\tau_1]\!]_{\ell} \times [\![\tau_2]\!]_{\ell} <: [\![\tau_1']\!]_{\ell} \times [\![\tau_2']\!]_{\ell'}}\text{ FG}^{-}\text{sub-prod}}{\Sigma; \Psi \vdash [\![\tau_1 \times \tau_2]\!]_{\ell} <: [\![\tau_1' \times \tau_2']\!]_{\ell'}}\text{ Definition of } [\![.]\!]$$

4. FGsub-sum:

P1:

$$\cfrac{\cfrac{\overline{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'}\ \text{Given}}{\Sigma; \Psi \vdash \tau_1 <: \tau_1'}\ \text{By inversion}}{\Sigma; \Psi \vdash [\![\tau_1]\!]_\ell <: [\![\tau_1']\!]_{\ell'}}\ \text{IH(1) on } \tau_1 <: \tau_1'$$

P2:

$$\cfrac{\cfrac{\overline{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'}\ \text{Given}}{\Sigma; \Psi \vdash \tau_2 <: \tau_2'}\ \text{By inversion}}{\Sigma; \Psi \vdash [\![\tau_2]\!]_\ell <: [\![\tau_2']\!]_{\ell'}}\ \text{IH(1) on } \tau_2 <: \tau_2'$$

Main derivation:

$$\cfrac{\cfrac{P1 \qquad P2}{\Sigma; \Psi \vdash [\![\tau_1]\!]_\ell + [\![\tau_2]\!]_\ell <: [\![\tau_1']\!]_\ell + [\![\tau_2']\!]_{\ell'}}\ \text{FG}^{-}\text{sub-prod}}{\Sigma; \Psi \vdash [\![\tau_1 + \tau_2]\!]_\ell <: [\![\tau_1' + \tau_2']\!]_{\ell'}}\ \text{Definition of } [\![.]\!]$$

5. FGsub-arrow:

$T_1 = \forall\alpha.\alpha, (\forall\beta.\alpha, ((\ell \sqsubseteq \alpha \sqsubseteq \ell_e \wedge \beta \sqsubseteq \alpha) \overset{\alpha}{\Rightarrow} ([\![\tau_1]\!]_\beta \overset{\alpha}{\to} [\![\tau_2]\!]_\alpha)^\alpha)^\alpha)^\alpha$

$T_{1.0} = \forall\beta.\alpha, ((\ell \sqsubseteq \alpha \sqsubseteq \ell_e \wedge \beta \sqsubseteq \alpha) \overset{\alpha}{\Rightarrow} ([\![\tau_1]\!]_\beta \overset{\alpha}{\to} [\![\tau_2]\!]_\alpha)^\alpha)^\alpha$

$T_{1.1} = ((\ell \sqsubseteq \alpha \sqsubseteq \ell_e \wedge \beta \sqsubseteq \alpha) \overset{\alpha}{\Rightarrow} ([\![\tau_1]\!]_\beta \overset{\alpha}{\to} [\![\tau_2]\!]_\alpha)^\alpha$

$T_{1.2} = ([\![\tau_1]\!]_\beta \overset{\alpha}{\to} [\![\tau_2]\!]_\alpha)^\alpha$

$c_1 = (\ell \sqsubseteq \alpha \sqsubseteq \ell_e \wedge \beta \sqsubseteq \alpha)$

$T_2 = \forall\alpha.\alpha, (\forall\beta.\alpha, ((\ell' \sqsubseteq \alpha \sqsubseteq \ell_e' \wedge \beta \sqsubseteq \alpha) \overset{\alpha}{\Rightarrow} ([\![\tau_1']\!]_\beta \overset{\alpha}{\to} [\![\tau_2']\!]_\alpha)^\alpha)^\alpha)^\alpha$

$T_{2.0} = \forall\beta.\alpha, ((\ell' \sqsubseteq \alpha \sqsubseteq \ell_e' \wedge \beta \sqsubseteq \alpha) \overset{\alpha}{\Rightarrow} ([\![\tau_1']\!]_\beta \overset{\alpha}{\to} [\![\tau_2']\!]_\alpha)^\alpha)^\alpha$

$T_{2.1} = ((\ell' \sqsubseteq \alpha \sqsubseteq \ell_e' \wedge \beta \sqsubseteq \alpha) \overset{\alpha}{\Rightarrow} ([\![\tau_1']\!]_\beta \overset{\alpha}{\to} [\![\tau_2']\!]_\alpha)^\alpha$

$T_{2.2} = ([\![\tau_1']\!]_\beta \overset{\alpha}{\to} [\![\tau_2']\!]_\alpha)^\alpha$

$c_2 = (\ell' \sqsubseteq \alpha \sqsubseteq \ell_e' \wedge \beta \sqsubseteq \alpha)$

P3:

$$\cfrac{\cfrac{\overline{\Sigma; \Psi \vdash \tau_1 \overset{\ell_e}{\to} \tau_2 <: \tau_1' \overset{\ell_e'}{\to} \tau_2'}\ \text{Given}}{\Sigma; \Psi \vdash \tau_2 <: \tau_2'}\ \text{By inversion}}{\Sigma; \Psi \vdash [\![\tau_2]\!]_\alpha <: [\![\tau_2']\!]_\alpha}\ \text{IH(1) with } \ell = \ell' = \alpha$$

P2:

$$\cfrac{\cfrac{\overline{\Sigma; \Psi \vdash \tau_1 \overset{\ell_e}{\to} \tau_2 <: \tau_1' \overset{\ell_e'}{\to} \tau_2'}\ \text{Given}}{\Sigma; \Psi \vdash \tau_1' <: \tau_1}\ \text{By inversion}}{\Sigma; \Psi \vdash [\![\tau_1']\!]_\beta <: [\![\tau_1]\!]_\beta}\ \text{IH(1) with } \ell = \ell' = \beta$$

P1:

$$\cfrac{P2 \qquad P3}{\Sigma, \alpha, \beta; \Psi \vdash T_{1.3} <: T_{2.3}}\ \text{FG}^{-}\text{sub-arrow}$$

P0:

$$\dfrac{\dfrac{\dfrac{}{\Sigma,\alpha,\beta;\Psi\vdash \ell\sqsubseteq\ell'}\text{ Given, Weakening}}{\Sigma,\alpha,\beta;\Psi\vdash \ell'\sqsubseteq\alpha \implies \ell\sqsubseteq\alpha} \quad \dfrac{\dfrac{}{\Sigma,\alpha,\beta;\Psi\vdash \ell_e'\sqsubseteq\ell_e}\text{ Given, Weakening}}{\Sigma,\alpha,\beta;\Psi\vdash \alpha\sqsubseteq\ell_e' \implies \alpha\sqsubseteq\ell_e}}{\begin{array}{c}\Sigma,\alpha,\beta;\Psi\vdash c_2 \implies c_1 \\ \dfrac{P1}{\Sigma,\alpha,\beta;\Psi\vdash T_{1.2} <: T_{2.2}}\text{ Weakening, FG}^{-}\text{sub-label}\end{array}}$$

$$\dfrac{\cdots}{\Sigma,\alpha;\Psi\vdash T_{1.1} <: T_{2.1}}\text{ FG}^{-}\text{sub-constraint}$$

P0.1:

$$\dfrac{P0}{\Sigma,\alpha;\Psi\vdash T_{1.0} <: T_{2.0}}\text{ FG}^{-}\text{sub-forall}$$

Main derivation:

$$\dfrac{\dfrac{P0.1}{\Sigma;\Psi\vdash T_1 <: T_2}\text{ FG}^{-}\text{sub-label}}{\Sigma;\Psi\vdash \left[\!\!\left[\tau_1 \xrightarrow{\ell_e} \tau_2\right]\!\!\right]_{\ell} <: \left[\!\!\left[\tau_1' \xrightarrow{\ell_e'} \tau_2'\right]\!\!\right]_{\ell'}}\text{ Definition of } [\![.]\!]$$

6. FGsub-unit:

$$\dfrac{\dfrac{}{\Sigma;\Psi\vdash \mathsf{unit} <: \mathsf{unit}}\text{ FG}^{-}\text{sub-unit}}{\Sigma;\Psi\vdash [\![\mathsf{unit}]\!]_{\ell} <: [\![\mathsf{unit}]\!]_{\ell'}}\text{ Definition of } [\![.]\!]$$

7. FGsub-forall:

$T_1 = \forall\alpha.\alpha, ((\ell\sqsubseteq\alpha\sqsubseteq\ell_e) \overset{\alpha}{\Rightarrow} (\forall\gamma.\alpha, [\![\tau]\!]_{\alpha})^{\alpha})^{\alpha}$

$T_{1.0} = (\ell\sqsubseteq\alpha\sqsubseteq\ell_e) \overset{\alpha}{\Rightarrow} (\forall\gamma.\alpha, [\![\tau]\!]_{\alpha})^{\alpha}$

$T_{1.1} = (\forall\gamma.\alpha, [\![\tau]\!]_{\alpha})^{\alpha}$

$c_1 = (\ell\sqsubseteq\alpha\sqsubseteq\ell_e)$

$T_{1.2} = [\![\tau]\!]_{\alpha}$

$T_2 = \forall\alpha.\alpha, ((\ell'\sqsubseteq\alpha\sqsubseteq\ell_e') \overset{\alpha}{\Rightarrow} (\forall\gamma.\alpha, [\![\tau']\!]_{\alpha})^{\alpha})^{\alpha}$

$T_{2.0} = (\ell'\sqsubseteq\alpha\sqsubseteq\ell_e') \overset{\alpha}{\Rightarrow} (\forall\gamma.\alpha, [\![\tau']\!]_{\alpha})^{\alpha}$

$T_{2.1} = (\forall\gamma.\alpha, [\![\tau']\!]_{\alpha})^{\alpha}$

$c_2 = (\ell'\sqsubseteq\alpha\sqsubseteq\ell_e')$

$T_{2.2} = [\![\tau']\!]_{\alpha}$

P0:

$$\dfrac{\dfrac{\dfrac{}{\Sigma,\alpha;\Psi\vdash \ell\sqsubseteq\ell'}\text{ Given, Weakening}}{\Sigma,\alpha;\Psi\vdash \ell'\sqsubseteq\alpha \implies \ell\sqsubseteq\alpha} \quad \dfrac{\dfrac{}{\Sigma,\alpha;\Psi\vdash \ell_e'\sqsubseteq\ell_e}\text{ Given, Weakening}}{\Sigma,\alpha;\Psi\vdash \alpha\sqsubseteq\ell_e' \implies \alpha\sqsubseteq\ell_e}}{\Sigma,\alpha;\Psi\vdash c_2 \implies c_1}$$

P1:

$$\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha, \gamma; \Psi \vdash T_{1.2} <: T_{2.2}}\text{ IH}}{\Sigma, \alpha; \Psi \vdash T_{1.1} <: T_{2.1}}\text{ FG}^{-}\text{sub-forall} \qquad \dfrac{P0}{\Sigma; \Psi \vdash c_2 \implies c_1}}{\dfrac{\Sigma, \alpha; \Psi \vdash T_{1.0} <: T_{2.0}}{\Sigma; \Psi \vdash T_1 <: T_2}\text{ FG}^{-}\text{sub-forall}}\text{ FG}^{-}\text{sub-constraint}$$

Main derivation:

$$\dfrac{P0.1}{\Sigma; \Psi \vdash [\![\forall \gamma.\tau_1]\!]_\ell <: [\![\forall \gamma.\tau_2]\!]_{\ell'}}\text{ Definition of } [\![.]\!]$$

8. FGsub-constraint:

$T_1 = \forall \alpha.\alpha, (((c \wedge \ell \sqsubseteq \alpha \sqsubseteq \ell_e) \overset{\alpha}{\Rightarrow} [\![\tau]\!]_\alpha)^\alpha)^\alpha$

$T_{1.1} = ((c \wedge \ell \sqsubseteq \alpha \sqsubseteq \ell_e) \overset{\alpha}{\Rightarrow} [\![\tau]\!]_\alpha)^\alpha$

$T_{1.2} = [\![\tau]\!]_\alpha$

$c_1 = (c \wedge \ell \sqsubseteq \alpha \sqsubseteq \ell_e)$

$T_2 = \forall \alpha.\alpha, (((c' \wedge \ell' \sqsubseteq \alpha \sqsubseteq \ell'_e) \overset{\alpha}{\Rightarrow} [\![\tau']\!]_\alpha)^\alpha)^\alpha$

$T_{2.1} = ((c' \wedge \ell' \sqsubseteq \alpha \sqsubseteq \ell'_e) \overset{\alpha}{\Rightarrow} [\![\tau']\!]_\alpha)^\alpha$

$T_{2.2} = [\![\tau']\!]_\alpha$

$c_2 = (c' \wedge \ell' \sqsubseteq \alpha \sqsubseteq \ell'_e)$

P2:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash c_1 \Rightarrow \tau_1 <: c_2 \Rightarrow \tau_2}\text{ Given}}{\Sigma; \Psi \vdash \tau_1 <: \tau_2}\text{ By inversion}}{\Sigma; \Psi \vdash [\![\tau_1]\!]_\ell <: [\![\tau_2]\!]_{\ell'}}\text{ IH(1) on } \tau_1 <: \tau_2$$

P1:

$$\dfrac{\dfrac{}{\Sigma, \alpha; \Psi \vdash c \Rightarrow \tau <: c' \Rightarrow \tau'}\text{ Given, Weakening}}{\Sigma, \alpha; \Psi \vdash c' \implies c}\text{ By inversion}$$

P0:

$$\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha; \Psi \vdash \ell \sqsubseteq \ell'}\text{ Given, Weakening}}{\Sigma, \alpha; \Psi \vdash \ell' \sqsubseteq \alpha \implies \ell \sqsubseteq \alpha} \qquad \dfrac{\dfrac{}{\Sigma, \alpha; \Psi \vdash \ell'_e \sqsubseteq \ell_e}\text{ Given, Weakening}}{\Sigma, \alpha; \Psi \vdash \alpha \sqsubseteq \ell'_e \implies \alpha \sqsubseteq \ell_e} \qquad P1}{\Sigma, \alpha; \Psi \vdash c_2 \implies c_1}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{P0 \qquad \dfrac{}{\Sigma, \alpha; \Psi \vdash [\![\tau]\!]_\alpha <: [\![\tau']\!]_\alpha}\text{ IH}}{\Sigma, \alpha; \Psi \vdash T_{1.1} <: T_{2.1}}}{\Sigma; \Psi \vdash T_1 <: T_2}\text{ FG}^{-}\text{sub-constraint}}{\Sigma; \Psi \vdash [\![c_1 \implies \tau_1]\!]_\ell <: [\![c_2 \implies \tau_2]\!]_{\ell'}}\text{ Definition of } [\![.]\!]_\ell$$

$\square$

Lemma 3.25 (FG ⇝ FG$^-$: Subtyping with label)**.** *If* $\Sigma; \Psi \vdash \ell \sqsubseteq \ell'$, *then* $\Sigma; \Psi \vdash [\![\tau]\!]_\ell <: [\![\tau]\!]_{\ell'}$ *in FG$^-$.*

Proof. From Lemma 3.24 with $\tau = \tau'$ and from Lemma 3.21 □

Lemma 3.26 (FG ⇝ FG$^-$: Subtyping for $\tau \searrow \ell$)**.** *If* $\Sigma; \Psi \vdash \tau \searrow \ell$, *then* $\Sigma; \Psi \vdash [\![\tau]\!]_{\ell \sqcup \ell'} <: [\![\tau]\!]_{\ell'}$ *in FG$^-$.*

Proof. Since $\Sigma; \Psi \vdash \tau \searrow \ell$, there exists ℓ'' such that $\tau = \mathsf{A}^{\ell''}$ and $\Sigma; \Psi \vdash \ell \sqsubseteq \ell''$. Now we have:

$$\begin{array}{lll} & \Sigma; \Psi \vdash [\![\tau]\!]_{\ell \sqcup \ell'} <: [\![\tau]\!]_{\ell'} & \\ = & \Sigma; \Psi \vdash [\![\mathsf{A}^{\ell''}]\!]_{\ell \sqcup \ell'} <: [\![\mathsf{A}^{\ell''}]\!]_{\ell'} & (\tau = \mathsf{A}^{\ell''}) \\ = & \Sigma; \Psi \vdash ([\![\mathsf{A}]\!]_{\ell \sqcup \ell' \sqcup \ell''})^{\ell \sqcup \ell' \sqcup \ell''} <: ([\![\mathsf{A}]\!]_{\ell' \sqcup \ell''})^{\ell' \sqcup \ell''} & (\text{Definition of } [\![\cdot]\!]) \\ = & \Sigma; \Psi \vdash [\![\mathsf{A}^{\ell'}]\!]_{\ell \sqcup \ell''} <: [\![\mathsf{A}^{\ell'}]\!]_{\ell''} & (\text{Definition of } [\![\cdot]\!]) \end{array}$$

The last statement holds by Lemma 3.25, since $\Sigma; \Psi \vdash \ell \sqcup \ell'' \sqsubseteq \ell''$ follows from our earlier assertion that $\Sigma; \Psi \vdash \ell \sqsubseteq \ell''$. □

Lemma 3.27 (FG ⇝ FG$^-$: Lemma for protection relation)**.** $\forall \Sigma, \Psi, \alpha, \tau, \ell, \ell'.$
$\Sigma, \alpha; \Psi \vdash \tau \searrow \ell \implies \Sigma; \Psi \vdash \tau[\ell'/\alpha] \searrow \ell[\ell'/\alpha]$, *where* $FV(\ell') \in \Sigma$

Proof. Say $\tau = \mathsf{A}^{\ell_g}$

$$\cfrac{\cfrac{\cfrac{}{\Sigma, \alpha; \Psi \vdash \ell \sqsubseteq \ell_g}\ \text{By inversion on } \Sigma, \alpha; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi \vdash \ell[\ell'/\alpha] \sqsubseteq \ell_g[\ell'/\alpha]}\ \text{Substitution over constraints}}{\Sigma; \Psi \vdash \mathsf{A}^{\ell_g}[\ell'/\alpha] \searrow \ell[\ell'/\alpha]}\ \text{Definition of } \searrow$$

□

Lemma 3.28 (FG ⇝ FG$^-$: Substitution lemma)**.** *Forall* ℓ, ℓ' *the following hold:*

1. $\forall \tau.\ [\![\tau]\!]_\ell[\ell'/\alpha] = [\![\tau[\ell'/\alpha]]\!]_{(\ell[\ell'/\alpha])}$
2. $\forall \mathsf{A}.\ [\![\mathsf{A}]\!]_\ell[\ell'/\alpha] = [\![\mathsf{A}[\ell'/\alpha]]\!]_{(\ell[\ell'/\alpha])}$

Proof. Proof by simultaneous induction on τ and A

Proof of statement (1)

Let $\tau = \mathsf{A}^{\ell_i}$

$$\begin{array}{lll} & [\![\mathsf{A}^{\ell_i}]\!]_\ell\ [\ell'/\alpha] & \\ = & ([\![\mathsf{A}]\!]_{\ell_i \sqcup \ell})^{\ell_i \sqcup \ell}\ [\ell'/\alpha] & \text{Definition of } [\![\cdot]\!] \\ = & ([\![\mathsf{A}]\!]_{\ell_i \sqcup \ell}[\ell'/\alpha])^{\ell_i[\ell'/\alpha] \sqcup \ell[\ell'/\alpha]} & \\ = & ([\![\mathsf{A}[\ell'/\alpha]]\!]_{\ell_i[\ell'/\alpha] \sqcup \ell[\ell'/\alpha]})^{\ell_i[\ell'/\alpha] \sqcup \ell[\ell'/\alpha]} & \text{IH(2) on } \mathsf{A} \\ = & \left[\!\!\left[(\mathsf{A}[\ell'/\alpha])^{\ell_i[\ell'/\alpha]}\right]\!\!\right]_{\ell[\ell'/\alpha]} & \\ = & [\![\mathsf{A}^{\ell_i}[\ell'/\alpha]]\!]_{\ell[\ell'/\alpha]} & \end{array}$$

Proof of statement (2)

We consider cases of A

1. $\mathsf{A} = \mathsf{b}$:

$$\begin{array}{lll} & [\![\mathsf{b}]\!]_\ell[\ell'/\alpha] & \\ = & \mathsf{b}[\ell'/\alpha] & (\text{Definition of } [\![\cdot]\!]) \\ = & \mathsf{b} & \alpha \notin \text{FV}(\mathsf{b}) \\ = & [\![\mathsf{b}]\!]_\ell & (\text{Definition of } [\![\cdot]\!]) \\ = & [\![\mathsf{b}[\ell'/\alpha]]\!]_\ell & \end{array}$$

2. $\mathsf{A} = \mathsf{ref}\ \tau_i$:

$$\begin{array}{ll} & [\![\mathsf{ref}\ \tau_i]\!]_\ell[\ell'/\alpha] \\ = & \mathsf{ref}\ [\![\tau_i]\!]_\perp[\ell'/\alpha] \qquad \text{(Definition of } [\![\cdot]\!]) \\ = & \mathsf{ref}\ ([\![\tau_i]\!]_\perp[\ell'/\alpha]) \\ = & \mathsf{ref}\ [\![\tau_i[\ell'/\alpha]]\!]_\perp \qquad \text{IH(1) on } \tau_i \\ = & [\![\mathsf{ref}\ \tau_i[\ell'/\alpha]]\!]_\ell \end{array}$$

3. $\mathsf{A} = \tau_1 \times \tau_2$:

$$\begin{array}{lll} & [\![\tau_1 \times \tau_2]\!]_\ell[\ell'/\alpha] & \\ = & ([\![\tau_1]\!]_\ell \times [\![\tau_2]\!]_\ell)[\ell'/\alpha] & \text{(Definition of } [\![\cdot]\!]) \\ = & [\![\tau_1]\!]_\ell[\ell'/\alpha] \times [\![\tau_2]\!]_\ell[\ell'/\alpha] & \\ = & [\![\tau_1[\ell'/\alpha]]\!]_{\ell[\ell'/\alpha]} \times [\![\tau_2[\ell'/\alpha]]\!]_{\ell[\ell'/\alpha]} & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\ = & [\![(\tau_1[\ell'/\alpha] \times \tau_2[\ell'/\alpha])]\!]_{\ell[\ell'/\alpha]} & \text{(Definition of } [\![\cdot]\!]) \\ = & [\![(\tau_1 \times \tau_2)[\ell'/\alpha]]\!]_{\ell[\ell'/\alpha]} & \end{array}$$

4. $\mathsf{A} = \tau_1 + \tau_2$:

$$\begin{array}{lll} & [\![\tau_1 + \tau_2]\!]_\ell[\ell'/\alpha] & \\ = & ([\![\tau_1]\!]_\ell + [\![\tau_2]\!]_\ell)[\ell'/\alpha] & \text{(Definition of } [\![\cdot]\!]) \\ = & [\![\tau_1]\!]_\ell[\ell'/\alpha] + [\![\tau_2]\!]_\ell[\ell'/\alpha] & \\ = & [\![\tau_1[\ell'/\alpha]]\!]_{\ell[\ell'/\alpha]} + [\![\tau_2[\ell'/\alpha]]\!]_{\ell[\ell'/\alpha]} & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\ = & [\![(\tau_1[\ell'/\alpha] + \tau_2[\ell'/\alpha])]\!]_{\ell[\ell'/\alpha]} & \text{(Definition of } [\![\cdot]\!]) \\ = & [\![(\tau_1 + \tau_2)[\ell'/\alpha]]\!]_{\ell[\ell'/\alpha]} & \end{array}$$

5. $\mathsf{A} = \tau_1 \xrightarrow{\ell_e} \tau_2$:

$$\begin{array}{ll} & \left[\!\!\left[\tau_1 \xrightarrow{\ell_e} \tau_2\right]\!\!\right]_\ell[\ell'/\alpha] \\ = & \forall\beta_1.\beta_1, (\forall\beta.\beta_1, ((\ell \sqsubseteq \beta_1 \sqsubseteq \ell_e \wedge \beta \sqsubseteq \beta_1) \overset{\beta_1}{\Rightarrow} ([\![\tau_1]\!]_\beta \xrightarrow{\beta_1} [\![\tau_2]\!]_{\beta_1})^{\beta_1})^{\beta_1})^{\beta_1}[\ell'/\alpha] \\ & \text{(Definition of } [\![\cdot]\!]) \\ = & \forall\beta_1.\beta_1, (\forall\beta.\beta_1, ((\ell[\ell'/\alpha] \sqsubseteq \beta_1 \sqsubseteq \ell_e[\ell'/\alpha] \wedge \beta \sqsubseteq \beta_1) \overset{\beta_1}{\Rightarrow} ([\![\tau_1]\!]_\beta[\ell'/\alpha] \xrightarrow{\beta_1} [\![\tau_2]\!]_{\beta_1}[\ell'/\alpha])^{\beta_1})^{\beta_1})^{\beta_1} \\ = & \forall\beta_1.\beta_1, (\forall\beta.\beta_1, ((\ell[\ell'/\alpha] \sqsubseteq \beta_1 \sqsubseteq \ell_e[\ell'/\alpha] \wedge \beta \sqsubseteq \beta_1) \overset{\beta_1}{\Rightarrow} ([\![\tau_1[\ell'/\alpha]]\!]_\beta \xrightarrow{\beta_1} [\![\tau_2[\ell'/\alpha]]\!]_{\beta_1})^{\beta_1})^{\beta_1})^{\beta_1} \\ & \text{(IH1 on } \tau_1 \text{ and } \tau_2) \\ = & \left[\!\!\left[(\tau_1[\ell'/\alpha] \xrightarrow{\ell_e[\ell'/\alpha]} \tau_2[\ell'/\alpha])\right]\!\!\right]_{\ell[\ell'/\alpha]} \\ = & \left[\!\!\left[(\tau_1 \xrightarrow{\ell_e} \tau_2)[\ell'/\alpha]\right]\!\!\right]_{\ell[\ell'/\alpha]} \end{array}$$

6. $\mathsf{A} = \forall\gamma.\tau_i$:

$$\begin{array}{ll} & [\![\forall\beta.\tau_i]\!]_\ell[\ell'/\alpha] \\ = & \forall\beta.\beta, ((\ell \sqsubseteq \beta \sqsubseteq \ell_e) \overset{\beta}{\Rightarrow} (\forall\gamma.\beta, [\![\tau_i]\!]_\beta)^\beta)^\beta[\ell'/\alpha] \\ & \text{(Definition of } [\![\cdot]\!]) \\ = & \forall\beta.\beta, ((\ell[\ell'/\alpha] \sqsubseteq \beta \sqsubseteq \ell_e[\ell'/\alpha]) \overset{\beta}{\Rightarrow} (\forall\gamma.\beta, [\![\tau_i]\!]_\beta[\ell'/\alpha])^\beta)^\beta \\ = & \forall\beta.\beta, ((\ell[\ell'/\alpha] \sqsubseteq \beta \sqsubseteq \ell_e[\ell'/\alpha]) \overset{\beta}{\Rightarrow} (\forall\gamma.\beta, [\![\tau_i[\ell'/\alpha]]\!]_\beta)^\beta)^\beta \\ & \text{IH1 on } \tau_i \\ = & [\![\forall\beta.\ell_e[\ell'/\alpha], \tau_i[\ell'/\alpha]]\!]_{\ell[\ell'/\alpha]} \end{array}$$

7. $\mathsf{A} = c \Rightarrow \tau_i$:

$$
\begin{array}{rl}
& [\![c \Rightarrow \tau_i]\!]_\ell[\ell'/\alpha] \\
= & \forall\beta.\beta, (((c \wedge \ell \sqsubseteq \beta \sqsubseteq \ell_e) \overset{\beta}{\Rightarrow} [\![\tau]\!]_\beta)^\beta)^\beta[\ell'/\alpha] \\
& \text{(Definition of } [\![\cdot]\!]) \\
= & \forall\beta.\beta, (((c[\ell'/\alpha] \wedge \ell[\ell'/\alpha] \sqsubseteq \beta \sqsubseteq \ell_e[\ell'/\alpha]) \overset{\beta}{\Rightarrow} [\![\tau]\!]_\beta[\ell'/\alpha])^\beta)^\beta \\
= & \forall\beta.\beta, (((c[\ell'/\alpha] \wedge \ell[\ell'/\alpha] \sqsubseteq \beta \sqsubseteq \ell_e[\ell'/\alpha]) \overset{\beta}{\Rightarrow} [\![\tau[\ell'/\alpha]]\!]_\beta)^\beta)^\beta \\
& \text{IH1 on } \tau_i \\
= & \left[\!\!\left[(c[\ell'/\alpha] \overset{\ell_e[\ell'/\alpha]}{\Rightarrow} \tau_i[\ell'/\alpha])\right]\!\!\right]_{\ell[\ell'/\alpha]} \\
= & \left[\!\!\left[(c \overset{\ell_e}{\Rightarrow} \tau_i)[\ell'/\alpha]\right]\!\!\right]_{\ell[\ell'/\alpha]}
\end{array}
$$

□

Lemma 3.29 (FG $\rightsquigarrow$ FG$^-$: Preservation of protection relation)**.** $\forall\tau, \ell, \ell'.$
$\tau \searrow \ell \implies [\![\tau]\!]_{\ell'} \searrow \ell$

Proof. Let $\tau = \mathsf{A}^{\ell_i}$

$$
\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\overline{\tau \searrow \ell}\ \text{Given}}{\ell \sqsubseteq \ell_i}\ \text{Given}}{\ell \sqsubseteq (\ell' \sqcup \ell_i)}\ \text{By inversion}}{([\![\mathsf{A}]\!]_{\ell' \sqcup \ell_i})^{\ell' \sqcup \ell_i} \searrow \ell}}{\left[\!\!\left[\mathsf{A}^{\ell_i}\right]\!\!\right]_{\ell'} \searrow \ell}\ \text{Definition of } [\![\cdot]\!]}{[\![\tau]\!]_{\ell'} \searrow \ell}
$$

□

3.3 Translation from FG to SLIO*

3.3.1 Type directed (direct) translation from FG to SLIO*

Definition 3.30 (FG $\rightsquigarrow$ SLIO*: Type translation)**.**

$$
\begin{array}{lcl}
(\!|\mathsf{b}|\!)_\ell & = & \mathsf{b} \\
(\!|\mathsf{unit}|\!)_\ell & = & \mathsf{unit} \\
(\!|\tau_1 \xrightarrow{\ell_e} \tau_2|\!)_\ell & = & \forall \alpha, \beta, \gamma.(\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_\beta \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_\alpha \\
(\!|\tau_1 \times \tau_2|\!)_\ell & = & (\!|\tau_1|\!)_\ell \times (\!|\tau_2|\!)_\ell \\
(\!|\tau_1 + \tau_2|\!)_\ell & = & (\!|\tau_1|\!)_\ell + (\!|\tau_2|\!)_\ell \\
(\!|\mathsf{ref}\ \mathsf{A}^{\ell'}|\!)_\ell & = & \mathsf{ref}\ \ell'\ (\!|\mathsf{A}|\!)_{\ell'} \\
(\!|\forall \alpha.(\ell_e, \tau)|\!)_\ell & = & \forall \alpha, \alpha', \gamma.(\ell \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau|\!)_{\alpha'} \\
(\!|c \overset{\ell_e}{\Rightarrow} \tau|\!)_\ell & = & \forall \alpha, \gamma.(c \wedge \ell \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau|\!)_\alpha \\
 & & \\
(\!|\mathsf{A}^{\ell'}|\!)_\ell & = & \mathsf{Labeled}\ (\ell \sqcup \ell')\ (\!|\mathsf{A}|\!)_{\ell \sqcup \ell'}
\end{array}
$$

For $\Gamma = x_1 : \tau_1, \ldots, x_n : \tau_n$ and $\overline{\ell} = \ell_1, \ldots, \ell_n$, define $(\!|\Gamma|\!)_{\overline{\ell}} = x_1 : (\!|\tau_1|\!)_{\ell_1}, \ldots, x_n : (\!|\tau_n|\!)_{\ell_n}$.
We use a coersion function defined as follows:

$$
\begin{array}{l}
\texttt{coerce\_taint} \ :\ \mathbb{SLIO}\ \gamma\ \alpha_c\ \tau' \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ \tau' \quad \text{when } \tau' = \mathsf{Labeled}\ \alpha'_c\ \tau \text{ and } \Sigma, \Psi \models \alpha_c \sqsubseteq \alpha'_c \\
\texttt{coerce\_taint} \triangleq \lambda x.\mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y)))
\end{array}
$$

$$
\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash_{pc} x : \tau \rightsquigarrow \mathsf{ret}\ x}\ \text{FC-var}
$$

$$
\frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{\ell_e} e : \tau_2 \rightsquigarrow e_{c1}}{\Sigma; \Psi; \Gamma \vdash_{pc} \lambda x.e : (\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(\lambda x.e_{c1}))))}\ \text{FC-lam}
$$

$$
\frac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\ell_e} \tau_2)^\ell \rightsquigarrow e_{c1} \\ \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_1 \rightsquigarrow e_{c2} \qquad \Sigma; \Psi \vdash \ell \sqcup pc \sqsubseteq \ell_e \qquad \Sigma; \Psi \vdash \tau \searrow \ell\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1\ e_2 : \tau_2 \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[\,][\,][\,]\bullet)\ b))))}\ \text{FC-app}
$$

$$
\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : \tau_1 \rightsquigarrow e_{c1} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_2 \rightsquigarrow e_{c2}}{\Sigma; \Psi; \Gamma \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^\perp \rightsquigarrow \mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{ret}(\mathsf{Lb}(a, b))))}\ \text{FC-prod}
$$

$$
\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^\ell \rightsquigarrow e_c \qquad \Sigma; \Psi \vdash \tau_1 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{fst}(e) : \tau_1 \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))}\ \text{FC-fst}
$$

$$
\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^\ell \rightsquigarrow e_c \qquad \Sigma; \Psi \vdash \tau_1 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{snd}(e) : \tau_2 \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b)))))}\ \text{FC-snd}
$$

$$
\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau_1 \rightsquigarrow e_c}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inl}(e) : (\tau_1 + \tau_2)^\perp \rightsquigarrow \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinl}(a)))}\ \text{FC-inl}
$$

$$
\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau_2 \rightsquigarrow e_c}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inr}(e) : (\tau_1 + \tau_2)^\perp \rightsquigarrow \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinr}(a)))}\ \text{FC-inr}
$$

$$\frac{\begin{array}{c}\Sigma;\Psi;\Gamma \vdash_{pc} e : (\tau_1+\tau_2)^{\ell} \rightsquigarrow e_c \\ \Sigma;\Psi;\Gamma, x:\tau_1 \vdash_{pc\sqcup\ell} e_1 : \tau \rightsquigarrow e_{c1} \qquad \Sigma;\Psi;\Gamma, x:\tau_1 \vdash_{pc\sqcup\ell} e_2 : \tau \rightsquigarrow e_{c2} \qquad \Sigma;\Psi \vdash \tau \searrow \ell\end{array}}{\begin{array}{c}\Sigma;\Psi;\Gamma \vdash_{pc} \mathsf{case}(e, x.e_1, y.e_2) : \tau \rightsquigarrow \\ \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2}))))\end{array}} \text{FC-case}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e : \tau \rightsquigarrow e_c \qquad \Sigma;\Psi \vdash \tau \searrow pc}{\Sigma;\Psi;\Gamma \vdash_{pc} \mathsf{new}\ (e) : (\mathsf{ref}\ \tau)^{\perp} \rightsquigarrow \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb}b)))} \text{FC-ref}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e : (\mathsf{ref}\ \tau)^{\ell} \rightsquigarrow e_c \qquad \Sigma;\Psi \vdash \tau <: \tau' \qquad \Sigma;\Psi \vdash \tau' \searrow \ell}{\Sigma;\Psi;\Gamma \vdash_{pc} !e : \tau \rightsquigarrow \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))} \text{FC-deref}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e_1 : (\mathsf{ref}\ \tau)^{\ell} \rightsquigarrow e_{c1} \qquad \Sigma;\Psi;\Gamma \vdash_{pc} e_2 : \tau \rightsquigarrow e_{c2} \qquad \tau \searrow (pc \sqcup \ell)}{\begin{array}{c}\Sigma;\Psi;\Gamma \vdash_{pc} e_1 := e_2 : \mathsf{unit} \rightsquigarrow \\ \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())\end{array}} \text{FC-assign}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash_{\ell_e} e : \tau \rightsquigarrow e_c}{\Sigma;\Psi;\Gamma \vdash_{pc} \Lambda e : (\forall \alpha_g.(\ell_e, \tau))^{\perp} \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(e_c))))} \text{FC-FI}$$

$$\frac{\begin{array}{c}\Sigma;\Psi;\Gamma \vdash_{pc} e : (\forall \alpha_g.(\ell_e, \tau))^{\ell} \rightsquigarrow e_c \\ \mathrm{FV}(\ell') \subseteq \Sigma \qquad \Sigma;\Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e[\ell'/\alpha] \qquad \Sigma;\Psi \vdash \tau[\ell'/\alpha] \searrow \ell\end{array}}{\Sigma;\Psi;\Gamma \vdash_{pc} e[] : \tau \rightsquigarrow \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][][]\bullet)))} \text{FC-FE}$$

$$\frac{\Sigma;\Psi, c;\Gamma \vdash_{\ell_e} e : \tau \rightsquigarrow e_c}{\Sigma;\Psi;\Gamma \vdash_{pc} \nu e : (c \overset{\ell_e}{\Rightarrow} \tau))^{\perp} \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda(\nu(e_c))))} \text{FC-CI}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e : (c \overset{\ell_e}{\Rightarrow} \tau))^{\ell} \rightsquigarrow e_c \qquad \Sigma;\Psi \vdash c \qquad \Sigma;\Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e \qquad \Sigma;\Psi \vdash \tau \searrow \ell}{\Sigma;\Psi;\Gamma \vdash_{pc} e\bullet : \tau \rightsquigarrow \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][]\bullet)))} \text{FC-CE}$$

3.3.2 Type preservation for FG to SLIO* translation

Lemma 3.31 (Coercion lemma - typing)**.** $\forall \Sigma, \Psi, \Gamma, \alpha_c, \alpha_c', \tau.$
$\Sigma, \Psi \models \alpha_c \sqsubseteq \alpha_c' \implies$
$\Sigma;\Psi;\Gamma \vdash \mathtt{coerce\_taint} : \mathbb{SLIO}\ \gamma\ \alpha_c\ \mathsf{Labeled}\ \alpha_c'\ \tau \to \mathbb{SLIO}\ \gamma\ \gamma\ \mathsf{Labeled}\ \alpha_c'\ \tau$

Proof. $T_{c4} = \mathsf{Labeled}\ \alpha_c'\ \tau$
$T_{c3} = \mathbb{SLIO}\ \alpha_c\ \alpha_c'\ \tau$
$T_{c2} = \mathbb{SLIO}\ \gamma\ \alpha_c'\ \tau$
$T_{c1} = \mathbb{SLIO}\ \gamma\ \gamma\ \mathsf{Labeled}\ \alpha_c'\ \tau$
$T_{c0} = \mathbb{SLIO}\ \gamma\ \alpha_c\ \mathsf{Labeled}\ \alpha_c'\ \tau$
$T_c = T_{c0} \to T_{c1}$
Pc2:

$$\frac{\dfrac{}{\Sigma;\Psi;\Gamma, x : T_{c0}, y : T_{c4} \vdash y : T_{c4}} \text{SLIO*-var} \qquad \dfrac{}{\Sigma, \Psi \models \alpha_c \sqsubseteq \alpha_c'} \text{Given}}{\Sigma;\Psi;\Gamma, x : T_{c0}, y : T_{c4} \vdash \mathsf{unlabel}(y) : T_{c3}} \text{SLIO*-unlabel}$$

Pc1:

$$\frac{}{\Sigma; \Psi; \Gamma, x : T_{c0} \vdash x : T_{c0}} \text{ SLIO}^*\text{-var}$$

Pc0:

$$\frac{\dfrac{Pc1 \qquad Pc2}{\Sigma; \Psi; \Gamma, x : T_{c0} \vdash \mathsf{bind}(x, y.\mathsf{unlabel}(y)) : T_{c2}} \text{ SLIO}^*\text{-bind}}{\Sigma; \Psi; \Gamma, x : T_{c0} \vdash \mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_{c1}} \text{ SLIO}^*\text{-tolabeled}$$

Pc:

$$\frac{\dfrac{Pc0}{\Sigma; \Psi; \Gamma \vdash \lambda x.\mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_c} \text{ SLIO}^*\text{-lam}}{\Sigma; \Psi; \Gamma \vdash \texttt{coerce\_taint} : T_c} \text{ From Definition of } \texttt{coerce\_taint}$$

□

Theorem 3.32 (FG $\rightsquigarrow$ SLIO*: Type preservation)**.** *Suppose* $\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau$ *in FG. Then, there exists* e' *such that* $\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau \rightsquigarrow e'$ *and for any* $\alpha', \overline{\beta'}, \gamma'$ *with* $\overline{\beta'} \sqcup \gamma' \sqsubseteq pc \sqcap \alpha'$*, there is a derivation of* $\Sigma; \Psi; (\!|\Gamma|\!)_{\overline{\beta'}} \vdash e' : \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\tau|\!)_{\alpha'}$ *in SLIO*.*

Proof. Proof by induction on the $\rightsquigarrow$ relation

1. FC-var:

$$\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash_{pc} x : \tau \rightsquigarrow \mathsf{ret}\ x} \text{ FC-var}$$

$$\frac{\dfrac{\dfrac{\dfrac{}{(\!|\Gamma|\!)_{\overline{\beta'_o}}(x) = (\!|\tau|\!)_{\beta''_o}} \text{ Given}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\overline{\beta'_o}} \vdash x : (\!|\tau|\!)_{\beta'_o}} \text{ SLIO}^*\text{-var} \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash \beta'_o \sqcup \gamma'_o \sqsubseteq \alpha'_o \sqcap pc} \text{ Given}}{\Sigma; \Psi \vdash \beta'_o \sqsubseteq \alpha'_o}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\overline{\beta'_o}} \vdash x : (\!|\tau|\!)_{\alpha'_o}} \text{ Lemma 3.33, SLIO}^*\text{-sub}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\overline{\beta'_o}} \vdash \mathsf{ret}\ x : \mathbb{SLIO}\ \gamma'_o\ \gamma'_o\ (\!|\tau|\!)_{\alpha'_o}}$$

2. FC-lam:

$$\frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{\ell_e} e : \tau_2 \rightsquigarrow e_{c1}}{\Sigma; \Psi; \Gamma \vdash_{pc} \lambda x.e : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\perp} \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(\lambda x.e_{c1}))))} \text{ FC-lam}$$

$$T_0 = \mathbb{SLIO}\ \gamma'_j\ \gamma'_j\ (\!|(\tau_1 \xrightarrow{\ell_e} \tau_2)^{\perp}|\!)_{\alpha'_j} = \mathbb{SLIO}\ \gamma'_j\ \gamma'_j\ \mathsf{Labeled}\ \alpha'_j\ (\!|(\tau_1 \xrightarrow{\ell_e} \tau_2)|\!)_{\alpha'_j}$$
$$T_1 = \mathbb{SLIO}\ \gamma'_j\ \gamma'_j\ \mathsf{Labeled}\ \alpha'_j\ \forall \alpha_t, \beta_t, \gamma_t.(\alpha'_j \sqcup \beta_t \sqcup \gamma_t \sqsubseteq \alpha_t \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_{\beta_t} \rightarrow \mathbb{SLIO}\ \gamma_t\ \gamma_t\ (\!|\tau_2|\!)_{\alpha_t}$$
$$T_{1.0} = \mathsf{Labeled}\ \alpha'_j\ \forall \alpha_t, \beta_t, \gamma_t.(\alpha'_j \sqcup \beta_t \sqcup \gamma_t \sqsubseteq \alpha_t \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_{\beta_t} \rightarrow \mathbb{SLIO}\ \gamma_t\ \gamma_t\ (\!|\tau_2|\!)_{\alpha_t}$$
$$T_{1.1} = \forall \alpha_t, \beta_t, \gamma_t.(\alpha'_j \sqcup \beta_t \sqcup \gamma_t \sqsubseteq \alpha_t \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_{\beta_t} \rightarrow \mathbb{SLIO}\ \gamma_t\ \gamma_t\ (\!|\tau_2|\!)_{\alpha_t}$$
$$T_{1.2} = (\alpha'_j \sqcup \beta_t \sqcup \gamma_t \sqsubseteq \alpha_t \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_{\beta_t} \rightarrow \mathbb{SLIO}\ \gamma_t\ \gamma_t\ (\!|\tau_2|\!)_{\alpha_t}$$
$$T_{1.3} = (\!|\tau_1|\!)_{\beta_t} \rightarrow \mathbb{SLIO}\ \gamma_t\ \gamma_t\ (\!|\tau_2|\!)_{\alpha_t}$$
$$T_{1.4} = \mathbb{SLIO}\ \gamma_t\ \gamma_t\ (\!|\tau_2|\!)_{\alpha_t}$$

P3:

$$\dfrac{\dfrac{}{\Sigma, \alpha_t, \beta_t, \gamma_t; \Psi, (\alpha'_j \sqcup \beta_t \sqcup \gamma_t \sqsubseteq \alpha_t \sqcap \ell_e) \vdash \overline{\beta'_j} \sqcup \gamma_j \sqsubseteq \alpha'_j \sqcap pc}\text{ Given, Weakening}}{\Sigma, \alpha_t, \beta_t, \gamma_t; \Psi, (\alpha'_j \sqcup \beta_t \sqcup \gamma_t \sqsubseteq \alpha_t \sqcap \ell_e) \vdash \overline{\beta'_j} \sqsubseteq \alpha'_j}$$

P2:

$$\dfrac{\dfrac{}{\Sigma, \alpha_t, \beta_t, \gamma_t; \Psi, (\alpha'_j \sqcup \beta_t \sqcup \gamma_t \sqsubseteq \alpha_t \sqcap \ell_e) \vdash \alpha'_j \sqcup \beta_t \sqcup \gamma_t \sqsubseteq \alpha_t \sqcap \ell_e} \quad P3}{\Sigma, \alpha_t, \beta_t, \gamma_t; \Psi, (\alpha'_j \sqcup \beta_t \sqcup \gamma_t \sqsubseteq \alpha_t \sqcap \ell_e) \vdash \overline{\beta'_j} \sqcup \beta_t \sqcup \gamma_t \sqsubseteq \alpha_t \sqcap \ell_e}$$

P1:

$$\dfrac{\dfrac{P2}{\Sigma, \alpha_t, \beta_t, \gamma_t; \Psi, (\alpha'_j \sqcup \beta_t \sqcup \gamma_t \sqsubseteq \alpha_t \sqcap \ell_e); (\!|\Gamma|\!)_{\overline{\beta'_j}}, x : (\!|\tau_1|\!)_{\beta_t} \vdash e_{c1} : T_{1.4}}\text{ IH}}{\Sigma, \alpha_t, \beta_t, \gamma_t; \Psi, (\alpha'_j \sqcup \beta_t \sqcup \gamma_t \sqsubseteq \alpha_t \sqcap \ell_e); (\!|\Gamma|\!)_{\overline{\beta'_j}} \vdash \lambda x.e_{c1} : T_{1.3}}\text{ SLIO}^*\text{-lam}$$

P0:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \overline{\beta'_j} \sqcup \gamma'_j \sqsubseteq \alpha'_j}\text{ Given}}{\Sigma; \Psi \vdash \gamma_j \sqsubseteq \alpha_j}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{P1}{\Sigma, \alpha_t, \beta_t, \gamma_t; \Psi; (\!|\Gamma|\!)_{\overline{\beta'_j}} \vdash \nu(\lambda x.e_{c1}) : T_{1.2}}\text{ SLIO}^*\text{-CI}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\overline{\beta'_j}} \vdash \Lambda\Lambda\Lambda(\nu(\lambda x.e_{c1})) : T_{1.1}}\text{ 3 applications SLIO}^*\text{-FI} \quad P0}{\Sigma; \Psi; (\!|\Gamma|\!)_{\overline{\beta'_j}} \vdash \mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(\lambda x.e_{c1}))) : T_{1.0}}\text{ SLIO}^*\text{-label}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\overline{\beta'_j}} \vdash \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(\lambda x.e_{c1})))) : T_1}\text{ SLIO}^*\text{-ret}$$

3. FC-app:

$$\dfrac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell} \rightsquigarrow e_{c1} \\ \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_1 \rightsquigarrow e_{c2} \qquad \Sigma; \Psi \vdash \ell \sqcup pc \sqsubseteq \ell_e \qquad \Sigma; \Psi \vdash \tau \searrow \ell\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1\ e_2 : \tau_2 \rightsquigarrow \mathtt{coerce\_taint}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b))))}\text{ FC-app}$$

$\beta' = \bigcup_{\beta_i \in \overline{\beta'}} \beta_i$

$T_0 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell}|\!)_{\beta' \sqcup \gamma'} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\!|(\tau_1 \xrightarrow{\ell_e} \tau_2)|\!)_{\beta' \sqcup \gamma' \sqcup \ell}$

$T_1 = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ ((\beta' \sqcup \gamma') \sqcup \ell)\ \forall \alpha, \beta, \gamma.(((\beta' \sqcup \gamma') \sqcup \ell) \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_{\beta} \to \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha}$

$T_{1.1} = \mathsf{Labeled}\ ((\beta' \sqcup \gamma') \sqcup \ell)\ \forall \alpha, \beta, \gamma.(((\beta' \sqcup \gamma') \sqcup \ell) \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_{\beta} \to \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha}$

$T_{1.2} = \mathbb{SLIO}\ \gamma'\ (\gamma' \sqcup (\beta' \sqcup \gamma') \sqcup \ell)\ \forall \alpha, \beta, \gamma.(((\beta' \sqcup \gamma') \sqcup \ell) \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_{\beta} \to \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha}$

$T_{1.3} = \forall \alpha, \beta, \gamma.(((\beta' \sqcup \gamma') \sqcup \ell) \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_{\beta} \to \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha}$

$T_{1.4} = \forall \beta, \gamma.(((\beta' \sqcup \gamma') \sqcup \ell) \sqcup \beta \sqcup \gamma \sqsubseteq ((\beta' \sqcup \gamma') \sqcup \ell) \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_{\beta} \to \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{((\beta' \sqcup \gamma') \sqcup \ell)}$

$T_{1.5} = \forall\gamma.(((\beta' \sqcup \gamma') \sqcup \ell) \sqcup (\beta' \sqcup \gamma') \sqcup \gamma \sqsubseteq ((\beta' \sqcup \gamma') \sqcup \ell) \sqcap \ell_e) \Rightarrow \llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma')} \to \mathbb{SLIO}\ \gamma\ \gamma\ \llparenthesis \tau_2 \rrparenthesis_{((\beta' \sqcup \gamma') \sqcup \ell)}$

$T_{1.6} = (((\beta' \sqcup \gamma') \sqcup \ell) \sqcup (\beta' \sqcup \gamma') \sqcup (\beta' \sqcup \gamma' \sqcup \ell) \sqsubseteq ((\beta' \sqcup \gamma') \sqcup \ell) \sqcap \ell_e) \Rightarrow T_{1.7}$

$T_{1.7} = \llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma')} \to \mathbb{SLIO}\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\beta' \sqcup \gamma' \sqcup \ell)\ \llparenthesis \tau_2 \rrparenthesis_{((\beta' \sqcup \gamma') \sqcup \ell)}$

$T_{1.8} = \mathbb{SLIO}\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\beta' \sqcup \gamma' \sqcup \ell)\ \llparenthesis \tau_2 \rrparenthesis_{((\beta' \sqcup \gamma') \sqcup \ell)}$

$T_{1.9} = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ \llparenthesis \tau_2 \rrparenthesis_{((\beta' \sqcup \gamma') \sqcup \ell)}$

$T_{1.10} = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ \llparenthesis \mathsf{A}^{\ell_i} \rrparenthesis_{((\beta' \sqcup \gamma') \sqcup \ell)}$

$T_{1.11} = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ \mathsf{Labeled}\ (\ell_i \sqcup \beta' \sqcup \gamma' \sqcup \ell)\ \llparenthesis \mathsf{A} \rrparenthesis_{(\ell_i \sqcup \beta' \sqcup \gamma' \sqcup \ell)}$

$T_{1.12} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \mathsf{Labeled}\ (\ell_i \sqcup \beta' \sqcup \gamma' \sqcup \ell)\ \llparenthesis \mathsf{A} \rrparenthesis_{(\ell_i \sqcup \beta' \sqcup \gamma' \sqcup \ell)}$

$T_{1.13} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \mathsf{Labeled}\ (\ell_i \sqcup \beta' \sqcup \gamma')\ \llparenthesis \mathsf{A} \rrparenthesis_{(\ell_i \sqcup \beta' \sqcup \gamma')}$

$T_2 = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \llparenthesis \tau_2 \rrparenthesis_{(\beta' \sqcup \gamma')}$

$T_3 = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma')}$

P8:

$$\frac{}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\overline{\beta'}}, a : T_{1.1}, b : \llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma')}, c : T_{1.3} \vdash b : \llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma')}}\ \text{SLIO}^*\text{-var}$$

P7:

$$\frac{\frac{\frac{\frac{}{\Sigma; \Psi \vdash \ell \sqcup pc \sqsubseteq \ell_e}\ \text{Given}}{\Sigma; \Psi \vdash pc \sqsubseteq \ell_e}}{\Sigma; \Psi \vdash \alpha' \sqcap pc \sqsubseteq \ell_e}}{\Sigma; \Psi \vdash \beta' \sqcup \gamma' \sqsubseteq \alpha' \sqcap pc \sqsubseteq \ell_e}$$

P6:

$$\frac{P7 \qquad \frac{\frac{}{\Sigma; \Psi \vdash \ell \sqcup pc \sqsubseteq \ell_e}\ \text{Given}}{\Sigma; \Psi \vdash \ell \sqsubseteq \ell_e}}{\Sigma; \Psi \vdash (\ell \sqcup \beta' \sqcup \gamma') \sqsubseteq \ell_e}$$

P5:

$$\frac{\frac{\frac{\frac{\frac{}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\overline{\beta'}}, a : T_{1.1}, b : \llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma')}, c : T_{1.3} \vdash c : T_{1.3}}\ \text{SLIO}^*\text{-var}}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\overline{\beta'}}, a : T_{1.1}, b : \llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma')}, c : T_{1.3} \vdash c[] : T_{1.4}}\ \text{SLIO}^*\text{-FE}}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\overline{\beta'}}, a : T_{1.1}, b : \llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma')}, c : T_{1.3} \vdash c[][] : T_{1.5}}\ \text{SLIO}^*\text{-FE}}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\overline{\beta'}}, a : T_{1.1}, b : \llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma')}, c : T_{1.3} \vdash c[][][] : T_{1.6}}\ \text{SLIO}^*\text{-FE} \qquad P6}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\overline{\beta'}}, a : T_{1.1}, b : \llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma')}, c : T_{1.3} \vdash c[][][]\bullet : T_{1.7}}\ \text{SLIO}^*\text{-CE}$$

P4:

$$\frac{P5 \qquad P8}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\overline{\beta'}}, a : T_{1.1}, b : \llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma')}, c : T_{1.3} \vdash (c[][][]\bullet)\ b : T_{1.8}}\ \text{SLIO}^*\text{-app}$$

P3:

$$\frac{}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\overline{\beta'}}, a : T_{1.1}, b : \llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma')} \vdash a : T_{1.1}}\ \text{SLIO}^*\text{-var}$$

P2:

$$\dfrac{\dfrac{P3}{\Sigma;\Psi;(\!|\Gamma|\!)_{\overline{\beta'}}, a : T_{1.1}, b : (\!|\tau_1|\!)_{(\beta' \sqcup \gamma')} \vdash \mathsf{unlabel}\ a : T_{1.2}}\ \text{SLIO}^*\text{-unlabel} \qquad P4}{\Sigma;\Psi;(\!|\Gamma|\!)_{\overline{\beta'}}, a : T_{1.1}, b : (\!|\tau_1|\!)_{(\beta' \sqcup \gamma')} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b) : T_{1.9}}\ \text{SLIO}^*\text{-bind}$$

P1:

$$\dfrac{\dfrac{}{\Sigma;\Psi;(\!|\Gamma|\!)_{\overline{\beta'}}, a : T_{1.1} \vdash e_{c2} : T_3}\ \text{IH2, Weakening} \qquad P2}{\Sigma;\Psi;(\!|\Gamma|\!)_{\overline{\beta'}}, a : T_{1.1} \vdash \mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b)) : T_{1.9}}\ \text{SLIO}^*\text{-bind}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi;(\!|\Gamma|\!)_{\overline{\beta'}} \vdash e_{c1} : T_1}\ \text{IH1 with } (\beta' \sqcup \gamma'), \overline{\beta'}, \gamma' \qquad P1}{\Sigma;\Psi;(\!|\Gamma|\!)_{\overline{\beta'}} \vdash \mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b))) : T_{1.9}}\ \text{SLIO}^*\text{-bind}}{\Sigma;\Psi;(\!|\Gamma|\!)_{\overline{\beta'}} \vdash \mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b))) : T_{1.10}}}{\Sigma;\Psi;(\!|\Gamma|\!)_{\overline{\beta'}} \vdash \mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b))) : T_{1.11}}}{\Sigma;\Psi;(\!|\Gamma|\!)_{\overline{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b)))) : T_{1.12}}\ \text{Lemma 3.31}}{\Sigma;\Psi;(\!|\Gamma|\!)_{\overline{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b)))) : T_{1.13}}}{\Sigma;\Psi;(\!|\Gamma|\!)_{\overline{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b)))) : T_2}$$

4. FC-prod:

$$\dfrac{\Sigma;\Psi;\Gamma \vdash_{pc} e_1 : \tau_1 \rightsquigarrow e_{c1} \qquad \Sigma;\Psi;\Gamma \vdash_{pc} e_2 : \tau_2 \rightsquigarrow e_{c2}}{\Sigma;\Psi;\Gamma \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^{\perp} \rightsquigarrow \mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{ret}(\mathsf{Lb}(a, b))))}\ \text{FC-prod}$$

$T_1 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(\tau_1 \times \tau_2)^{\perp}|\!)_{\alpha'}$

$T_2 = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \alpha'\ (\!|(\tau_1 \times \tau_2)|\!)_{\alpha'}$

$T_3 = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \alpha'\ (\!|\tau_1|\!)_{\alpha'} \times (\!|\tau_2|\!)_{\alpha'}$

$T_{3.1} = \mathsf{Labeled}\ \alpha'\ (\!|\tau_1|\!)_{\alpha'} \times (\!|\tau_2|\!)_{\alpha'}$

$T_4 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\tau_1|\!)_{\alpha'}$

$T_5 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\tau_2|\!)_{\alpha'}$

P4:

$$\dfrac{}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'}, b : (\!|\tau_1|\!)_{\alpha'} \vdash a : (\!|\tau_1|\!)_{\alpha'}}\ \text{SLIO}^*\text{-var}$$

P3:

$$\dfrac{}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'}, b : (\!|\tau_1|\!)_{\alpha'} \vdash b : (\!|\tau_2|\!)_{\alpha'}}\ \text{SLIO}^*\text{-var}$$

P2:

$$\dfrac{\dfrac{\dfrac{P3 \qquad P4}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'}, b : (\!|\tau_1|\!)_{\alpha'} \vdash (a, b) : (\!|\tau_1|\!)_{\alpha'} \times (\!|\tau_2|\!)_{\alpha'}}\ \text{SLIO}^*\text{-prod}}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'}, b : (\!|\tau_2|\!)_{\alpha'} \vdash \mathsf{Lb}(a, b) : T_{3.1}}\ \text{SLIO}^*\text{-label}}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'}, b : (\!|\tau_2|\!)_{\alpha'} \vdash \mathsf{ret}(\mathsf{Lb}(a, b)) : T_3}\ \text{SLIO}^*\text{-ret}$$

P1:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'} \vdash e_{c2} : T_5}\text{ IH2} \qquad P2}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'} \vdash \mathsf{bind}(e_{c2}, b.\mathsf{ret}(\mathsf{Lb}(a, b))) : T_3}\text{ SLIO}^*\text{-bind}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash e_{c1} : T_4}\text{ IH1} \qquad P1}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{ret}(\mathsf{Lb}(a, b)))) : T_3}\text{ SLIO}^*\text{-bind}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{ret}(\mathsf{Lb}(a, b)))) : T_1}\text{ Definition 3.30}$$

5. FC-fst:

$$\dfrac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^{\ell} \rightsquigarrow e_c \qquad \Sigma; \Psi \vdash \tau_1 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{fst}(e) : \tau_1 \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))}\text{ FC-fst}$$

$T_1 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\tau_1|\!)_{\alpha'}$

$T_2 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(\tau_1 \times \tau_2)^{\ell}|\!)_{\alpha'}$

$T_{2.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell \sqcup \alpha'\ (\!|(\tau_1 \times \tau_2)|\!)_{\alpha' \sqcup \ell}$

$T_{2.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell \sqcup \alpha'\ (\!|\tau_1|\!)_{\alpha' \sqcup \ell} \times (\!|\tau_2|\!)_{\alpha' \sqcup \ell}$

$T_{2.3} = \mathsf{Labeled}\ \ell \sqcup \alpha'\ (\!|\tau_1|\!)_{\alpha' \sqcup \ell} \times (\!|\tau_2|\!)_{\alpha' \sqcup \ell}$

$T_{2.4} = (\!|\tau_1|\!)_{\alpha' \sqcup \ell} \times (\!|\tau_2|\!)_{\alpha' \sqcup \ell}$

$T_{2.5} = \mathbb{SLIO}\ (\gamma')\ (\gamma' \sqcup \alpha' \sqcup \ell)\ (\!|\tau_1|\!)_{\alpha' \sqcup \ell} \times (\!|\tau_2|\!)_{\alpha' \sqcup \ell}$

$T_3 = \mathbb{SLIO}\ (\gamma' \sqcup \alpha' \sqcup \ell)\ (\gamma' \sqcup \alpha' \sqcup \ell)\ (\!|\tau_1|\!)_{\alpha' \sqcup \ell}$

$T_{3.1} = \mathbb{SLIO}\ (\gamma')\ (\gamma' \sqcup \alpha' \sqcup \ell)\ (\!|\tau_1|\!)_{\alpha' \sqcup \ell}$

$T_{3.2} = \mathbb{SLIO}\ (\gamma')\ (\alpha' \sqcup \ell)\ (\!|\tau_1|\!)_{\alpha' \sqcup \ell}$

$T_{3.3} = \mathbb{SLIO}\ (\gamma')\ (\alpha' \sqcup \ell)\ (\!|\mathsf{A}^{\ell_i}|\!)_{\alpha' \sqcup \ell}$

$T_{3.4} = \mathbb{SLIO}\ (\gamma')\ (\alpha' \sqcup \ell)\ \mathsf{Labeled}\ \ell \sqcup \ell_i \sqcup \alpha'\ (\!|\mathsf{A}|\!)_{\alpha' \sqcup \ell \sqcup \ell_i}$

$T_{3.5} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \mathsf{Labeled}\ \ell \sqcup \ell_i \sqcup \alpha'\ (\!|\mathsf{A}|\!)_{\alpha' \sqcup \ell \sqcup \ell_i}$

$T_{3.6} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \mathsf{Labeled}\ \ell_i \sqcup \alpha'\ (\!|\mathsf{A}|\!)_{\alpha' \sqcup \ell_i}$

$T_{3.7} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ (\!|\mathsf{A}^{\ell_i}|\!)_{\alpha'}$

P2:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.4} \vdash b : T_{2.4}}\text{ SLIO}^*\text{-var}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.4} \vdash \mathsf{fst}(b) : (\!|\tau_1|\!)_{\alpha' \sqcup \ell}}\text{ SLIO}^*\text{-fst}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.4} \vdash \mathsf{ret}(\mathsf{fst}(b)) : T_3}\text{ SLIO}^*\text{-ret}$$

P1:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3} \vdash \mathsf{unlabel}\ (a) : T_{2.5}}\text{ SLIO}^*\text{-unlabel} \qquad P2}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b))) : T_{3.1}}\text{ SLIO}^*\text{-bind}$$

P0:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash e_c : T_{2.2}}\text{ IH} \qquad P1}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))) : T_{3.1}}\text{ SLIO}^*\text{-bind}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \gamma' \sqsubseteq \alpha'}\text{ Given}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))) : T_{3.2}}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))) : T_{3.3}}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))) : T_{3.4}}\text{ Definition 3.30}$$

$$\dfrac{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))) : T_{3.4}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b))))) : T_{3.5}}\text{ Lemma 3.31}$$

Main derivation:

$$\dfrac{\dfrac{P0 \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{A}^{\ell_i} \searrow \ell}\text{ By inversion}}{\Sigma; \Psi \vdash \ell \sqsubseteq \ell_i}\text{ By inversion}}{\dfrac{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b))))) : T_{3.6}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b))))) : T_{3.7}}\text{ Definition 3.30}}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b))))) : T_1}$$

6. FC-snd:

$$\dfrac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^{\ell} \rightsquigarrow e_c \qquad \Sigma; \Psi \vdash \tau_1 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{snd}(e) : \tau_2 \rightsquigarrow \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b)))))}\text{ FC-snd}$$

$T_1 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\tau_2|\!)_{\alpha'}$

$T_2 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(\tau_1 \times \tau_2)^{\ell}|\!)_{\alpha'}$

$T_{2.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell \sqcup \alpha'\ (\!|(\tau_1 \times \tau_2)|\!)_{\alpha' \sqcup \ell}$

$T_{2.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell \sqcup \alpha'\ (\!|\tau_1|\!)_{\alpha' \sqcup \ell} \times (\!|\tau_2|\!)_{\alpha' \sqcup \ell}$

$T_{2.3} = \mathsf{Labeled}\ \ell \sqcup \alpha'\ (\!|\tau_1|\!)_{\alpha' \sqcup \ell} \times (\!|\tau_2|\!)_{\alpha' \sqcup \ell}$

$T_{2.4} = (\!|\tau_1|\!)_{\alpha' \sqcup \ell} \times (\!|\tau_2|\!)_{\alpha' \sqcup \ell}$

$T_{2.5} = \mathbb{SLIO}\ (\gamma')\ (\gamma' \sqcup \alpha' \sqcup \ell)\ (\!|\tau_1|\!)_{\alpha' \sqcup \ell} \times (\!|\tau_2|\!)_{\alpha' \sqcup \ell}$

$T_3 = \mathbb{SLIO}\ (\gamma' \sqcup \alpha' \sqcup \ell)\ (\gamma' \sqcup \alpha' \sqcup \ell)\ (\!|\tau_2|\!)_{\alpha' \sqcup \ell}$

$T_{3.1} = \mathbb{SLIO}\ (\gamma')\ (\gamma' \sqcup \alpha' \sqcup \ell)\ (\!|\tau_2|\!)_{\alpha' \sqcup \ell}$

$T_{3.2} = \mathbb{SLIO}\ (\gamma')\ (\alpha' \sqcup \ell)\ (\!|\tau_2|\!)_{\alpha' \sqcup \ell}$

$T_{3.3} = \mathbb{SLIO}\ (\gamma')\ (\alpha' \sqcup \ell)\ (\!|\mathsf{A}^{\ell_i}|\!)_{\alpha' \sqcup \ell}$

$T_{3.4} = \mathbb{SLIO}\ (\gamma')\ (\alpha' \sqcup \ell)\ \mathsf{Labeled}\ \ell \sqcup \ell_i \sqcup \alpha'\ (\!|\mathsf{A}|\!)_{\alpha' \sqcup \ell \sqcup \ell_i}$

$T_{3.5} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \mathsf{Labeled}\ \ell \sqcup \ell_i \sqcup \alpha'\ (\!|\mathsf{A}|\!)_{\alpha' \sqcup \ell \sqcup \ell_i}$

$T_{3.6} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \mathsf{Labeled}\ \ell_i \sqcup \alpha'\ (\!|\mathsf{A}|\!)_{\alpha' \sqcup \ell_i}$

$T_{3.7} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ (\!|\mathsf{A}^{\ell_i}|\!)_{\alpha'}$

P2:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.4} \vdash b : T_{2.4}}\text{ SLIO}^*\text{-var}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.4} \vdash \mathsf{snd}(b) : (\!|\tau_2|\!)_{\alpha' \sqcup \ell}}\text{ SLIO}^*\text{-snd}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.4} \vdash \mathsf{ret}(\mathsf{snd}(b)) : T_3}\text{ SLIO}^*\text{-ret}$$

P1:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3} \vdash \mathsf{unlabel}\ (a) : T_{2.5}}\text{ SLIO}^*\text{-unlabel} \qquad P2}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b))) : T_{3.1}}\text{ SLIO}^*\text{-bind}$$

P0:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash e_c : T_{2.2}}\text{ IH} \qquad P1}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b)))) : T_{3.1}}\text{ SLIO}^*\text{-bind} \qquad \dfrac{}{\Sigma; \Psi \vdash \gamma' \sqsubseteq \alpha'}\text{ Given}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b)))) : T_{3.2}}}{\dfrac{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b)))) : T_{3.3}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b)))) : T_{3.4}}\text{ Definition 3.30}}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b))))) : T_{3.5}}\text{ Lemma 3.31}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{P0 \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{A}^{\ell_i} \searrow \ell}\text{ By inversion}}{\Sigma; \Psi \vdash \ell \sqsubseteq \ell_i}\text{ By inversion}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b))))) : T_{3.6}}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b))))) : T_{3.7}}\text{ Definition 3.30}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b))))) : T_1}$$

7. FC-inl:

$$\dfrac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau_1 \rightsquigarrow e_c}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inl}(e) : (\tau_1 + \tau_2)^{\perp} \rightsquigarrow \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinl}(a)))}\text{ FC-inl}$$

$T_1 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(\tau_1 + \tau_2)^{\perp}|\!)_{\alpha'}$

$T_{1.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \alpha'\ (\!|(\tau_1 + \tau_2)|\!)_{\alpha'}$

$T_{1.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \alpha'\ (\!|\tau_1|\!)_{\alpha'} + (\!|\tau_2|\!)_{\alpha'}$

$T_{1.3} = \mathsf{Labeled}\ \alpha'\ (\!|\tau_1|\!)_{\alpha'} + (\!|\tau_2|\!)_{\alpha'}$

$T_2 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\tau_1|\!)_{\alpha'}$

P1:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'} \vdash a : (\!|\tau_1|\!)_{\alpha'}}\text{ SLIO}^*\text{-var}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'} \vdash \mathsf{inl}(a) : (\!|\tau_1|\!)_{\alpha'} + (\!|\tau_2|\!)_{\alpha'}}\text{ SLIO}^*\text{-inl}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'} \vdash \mathsf{Lbinl}(a) : T_{1.3}}\text{ SLIO}^*\text{-label}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'} \vdash \mathsf{ret}(\mathsf{Lbinl}(a)) : T_{1.2}}\text{ SLIO}^*\text{-ret}$$

Main derivation:

$$\dfrac{\dfrac{\overline{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash e_c : T_2}\ \text{IH} \qquad P1}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinl}(a))) : T_{1.2}}\ \text{SLIO}^*\text{-bind}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinl}(a))) : T_1}\ \text{Definition 3.30}$$

8. FC-inr:

$$\dfrac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau_2 \rightsquigarrow e_c}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inr}(e) : (\tau_1 + \tau_2)^{\perp} \rightsquigarrow \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinr}(a)))}\ \text{FC-inr}$$

$T_1 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(\tau_1 + \tau_2)^{\perp}|\!)_{\alpha'}$

$T_{1.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \alpha'\ (\!|(\tau_1 + \tau_2)|\!)_{\alpha'}$

$T_{1.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \alpha'\ (\!|\tau_1|\!)_{\alpha'} + (\!|\tau_2|\!)_{\alpha'}$

$T_{1.3} = \mathsf{Labeled}\ \alpha'\ (\!|\tau_1|\!)_{\alpha'} + (\!|\tau_2|\!)_{\alpha'}$

$T_2 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\tau_2|\!)_{\alpha'}$

P1:

$$\dfrac{\dfrac{\dfrac{\overline{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'} \vdash a : (\!|\tau_1|\!)_{\alpha'}}\ \text{SLIO}^*\text{-var}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'} \vdash \mathsf{inr}(a) : (\!|\tau_1|\!)_{\alpha'} + (\!|\tau_2|\!)_{\alpha'}}\ \text{SLIO}^*\text{-inr}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'} \vdash \mathsf{Lbinr}(a) : T_{1.3}}\ \text{SLIO}^*\text{-label}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : (\!|\tau_1|\!)_{\alpha'} \vdash \mathsf{ret}(\mathsf{Lbinr}(a)) : T_{1.2}}\ \text{SLIO}^*\text{-ret}$$

Main derivation:

$$\dfrac{\dfrac{\overline{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash e_c : T_2}\ \text{IH} \qquad P1}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinr}(a))) : T_{1.2}}\ \text{SLIO}^*\text{-bind}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinr}(a))) : T_1}\ \text{Definition 3.30}$$

9. FC-case:

$$\dfrac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 + \tau_2)^{\ell} \rightsquigarrow e_c \\ \Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_1 : \tau \rightsquigarrow e_{c1} \qquad \Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_2 : \tau \rightsquigarrow e_{c2} \qquad \Sigma; \Psi \vdash \tau \searrow \ell\end{array}}{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{case}(e, x.e_1, y.e_2) : \tau \rightsquigarrow \\ \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2}))))\end{array}}\ \text{FC-case}$$

$\beta' = \bigcup_{\beta_i \in \overline{\beta'}} \beta_i$

$T_1 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\tau|\!)_{(\alpha')}$

$T_2 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(\tau_1 + \tau_2)^{\ell}|\!)_{(\beta' \sqcup \gamma')}$

$T_{2.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ ((\beta' \sqcup \gamma') \sqcup \ell)\ (\!|\tau_1 + \tau_2|\!)_{(\beta' \sqcup \gamma') \sqcup \ell}$

$T_{2.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ ((\beta' \sqcup \gamma') \sqcup \ell)\ (\llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma') \sqcup \ell} + \llparenthesis \tau_2 \rrparenthesis_{(\beta' \sqcup \gamma') \sqcup \ell})$

$T_{2.3} = \mathsf{Labeled}\ ((\beta' \sqcup \gamma') \sqcup \ell)\ (\llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma') \sqcup \ell} + \llparenthesis \tau_2 \rrparenthesis_{(\beta' \sqcup \gamma') \sqcup \ell})$

$T_{2.4} = \mathbb{SLIO}\ \gamma'\ (\gamma' \sqcup (\beta' \sqcup \gamma') \sqcup \ell)\ (\llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma') \sqcup \ell} + \llparenthesis \tau_2 \rrparenthesis_{(\beta' \sqcup \gamma') \sqcup \ell})$

$T_{2.5} = (\llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma') \sqcup \ell} + \llparenthesis \tau_2 \rrparenthesis_{(\beta' \sqcup \gamma') \sqcup \ell})$

$T_3 = \mathbb{SLIO}\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\beta' \sqcup \gamma' \sqcup \ell)\ \llparenthesis \tau \rrparenthesis_{(\beta' \sqcup \gamma' \sqcup \ell)}$

$T_4 = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ \llparenthesis \tau \rrparenthesis_{(\beta' \sqcup \gamma' \sqcup \ell)}$

$T_5 = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ \llparenthesis \mathsf{A}^{\ell_i} \rrparenthesis_{(\beta' \sqcup \gamma' \sqcup \ell)}$

$T_{5.1} = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ \mathsf{Labeled}\ \ell_i \sqcup (\beta' \sqcup \gamma' \sqcup \ell)\ \llparenthesis \mathsf{A} \rrparenthesis_{\ell_i \sqcup (\beta' \sqcup \gamma' \sqcup \ell)}$

$T_{5.2} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \mathsf{Labeled}\ \ell_i \sqcup (\beta' \sqcup \gamma' \sqcup \ell)\ \llparenthesis \mathsf{A} \rrparenthesis_{\ell_i \sqcup (\beta' \sqcup \gamma' \sqcup \ell)}$

$T_{5.3} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \mathsf{Labeled}\ \ell_i \sqcup \beta' \sqcup \gamma'\ \llparenthesis \mathsf{A} \rrparenthesis_{\ell_i \sqcup \beta' \sqcup \gamma'}$

$T_{5.4} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \llparenthesis \mathsf{A}^{\ell_i} \rrparenthesis_{\beta' \sqcup \gamma'}$

$T_{5.5} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \llparenthesis \tau \rrparenthesis_{\beta' \sqcup \gamma'}$

P2:

$$\dfrac{\dfrac{}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5} \vdash b : T_{2.5}}\ \text{SLIO}^*\text{-var} \quad \dfrac{}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5}, x : \llparenthesis \tau_1 \rrparenthesis_{(\beta' \sqcup \gamma') \sqcup \ell} \vdash e_{c1} : T_3}\ \text{IH2, Weakening} \quad \dfrac{}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5}, y : \llparenthesis \tau_2 \rrparenthesis_{(\beta' \sqcup \gamma') \sqcup \ell} \vdash e_{c2} : T_3}\ \text{IH3, Weakening}}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5} \vdash \mathsf{case}(b, x.e_{c1}, y.e_{c2}) : T_3}\ \text{SLIO}^*\text{-case}$$

P1:

$$\dfrac{\dfrac{}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\vec{\beta'}}, a : T_{2.3} \vdash \mathsf{unlabel}\ a : T_{2.4}}\ \text{SLIO}^*\text{-unlabel} \qquad P2}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\vec{\beta'}}, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2})) : T_4}\ \text{SLIO}^*\text{-bind}$$

P0:

$$\dfrac{\dfrac{}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\vec{\beta'}} \vdash e_c : T_{2.2}}\ \text{IH1} \qquad P1}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2}))) : T_4}\ \text{SLIO}^*\text{-bind}$$

P0.1:

$$\dfrac{\dfrac{\dfrac{P0}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2}))) : T_5}}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2}))) : T_{5.1}}\ \text{Definition 3.30}}{\Sigma; \Psi; \llparenthesis \Gamma \rrparenthesis_{\vec{\beta'}} \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2})))) : T_{5.2}}\ \text{Lemma 3.31}$$

Main derivation:

$$\dfrac{P0.1 \qquad \dfrac{\dfrac{}{\Sigma;\Psi \vdash \mathsf{A}^{\ell_i} \searrow \ell}\text{ Given}}{\Sigma;\Psi \vdash \ell \sqsubseteq \ell_i}\text{ By inversion}}{\dfrac{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}} \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2})))) : T_{5.3}}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}} \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2}))))T_{5.4}}\text{ Definition 3.30}}$$

$$\dfrac{\dfrac{\cdots}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}} \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2})))) : T_{5.5}} \qquad \dfrac{}{\Sigma;\Psi \vdash (\beta' \sqcup \gamma') \sqsubseteq \alpha'}\text{ Given}}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}} \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2})))) : T_1}$$

10. FC-ref:

$$\dfrac{\Sigma;\Psi;\Gamma \vdash_{pc} e : \tau \leadsto e_c \qquad \Sigma;\Psi \vdash \tau \searrow pc}{\Sigma;\Psi;\Gamma \vdash_{pc} \mathsf{new}\ (e) : (\mathsf{ref}\ \tau)^{\perp} \leadsto \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb}b)))}\text{ FC-ref}$$

$\beta' = \bigcup_{\beta_i \in \overline{\beta'}} \beta_i$

$T_1 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(\mathsf{ref}\ \tau)^{\perp}|\!)_{\alpha'}$

$T_{1.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(\mathsf{ref}\ \mathsf{A}^{\ell_i})^{\perp}|\!)_{\alpha'}$

$T_{1.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \alpha'\ (\!|(\mathsf{ref}\ \mathsf{A}^{\ell_i})|\!)_{\alpha'}$

$T_{1.3} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \alpha'\ \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)_{\ell_i}$

$T_2 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\tau|\!)_{(\beta' \sqcup \gamma')}$

$T_{2.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\mathsf{A}^{\ell_i}|\!)_{(\beta' \sqcup \gamma')}$

$T_{2.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell_i \sqcup (\beta' \sqcup \gamma')\ (\!|\mathsf{A}|\!)_{\ell_i \sqcup (\beta' \sqcup \gamma')}$

$T_{2.3} = \mathsf{Labeled}\ \ell_i \sqcup (\beta' \sqcup \gamma')\ (\!|\mathsf{A}|\!)_{\ell_i \sqcup (\beta' \sqcup \gamma')}$

$T_{2.4} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{ref}\ \ell_i \sqcup (\beta' \sqcup \gamma')\ (\!|\mathsf{A}|\!)_{\ell_i \sqcup (\beta' \sqcup \gamma')}$

$T_{2.5} = \mathsf{ref}\ \ell_i \sqcup (\beta' \sqcup \gamma')\ (\!|\mathsf{A}|\!)_{\ell_i \sqcup (\beta' \sqcup \gamma')}$

$T_{2.51} = \mathsf{Labeled}\ \alpha'\ \mathsf{ref}\ \ell_i \sqcup (\beta' \sqcup \gamma')\ (\!|\mathsf{A}|\!)_{\ell_i \sqcup (\beta' \sqcup \gamma')}$

$T_{2.6} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \alpha'\ \mathsf{ref}\ \ell_i \sqcup (\beta' \sqcup \gamma')\ (\!|\mathsf{A}|\!)_{\ell_i \sqcup (\beta' \sqcup \gamma')}$

$T_{2.7} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \alpha'\ \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)_{\ell_i}$

P3:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi \vdash \mathsf{A}^{\ell_i} \searrow pc}\text{ Given}}{\Sigma;\Psi \vdash pc \sqsubseteq \ell_i}\text{ By inversion} \qquad \dfrac{}{\Sigma;\Psi \vdash \beta' \sqcup \gamma' \sqsubseteq pc}\text{ Given}}{\Sigma;\Psi \vdash (\beta' \sqcup \gamma') \sqsubseteq \ell_i}$$

P2:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5} \vdash b : T_{2.5}}\text{ SLIO}^*\text{-var}}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5} \vdash \mathsf{Lb}b : T_{2.51}}\text{ SLIO}^*\text{-label}}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5} \vdash \mathsf{ret}(\mathsf{Lb}b) : T_{2.6}}\text{ SLIO}^*\text{-ret} \qquad P3}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5} \vdash \mathsf{ret}(\mathsf{Lb}b) : T_{1.3}}$$

P1:

$$\cfrac{\overline{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3} \vdash \mathsf{new}\ (a) : T_{2.4}}\ \text{SLIO}^*\text{-new} \qquad P2}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{L}b b)) : T_{1.3}}\ \text{SLIO}^*\text{-bind}$$

Main derivation:

$$\cfrac{\cfrac{\overline{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}} \vdash e_c : T_{2.2}}\ \text{IH} \qquad P1}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{L}b b))) : T_{1.3}}\ \text{SLIO}^*\text{-bind}}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{L}b b))) : T_1}\ \text{Definition 3.30}$$

11. FC-deref:

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e : (\mathsf{ref}\ \tau)^{\ell} \leadsto e_c \qquad \Sigma;\Psi \vdash \tau <: \tau' \qquad \Sigma;\Psi \vdash \tau' \searrow \ell}{\Sigma;\Psi;\Gamma \vdash_{pc} !e : \tau \leadsto \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))}\ \text{FC-deref}$$

$\beta' = \bigcup_{\beta_i \in \overline{\beta'}} \beta_i$

$T_1 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\tau'|\!)_{\alpha'}$

$T_{1.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\mathsf{A}'^{\ell'_i}|\!)_{\alpha'}$

$T_{1.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell'_i \sqcup \alpha'\ (\!|\mathsf{A}'|\!)_{\ell'_i \sqcup \alpha'}$

$T_2 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(\mathsf{ref}\ \tau)^{\ell}|\!)_{(\beta' \sqcup \gamma')}$

$T_{2.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ (\ell \sqcup (\beta' \sqcup \gamma'))\ (\!|(\mathsf{ref}\ \tau)|\!)_{\ell \sqcup (\beta' \sqcup \gamma')}$

$T_{2.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ (\ell \sqcup (\beta' \sqcup \gamma'))\ (\!|(\mathsf{ref}\ \mathsf{A}^{\ell_i})|\!)_{\ell \sqcup (\beta' \sqcup \gamma')}$

$T_{2.3} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ (\ell \sqcup (\beta' \sqcup \gamma'))\ (\mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)_{\ell_i})$

$T_{2.4} = \mathsf{Labeled}\ (\ell \sqcup (\beta' \sqcup \gamma'))\ (\mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)_{\ell_i})$

$T_{2.5} = \mathbb{SLIO}\ \gamma'\ \beta' \sqcup \gamma' \sqcup \ell\ (\mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)_{\ell_i})$

$T_{2.6} = (\mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)_{\ell_i})$

$T_{2.7} = \mathbb{SLIO}\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)_{\ell_i})$

$T_{2.8} = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)_{\ell_i})$

$T_{2.9} = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\mathsf{Labeled}\ \ell'_i\ (\!|\mathsf{A}'|\!)_{\ell'_i})$

$T_{2.10} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ (\mathsf{Labeled}\ \beta' \sqcup \gamma' \sqcup \ell \sqcup \ell'_i\ (\!|\mathsf{A}'|\!)_{\ell'_i})$

$T_{2.11} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ (\mathsf{Labeled}\ \alpha \sqcup \ell'_i\ (\!|\mathsf{A}'|\!)_{\ell'_i})$

P2:

$$\cfrac{\overline{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.4}, b : T_{2.6} \vdash b : T_{2.6}}\ \text{SLIO}^*\text{-var}}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.4}, b : T_{2.6} \vdash !b : T_{2.7}}\ \text{SLIO}^*\text{-deref}$$

P1:

$$\cfrac{\overline{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.4} \vdash \mathsf{unlabel}\ a : T_{2.5}}\ \text{SLIO}^*\text{-unlabel} \qquad P2}{\Sigma;\Psi;(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.4} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.!b) : T_{2.8}}\ \text{SLIO}^*\text{-bind}$$

P0:

$$\dfrac{\overline{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash e_c : T_{2.3}} \qquad P1}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)) : T_{2.8}} \text{ SLIO}^*\text{-bind}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{P0}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)) : T_{2.9}} \text{ Lemma 3.33}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b))) : T_{2.10}} \text{ Lemma 3.31} \quad \dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{A}^{\ell_i} \searrow \ell} \text{ Given}}{\Sigma; \Psi \vdash \ell \sqsubseteq \ell_i} \text{ By inversion} \quad \dfrac{}{\Sigma; \Psi \vdash \beta' \sqcup \gamma' \sqsubseteq \alpha'} \text{ Given}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b))) : T_{1.1}} \text{ SLIO}^*\text{-sub}$$

12. FC-assign:

$$\dfrac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\mathsf{ref}\ \tau)^{\ell} \rightsquigarrow e_{c1} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau \rightsquigarrow e_{c2} \qquad \tau \searrow (pc \sqcup \ell)}{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e_1 := e_2 : \mathsf{unit} \rightsquigarrow \\ \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())\end{array}} \text{ FC-assign}$$

$\beta' = \bigcup_{\beta_i \in \overline{\beta'}} \beta_i$

$T_1 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\mathsf{unit}|\!)_{\alpha'}$

$T_{1.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{unit}$

$T_2 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(\mathsf{ref}\ \tau)^{\ell}|\!)_{(\beta' \sqcup \gamma')}$

$T_{2.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell \sqcup (\beta' \sqcup \gamma')\ (\!|(\mathsf{ref}\ \tau)|\!)_{\ell \sqcup (\beta' \sqcup \gamma')}$

$T_{2.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell \sqcup (\beta' \sqcup \gamma')\ (\!|(\mathsf{ref}\ \mathsf{A}^{\ell_i})|\!)_{\ell \sqcup (\beta' \sqcup \gamma')}$

$T_{2.3} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell \sqcup (\beta' \sqcup \gamma')\ \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)_{\ell_i}$

$T_{2.4} = \mathsf{Labeled}\ \ell \sqcup (\beta' \sqcup \gamma')\ \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)_{\ell_i}$

$T_{2.5} = \mathbb{SLIO}\ \gamma'\ \ell \sqcup (\beta' \sqcup \gamma')\ \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)_{\ell_i}$

$T_{2.6} = \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)_{\ell_i}$

$T_{2.7} = \mathbb{SLIO}\ \ell \sqcup (\beta' \sqcup \gamma')\ \ell \sqcup (\beta' \sqcup \gamma')\ \mathsf{unit}$

$T_{2.8} = \mathbb{SLIO}\ \gamma'\ \ell \sqcup (\beta' \sqcup \gamma')\ \mathsf{unit}$

$T_{2.9} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell \sqcup (\beta' \sqcup \gamma')\ \mathsf{unit}$

$T_3 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\tau|\!)_{(\beta' \sqcup \gamma')}$

$T_{3.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\mathsf{A}^{\ell_i}|\!)_{(\beta' \sqcup \gamma')}$

$T_{3.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell_i \sqcup (\beta' \sqcup \gamma')\ (\!|\mathsf{A}|\!)_{\ell_i \sqcup (\beta' \sqcup \gamma')}$

$T_{3.3} = \mathsf{Labeled}\ \ell_i \sqcup (\beta' \sqcup \gamma')\ (\!|\mathsf{A}|\!)_{\ell_i \sqcup (\beta' \sqcup \gamma')}$

$T_{3.4} = \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)_{\ell_i}$

P4:

$$\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.4}, b : T_{3.3}, c : T_{2.6} \vdash c : T_{2.6}} \text{ SLIO}^*\text{-var}$$

P5:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.4}, b : T_{3.3}, c : T_{2.6} \vdash b : T_{3.3}}\text{ SLIO}^*\text{-var} \quad \dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau = \mathsf{A}^{\ell_i} \searrow (pc \sqcup \ell)}\text{ Given}}{\Sigma; \Psi \vdash (pc \sqcup \ell) \sqsubseteq \ell_i}\text{ By inversion} \quad \dfrac{}{\Sigma; \Psi \vdash \beta' \sqcup \gamma' \sqsubseteq pc}\text{ Given}}{\Sigma; \Psi \vdash \beta' \sqcup \gamma' \sqsubseteq \ell_i}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.4}, b : T_{3.3}, c : T_{2.6} \vdash b : T_{3.4}}$$

P3:

$$\dfrac{P4 \qquad P5}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.4}, b : T_{3.3}, c : T_{2.6} \vdash c := b : T_{2.7}}\text{ SLIO}^*\text{-assign}$$

P2:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.4}, b : T_{3.3} \vdash \mathsf{unlabel}\ a : T_{2.5}}\text{ SLIO}^*\text{-unlabel} \qquad P3}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.4}, b : T_{3.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, c.c := b) : T_{2.8}}\text{ SLIO}^*\text{-bind}$$

P1:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.4} \vdash e_{c2} : T_{3.2}}\text{ IH2} \qquad P2}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.4} \vdash \mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b))) : T_{2.8}}\text{ SLIO}^*\text{-bind}$$

P0:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash e_{c1} : T_{2.3}}\text{ IH1} \qquad P1}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b))) : T_{2.8}}\text{ SLIO}^*\text{-bind}$$

P0.1:

$$\dfrac{P0}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{toLabeled}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))) : T_{2.9}}\text{ SLIO}^*\text{-toLabeled}$$

Main derivation:

$$\dfrac{P0.1}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}()) : T_{1.1}}\text{ SLIO}^*\text{-bind}$$

13. FC-FI:

$$\dfrac{\Sigma; \Psi; \Gamma \vdash_{\ell_e} e : \tau \rightsquigarrow e_c}{\Sigma; \Psi; \Gamma \vdash_{pc} \Lambda e : (\forall \alpha_g.(\ell_e, \tau))^{\perp} \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(e_c))))}\text{ FC-FI}$$

$T_1 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(\forall \alpha.(\ell_e, \tau))^{\perp}|\!)_{\alpha'}$

$T_{1.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \alpha'\ (\!|\forall \alpha.(\ell_e, \tau)|\!)_{\alpha'}$

$T_{1.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \alpha'\ \forall \alpha.\forall \alpha_i, \gamma_i.(\alpha' \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}$

$T_2 = \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}$

$T_{2.1} = (\alpha' \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}$

$T_{2.2} = \forall \alpha, \alpha_i, \gamma_i.(\alpha' \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}$

$T_{2.3} = \mathsf{Labeled}\ \alpha'\ \forall \alpha, \alpha_i, \gamma_i.(\alpha' \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}$

Main derivation:

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{\Sigma, \alpha, \alpha_i, \gamma_i; \Psi, (\alpha' \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e); (\!|\Gamma|\!)_{\vec{\beta'}} \vdash e_c : T_2}\text{ IH, Weakening}}{\Sigma, \alpha, \alpha_i, \gamma_i; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \nu(e_c) : T_{2.1}}\text{ SLIO}^*\text{-CI}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \Lambda\Lambda\Lambda(\nu(e_c)) : T_{2.2}}\text{ SLIO}^*\text{-FI}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(e_c))) : T_{2.3}}\text{ SLIO}^*\text{-label}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(e_c)))) : T_{1.2}}$$

14. FC-FE:

$$\cfrac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\forall \alpha_g.(\ell_e, \tau))^{\ell} \rightsquigarrow e_c \qquad \text{FV}(\ell') \subseteq \Sigma \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e[\ell'/\alpha] \qquad \Sigma; \Psi \vdash \tau[\ell'/\alpha] \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e[] : \tau \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][][]\bullet)))}\text{ FC-FE}$$

$\beta' = \bigcup_{\beta_i \in \overline{\beta'}} \beta_i$

$T_1 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\tau[\ell''/\alpha]|\!)_{\alpha'}$

$T_2 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(\forall \alpha.(\ell_e, \tau))^{\ell}|\!)_{(\beta' \sqcup \gamma')}$

$T_{2.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell \sqcup (\beta' \sqcup \gamma')\ (\!|\forall \alpha.(\ell_e, \tau)|\!)_{\ell \sqcup (\beta' \sqcup \gamma')}$

$T_{2.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell \sqcup (\beta' \sqcup \gamma')\ \forall \alpha.\forall \alpha_i, \gamma_i.((\ell \sqcup (\beta' \sqcup \gamma')) \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}$

$T_{2.3} = \mathsf{Labeled}\ \ell \sqcup (\beta' \sqcup \gamma')\ \forall \alpha.\forall \alpha_i, \gamma_i.((\ell \sqcup (\beta' \sqcup \gamma')) \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}$

$T_{2.4} = \mathbb{SLIO}\ \gamma'\ (\gamma' \sqcup \ell \sqcup (\beta' \sqcup \gamma'))\ \forall \alpha.\forall \alpha_i, \gamma_i.((\ell \sqcup (\beta' \sqcup \gamma')) \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}$

$T_{2.5} = \forall \alpha.\forall \alpha_i, \gamma_i.((\ell \sqcup (\beta' \sqcup \gamma')) \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}$

$T_{2.6} = \forall \alpha_i, \gamma_i.((\ell \sqcup (\beta' \sqcup \gamma')) \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e[\ell''/\alpha]) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}[\ell''/\alpha]$

$T_{2.7} = \forall \gamma_i.((\ell \sqcup (\beta' \sqcup \gamma')) \sqcup \gamma_i \sqsubseteq (\beta' \sqcup \gamma' \sqcup \ell) \sqcap \ell_e[\ell''/\alpha]) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{(\beta' \sqcup \gamma' \sqcup \ell)}[\ell''/\alpha]$

$T_{2.8} = ((\ell \sqcup (\beta' \sqcup \gamma')) \sqcup (\beta' \sqcup \gamma' \sqcup \ell) \sqsubseteq (\beta' \sqcup \gamma' \sqcup \ell) \sqcap \ell_e[\ell''/\alpha]) \Rightarrow \mathbb{SLIO}\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\!|\tau|\!)_{(\beta' \sqcup \gamma' \sqcup \ell)}[\ell''/\alpha]$

$T_{2.81} = ((\ell \sqcup (\beta' \sqcup \gamma')) \sqsubseteq (\beta' \sqcup \gamma' \sqcup \ell) \sqcap \ell_e[\ell''/\alpha]) \Rightarrow \mathbb{SLIO}\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\!|\tau|\!)_{(\beta' \sqcup \gamma' \sqcup \ell)}[\ell''/\alpha]$

$T_{2.9} = \mathbb{SLIO}\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\!|\tau|\!)_{(\beta' \sqcup \gamma' \sqcup \ell)}[\ell''/\alpha]$

$T_{2.10} = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\!|\tau|\!)_{(\beta' \sqcup \gamma' \sqcup \ell)}[\ell''/\alpha]$

$T_{2.11} = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\!|\tau[\ell''/\alpha]|\!)_{(\beta' \sqcup \gamma' \sqcup \ell)}$

$T_{2.12} = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\!|\mathsf{A}^{\ell_i}[\ell''/\alpha]|\!)_{(\beta' \sqcup \gamma' \sqcup \ell)}$

$T_{2.13} = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ \mathsf{Labeled}\ \ell_i[\ell''/\alpha] \sqcup (\beta' \sqcup \gamma' \sqcup \ell)\ (\!|\mathsf{A}[\ell''/\alpha]|\!)_{\ell_i[\ell''/\alpha] \sqcup (\beta' \sqcup \gamma' \sqcup \ell)}$

$T_{2.14} = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ \mathsf{Labeled}\ \ell_i[\ell''/\alpha] \sqcup \beta' \sqcup \gamma'\ (\!|\mathsf{A}[\ell''/\alpha]|\!)_{\ell_i[\ell''/\alpha] \sqcup (\beta' \sqcup \gamma')}$

$T_{2.15} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \mathsf{Labeled}\ \ell_i[\ell''/\alpha] \sqcup \beta' \sqcup \gamma'\ (\!|\mathsf{A}[\ell''/\alpha]|\!)_{\ell_i[\ell''/\alpha] \sqcup (\beta' \sqcup \gamma')}$

$T_{2.16} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ (\!| \mathsf{A}[\ell''/\alpha]^{\ell_i[\ell''/\alpha]} |\!)_{(\beta' \sqcup \gamma')}$

P3:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \ell \sqsubseteq \ell_e[\ell''/\alpha])}\text{ Given} \qquad \dfrac{}{\Sigma; \Psi \vdash (\beta' \sqcup \gamma') \sqsubseteq pc \sqsubseteq \ell_e[\ell''/\alpha])}\text{ Given}}{\Sigma; \Psi \vdash ((\ell \sqcup (\beta' \sqcup \gamma')) \sqsubseteq \ell_e[\ell''/\alpha])}}{\Sigma; \Psi \vdash ((\ell \sqcup (\beta' \sqcup \gamma')) \sqsubseteq (\beta' \sqcup \gamma' \sqcup \ell) \sqcap \ell_e[\ell''/\alpha])}$$

P2:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}}, a : T_{2.3}, b : T_{2.5} \vdash b : T_{2.5}}\text{ SLIO}^*\text{-var}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}}, a : T_{2.3}, b : T_{2.5} \vdash b[] : T_{2.6}}\text{ SLIO}^*\text{-FE}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}}, a : T_{2.3}, b : T_{2.5} \vdash b[][] : T_{2.7}}\text{ SLIO}^*\text{-FE}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}}, a : T_{2.3}, b : T_{2.5} \vdash b[][][] : T_{2.81}}\text{ SLIO}^*\text{-FE} \qquad P3}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}}, a : T_{2.3}, b : T_{2.5} \vdash b[][][]\bullet : T_{2.9}}\text{ SLIO}^*\text{-CE}$$

P1:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}}, a : T_{2.3} \vdash \mathsf{unlabel}\ a : T_{2.4}}\text{ SLIO}^*\text{-unlabel} \qquad P2}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}}, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a.b.b[][][]\bullet) : T_{2.10}}\text{ SLIO}^*\text{-bind}$$

P0:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}} \vdash e_c : T_{2.2}}\text{ IH} \qquad P1}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][][]\bullet)) : T_{2.10}}\text{ SLIO}^*\text{-bind}$$

P0.1:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{A}[\ell''/\alpha]^{\ell_i[\ell''/\alpha]} \searrow \ell}\text{ Given}}{\Sigma; \Psi \vdash \ell \sqsubseteq \ell_i[\ell''/\alpha]}\text{ By inversion}$$

P0.2:

$$\dfrac{\dfrac{\dfrac{\dfrac{P0}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][][]\bullet)) : T_{2.11}}\text{ Lemma 3.36}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][][]\bullet)) : T_{2.12}}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][][]\bullet)) : T_{2.13}}\text{ Definition 3.30} \quad P0.1}{\dfrac{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][][]\bullet)) : T_{2.14}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][][]\bullet))) : T_{2.15}}\text{ Lemma 3.31}}$$

Main derivation:

$$\dfrac{P0.2}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][][]\bullet))) : T_1}\text{ Definition 3.30}$$

15. FC-CI:

$$\frac{\Sigma; \Psi, c; \Gamma \vdash_{\ell_e} e : \tau \rightsquigarrow e_c}{\Sigma; \Psi; \Gamma \vdash_{pc} \nu e : (c \stackrel{\ell_e}{\Rightarrow} \tau))^\perp \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda(\nu(e_c))))} \text{ FC-CI}$$

$T_1 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(c \stackrel{\ell_e}{\Rightarrow} \tau)^\perp|\!)_{\alpha'}$

$T_{1.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \alpha'\ (\!|(c \stackrel{\ell_e}{\Rightarrow} \tau)|\!)_{\alpha'}$

$T_{1.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \alpha'\ \forall \alpha_i, \gamma_i.(c \wedge \alpha' \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}$

$T_{1.3} = \mathsf{Labeled}\ \alpha'\ \forall \alpha_i, \gamma_i.(c \wedge \alpha' \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}$

$T_{1.4} = \forall \alpha_i, \gamma_i.(c \wedge \alpha' \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}$

$T_{1.5} = (c \wedge \alpha' \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}$

$T_2 = \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\alpha_i}$

Main derivation:

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{\Sigma, \alpha_i, \gamma_i; \Psi, (c \wedge \alpha' \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e); (\!|\Gamma|\!) \vdash e_c : T_2} \text{ IH, Weakening}}{\Sigma; \Psi; \Gamma \vdash \nu(e_c) : T_{1.5}} \text{ SLIO}^*\text{-CI}}{\Sigma; \Psi; \Gamma \vdash \Lambda\Lambda(\nu(e_c)) : T_{1.4}} \text{ SLIO}^*\text{-FI}}{\Sigma; \Psi; \Gamma \vdash \mathsf{Lb}(\Lambda\Lambda(\nu(e_c))) : T_{1.3}} \text{ SLIO}^*\text{-label}}{\Sigma; \Psi; \Gamma \vdash \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda(\nu(e_c)))) : T_{1.2}}$$

16. FC-CE:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (c \stackrel{\ell_e}{\Rightarrow} \tau))^\ell \rightsquigarrow e_c \qquad \Sigma; \Psi \vdash c \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e \qquad \Sigma; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e \bullet : \tau \rightsquigarrow \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][]\bullet)))} \text{ FC-CE}$$

$\beta' = \bigcup_{\beta_i \in \overline{\beta'}} \beta_i$

$T_1 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|\tau|\!)_{\alpha'}$

$T_2 = \mathbb{SLIO}\ \gamma'\ \gamma'\ (\!|(c \stackrel{\ell_e}{\Rightarrow} \tau)^\ell|\!)_{(\beta' \sqcup \gamma')}$

$T_{2.1} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell \sqcup (\beta' \sqcup \gamma')\ (\!|(c \stackrel{\ell_e}{\Rightarrow} \tau)|\!)_{\ell \sqcup (\beta' \sqcup \gamma')}$

$T_{2.2} = \mathbb{SLIO}\ \gamma'\ \gamma'\ \mathsf{Labeled}\ \ell \sqcup (\beta' \sqcup \gamma')\ \forall \alpha_i, \gamma_i.(c \wedge (\beta' \sqcup \gamma' \sqcup \ell) \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\ell \sqcup \alpha_i}$

$T_{2.3} = \mathsf{Labeled}\ \ell \sqcup (\beta' \sqcup \gamma')\ \forall \alpha_i, \gamma_i.(c \wedge (\beta' \sqcup \gamma' \sqcup \ell) \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\ell \sqcup \alpha_i}$

$T_{2.4} = \mathbb{SLIO}\ \gamma'\ (\gamma' \sqcup \ell \sqcup (\beta' \sqcup \gamma'))\ \forall \alpha_i, \gamma_i.(c \wedge (\beta' \sqcup \gamma' \sqcup \ell) \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\ell \sqcup \alpha_i}$

$T_{2.5} = \forall \alpha_i, \gamma_i.(c \wedge (\beta' \sqcup \gamma' \sqcup \ell) \sqcup \gamma_i \sqsubseteq \alpha_i \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\ell \sqcup \alpha_i}$

$T_{2.6} = \forall \gamma_i.(c \wedge (\beta' \sqcup \gamma' \sqcup \ell) \sqcup \gamma_i \sqsubseteq (\beta' \sqcup \gamma') \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma_i\ \gamma_i\ (\!|\tau|\!)_{\ell \sqcup (\beta' \sqcup \gamma')}$

$T_{2.7} = (c \wedge (\beta' \sqcup \gamma' \sqcup \ell) \sqcup (\beta' \sqcup \gamma') \sqsubseteq (\beta' \sqcup \gamma' \sqcup \ell) \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\!|\tau|\!)_{\ell \sqcup (\beta' \sqcup \gamma')}$

$T_{2.71} = (c \wedge (\beta' \sqcup \gamma' \sqcup \ell) \sqsubseteq (\beta' \sqcup \gamma') \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\!|\tau|\!)_{\ell \sqcup (\beta' \sqcup \gamma')}$

$T_{2.8} = \mathbb{SLIO}\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\!|\tau|\!)_{\ell \sqcup (\beta' \sqcup \gamma')}$

$T_{2.9} = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\!|\tau|\!)_{\ell \sqcup (\beta' \sqcup \gamma')}$

$T_{2.10} = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ (\!|\mathsf{A}^{\ell_i}|\!)_{\ell \sqcup (\beta' \sqcup \gamma')}$

$T_{2.11} = \mathbb{SLIO}\ (\gamma')\ (\beta' \sqcup \gamma' \sqcup \ell)\ \mathsf{Labeled}\ \ell_i \sqcup \ell \sqcup (\beta' \sqcup \gamma')\ (\!|\mathsf{A}|\!)_{\ell_i \sqcup \ell \sqcup (\beta' \sqcup \gamma')}$

$T_{2.12} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \mathsf{Labeled}\ \ell_i \sqcup \ell \sqcup (\beta' \sqcup \gamma')\ (\!|\mathsf{A}|\!)_{\ell_i \sqcup \ell \sqcup (\beta' \sqcup \gamma')}$

$T_{2.13} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ \mathsf{Labeled}\ \ell_i \sqcup (\beta' \sqcup \gamma')\ (\!|\mathsf{A}|\!)_{\ell_i \sqcup (\beta' \sqcup \gamma')}$

$T_{2.14} = \mathbb{SLIO}\ (\gamma')\ (\gamma')\ (\!|\mathsf{A}^{\ell_i}|\!)_{(\beta' \sqcup \gamma')}$

P2:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5} \vdash b : T_{2.5}}\ \text{SLIO}^*\text{-var}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5} \vdash b[] : T_{2.6}}\ \text{SLIO}^*\text{-FE}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5} \vdash b[][] : T_{2.71}}\ \text{SLIO}^*\text{-FE}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5} \vdash b[][]\bullet : T_{2.8}}\ \text{SLIO}^*\text{-CE}$$

P1:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3} \vdash \mathsf{unlabel}\ a : T_{2.4}}\ \text{SLIO}^*\text{-unlabel} \qquad P2}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a.b.b[][]\bullet) : T_{2.9}}\ \text{SLIO}^*\text{-bind}$$

P0:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash e_c : T_{2.2}}\ \text{IH} \qquad P1}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][]\bullet)) : T_{2.9}}\ \text{SLIO}^*\text{-bind}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P0}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][]\bullet)) : T_{2.10}}\ \text{SLIO}^*\text{-bind}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][]\bullet)) : T_{2.11}}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][]\bullet))) : T_{2.12}}\ \text{Lemma 3.31}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][]\bullet))) : T_{2.13}}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][]\bullet))) : T_{2.14}}}{\Sigma; \Psi; (\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][]\bullet))) : T_1}$$

□

Lemma 3.33 (FG $\rightsquigarrow$ SLIO*: Subtyping preservation)**.** $\forall \Sigma, \Psi, \ell, \ell'$. $\Sigma; \Psi \vdash \ell \sqsubseteq \ell'$ *and the following holds:*

1. $\forall \tau, \tau'$.
   $\Sigma; \Psi \vdash \tau <: \tau' \implies [\![\tau]\!]_\ell <: [\![\tau']\!]_{\ell'}$
2. $\forall \mathsf{A}, \mathsf{A}'$.
   $\Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}' \implies \Sigma; \Psi \vdash [\![\mathsf{A}]\!]_\ell <: [\![\mathsf{A}']\!]_{\ell'}$

Proof. Proof by simultaneous induction on $\tau <: \tau$ and $\mathsf{A} <: \mathsf{A}$

Proof of statement (1)

Let $\tau = \mathsf{A}_1^{\ell_1}$ and $\tau' = \mathsf{A}_2^{\ell_2}$

P2:

$$\dfrac{\dfrac{\dfrac{}{\mathsf{A}_1^{\ell_1} <: \mathsf{A}_2^{\ell_2}}\ \text{Given}}{\Sigma; \Psi \vdash \mathsf{A}_1 <: \mathsf{A}_2}\ \text{By inversion} \qquad P1}{\Sigma; \Psi \vdash (\llbracket \mathsf{A}_1 \rrbracket_{\ell \sqcup \ell_1}) <: (\llbracket \mathsf{A}_2 \rrbracket_{\ell' \sqcup \ell_2})}\ \text{IH(2) on } \mathsf{A}_1 <: \mathsf{A}_2$$

P1:

$$\dfrac{\dfrac{\dfrac{}{\mathsf{A}_1^{\ell_1} <: \mathsf{A}_2^{\ell_2}}\ \text{Given}}{\Sigma; \Psi \vdash \ell_1 \sqsubseteq \ell_2}\ \text{By inversion} \qquad \dfrac{}{\Sigma; \Psi \vdash \ell \sqsubseteq \ell'}\ \text{Given}}{\Sigma; \Psi \vdash \ell \sqcup \ell_1 \sqsubseteq \ell' \sqcup \ell_2}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad P2}{\Sigma; \Psi \vdash \mathsf{Labeled}\ \ell \sqcup \ell_1\ (\llbracket \mathsf{A}_1 \rrbracket_{\ell \sqcup \ell_1}) <: \mathsf{Labeled}\ \ell' \sqcup \ell_2\ (\llbracket \mathsf{A}_2 \rrbracket_{\ell' \sqcup \ell_2})}\ \text{SLIO}^*\text{sub-labeled}}{\Sigma; \Psi \vdash \left\llbracket \mathsf{A}_1^{\ell_1} \right\rrbracket_{\ell} <: \left\llbracket \mathsf{A}_2^{\ell_2} \right\rrbracket_{\ell'}}$$

Proof of statement (2)

We proceed by cases on $\mathsf{A} <: \mathsf{A}$

1. FGsub-base:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{b} <: \mathsf{b}}\ \text{SLIO}^*\text{-refl}}{\Sigma; \Psi \vdash \llbracket \mathsf{b} \rrbracket_{\ell} <: \llbracket \mathsf{b} \rrbracket_{\ell'}}\ \text{Definition 3.30}$$

2. FGsub-ref:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{ref}\ \ell_i\ \llbracket \mathsf{A} \rrbracket_{\ell_i} <: \mathsf{ref}\ \ell_i\ \llbracket \mathsf{A} \rrbracket_{\ell_i}}\ \text{SLIO}^*\text{-refl}}{\Sigma; \Psi \vdash \left\llbracket \mathsf{ref}\ \mathsf{A}^{\ell_i} \right\rrbracket_{\ell} <: \left\llbracket \mathsf{ref}\ \mathsf{A}^{\ell_i} \right\rrbracket_{\ell'}}\ \text{Definition 3.30}$$

3. FGsub-prod:

P1:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}\ \text{Given}}{\Sigma; \Psi \vdash \tau_1 <: \tau_1'}\ \text{By inversion}}{\Sigma; \Psi \vdash \llbracket \tau_1 \rrbracket_{\ell} <: \llbracket \tau_1' \rrbracket_{\ell'}}\ \text{IH(1) on } \tau_1 <: \tau_1'$$

P2:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}\ \text{Given}}{\Sigma; \Psi \vdash \tau_2 <: \tau_2'}\ \text{By inversion}}{\Sigma; \Psi \vdash \llbracket \tau_2 \rrbracket_{\ell} <: \llbracket \tau_2' \rrbracket_{\ell'}}\ \text{IH(1) on } \tau_2 <: \tau_2'$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad P2}{\Sigma; \Psi \vdash [\![\tau_1]\!]_\ell \times [\![\tau_2]\!]_\ell <: [\![\tau_1']\!]_\ell \times [\![\tau_2']\!]_{\ell'}} \text{ SLIO}^*\text{sub-prod}}{\Sigma; \Psi \vdash [\![\tau_1 \times \tau_2]\!]_\ell <: [\![\tau_1' \times \tau_2']\!]_{\ell'}} \text{ Definition 3.30}$$

4. FGsub-sum:

P1:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'} \text{ Given}}{\Sigma; \Psi \vdash \tau_1 <: \tau_1'} \text{ By inversion}}{\Sigma; \Psi \vdash [\![\tau_1]\!]_\ell <: [\![\tau_1']\!]_{\ell'}} \text{ IH(1) on } \tau_1 <: \tau_1'$$

P2:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'} \text{ Given}}{\Sigma; \Psi \vdash \tau_2 <: \tau_2'} \text{ By inversion}}{\Sigma; \Psi \vdash [\![\tau_2]\!]_\ell <: [\![\tau_2']\!]_{\ell'}} \text{ IH(1) on } \tau_2 <: \tau_2'$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad P2}{\Sigma; \Psi \vdash [\![\tau_1]\!]_\ell + [\![\tau_2]\!]_\ell <: [\![\tau_1']\!]_\ell + [\![\tau_2']\!]_{\ell'}} \text{ SLIO}^*\text{sub-prod}}{\Sigma; \Psi \vdash [\![\tau_1 + \tau_2]\!]_\ell <: [\![\tau_1' + \tau_2']\!]_{\ell'}} \text{ Definition 3.30}$$

5. FGsub-arrow:

$T_1 = \forall \alpha, \beta, \gamma.(\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_\beta \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_\alpha$

$T_{1.0} = \forall \beta, \gamma.(\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_\beta \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_\alpha$

$T_{1.1} = \forall \gamma.(\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_\beta \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_\alpha$

$T_{1.2} = (\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_\beta \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_\alpha$

$T_{1.3} = (\!|\tau_1|\!)_\beta \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_\alpha$

$c_1 = (\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e)$

$T_2 = \forall \alpha, \beta, \gamma.(\ell' \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e') \Rightarrow (\!|\tau_1'|\!)_\beta \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2'|\!)_\alpha$

$T_{2.0} = \forall \beta, \gamma.(\ell' \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e') \Rightarrow (\!|\tau_1'|\!)_\beta \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2'|\!)_\alpha$

$T_{2.1} = \forall \gamma.(\ell' \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e') \Rightarrow (\!|\tau_1'|\!)_\beta \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2'|\!)_\alpha$

$T_{2.2} = (\ell' \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e') \Rightarrow (\!|\tau_1'|\!)_\beta \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2'|\!)_\alpha$

$T_{2.3} = (\!|\tau_1'|\!)_\beta \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2'|\!)_\alpha$

$c_2 = (\ell' \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e')$

P3:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'} \text{ Given}}{\Sigma, \alpha, \beta, \gamma; \Psi \vdash \tau_2 <: \tau_2'} \text{ By inversion, Weakening}}{\Sigma, \alpha, \beta, \gamma; \Psi \vdash \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_\alpha <: \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2'|\!)_\alpha} \text{ IH(1) with } \ell = \ell' = \alpha, \text{SLIO}^*\text{sub-monad}$$

P2:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'}\ \text{Given}}{\Sigma, \alpha, \beta, \gamma; \Psi \vdash \tau_1' <: \tau_1}\ \text{By inversion, Weakening}}{\Sigma, \alpha, \beta, \gamma; \Psi \vdash \llbracket \tau_1' \rrbracket_\beta <: \llbracket \tau_1 \rrbracket_\beta}\ \text{IH(1) with } \ell = \ell' = \beta$$

P1:

$$\dfrac{P2 \qquad P3}{\Sigma; \Psi \vdash T_{1.3} <: T_{2.3}}\ \text{SLIO}^*\text{sub-arrow}$$

P0.1:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha, \beta, \gamma; \Psi \vdash \ell \sqsubseteq \ell'}\ \text{Given, Weakening}}{\Sigma, \alpha, \beta, \gamma; \Psi \vdash (\ell' \sqcup \beta \sqcup \gamma \sqsubseteq \alpha) \implies (\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha)} \quad \dfrac{\dfrac{}{\Sigma, \alpha, \beta, \gamma; \Psi \vdash \ell_e' \sqsubseteq \ell_e}\ \text{Given, Weakening}}{\Sigma, \alpha, \beta, \gamma; \Psi \vdash (\ell' \sqcup \beta \sqcup \gamma \sqsubseteq \ell_e') \implies (\ell \sqcup \beta \sqcup \gamma \sqsubseteq \ell_e)}}{\Sigma, \alpha, \beta, \gamma; \Psi \vdash c_2 \implies c_1}}{}$$

P0:

$$\dfrac{\dfrac{P0.1 \qquad \dfrac{P1}{\Sigma, \alpha, \beta, \gamma; \Psi \vdash T_{1.3} <: T_{2.3}}\ \text{SLIO}^*\text{sub-arrow}}{\Sigma, \alpha, \beta, \gamma; \Psi \vdash T_{1.2} <: T_{2.2}}\ \text{SLIO}^*\text{sub-constraint}}{\Sigma; \Psi \vdash T_1 <: T_2}\ \text{SLIO}^*\text{sub-forall}$$

Main derivation:

$$\dfrac{P0}{\Sigma; \Psi \vdash \left\llbracket \tau_1 \xrightarrow{\ell_e} \tau_2 \right\rrbracket_\ell <: \left\llbracket \tau_1' \xrightarrow{\ell_e'} \tau_2' \right\rrbracket_{\ell'}}\ \text{Definition 3.30}$$

6. FGsub-unit:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}}\ \text{SLIO}^*\text{sub-unit}}{\Sigma; \Psi \vdash \llbracket \mathsf{unit} \rrbracket_\ell <: \llbracket \mathsf{unit} \rrbracket_{\ell'}}\ \text{Definition 3.30}$$

7. FGsub-forall:

$T_1 = \forall \alpha, \alpha', \gamma.(\ell \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_1|\!)_{\alpha'}$

$T_{1.0} = \forall \alpha', \gamma.(\ell \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_1|\!)_{\alpha'}$

$T_{1.1} = \forall \gamma.(\ell \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_1|\!)_{\alpha'}$

$T_{1.2} = (\ell \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_1|\!)_{\alpha'}$

$T_{1.3} = \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_1|\!)_{\alpha'}$

$c_1 = (\ell \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e)$

$T_2 = \forall \alpha, \alpha', \gamma.(\ell' \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e') \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha'}$

$T_{2.0} = \forall\alpha', \gamma.(\ell' \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell'_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha'}$

$T_{2.1} = \forall\gamma.(\ell' \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell'_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha'}$

$T_{2.2} = (\ell' \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell'_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha'}$

$T_{2.3} = \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha'}$

$c_2 = (\ell' \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell'_e)$

P3:

$$\dfrac{\dfrac{\overline{\Sigma, \alpha, \alpha', \gamma; \Psi \vdash \tau_1 <: \tau_2}\ \text{Given, Weakening}}{\Sigma, \alpha, \alpha', \gamma; \Psi \vdash (\!|\tau_1|\!)_{\alpha'} <: \tau_{2\alpha'}}\ \text{IH(1) with } \ell = \ell' = \alpha'}{\Sigma, \alpha, \alpha', \gamma; \Psi \vdash \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_1|\!)_{\alpha'} <: \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha'}}$$

P2:

$$\dfrac{\overline{\Sigma, \alpha, \alpha', \gamma; \Psi \vdash (\ell'_e \sqsubseteq \ell_e)}\ \text{Given}}{\Sigma, \alpha, \alpha', \gamma; \Psi \vdash (\ell' \sqcup \gamma \sqsubseteq \ell'_e) \implies (\ell \sqcup \gamma \sqsubseteq \ell_e)}$$

P1:

$$\dfrac{\overline{(\ell \sqsubseteq \ell')}\ \text{Given}}{\Sigma, \alpha, \alpha', \gamma; \Psi \vdash (\ell' \sqcup \gamma \sqsubseteq \alpha') \implies (\ell \sqcup \gamma \sqsubseteq \alpha')}$$

P0:

$$\dfrac{P1 \qquad P2}{\Sigma, \alpha, \alpha', \gamma; \Psi \vdash c_2 \implies c_1}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{P0 \qquad P3}{\Sigma, \alpha, \alpha', \gamma; \Psi \vdash T_{1.2} <: T_{2.2}}\ \text{SLIO}^*\text{sub-constraint}}{\Sigma; \Psi \vdash T_1 <: T_2}\ \text{SLIO}^*\text{sub-forall}}{\Sigma; \Psi \vdash [\![\forall\alpha.\tau_1]\!]_{\ell} <: [\![\forall\alpha.\tau_2]\!]_{\ell'}}\ \text{Definition 3.30}$$

8. FGsub-constraint:

$T_1 = \forall\alpha, \gamma.(c_1 \wedge \ell \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_1|\!)_{\alpha}$

$T_{1.0} = \forall\gamma.(c_1 \wedge \ell \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_1|\!)_{\alpha}$

$T_{1.1} = (c_1 \wedge \ell \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_1|\!)_{\alpha}$

$T_{1.2} = \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_1|\!)_{\alpha}$

$C_1 = (c_1 \wedge \ell \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e)$

$T_2 = \forall\alpha, \gamma.(c_2 \wedge \ell \sqcup \gamma \sqsubseteq \alpha \sqcap \ell'_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha}$

$T_{2.0} = \forall\gamma.(c_2 \wedge \ell \sqcup \gamma \sqsubseteq \alpha \sqcap \ell'_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha}$

$T_{2.1} = (c_2 \wedge \ell \sqcup \gamma \sqsubseteq \alpha \sqcap \ell'_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha}$

$T_{2.2} = \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha}$

$C_2 = (c_2 \wedge \ell' \sqcup \gamma \sqsubseteq \alpha \sqcap \ell'_e)$

P1:

$$\dfrac{\dfrac{\overline{\Sigma, \alpha, \gamma; \Psi \vdash \tau_1 <: \tau_2}\text{ Given, Weakening}}{\Sigma, \alpha, \gamma; \Psi \vdash (\!|\tau_1|\!)_\alpha <: \tau_{2\alpha}}\text{ IH(1) with } \ell = \ell' = \alpha}{\Sigma, \alpha, \gamma; \Psi \vdash \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_1|\!)_\alpha <: \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_\alpha}$$

P0:

$$\dfrac{\dfrac{\overline{\Sigma; \Psi \vdash c_2 \implies c_1}\text{ Given}}{\Sigma, \alpha, \gamma; \Psi \vdash c_2 \wedge (\ell' \sqcup \gamma \sqsubseteq \alpha \sqcap \ell'_e) \implies c_1 \wedge (\ell \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e)}\text{ Weakening, } \ell \sqsubseteq \ell',\ \ell'_e \sqsubseteq \ell_e}{\Sigma, \alpha, \gamma; \Psi \vdash C_2 \implies C_1}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{P0 \qquad P1}{\Sigma, \alpha, \gamma; \Psi \vdash T_{1.1} <: T_{2.1}}\text{ SLIO}^*\text{sub-constraint}}{\Sigma; \Psi \vdash T_1 <: T_2}\text{ SLIO}^*\text{sub-forall}}{\Sigma; \Psi \vdash \left[\!\!\left[c_1 \overset{\ell_e}{\Rightarrow} \tau_1 \right]\!\!\right]_\ell <: \left[\!\!\left[c_2 \overset{\ell'_e}{\Rightarrow} \tau_2 \right]\!\!\right]_{\ell'}}\text{ Definition 3.30}$$

□

Lemma 3.34 (FG ⇝ SLIO*: Preservation of well-formedness)**.** *Forall* Σ, Ψ *and* ℓ *s.t* $FV(\ell) \in \Sigma$ *the following hold:*

1. $\forall \tau.\ \Sigma; \Psi \vdash \tau\ WF \implies \Sigma; \Psi \vdash (\!|\tau|\!)_\ell\ WF$
2. $\forall \mathsf{A}.\ \Sigma; \Psi \vdash \mathsf{A}\ WF \implies \Sigma; \Psi \vdash (\!|\mathsf{A}|\!)_\ell\ WF$

Proof. Proof by simulataneous induction on the WF relation of FG

Proof of statement (1)

Let $\tau = \mathsf{A}^{\ell'}$

$$\dfrac{\dfrac{\dfrac{\overline{\text{FV}(\ell') \in \Sigma}\text{ By inversion}}{\text{FV}(\ell' \sqcup \ell) \in \Sigma}}{\Sigma; \Psi \vdash (\!|\mathsf{A}|\!)_{\ell' \sqcup \ell}\ WF}\text{ IH(2) on A}}{\Sigma; \Psi \vdash \mathsf{Labeled}\ \ell' \sqcup \ell\ (\!|\mathsf{A}|\!)_{\ell' \sqcup \ell}\ WF}\text{ SLIO}^*\text{-wff-labeled}$$

Proof of statement (2)

We proceed by case analyzing the last rule of given WF judgment.

1. FG-wff-base:

$$\overline{\Sigma; \Psi \vdash \mathsf{b}\ WF}\text{ SLIO}^*\text{-wff-base}$$

2. FG-wff-unit:

$$\overline{\Sigma; \Psi \vdash \mathsf{unit}\ WF}\text{ SLIO}^*\text{-wff-unit}$$

3. FG-wff-arrow:

   P1:

$$\dfrac{\dfrac{}{\Sigma, \alpha, \beta, \gamma; \Psi, (\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \vdash (\!|\tau_2|\!)_\alpha \ WF}\ \text{IH(1) on } \tau_2}{\Sigma, \alpha, \beta, \gamma; \Psi, (\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \vdash \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_\alpha \ WF}\ \text{SLIO}^*\text{-wff-monad}$$

   P0:

$$\dfrac{\dfrac{}{\Sigma, \alpha, \beta, \gamma; \Psi, (\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \vdash (\!|\tau_1|\!)_\beta \ WF}\ \text{IH(1) on } \tau_1 \qquad P1}{\Sigma, \alpha, \beta, \gamma; \Psi, (\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \vdash ((\!|\tau_1|\!)_\beta \to \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_\alpha) \ WF}\ \text{SLIO}^*\text{-wff-arrow}$$

   Main derivation:

$$\dfrac{\dfrac{P0}{\Sigma, \alpha, \beta, \gamma; \Psi \vdash ((\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_\beta \to \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_\alpha) \ WF}\ \text{SLIO}^*\text{-wff-constraint}}{\Sigma; \Psi \vdash (\forall \alpha, \beta, \gamma.(\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_\beta \to \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_\alpha) \ WF}$$

4. FG-wff-prod:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash (\!|\tau_1|\!)_\ell \ WF}\ \text{IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash (\!|\tau_2|\!)_\ell \ WF}\ \text{IH(1) on } \tau_2}{\Sigma; \Psi \vdash (\!|\tau_1|\!)_\ell \times (\!|\tau_2|\!)_\ell \ WF}\ \text{SLIO}^*\text{-wff-prod}$$

5. FG-wff-sum:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash (\!|\tau_1|\!)_\ell \ WF}\ \text{IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash (\!|\tau_2|\!)_\ell \ WF}\ \text{IH(1) on } \tau_2}{\Sigma; \Psi \vdash (\!|\tau_1|\!)_\ell + (\!|\tau_2|\!)_\ell \ WF}\ \text{SLIO}^*\text{-wff-prod}$$

6. FG-wff-ref:

   Let $\tau = \mathsf{A}^{\ell'}$

$$\dfrac{\dfrac{\dfrac{}{\text{FV}(\mathsf{A}) = \emptyset}\ \text{By inversion} \qquad \dfrac{}{\text{FV}(\ell') = \emptyset}\ \text{By inversion}}{\text{FV}((\!|\mathsf{A}|\!)_{\ell'}) = \emptyset}\ \text{Lemma 3.35}}{\Sigma; \Psi \vdash \mathsf{ref}\ \ell'\ (\!|\mathsf{A}|\!)_{\ell'} \ WF}\ \text{SLIO}^*\text{-wff-ref}$$

7. FG-wff-forall:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha, \alpha', \gamma; \Psi, (\ell \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e) \vdash (\!|\tau|\!)_{\alpha'} \ WF}\ \text{IH(1) on } \tau}{\Sigma, \alpha, \alpha', \gamma; \Psi, (\ell \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e) \vdash \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau|\!)_{\alpha'} \ WF}\ \text{SLIO}^*\text{-wff-monad}}{\Sigma, \alpha, \alpha', \gamma; \Psi \vdash (\ell \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau|\!)_{\alpha'} \ WF}\ \text{SLIO}^*\text{-wff-constraint}}{\Sigma; \Psi \vdash (\forall \alpha, \alpha', \gamma.(\ell \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau|\!)_{\alpha'}) \ WF}$$

8. FG-wff-constraint:

$$\dfrac{\dfrac{\dfrac{\overline{\Sigma, \alpha, \gamma; \Psi, (c \wedge \ell \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \vdash (\!|\tau|\!)_\alpha \; WF} \text{ IH(1) on } \tau}{\Sigma, \alpha, \gamma; \Psi, (c \wedge \ell \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \vdash \mathbb{SLIO} \; \gamma \; \gamma \; (\!|\tau|\!)_\alpha \; WF} \text{ SLIO}^*\text{-wff-monad}}{\Sigma, \alpha, \gamma; \Psi \vdash (c \wedge \ell \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow \mathbb{SLIO} \; \gamma \; \gamma \; (\!|\tau|\!)_\alpha \; WF} \text{ SLIO}^*\text{-wff-constraint}}{\Sigma; \Psi \vdash (\forall \alpha, \gamma.(c \wedge \ell \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow \mathbb{SLIO} \; \gamma \; \gamma \; (\!|\tau|\!)_\alpha) \; WF}$$

□

Lemma 3.35 (FG $\rightsquigarrow$ SLIO*: Free variable lemma)**.** *$\forall \Sigma, \ell.\ FV(\ell) \in \Sigma$, the following hold*

1. *$\forall \tau.\ FV((\!|\tau|\!)_\ell) \subseteq FV(\tau) \cup FV(\ell)$*
2. *$\forall \mathsf{A}.\ FV((\!|\mathsf{A}|\!)_\ell) \subseteq FV(\mathsf{A}) \cup FV(\ell)$*

Proof. Proof by simultaneous induction on τ and A

Proof for (1)

Let $\tau = \mathsf{A}^{\ell_i}$

$$\begin{array}{lll} & \text{FV}((\!|\mathsf{A}^{\ell_i}|\!)) & \\ = & \text{FV}(\mathsf{Labeled}\ \ell_i \sqcup \ell\ (\!|\mathsf{A}|\!)_{\ell_i \sqcup \ell}) & \text{Definition 3.30} \\ = & \text{FV}(\ell_i) \cup \text{FV}(\ell) \cup \text{FV}((\!|\mathsf{A}|\!)_{\ell_i \sqcup \ell}) & \\ \subseteq & \text{FV}(\ell_i) \cup \text{FV}(\ell) \cup \text{FV}(\mathsf{A}) & \text{IH(2) on } \mathsf{A} \\ = & \text{FV}(\mathsf{A}^{\ell_i}) \cup \text{FV}(\ell) & \end{array}$$

Proof for (2)

1. $\mathsf{A} = \mathsf{b}$:

$$\begin{array}{lll} & \text{FV}((\!|\mathsf{b}|\!)_\ell) & \\ = & \text{FV}(\mathsf{b}) & \text{Definition 3.30} \\ \subseteq & \text{FV}(\mathsf{b}) \cup \text{FV}(\ell) & \end{array}$$

2. $\mathsf{A} = \mathsf{unit}$:

$$\begin{array}{lll} & \text{FV}((\!|\mathsf{unit}|\!)_\ell) & \\ = & \text{FV}(\mathsf{unit}) & \text{Definition 3.30} \\ \subseteq & \text{FV}(\mathsf{unit}) \cup \text{FV}(\ell) & \end{array}$$

3. $\mathsf{A} = \tau_1 \xrightarrow{\ell_e} \tau_2$:

$$\begin{array}{lll} & \text{FV}((\!|\tau_1 \xrightarrow{\ell_e} \tau_2|\!)_\ell) & \\ = & \text{FV}(\forall \alpha, \beta, \gamma.(\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_\beta \to \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_\alpha) & \text{Definition 3.30} \\ = & \text{FV}(\ell) \cup \text{FV}((\!|\tau_1|\!)_\beta) \cup \text{FV}(\ell_e) \cup \text{FV}((\!|\tau_2|\!)_\alpha) & \\ \subseteq & \text{FV}(\tau_1) \cup \text{FV}(\ell_e) \cup \text{FV}(\tau_2) \cup \text{FV}(\ell) & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\ = & \text{FV}(\tau_1 \xrightarrow{\ell_e} \tau_2) \cup \text{FV}(\ell) & \end{array}$$

4. $\mathsf{A} = \tau_1 \times \tau_2$:

$$\begin{array}{lll} & \text{FV}((\!|\tau_1 \times \tau_2|\!)_\ell) & \\ = & \text{FV}((\!|\tau_1|\!)_\ell \times (\!|\tau_2|\!)_\ell) & \text{Definition 3.30} \\ = & \text{FV}((\!|\tau_1|\!)_\ell) \cup \text{FV}((\!|\tau_2|\!)_\ell) \cup \text{FV}(\ell) & \\ \subseteq & \text{FV}(\tau_1) \cup \text{FV}(\tau_2) \cup \text{FV}(\ell) & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\ = & \text{FV}(\tau_1 \times \tau_2) \cup \text{FV}(\ell) & \end{array}$$

5. $\mathsf{A} = \tau_1 + \tau_2$:

$$\begin{array}{lll} & \mathrm{FV}((\!|\tau_1 + \tau_2|\!)_\ell) & \\ = & \mathrm{FV}((\!|\tau_1|\!)_\ell + (\!|\tau_2|\!)_\ell) & \text{Definition 3.30} \\ = & \mathrm{FV}((\!|\tau_1|\!)_\ell) \cup \mathrm{FV}((\!|\tau_2|\!)_\ell) \cup \mathrm{FV}(\ell) & \\ \subseteq & \mathrm{FV}(\tau_1) \cup \mathrm{FV}(\tau_2) \cup \mathrm{FV}(\ell) & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\ = & \mathrm{FV}(\tau_1 + \tau_2) \cup \mathrm{FV}(\ell) & \end{array}$$

6. $\mathsf{A} = \mathsf{ref}\ \tau_i$:

Let $\tau_i = \mathsf{A}_i^{\ell_i}$

$$\begin{array}{lll} & \mathrm{FV}((\!|\mathsf{ref}\ \tau_i|\!)_\ell) & \\ = & \mathrm{FV}(\mathsf{ref}\ \ell_i\ (\!|\mathsf{A}_i|\!)) & \text{Definition 3.30} \\ = & \mathrm{FV}(\ell_i) \cup \mathrm{FV}((\!|\mathsf{A}_i|\!)) & \\ \subseteq & \mathrm{FV}(\ell_i) \cup \mathrm{FV}(\mathsf{A}_i) \cup \mathrm{FV}(\ell) & \text{IH(2) on } \mathsf{A}_i \\ = & \mathrm{FV}(\mathsf{ref}\ \mathsf{A}_i^{\ell_i}) \cup \mathrm{FV}(\ell) & \\ = & \mathrm{FV}(\mathsf{ref}\ \tau_i) \cup \mathrm{FV}(\ell) & \end{array}$$

7. $\mathsf{A} = \forall \alpha.(\ell_e, \tau_i)$:

$$\begin{array}{lll} & \mathrm{FV}((\!|\forall \alpha.(\ell_e, \tau_i)|\!)) & \\ = & \mathrm{FV}(\forall \alpha, \alpha', \gamma.(\ell \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_i|\!)_{\alpha'}) & \text{Definition 3.30} \\ = & \mathrm{FV}(\ell) \cup \mathrm{FV}(\ell_e) \cup \mathrm{FV}((\!|\tau_i|\!)) & \\ \subseteq & \mathrm{FV}(\ell) \cup \mathrm{FV}(\ell_e) \cup \mathrm{FV}(\tau_i) & \text{IH(1) on } \tau_i \\ = & \mathrm{FV}(\ell) \cup \mathrm{FV}(\forall \alpha.(\ell_e, \tau_i)) & \end{array}$$

8. $\mathsf{A} = c \overset{\ell_e}{\Rightarrow} \tau_i$:

$$\begin{array}{lll} & \mathrm{FV}((\!|c \overset{\ell_e}{\Rightarrow} \tau_i|\!)) & \\ = & \mathrm{FV}(\forall \alpha, \gamma.(c \wedge \ell \sqcup \gamma \sqsubseteq \alpha \sqcap \ell_e) \Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau|\!)_{\alpha}) & \text{Definition 3.30} \\ = & \mathrm{FV}(\ell_e) \cup \mathrm{FV}(c) \cup \mathrm{FV}((\!|\tau_i|\!)) \cup \mathrm{FV}(\ell) & \\ \subseteq & \mathrm{FV}(\ell_e) \cup \mathrm{FV}(c) \cup \mathrm{FV}(\tau_i) \cup \mathrm{FV}(\ell) & \text{IH(1) on } \tau_i \\ = & \mathrm{FV}(c \overset{\ell_e}{\Rightarrow} \tau_i) \cup \mathrm{FV}(\ell) & \end{array}$$

□

Lemma 3.36 (FG $\rightsquigarrow$ SLIO*: Substitution lemma)**.** *$\forall \tau, \mathsf{A}, \ell$ s.t $\alpha \notin FV(\ell)$, $\vdash \tau\ WF$ and $\vdash \mathsf{A}\ WF$. The following holds*

1. $((\!|\tau|\!)_\ell[\ell'/\alpha]) = (\!|\tau[\ell'/\alpha]|\!)_\ell$

2. $((\!|\mathsf{A}|\!)_\ell)[\ell'/\alpha] = (\!|\mathsf{A}[\ell'/\alpha]|\!)_\ell)$

Proof. Proof by simultaneous induction on τ and A

Proof for (1)

Let $\tau = \mathsf{A}^{\ell_i}$

$$\begin{array}{lll} & ((\!|\mathsf{A}^{\ell_i}|\!)_\ell)[\ell'/\alpha] & \\ = & (\mathsf{Labeled}\ (\ell_i \sqcup \ell)\ (\!|\mathsf{A}|\!)_{\ell_i \sqcup \ell})[\ell'/\alpha] & \text{Definition 3.30} \\ = & (\mathsf{Labeled}\ (\ell_i[\ell'/\alpha] \sqcup \ell)\ (\!|\mathsf{A}|\!)_{\ell_i[\ell'/\alpha] \sqcup \ell}[\ell'/\alpha]) & \\ = & (\mathsf{Labeled}\ (\ell_i[\ell'/\alpha] \sqcup \ell)\ (\!|\mathsf{A}[\ell'/\alpha]|\!)_{\ell_i[\ell'/\alpha] \sqcup \ell}) & \text{IH(2)} \\ = & (\!|(\mathsf{A}[\ell'/\alpha]^{\ell_i[\ell'/\alpha]})|\!)_\ell & \\ = & (\!|(\mathsf{A}^{\ell_i}[\ell'/\alpha])|\!)_\ell & \end{array}$$

Proof for (2)

1. $\mathsf{A} = \mathsf{b}$:

$$\begin{array}{lll} & ((\!|\mathsf{b}|\!)_\ell)[\ell'/\alpha] & \\ = & (\mathsf{b})[\ell'/\alpha] & \text{Definition 3.30} \\ = & \mathsf{b} & \\ = & (\!|(\mathsf{b})|\!)_\ell & \\ = & (\!|(\mathsf{b}[\ell'/\alpha])|\!)_\ell & \end{array}$$

2. $\mathsf{A} = \mathsf{unit}$:

$$\begin{array}{lll} & ((\!|\mathsf{unit}|\!)_\ell)[\ell'/\alpha] & \\ = & (\mathsf{unit})[\ell'/\alpha] & \text{Definition 3.30} \\ = & \mathsf{unit} & \\ = & (\!|(\mathsf{unit})|\!)_\ell & \\ = & (\!|(\mathsf{unit}[\ell'/\alpha])|\!)_\ell & \end{array}$$

3. $\mathsf{A} = \tau_1 \xrightarrow{\ell_e} \tau_2$:

$$\begin{array}{lll} & ((\!|\tau_1 \xrightarrow{\ell_e} \tau_2|\!)_\ell)[\ell'/\alpha] & \\ = & (\forall \alpha', \beta, \gamma.(\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e) \Rightarrow (\!|\tau_1|\!)_\beta \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha'})[\ell'/\alpha] & \text{Definition 3.30} \\ = & (\forall \alpha', \beta, \gamma.(\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e[\ell'/\alpha]) \Rightarrow (\!|\tau_1|\!)_\beta[\ell'/\alpha] \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2|\!)_{\alpha'}[\ell'/\alpha]) & \\ = & (\forall \alpha', \beta, \gamma.(\ell \sqcup \beta \sqcup \gamma \sqsubseteq \alpha' \sqcap \ell_e[\ell'/\alpha]) \Rightarrow (\!|\tau_1[\ell'/\alpha]|\!)_\beta \rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_2[\ell'/\alpha]|\!)_{\alpha'}) & \text{IH(1)} \\ = & (\!|(\tau_1[\ell'/\alpha] \xrightarrow{\ell_e[\ell'/\alpha]} \tau_2[\ell'/\alpha])|\!)_\ell & \\ = & (\!|(\tau_1 \xrightarrow{\ell_e} \tau_2)[\ell'/\alpha]|\!)_\ell & \end{array}$$

4. $\mathsf{A} = \tau_1 \times \tau_2$:

$$\begin{array}{lll} & ((\!|\tau_1 \times \tau_2|\!)_\ell)[\ell'/\alpha] & \\ = & ((\!|\tau_1|\!)_\ell \times (\!|\tau_2|\!)_\ell)[\ell'/\alpha] & \text{Definition 3.30} \\ = & ((\!|\tau_1|\!)_\ell[\ell'/\alpha] \times (\!|\tau_2|\!)_\ell[\ell'/\alpha]) & \\ = & ((\!|\tau_1[\ell'/\alpha]|\!)_\ell \times (\!|\tau_2[\ell'/\alpha]|\!)_\ell) & \text{IH(1)} \\ = & (\!|(\tau_1[\ell'/\alpha] \times \tau_2[\ell'/\alpha])|\!)_\ell & \\ = & (\!|(\tau_1 \times \tau_2)[\ell'/\alpha]|\!)_\ell & \end{array}$$

5. $\mathsf{A} = \tau_1 + \tau_2$:

$$\begin{array}{lll} & ((\!|\tau_1 + \tau_2|\!)_\ell)[\ell'/\alpha] & \\ = & ((\!|\tau_1|\!)_\ell + (\!|\tau_2|\!)_\ell)[\ell'/\alpha] & \text{Definition 3.30} \\ = & ((\!|\tau_1|\!)_\ell[\ell'/\alpha] + (\!|\tau_2|\!)_\ell[\ell'/\alpha]) & \\ = & ((\!|\tau_1[\ell'/\alpha]|\!)_\ell + (\!|\tau_2[\ell'/\alpha]|\!)_\ell) & \text{IH(1)} \\ = & (\!|(\tau_1[\ell'/\alpha] + \tau_2[\ell'/\alpha])|\!)_\ell & \\ = & (\!|(\tau_1 + \tau_2)[\ell'/\alpha]|\!)_\ell & \end{array}$$

6. $\mathsf{A} = \mathsf{ref}\ \tau_i$:

   Let $\tau_i = \mathsf{A}_i^{\ell_i}$

$$\begin{array}{lll} & ((\!|\mathsf{ref}\ \tau_i|\!)_\ell)[\ell'/\alpha] & \\ = & (\mathsf{ref}\ \ell_i\ (\!|\mathsf{A}_i|\!))[\ell'/\alpha] & \text{Definition 3.30} \\ = & (\mathsf{ref}\ \ell_i\ (\!|\mathsf{A}_i|\!)) & \text{Lemma 3.34} \\ = & (\!|(\mathsf{ref}\ \mathsf{A}_i^{\ell_i})|\!)_\ell & \\ = & (\!|(\mathsf{ref}\ \mathsf{A}_i^{\ell_i})[\ell'/\alpha]|\!)_\ell & \text{Since} \vdash \mathsf{ref}\ \tau_i\ WF \\ = & (\!|(\mathsf{ref}\ \tau_i)[\ell'/\alpha]|\!)_\ell & \end{array}$$

7. $\mathsf{A} = \forall \alpha''.(\ell_e, \tau_i)$:

$$
\begin{array}{lll}
 & ((\!|\forall\alpha''.(\ell_e,\tau_i)|\!))[\ell'/\alpha] & \\
= & (\forall\alpha'',\alpha',\gamma.(\ell\sqcup\gamma\sqsubseteq\alpha'\sqcap\ell_e)\Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_i|\!)_{\alpha'})[\ell'/\alpha] & \text{Definition 3.30} \\
= & (\forall\alpha'',\alpha',\gamma.(\ell\sqcup\gamma\sqsubseteq\alpha'\sqcap\ell_e[\ell'/\alpha])\Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_i|\!)_{\alpha'}[\ell'/\alpha]) & \\
= & (\forall\alpha'',\alpha',\gamma.(\ell\sqcup\gamma\sqsubseteq\alpha'\sqcap\ell_e[\ell'/\alpha])\Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_i[\ell'/\alpha]|\!)_{\alpha'}) & \text{IH(1)} \\
= & (\!|(\forall\alpha''.(\ell_e[\ell'/\alpha],\tau_i[\ell'/\alpha]))|\!)_\ell & \\
= & (\!|(\forall\alpha''.(\ell_e,\tau_i))[\ell'/\alpha]|\!)_\ell &
\end{array}
$$

8. $\mathsf{A} = c \overset{\ell_e}{\Rightarrow} \tau_i$:

$$
\begin{array}{lll}
 & ((\!|c \overset{\ell_e}{\Rightarrow} \tau_i|\!))[\ell'/\alpha] & \\
= & (\forall\alpha',\gamma.(c\wedge\ell\sqcup\gamma\sqsubseteq\alpha'\sqcap\ell_e)\Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_i|\!)_{\alpha'})[\ell'/\alpha] & \text{Definition 3.30} \\
= & (\forall\alpha',\gamma.(c[\ell'/\alpha]\wedge\ell\sqcup\gamma\sqsubseteq\alpha'\sqcap\ell_e[\ell'/\alpha])\Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_i|\!)_{\alpha'}[\ell'/\alpha]) & \\
= & (\forall\alpha',\gamma.(c[\ell'/\alpha]\wedge\ell\sqcup\gamma\sqsubseteq\alpha'\sqcap\ell_e[\ell'/\alpha])\Rightarrow \mathbb{SLIO}\ \gamma\ \gamma\ (\!|\tau_i[\ell'/\alpha]|\!)_{\alpha'}) & \text{IH(1)} \\
= & (\!|(c[\ell'/\alpha] \overset{\ell_e[\ell'/\alpha]}{\Rightarrow} \tau_i[\ell'/\alpha])|\!)_\ell & \\
= & (\!|(c \overset{\ell_e}{\Rightarrow} \tau_i)[\ell'/\alpha]|\!)_\ell &
\end{array}
$$

□

3.3.3 Model for FG to SLIO* translation

Definition 3.37 (FG ⇝ SLIO*: ${}^s\theta_2$ extends ${}^s\theta_1$). ${}^s\theta_1 \sqsubseteq {}^s\theta_2 \triangleq$
$\forall a \in {}^s\theta_1.{}^s\theta_1(a) = \tau \implies {}^s\theta_2(a) = \tau$

Definition 3.38 (FG ⇝ SLIO*: $\hat\beta_2$ extends $\hat\beta_1$). $\hat\beta_1 \sqsubseteq \hat\beta_2 \triangleq$
$\forall (a_1, a_2) \in \hat\beta_1.(a_1, a_2) \in \hat\beta_2$

Definition 3.39 (FG ⇝ SLIO*: Unary value relation).

$$
\begin{array}{lll}
\lfloor \mathsf{b} \rfloor_V^{\hat\beta} & \triangleq & \{({}^s\theta, m, {}^sv, {}^tv) \mid {}^sv \in [\![\mathsf{b}]\!] \wedge {}^tv \in [\![\mathsf{b}]\!] \wedge {}^sv = {}^tv\} \\
\lfloor \mathsf{unit} \rfloor_V^{\hat\beta} & \triangleq & \{({}^s\theta, m, {}^sv, {}^tv) \mid {}^sv \in [\![\mathsf{unit}]\!] \wedge {}^tv \in [\![\mathsf{unit}]\!]\} \\
\lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat\beta} & \triangleq & \{({}^s\theta, m, ({}^sv_1, {}^sv_2), ({}^tv_1, {}^tv_2)) \mid \\
 & & ({}^s\theta, m, {}^sv_1, {}^tv_1) \in \lfloor \tau_1 \rfloor_V^{\hat\beta} \wedge ({}^s\theta, m, {}^sv_2, {}^tv_2) \in \lfloor \tau_2 \rfloor_V^{\hat\beta}\} \\
\lfloor \tau_1 + \tau_2 \rfloor_V^{\hat\beta} & \triangleq & \{({}^s\theta, m, \mathsf{inl}\ {}^sv, \mathsf{inl}\ {}^tv) \mid ({}^s\theta, m, {}^sv, {}^tv) \in \lfloor \tau_1 \rfloor_V^{\hat\beta}\} \cup \\
 & & \{({}^s\theta, m, \mathsf{inr}\ {}^sv, \mathsf{inr}\ {}^tv) \mid ({}^s\theta, m, {}^sv, {}^tv) \in \lfloor \tau_2 \rfloor_V^{\hat\beta}\} \\
\lfloor \tau_1 \overset{\ell_e}{\to} \tau_2 \rfloor_V^{\hat\beta} & \triangleq & \{({}^s\theta, m, \lambda x.e_s, \Lambda\Lambda(\nu(\lambda x.e_t))) \mid \\
 & & \forall {}^s\theta' \sqsupseteq {}^s\theta, {}^sv, {}^tv, j < m, \hat\beta \sqsubseteq \hat\beta'.({}^s\theta', j, {}^sv, {}^tv) \in \lfloor \tau_1 \rfloor_V^{\hat\beta'} \implies \\
 & & ({}^s\theta', j, e_s[{}^sv/x], e_t[{}^tv/x]) \in \lfloor \tau_2 \rfloor_E^{\hat\beta'}\} \\
\lfloor \forall\alpha.(\ell_e, \tau) \rfloor_V^{\hat\beta} & \triangleq & \{({}^s\theta, m, \Lambda e_s, \Lambda\Lambda(\nu(e_t))) \mid \\
 & & \forall {}^s\theta' \sqsupseteq {}^s\theta, j < m, \ell' \in \mathcal{L}, \hat\beta \sqsubseteq \hat\beta'.({}^s\theta', j, e_s, e_t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat\beta'}\} \\
\lfloor c \overset{\ell_e}{\Rightarrow} \tau \rfloor_V^{\hat\beta} & \triangleq & \{({}^s\theta, m, \nu e_s, \Lambda(\nu(e_t))) \mid \\
 & & \mathcal{L} \models c \implies \forall {}^s\theta' \sqsupseteq {}^s\theta, j < m, \hat\beta \sqsubseteq \hat\beta'.({}^s\theta', j, e_s, e_t) \in \lfloor \tau \rfloor_E^{\hat\beta'}\} \\
\lfloor \mathsf{ref}\ \tau \rfloor_V^{\hat\beta} & \triangleq & \{({}^s\theta, m, a_s, a_t) \mid {}^s\theta(a_s) = \tau \wedge ({}^sa, {}^ta) \in \hat\beta\} \\
\lfloor \mathsf{A}^{\ell'} \rfloor_V^{\hat\beta} & \triangleq & \{({}^s\theta, m, {}^sv, \mathsf{Lb}({}^tv)) \mid ({}^s\theta, m, {}^sv, {}^tv) \in \lfloor \mathsf{A} \rfloor_V^{\hat\beta}\}
\end{array}
$$

Definition 3.40 (FG $\rightsquigarrow$ SLIO*: Unary expression relation)**.**

$$\begin{array}{rcl}\lfloor\tau\rfloor_E^{\hat\beta} & \triangleq & \{({}^s\theta, n, e_s, e_t) \mid \\ & & \forall H_s, H_t.(n, H_s, H_t) \overset{\hat\beta}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, e_s) \Downarrow_i (H_s', {}^s v) \implies \\ & & \exists H_t', {}^t v.(H_t, e_t) \Downarrow^f (H_t', {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat\beta' \sqsupseteq \hat\beta.(n-i, H_s', H_t') \overset{\hat\beta'}{\triangleright} {}^s\theta' \\ & & \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor\tau\rfloor_V^{\hat\beta'}\}\end{array}$$

Definition 3.41 (FG $\rightsquigarrow$ SLIO*: Unary heap well formedness)**.**

$$\begin{array}{rcl}(n, H_s, H_t) \overset{\hat\beta}{\triangleright} {}^s\theta & \triangleq & dom({}^s\theta) \subseteq dom(H_s) \wedge \\ & & \hat\beta \subseteq (dom({}^s\theta) \times dom(H_t)) \wedge \\ & & \forall (a_1, a_2) \in \hat\beta.({}^s\theta, n-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a_1)\rfloor_V^{\hat\beta}\end{array}$$

Definition 3.42 (FG $\rightsquigarrow$ SLIO*: Label substitution)**.** $\sigma : Lvar \mapsto Label$

Definition 3.43 (FG $\rightsquigarrow$ SLIO*: Value substitution to values)**.** $\delta^s : Var \mapsto Val$, $\delta^t : Var \mapsto Val$

Definition 3.44 (FG $\rightsquigarrow$ SLIO*: Unary interpretation of Γ)**.**

$$\begin{array}{rcl}\lfloor\Gamma\rfloor_V^{\hat\beta} & \triangleq & \{({}^s\theta, n, \delta^s, \delta^t) \mid dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t) \wedge \\ & & \forall x \in dom(\Gamma).({}^s\theta, n, \delta^s(x), \delta^t(x)) \in \lfloor\Gamma(x)\rfloor_V^{\hat\beta}\}\end{array}$$

3.3.4 Soundness proof for FG to SLIO* translation

Lemma 3.45 (FG $\rightsquigarrow$ SLIO*: Monotonicity)**.** $\forall {}^s\theta, {}^s\theta', n, {}^s v, {}^t v, n', \beta, \beta'$.

1. $\forall \mathsf{A}.\ ({}^s\theta, n, {}^s v, {}^t v) \in \lfloor\mathsf{A}\rfloor_V^{\hat\beta} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat\beta \sqsubseteq \hat\beta' \wedge n' < n \implies ({}^s\theta', n', {}^s v, {}^t v) \in \lfloor\mathsf{A}\rfloor_V^{\hat\beta'}$

2. $\forall \tau.\ ({}^s\theta, n, {}^s v, {}^t v) \in \lfloor\tau\rfloor_V^{\hat\beta} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat\beta \sqsubseteq \hat\beta' \wedge n' < n \implies ({}^s\theta', n', {}^s v, {}^t v) \in \lfloor\tau\rfloor_V^{\hat\beta'}$

Proof. Proof by simultaneous induction on A and τ

Proof of statement (1)

We case analyze A in the last step

1. Case b:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor\mathsf{b}\rfloor_V^{\hat\beta} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat\beta \sqsubseteq \hat\beta' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor\mathsf{b}\rfloor_V^{\hat\beta'}$

   Since $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor\mathsf{b}\rfloor_V^{\hat\beta}$ therefore from Definition 3.39 we know that ${}^s v \in [\![\mathsf{b}]\!] \wedge {}^t v \in [\![\mathsf{b}]\!]$ and ${}^s v = {}^t v$

   Therefore from Definition 3.39 we get the desired

2. Case unit:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}'}$

   Since $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}}$ therefore from Definition 3.39 we know that ${}^s v \in [\![\mathsf{unit}]\!] \wedge {}^t v \in [\![\mathsf{unit}]\!]$

   Therefore from Definition 3.39 we get the desired

3. Case $\tau_1 \times \tau_2$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}'}$

   From Definition 3.39 we know that ${}^s v = ({}^s v_1, {}^s v_2)$ and ${}^t v = ({}^t v_1, {}^t v_2)$.

   We also know that $({}^s\theta, n, {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}}$ and $({}^s\theta, n, {}^s v_2, {}^t v_2) \in \lfloor \tau_2 \rfloor_V^{\hat{\beta}}$

   <u>IH1:</u> $({}^s\theta', n', {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}'}$ (From Statement (2))

   <u>IH2:</u> $({}^s\theta', n', {}^s v_2, {}^t v_2) \in \lfloor \tau_2 \rfloor_V^{\hat{\beta}'}$ (From Statement (2))

   Therefore from Definition 3.39, IH1 and IH2 we get

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}'}$

4. Case $\tau_1 + \tau_2$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}'}$

   From Definition 3.39 two cases arise

   (a) ${}^s v = \mathsf{inl}({}^s v')$ and ${}^t v = \mathsf{inl}({}^t v')$:
   <u>IH:</u> $({}^s\theta', n', {}^s v', {}^t v') \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}'}$ (From Statement (2))
   Therefore from Definition 3.39 and IH we get
   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}'}$

   (b) ${}^s v = \mathsf{inr}({}^s v')$ and ${}^t v = \mathsf{inr}({}^t v')$:
   Symmetric reasosning as in the previous case

5. Case $\tau_1 \xrightarrow{\ell_e} \tau_2$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau_1 \xrightarrow{\ell_e} \tau_2 \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 \xrightarrow{\ell_e} \tau_2 \rfloor_V^{\hat{\beta}'}$

   From Definition 3.39 we know that

   ${}^s v$ is of the form $\lambda x.e_s$ (for some e_s) and ${}^t v$ is of the form $\Lambda\Lambda\Lambda(\nu(\lambda x.e_t))$ (for some e_t) s.t

   $({}^s\theta', j, e_s[{}^s v/x], e_t[{}^t v/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}_1'}$ (A0)

   Similarly from Definition 3.39 we are required to prove

   $\forall {}^s\theta'' \sqsupseteq {}^s\theta', {}^s v_2, {}^t v_2, k < n', \hat{\beta}' \sqsubseteq \hat{\beta}''.({}^s\theta'', k, {}^s v_2, {}^t v_2) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}''} \implies$
   $({}^s\theta'', k, e_s[{}^s v_2/x], e_t[{}^t v_2/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}''}$

   This means we are given some

   ${}^s\theta'' \sqsupseteq {}^s\theta', {}^s v_2, {}^t v_2, k < n', \hat{\beta}' \sqsubseteq \hat{\beta}''$ s.t $({}^s\theta'', k, {}^s v_2, {}^t v_2) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}''}$

   and we are required to prove

   $({}^s\theta'', k, e_s[{}^s v_2/x], e_t[{}^t v_2/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}''}$

   Instantiating (A0) with ${}^s\theta'', {}^s v_2, {}^t v_2, k, \hat{\beta}''$ since

   ${}^s\theta'' \sqsupseteq {}^s\theta' \sqsupseteq {}^s\theta$, $k < n' < n$ and $\hat{\beta} \sqsubseteq \hat{\beta}' \sqsubseteq \hat{\beta}''$ therefore we get

   $({}^s\theta'', k, e_s[{}^s v_2/x], e_t[{}^t v_2/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}''}$

6. Case $\forall \alpha.\tau$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \forall \alpha.(\ell_e, \tau) \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \forall \alpha.(\ell_e, \tau) \rfloor_V^{\hat{\beta}'}$

   From Definition 3.39 we know that ${}^s v = \Lambda e_s'$ and ${}^t v = \Lambda\Lambda\Lambda(\nu(e_t))$ s.t

   $\forall {}^s\theta' \sqsupseteq {}^s\theta, j < n, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}_1'.({}^s\theta', j, e_s, e_t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}_1'}$ (F0)

   Similarly from Definition 3.39 we are required to prove

   $\forall {}^s\theta'' \sqsupseteq {}^s\theta', k < n', \ell'' \in \mathcal{L}, \hat{\beta}' \sqsubseteq \hat{\beta}''.({}^s\theta'', k, e_s, e_t) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\hat{\beta}''}$

   This means we are given ${}^s\theta_1'' \sqsupseteq {}^s\theta', k < n', \ell'' \in \mathcal{L}, \hat{\beta}' \sqsubseteq \hat{\beta}''$

   and we are required to prove

   $({}^s\theta'', k, e_s, e_t) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\hat{\beta}''}$

   Instantiating (F0) with ${}^s\theta_1'', k, \hat{\beta}''$ since ${}^s\theta'' \sqsupseteq {}^s\theta' \sqsupseteq {}^s\theta$, $k < n' < n$ and $\hat{\beta} \sqsubseteq \hat{\beta}' \sqsubseteq \hat{\beta}''$ therefore we get

   $({}^s\theta'', k, e_s, e_t) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\hat{\beta}''}$

7. Case $c \overset{\ell_e}{\Rightarrow} \tau$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor c \overset{\ell_e}{\Rightarrow} \tau \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor c \overset{\ell_e}{\Rightarrow} \tau \rfloor_V^{\hat{\beta}'}$

   From Definition 3.39 we know that ${}^s v = \nu\ (e_s')$ and ${}^t v = \Lambda\Lambda(\nu(e_t))$. And

   $\mathcal{L} \models c \implies \forall {}^s\theta' \sqsupseteq {}^s\theta, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, e_s, e_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}'}$ (C0)

   Similarly from Definition 3.39 we are required to prove

   $\mathcal{L} \models c \implies \forall {}^s\theta'' \sqsupseteq {}^s\theta', k < n', \hat{\beta}' \sqsubseteq \hat{\beta}''.({}^s\theta', k, e_s, e_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}''}$

   This means we are given $\mathcal{L} \models c, {}^s\theta'' \sqsupseteq {}^s\theta', k < n', \hat{\beta}' \sqsubseteq \hat{\beta}''$

   and we are required to prove

   $({}^s\theta', k, e_s, e_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}''}$

   Since $\mathcal{L} \models c$ and instantiating (C0) with ${}^s\theta_1'', k, \hat{\beta}''$ since ${}^s\theta'' \sqsupseteq {}^s\theta' \sqsupseteq {}^s\theta$, $k < n' < n$ and $\hat{\beta} \sqsubseteq \hat{\beta}' \sqsubseteq \hat{\beta}''$ therefore we get

   $({}^s\theta', k, e_s, e_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}''}$

8. Case $\mathsf{ref}\ \tau$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{ref}\ \tau \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{ref}\ \tau \rfloor_V^{\hat{\beta}'}$

   From Definition 3.39 we know that ${}^s v = a_s$ and ${}^t v = a_t$. We also know that

   ${}^s\theta(a_s) = \tau \wedge (a_s, a_t) \in \hat{\beta}$

   From Definition 3.39, Definition 3.37 and Definition 3.38 we get

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{ref}\ \tau \rfloor_V^{\hat{\beta}'}$

Proof of Statement (2)

Let $\tau = \mathsf{A}^{\ell''}$:

Given:

$({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{A}^{\ell''} \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

From Definition 3.39 we know that

$\exists {}^t v_i . {}^t v = \mathsf{Lb}({}^t v_i)$ and $({}^s\theta, n, {}^s v, {}^t v_i) \in \lfloor \mathsf{A} \rfloor_V^{\hat{\beta}}$

To prove:

$({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{A}^{\ell''} \rfloor_V^{\hat{\beta}'}$

This means from Definition 3.39 we need to prove
$({}^s\theta', n', {}^s v, {}^t v_i) \in \lfloor \mathsf{A} \rfloor_V^{\hat{\beta}'}$

IH: $({}^s\theta', n', {}^s v, {}^t v_i) \in \lfloor \mathsf{A} \rfloor_V^{\hat{\beta}'}$ (From Statement (1))

Therefore we get the desired directly from IH.

□

Lemma 3.46 (FG ⇝ SLIO*: Unary monotonicity for Γ)**.** $\forall {}^s\theta, {}^s\theta', \delta, \Gamma, n, n', \hat{\beta}, \hat{\beta}'.$
$({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}} \wedge n' < n \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \implies ({}^s\theta', n', \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}'}$

Proof. Given: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}} \wedge n' < n \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}'$
To prove: $({}^s\theta', n', \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}'}$

From Definition 3.44 it is given that
$dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t) \wedge \forall x_i \in dom(\Gamma).({}^s\theta, n, \delta^s(x_i), \delta^t(x_i)) \in \lfloor \Gamma(x_i) \rfloor_V^{\hat{\beta}}$

And again from Definition 3.44 we are required to prove that
$dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t) \wedge \forall x_i \in dom(\Gamma).({}^s\theta', n', \delta^s(x_i), \delta^t(x_i)) \in \lfloor \Gamma(x_i) \rfloor_V^{\hat{\beta}'}$

- $dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t)$:
  Given
- $\forall x_i \in dom(\Gamma).({}^s\theta', n', \delta^s(x_i), \delta^t(x_i)) \in \lfloor \Gamma(x_i) \rfloor_V^{\hat{\beta}'}$:
  Since we know that $\forall x_i \in dom(\Gamma).({}^s\theta, n, \delta^s(x_i), \delta^t(x_i)) \in \lfloor \Gamma(x_i) \rfloor_V^{\hat{\beta}}$ (given)
  Therefore from Lemma 3.45 we get
  $\forall x_i \in dom(\Gamma).({}^s\theta', n', \delta^s(x_i), \delta^t(x_i)) \in \lfloor \Gamma(x_i) \rfloor_V^{\hat{\beta}'}$

□

Lemma 3.47 (FG ⇝ SLIO*: Unary monotonicity for H)**.** $\forall {}^s\theta, H_s, H_t, n, n', \hat{\beta}.$
$(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge n' < n \implies (n', H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Proof. Given: $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge n' < n$
To prove: $(n', H_s, H_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta$

From Definition 3.41 it is given that
$dom({}^s\theta) \subseteq dom(H_S) \wedge \hat{\beta} \subseteq (dom({}^s\theta) \times dom(H_t)) \wedge \forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$

And again from Definition 3.41 we are required to prove that
$dom({}^s\theta) \subseteq dom(H_S) \wedge \hat{\beta} \subseteq (dom({}^s\theta) \times dom(H_t)) \wedge \forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n'-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$

- $dom({}^s\theta) \subseteq dom(H_S)$:
  Given

- $\hat{\beta} \subseteq (dom(^s\theta) \times dom(H_t))$:

  Given

- $\forall (a_1, a_2) \in \hat{\beta}.(^s\theta, n' - 1, H_s(a_1), H_t(a_2)) \in \lfloor ^s\theta(a) \rfloor_V^{\hat{\beta}}$:

  Since we know that $\forall (a_1, a_2) \in \hat{\beta}.(^s\theta, n - 1, H_s(a_1), H_t(a_2)) \in \lfloor ^s\theta(a) \rfloor_V^{\hat{\beta}}$ (given)

  Therefore from Lemma 3.45 we get

  $\forall (a_1, a_2) \in \hat{\beta}.(^s\theta, n' - 1, H_s(a_1), H_t(a_2)) \in \lfloor ^s\theta(a) \rfloor_V^{\hat{\beta}}$

□

Lemma 3.48 (Coercion lemma). $\forall H, e, v.$
$(H, e) \Downarrow_{-}^{f} (H', \mathsf{Lb}\, v) \implies$
$(H, \texttt{coerce\_taint}\ e) \Downarrow_{-}^{f} (H', \mathsf{Lb}\, v)$

Proof. Given: $(H, e) \Downarrow_{-}^{f} (H', \mathsf{Lb}\, v)$

To prove: $(H, \texttt{coerce\_taint}\ e) \Downarrow_{-}^{f} (H', \mathsf{Lb}\, v)$

From Definition of coerce_taintand SLIO*-Sem-app it suffices to prove that
$(H, \mathsf{toLabeled}(\mathsf{bind}(e, y.\mathsf{unlabel}(y)))) \Downarrow_{-}^{f} (H', \mathsf{Lb}\, v)$

From SLIO*-Sem-tolabeled it suffices to prove that
$(H, \mathsf{bind}(e, y.\mathsf{unlabel}(y))) \Downarrow_{-}^{f} (H', v)$

From SLIO*-Sem-bind it suffices to prove that

1. $(H, e) \Downarrow_{-}^{f} (H'_1, v_1)$:

   We are given that $(H, e) \Downarrow_{-}^{f} (H', v)$ therefore we have $H'_1 = H'$ and $v'_1 = \mathsf{Lb}\, v$

2. $(H'_1, \mathsf{unlabel}(y)[v_1/y]) \Downarrow_{-}^{f} (H', v)$:

   It sufffices to prove that

   $(H', \mathsf{unlabel}(\mathsf{Lb}\, v)) \Downarrow_{-}^{f} (H', v)$:

   We get this directly from SLIO*-Sem-unlabel

□

Theorem 3.49 (FG $\rightsquigarrow$ SLIO*: Fundamental theorem). $\forall \Sigma, \Psi, \Gamma, \tau, e_s, e_t, pc, \mathcal{L}, \delta^s, \delta^t, \sigma, {^s\theta}, n, \hat{\beta}.$
$\Sigma; \Psi; \Gamma \vdash_{pc} e_s : \tau \rightsquigarrow e_t \wedge$
$\mathcal{L} \models \Psi\ \sigma \wedge (^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$
$\implies$
$(^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

Proof. Proof by induction on the $\rightsquigarrow$ relation

1. FC-var:

$$\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash_{pc} x : \tau \rightsquigarrow \mathsf{ret}\ x}\ \text{FC-var}$$

   Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge (^s\theta, n, \delta^s, \delta^t) \in \lfloor (\Gamma \cup \{x \mapsto \tau\})\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, x\ \delta^s, \mathsf{ret}(x)\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.40 it suffices to prove that

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, x\ \delta^s) \Downarrow_i (H_s', {}^s v) \implies$
$\exists H_t', {}^t v.(H_t, \mathsf{ret}(x)\ \delta^t) \Downarrow^f (H_t', {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge$
$({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau \rfloor_V^{\hat{\beta}'}$

This means given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^s v$ s.t $(H_s, x\ \delta^s) \Downarrow_i (H_s', {}^s v)$

From fg-val we know that $i = 0$, ${}^s v = x\ \delta^s$. Also from SLIO*-Sem-ret we know that ${}^t v = x\ \delta^t$ and $H_t' = H_t$

And we are required to prove

$\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsubseteq \hat{\beta}.(n, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n, {}^s v, {}^t v) \in \lfloor \tau \rfloor_V^{\hat{\beta}'}$ (F-V0)

We choose ${}^s\theta'$ as ${}^s\theta$ and $\hat{\beta}'$ as $\hat{\beta}$

(a) $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$: Given

(b) $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau \rfloor_V^{\hat{\beta}}$:
Since we are given $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor (\Gamma \cup \{x \mapsto \tau\})\ \sigma \rfloor_V^{\hat{\beta}}$, therefore from Definition 3.44 we get $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}}$

2. FC-lam:

$$\frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{\ell_e} e_s : \tau_2 \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash_{pc} \lambda x.e_s : (\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(\lambda x.e_t))))}\ \text{FC-lam}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, (\lambda x.e_s)\ \delta^s, \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(\lambda x.e_t))))\ \delta^t) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 3.40 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, (\lambda x.e_s)\ \delta^s) \Downarrow_i (H_s', {}^s v) \implies$
$\exists H_t', {}^t v.(H_t, \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(\lambda x.e_t))))\ \delta^t) \Downarrow^f (H_t', {}^t v) \wedge$
$\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $(H_s, (\lambda x.e_s)\ \delta^s) \Downarrow_i (H_s', {}^s v)$

From fg-val we know that ${}^s v = (\lambda x.e_s)\ \delta^s$, $H_s' = H_s$ and $i = 0$. Also from SLIO*-Sem-ret, SLIO*-Sem-label and SLIO*-Sem-FI we know that $H_t' = H_t$ and ${}^t v = (\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(\lambda x.e_t))))\ \delta^t$

It suffices to prove that

$\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n, H_s, H_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n, {}^sv, {}^tv) \in \lfloor(\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp\ \sigma\rfloor_V^{\hat{\beta}'}$

We choose ${}^s\theta'$ as ${}^s\theta$ and $\hat{\beta}'$ as $\hat{\beta}$

(a) $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$: Given

(b) $({}^s\theta, n, \lambda x.e_s\ \delta^s, (\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(\lambda x.e_t))))\ \delta^t) \in \lfloor(\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp\ \sigma\rfloor_V^{\hat{\beta}}$:
From Definition 3.39 it suffices to prove that
$({}^s\theta, n, \lambda x.e_s\ \delta^s, (\Lambda\Lambda\Lambda(\nu(\lambda x.e_t)))\ \delta^t) \in \lfloor(\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma\rfloor_V^{\hat{\beta}}$

Again from Definition 3.39 it suffices to prove that
$\forall^s\theta' \sqsupseteq {}^s\theta, {}^sv_d, {}^tv_d, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, {}^sv_d, {}^tv_d) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}'} \implies$
$({}^s\theta', j, e_s[{}^sv_d/x]\ \delta^s, e_t[{}^tv_d/x]\ \delta^t) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}'}$

This further means that given ${}^s\theta' \sqsupseteq {}^s\theta, {}^sv_d, {}^tv_d, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t $({}^s\theta', j, {}^sv_d, {}^tv_d) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}'}$

And we a re required to prove
$({}^s\theta', j, e_s[{}^sv_d/x]\ \delta^s, e_t[{}^tv_d/x]\ \delta^t) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}'}$ (F-L0)

Since we are given $({}^s\theta', j, {}^sv_d, {}^tv_d) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}'}$, therefore from Definition 3.44 and Lemma 3.46 we have
$({}^s\theta', j, \delta^s \cup \{x \mapsto {}^sv_d\}, \delta^t \cup \{x \mapsto {}^tv_d\}) \in \lfloor(\Gamma \cup \{x \mapsto \tau_1\})\ \sigma\rfloor_V^{\hat{\beta}'}$.
Therefore from IH we get
$({}^s\theta', j, e_s\ \delta^s \cup \{x \mapsto {}^sv_d\}, e_t\ \delta^t \cup \{x \mapsto {}^tv_d\}) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}'}$

We get (F-L0) directly from IH

3. FC-app:

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e_{s1} : (\tau_1 \xrightarrow{\ell_e} \tau_2)^\ell \rightsquigarrow e_{t1} \qquad \Sigma;\Psi;\Gamma \vdash_{pc} e_{s2} : \tau_1 \rightsquigarrow e_{t2} \qquad \Sigma;\Psi \vdash \ell \sqcup pc \sqsubseteq \ell_e \qquad \Sigma;\Psi \vdash \tau \searrow \ell}{\Sigma;\Psi;\Gamma \vdash_{pc} e_{s1}\ e_{s2} : \tau_2 \rightsquigarrow \mathtt{coerce\_taint}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b))))}\ \text{FC-app}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor\Gamma\ \sigma\rfloor_V^{\hat{\beta}}$

To prove:
$({}^s\theta, n, (e_{s1}\ e_{s2})\ \delta^s, \mathtt{coerce\_taint}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b))))\ \delta^t) \in \lfloor\tau\ \sigma\rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv.(H_s, (e_{s1}\ e_{s2})\ \delta^s) \Downarrow_i (H_s', {}^sv) \implies$
$\exists H_t', {}^tv.(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b))))\ \delta^t) \Downarrow^f (H_t', {}^tv) \wedge$
$\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor\tau_2\ \sigma\rfloor_V^{\hat{\beta}'}$

This further means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^sv$ s.t

$(H_s, (e_{s1}\ e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$

And we need to prove

$\exists H'_t, {}^t v.(H_t, \mathsf{coerce\_taint}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b))))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge$
$\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-A0)

<u>IH1:</u>

$({}^s\theta, n, e_{s1}\ \delta^s, e_{t1}\ \delta^t) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^\ell\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_{s1}) \Downarrow_j (H'_{s1}, {}^s v_1) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge$
$({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$

We instantiate with H_s, H_t. And since we know that $(H_s, (e_{s1}\ e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists j < i < n$ s.t $(H_{s1}, e_{s1}) \Downarrow_j (H'_{s1}, {}^s v_1)$.

This means we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-A1.0)

Since we know that $({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$ therefore from Definition 3.39 we know that $\exists^t v_i.{}^t v_1 = \mathsf{Lb}({}^t v_i)$ s.t

$({}^s\theta'_1, n-j, {}^s v_1, {}^t v_i) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-A1.1)

From Definition 3.39 we know that ${}^s v_1 = \lambda x.e'_s$ and ${}^t v_i = \Lambda\Lambda\Lambda(\nu(\lambda x.e'_t))$ s.t
$\forall^s\theta''_1 \sqsupseteq {}^s\theta'_1, {}^s v', {}^t v', l < (n-j), \hat{\beta}'_1 \sqsubseteq \hat{\beta}''_1.$
$({}^s\theta''_1, l, {}^s v', {}^t v') \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}''_1} \implies ({}^s\theta''_1, l, e'_s[{}^s v'/x], e'_t[{}^t v'/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}''_1}$ (F-A1)

<u>IH2:</u>

$({}^s\theta'_1, n-j, e_{s2}\ \delta^s, e_{t2}\ \delta^t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}'_1}$

This means from Definition 3.40 we have

$\forall H_{s2}, H_{t2}.(n-j, H_{s2}, H_{t2}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta \wedge \forall k < n-j, {}^s v_2.(H_{s2}, e_{s2}\ \delta^s) \Downarrow_j (H'_{s2}, {}^s v_2) \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t2}) \Downarrow^f (H'_{t2}, {}^t v_2\ \delta^t) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_1.(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'_2}$

We instantiate with $H'_{s1}, H'_{t1},$. And since we know that $(H_s, (e_{s1}\ e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists k < i-j < n-j$ s.t $(H'_{s1}, e_{s2}\ \delta^s) \Downarrow_k (H'_{s2}, {}^s v_2)$.

This means we have

$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t2}) \Downarrow^f (H'_{t2}, {}^t v_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_1.(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'_2}$ (F-A2)

We instantiate (F-A1) with θ''_1 as θ'_2, ${}^s v'$ as ${}^s v_2$, ${}^t v'$ as ${}^t v_2$, l as $n - j - k$ and $\hat{\beta}''_1$ as $\hat{\beta}'_2$. Therefore we get

$({}^s\theta'_2, n - j - k, e'_s[{}^s v_2/x], e'_t[{}^t v_2/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}'_2}$

From Definition 3.40 we have

$\forall H_s, H_t.(n - j - k, H_s, H_t) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge \forall a < n - j - k, {}^s v.(H_s, e'_s[{}^s v_2/x]) \Downarrow_i (H'_{s3}, {}^s v_3) \implies$
$\exists H'_{t3}, {}^t v_3.(H_t, e'_t[{}^t v_2/x]) \Downarrow^f (H'_{t3}, {}^t v_3) \wedge \exists^s\theta'_3 \sqsupseteq {}^s\theta'_2, \hat{\beta}'_3 \sqsupseteq \hat{\beta}'_2.$
$(n - j - k - a, H'_{s3}, H'_{t3}) \overset{\hat{\beta}'_3}{\triangleright} {}^s\theta'_3 \wedge ({}^s\theta'_3, n - j - k - a, {}^s v_3, {}^t v_3) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'_3}$

Instantiating with H'_{s2}, H'_{t2}. since we know that $(H_s, (e_{s1}\ e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists a < i - j - k < n - j - k$ s.t $(H'_{s2}, e'_s[{}^s v/x]\ \delta^s) \Downarrow_a (H'_{s3}, {}^s v_3)$

Therefore we have
$\exists H'_{t3}, {}^t v_3.(H_t, e'_t[{}^t v_2/x]) \Downarrow^f (H'_{t3}, {}^t v_3) \wedge \exists^s\theta'_3 \sqsupseteq {}^s\theta'_2, \hat{\beta}'_3 \sqsupseteq \hat{\beta}'_2.$
$(n - j - k - a, H'_{s3}, H'_{t3}) \overset{\hat{\beta}'_3}{\triangleright} {}^s\theta'_3 \wedge ({}^s\theta'_3, n - j - k - a, {}^s v_3, {}^t v_3) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'_3}$ (F-A3)

Let $\tau_2\ \sigma = \mathsf{A}_2^{\ell_i}$, since $\tau_2\ \sigma \searrow \ell\ \sigma$ therefore $\ell\ \sigma \sqsubseteq \ell_i$ and
$({}^s\theta'_3, n - j - k - a, {}^s v_3, {}^t v_3) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'_3}$
Therefore from Definition 3.39 we know that
$({}^s\theta'_3, n - j - k - a, {}^s v_3, \mathsf{Lb}\,{}^t v_{3i}) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'_3}$ (F-A3.1)

In order to prove (F-A0) we choose H'_t as H'_{t3} and ${}^t v$ as $\mathsf{Lb}({}^t v_{3i})$. We need to prove:

(a) $(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b))))\ \delta^t) \Downarrow^f (H'_{t3}, \mathsf{Lb}\,{}^t v_{3i})$:

From Lemma 3.48 it suffices to prove that
$(H_t, (\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b))))\ \delta^t) \Downarrow^f (H'_{t3}, \mathsf{Lb}\,{}^t v_{3i})$

From SLIO*-Sem-bind it further suffices to show that

- $(H_t, e_{t1}\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1)$:
  We get this directly from (F-A1.0)
- $(H'_{t1}, \mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b))[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t3}, \mathsf{Lb}\,{}^t v_{3i})$:
  From SLIO*-Sem-bind it suffices to prove that
  - $(H'_{t1}, e_{t2}\ \delta^t) \Downarrow^f (H'_{t2}, {}^t v_2)$:
    We get this directly from (F-A2)
  - $(H'_{t2}, \mathsf{bind}(\mathsf{unlabel}\ a, c.(c[][][]\bullet)\ b)[{}^t v_1/a][{}^t v_2/b]\ \delta^t) \Downarrow^f (H'_{t3}, \mathsf{Lb}\,{}^t v_{3i})$:
    From SLIO*-Sem-bind again it suffices to prove
    * $(H'_{t2}, (\mathsf{unlabel}\ a)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t31}, {}^t v_{t2})$:
      Since from (F-A1.1) we know that $\exists^t v_i.{}^t v_1 = \mathsf{Lb}({}^t v_i)$

      Therefore from SLIO*-Sem-unlabel and (F-A1) we know that $H'_{t31} = H'_{t2}$ and ${}^t v_{t2} = {}^t v_i = \Lambda\Lambda\Lambda(\nu(\lambda x.e'_t))$

* $((c[][][] \bullet\ b)[{}^t v_2/b][{}^t v_{t2}/c]\ \delta^t) \Downarrow {}^t v_{t21}$:
  It suffices to prove that
  $(((\Lambda\Lambda\Lambda(\nu(\lambda x.e'_t)))[][][] \bullet\ {}^t v_2)\ \delta^t) \Downarrow {}^t v_{t21}$

  From SLIO*-Sem-FE it suffices to prove that
  $(((\Lambda\Lambda(\nu(\lambda x.e'_t)))[][] \bullet\ {}^t v_2)\ \delta^t) \Downarrow {}^t v_{t21}$

  Again from SLIO*-Sem-FE appleid two times it suffices to prove that
  $((\nu(\lambda x.e'_t) \bullet\ {}^t v_2)\ \delta^t) \Downarrow {}^t v_{t21}$

  From SLIO*-Sem-CE it suffices to prove that
  $(((\lambda x.e'_t)\ {}^t v_2)\ \delta^t) \Downarrow {}^t v_{t21}$

  From SLIO*-Sem-app we know that
  ${}^t v_{t21} = e'_t[{}^t v_2/x]\ \delta^t$
* $(H'_{t2}, {}^t v_{21}) \Downarrow^f (H'_{t3}, \mathsf{Lb}\,{}^t v_{3i})$:
  We get this from (F-A3) and (F-A3.1)

(b) $\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta'_3$ and $\hat{\beta}'$ as $\hat{\beta}'_3$. From fg-app we know that $i = j + k + a + 1$, ${}^s v = {}^s v_3$ and $H'_s = H'_{s3}$. Also from the termination proof (previous point) we know that $H'_t = H'_{t3}$ and ${}^t v = \mathsf{Lb}\ ({}^t v_3)$

We get $(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta'$ from (F-A3) and Lemma 3.47

Since ${}^t v = \mathsf{Lb}({}^t v_3)$ therefore from Definition 3.39 it suffices to prove that
$({}^s\theta'_3, n-j-k-a-1, {}^s v_3, {}^t v_3) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'_3}$

We get this directly from (F-A3) and Lemma 3.45

4. FC-prod:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_{s1} : \tau_1 \rightsquigarrow e_{t1} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_{s2} : \tau_2 \rightsquigarrow e_{t2}}{\Sigma; \Psi; \Gamma \vdash_{pc} (e_{s1}, e_{s2}) : (\tau_1 \times \tau_2)^\perp \rightsquigarrow \mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{ret}(\mathsf{Lb}(a, b))))} \text{ prod}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, (e_{s1}, e_{s2})\ \delta^s, (\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{ret}(\mathsf{Lb}(a, b)))))\ \delta^t) \in \lfloor (\tau_1 \times \tau_2)^\perp\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v_1, {}^s v_2.(H_s, (e_{s1}, e_{s2})) \Downarrow_i (H'_s, ({}^s v_1, {}^s v_2)) \implies$
$\exists H'_t, {}^t v.(H_t, (\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{ret}(\mathsf{Lb}(a, b)))))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \in \lfloor (\tau_1 \times \tau_2)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^s v_1, {}^s v_2$ s.t $(H_s, (e_{s1}, e_{s2})) \Downarrow_i (H'_s, ({}^s v_1, {}^s v_2))$

And we need to prove
$\exists H'_t, {}^t v.(H_t, (\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{ret}(\mathsf{Lb}(a, b)))))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, ({}^s v_1, {}^s v_2), {}^t v) \in \lfloor (\tau_1 \times \tau_2)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-P0)

IH1:

$({}^s\theta, n, e_{s1}\ \delta^s, e_{t1}\ \delta^t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we need to prove

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_{s1}\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-j, {}^s v_1, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'_1}$

Instantiating with H_s, H_t and since we know that $(H_s, (e_{s1}, e_{s2})) \Downarrow_i (H'_s, ({}^s v_1, {}^s v_2))$ therefore $\exists j < i < n$ s.t $(H_{s1}, e_{s1}\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1)$

Therefore we have
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1)) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-P1)

IH2:

$({}^s\theta'_1, n-j, e_{s2}\ \delta^s, e_{t2}\ \delta^t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}'_1}$

This means from Definition 3.40 we need to prove

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta'_1 \wedge \forall k < n-j, {}^s v_1.(H_{s2}, e_{s2}\ \delta^s) \Downarrow_j (H'_{s2}, {}^s v_1) \implies$
$\exists H'_{t2}, {}^t v_1.(H_{t2}, e_{t2}) \Downarrow^f (H'_{t2}, {}^t v_1) \wedge \exists {}^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_1.$
$(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_1, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'_2}$

Instantiating with H'_{s1}, H'_{t1} and since we know that $(H_s, (e_{s1}, e_{s2})) \Downarrow_i (H'_s, ({}^s v_1, {}^s v_2))$ therefore $\exists k < i-j < n-j$ s.t $(H_{s2}, e_{s2}\ \delta^s) \Downarrow_k (H'_{s2}, {}^s v_2)$

Therefore we have
$\exists H'_{t2}, {}^t v_1.(H_{t2}, e_{t2}) \Downarrow^f (H'_{t2}, {}^t v_1) \wedge \exists {}^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_1.$
$(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'_2}$ (F-P2)

In order to prove (F-P0) we choose H_t as H'_{t2} and ${}^t v$ as $\mathsf{Lb}({}^t v_1, {}^t v_2)$

(a) $(H_t, (\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{ret}(\mathsf{Lb}(a, b))))\ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}({}^t v_1, {}^t v_2))$:
From SLIO*-Sem-bind it suffices to prove that

- $(H_t, e_{t1}\ \delta^t) \Downarrow^f (H'_{tb1}, {}^t v_{tb1})$:
  From (F-P1) we know that $H'_{tb1} = H'_{t1}$ and ${}^t v_{tb1} = {}^t v_1$
- $(H'_{t1}, \mathsf{bind}(e_{t2}, b.\mathsf{ret}(\mathsf{Lb}(a, b)))[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}({}^t v_1, {}^t v_2))$:
  From SLIO*-Sem-bind it suffices to prove that
  - $(H_t, e_{t2}\ \delta^t) \Downarrow^f (H'_{tb2}, {}^t v_{tb2})$:
    From (F-P2) we know that $H'_{tb2} = H'_{t2}$ and ${}^t v_{tb2} = {}^t v_2$
  - $(H'_{t2}, \mathsf{ret}(\mathsf{Lb}(a, b))[{}^t v_1/a][{}^t v_2/b]\ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}({}^t v_1, {}^t v_2))$:
    From SLIO*-Sem-ret, (F-P1) and (F-P2)

(b) $\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, ({}^sv_1, {}^sv_2), {}^tv) \in \lfloor (\tau_1 \times \tau_2)^{\perp}\ \sigma \rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta_2'$ and $\hat{\beta}'$ as $\hat{\beta}_2'$ and since from fg-prod $i = j+k+1$ and $H_s' = H_{s2}'$. Therefore from (F-P2) and Lemma 3.47 we get

$(n-i, H_s', H_{t2}') \overset{\hat{\beta}'}{\triangleright} {}^s\theta'$

In order to prove $({}^s\theta', n-i, ({}^sv_1, {}^sv_2), {}^tv) \in \lfloor (\tau_1 \times \tau_2)^{\perp}\ \sigma \rfloor_V^{\hat{\beta}'}$
From Definition 3.39 it suffices to prove

$\exists^t v_i.{}^tv = \mathsf{Lb}({}^tv_i) \wedge ({}^s\theta', n-i, ({}^sv_1, {}^sv_2), {}^tv_i) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V^{\hat{\beta}_2'}$

Since ${}^tv = \mathsf{Lb}({}^tv_1, {}^tv_2)$ therefore we get the desired from (F-P1), (F-P2), Definition 3.39 and Lemma 3.45

5. FC-fst:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_s : (\tau_1 \times \tau_2)^{\ell} \rightsquigarrow e_t \qquad \Sigma; \Psi \vdash \tau_1 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{fst}(e_s) : \tau_1 \rightsquigarrow \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))}\ \text{fst}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$
To prove: $({}^s\theta, n, \mathsf{fst}(e_s)\ \delta^s, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))\ \delta^t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv.(H_s, \mathsf{fst}(e_s)) \Downarrow_i (H_s', {}^sv) \implies$
$\exists H_t', {}^tv.(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))) \Downarrow^f (H_t', {}^tv) \wedge$
$\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\gamma,\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^sv$ s.t $(H_s, \mathsf{fst}(e_s)) \Downarrow_i (H_s', {}^sv)$
We need to prove

$\exists H_t', {}^tv.(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))) \Downarrow^f (H_t', {}^tv) \wedge$
$\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-F0)

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\tau_1 \times \tau_2)^{\ell}\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv_1.(H_{s1}, e_s) \Downarrow_j (H_{s1}', {}^sv_1) \implies$
$\exists H_{t1}', {}^tv.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H_{t1}', {}^tv_1) \wedge \exists^s\theta_1' \sqsupseteq {}^s\theta, \hat{\beta}_1' \sqsupseteq \hat{\beta}.$
$(n-j, H_{s1}', H_{t1}') \overset{\hat{\beta}_1'}{\triangleright} {}^s\theta_1' \wedge ({}^s\theta_1', n-j, {}^sv_1, {}^tv_1) \in \lfloor (\tau_1 \times \tau_2)^{\ell}\ \sigma \rfloor_V^{\hat{\beta}_1'}$

Instantiating with H_s, H_t and since we know that $(H_s, \mathsf{fst}(e_s)) \Downarrow_i (H_s', {}^sv)$ therefore $\exists j < i < n$ s.t $(H_s, e_s) \Downarrow_j (H_{s1}', {}^sv_1)$

This means we have
$\exists H'_{t1}, {}^t v.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor(\tau_1 \times \tau_2)^\ell\ \sigma\rfloor_V^{\hat{\beta}'_1}$ (F-F1)

Since we know that $({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor(\tau_1 \times \tau_2)^\ell\ \sigma\rfloor_V^{\hat{\beta}'_1}$ therefore from Definition 3.39 we know that ${}^t v_1 = \mathsf{Lb}({}^t v_i)$ s.t

$({}^s\theta'_1, n-j, {}^s v_1, {}^t v_i) \in \lfloor(\tau_1 \times \tau_2)\ \sigma\rfloor_V^{\hat{\beta}'_1}$ (F-F1.1)

From Definition 3.39 we know that ${}^s v_1 = ({}^s v_{i1}, {}^s v_{i2})$ and ${}^t v_i = ({}^t v_{i1}, {}^t v_{i2})$ s.t

$({}^s\theta'_1, n-j, {}^s v_{i1}, {}^t v_{i1}) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}}$ (F-F1.2)

Let $\tau_1\ \sigma = \mathsf{A}_1^{\ell_i}$, since $\tau_1\ \sigma \searrow \ell\ \sigma$ therefore $\ell\ \sigma \sqsubseteq \ell_i$ and

Since $({}^s\theta'_1, n-j, {}^s v_{i1}, {}^t v_{i1}) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}}$
Therefore from Definition 3.39 we know that
$({}^s\theta'_1, n-j, {}^s v_{i1}, \mathsf{Lb}\,{}^t v_{i11}) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}}$ (F-F1.3)

In order to prove (F-F0) we choose H'_t as H'_{t1} and ${}^t v$ as $\mathsf{Lb}\,{}^t v_{i11}$ as we need to prove

(a) $(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))) \Downarrow^f (H'_{t1}, \mathsf{Lb}\,{}^t v_{i11})$:

From Lemma 3.48 it suffices to prove that
$(H_t, (\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))) \Downarrow^f (H'_{t1}, \mathsf{Lb}\,{}^t v_{i11})$
From SLIO*-Sem-bind it suffices to prove that

- $(H_t, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1)$:
  We get this from (F-F1)
- $(H'_{t1}, \mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t1}, \mathsf{Lb}\,{}^t v_{i11})$:
  Again from SLIO*-Sem-bind it suffices to prove that
  - $(H'_{t1}, \mathsf{unlabel}\ (a)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t21}, {}^t v_{t21})$:
    Since ${}^t v_1 = \mathsf{Lb}({}^t v_{i1}, {}^t v_{i2})$ from (F-F1.1) and (F-F1.2) therefore we get the desired from SLIO*-Sem-unlabel

    So, $H_{t21} = H'_{t1}$ and ${}^t v_{t21} = ({}^t v_{i1}, {}^t v_{i2})$
  - $(H'_{t1}, \mathsf{ret}(\mathsf{fst}(b))[({}^t v_{i1}, {}^t v_{i2})/b]\ \delta^t) \Downarrow^f (H'_{t1}, \mathsf{Lb}\,{}^t v_{i11})$:
    We get this from SLIO*-Sem-fst, SLIO*-Sem-ret and (F-F1.2) and (F-F1.3)

(b) $\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}'}$:

We choose ${}^s\theta'$ as ${}^s\theta'_1$ and $\hat{\beta}'$ as $\hat{\beta}'_1$. And from fg-fst we know that $i = j+1$ and $H'_s = H'_{s1}$ therefore from (F-F1) and Lemma 3.47 we get

$(n-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1$

Since from fg-fst we know that ${}^s v = {}^s v_{i1}$ therefore from (F-F1.2) and Lemma 3.45 we get

$({}^s\theta', n-i, {}^s v_{i1}, {}^t v_{i1}) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}'_1}$

6. FC-snd:

Symmetric reasoning as in the FC-fst case

7. FC-inl:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau_1 \leadsto e_t}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inl}(e_s) : (\tau_1 + \tau_2)^{\perp} \leadsto \mathsf{bind}(e_t, a.\mathsf{ret}(\mathsf{Lbinl}(a)))} \text{ inl}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{inl}(e_s)\ \delta^s, \mathsf{bind}(e_t, a.\mathsf{ret}(\mathsf{Lbinl}(a)))\ \delta^t) \in \lfloor (\tau_1 + \tau_2)^{\perp}\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we have

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, \mathsf{inl}(e_s)) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{bind}(e_t, a.\mathsf{ret}(\mathsf{Lbinl}(a)))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$

This means that we are given some H_s, H_t s.t $(n, H_s, H_t) \overset{\gamma,\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^s v$ s.t $(H_s, \mathsf{inl}(e_s)) \Downarrow_i (H'_s, {}^s v)$
And we need to prove
$\exists H'_t, {}^t v.(H_t, \mathsf{bind}(e_t, a.\mathsf{ret}(\mathsf{Lbinl}(a)))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor (\tau_1 + \tau_2)^{\perp}\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-IL0)

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we need to prove

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_s\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n - j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - j, {}^s v_1, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'_1}$

Instantiating with H_s, H_t and since we know that $(H_s, \mathsf{inl}(e_s)) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists j < i < n$ s.t $(H_s, e_s\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1)$

Therefore we have
$\exists H'_{t1}, {}^t v_1.(H_t, e_{t1}) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n - j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n - j, {}^s v_1, {}^t v_1)) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-IL1)

In order to prove (F-IL0) we choose H'_t as H'_{t1} and ${}^t v$ as $(\mathsf{Lb}\ \mathsf{inl}({}^t v_1))$ and we need to prove:

(a) $(H'_{t1}, \mathsf{bind}(e_t, a.\mathsf{ret}(\mathsf{Lbinl}(a)))\ \delta^t) \Downarrow^f (H'_{t1}, (\mathsf{Lb}\ \mathsf{inl}({}^t v_1)))$:
From SLIO*-Sem-bind it suffices to prove that

i. $(H'_{t1}, e_t\ \delta^t) \Downarrow^f (H'_{t11}, {}^t v_{t11})$:
From (F-IL1) we know that $H'_{t11} = H'_{t1}$ and ${}^t v_{t11} = {}^t v_1$

ii. $(H'_{t1}, \mathsf{ret}(\mathsf{Lbinl}(a))[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t1}, (\mathsf{Lb}\ \mathsf{inl}({}^t v_1)))$:
We get this from SLIO*-Sem-ret, (F-IL1)

(b) $\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor (\tau_1 + \tau_2)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$:

We choose ${}^s\theta'$ as ${}^s\theta'_1$ and $\hat{\beta}'$ as $\hat{\beta}'_1$. Since from fg-inl we know that $i = j+1$ and $H'_s = H'_{s1}$ therefore from (F-IL1) and Lemma 3.47 we get

$(n-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1$

Now we need to prove $({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor (\tau_1 + \tau_2)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$

Since ${}^sv = \mathsf{inl}\ {}^sv_1$ and ${}^tv = \mathsf{Lb}(\mathsf{inl}({}^tv_1))$ therefore from Definition 3.39 it suffices to prove that

$({}^s\theta', n-i, \mathsf{inl}\ {}^sv_1, \mathsf{inl}\ {}^tv_1) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V^{\hat{\beta}'}$

Since from (F-IL1) we know that $({}^s\theta', n-j, {}^sv_1, {}^tv_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'}$

Therefore from Lemma 3.45 and Definition 3.39 we get

$({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V^{\hat{\beta}'}$

8. FC-inr:

   Symmetric reasoning as in the FC-inl case

9. FC-case:

$$\frac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e_s : (\tau_1 + \tau_2)^\ell \rightsquigarrow e_t \\ \Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_{s1} : \tau \rightsquigarrow e_{t1} \qquad \Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_{s2} : \tau \rightsquigarrow e_{t2} \qquad \Sigma; \Psi \vdash \tau \searrow \ell\end{array}}{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{case}(e_s, x.e_{s1}, y.e_{s2}) : \tau \rightsquigarrow \\ \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{t1}, y.e_{t2}))))\end{array}} \text{case}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove:

$({}^s\theta, n, \mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{t1}, y.e_{t2}))))\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv.(H_s, \mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^sv) \implies$
$\exists H'_t, {}^tv.(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{t1}, y.e_{t2}))))\ \delta^t) \Downarrow^f (H'_t, {}^tv) \wedge$

$\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$

This means we are given some H_s, H_t s.t $(n, H_s, H_t) \overset{\gamma,\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^sv$ s.t $(H_s, \mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^sv)$

And we need to prove

$\exists H'_t, {}^tv.(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{t1}, y.e_{t2}))))\ \delta^t) \Downarrow^f (H'_t, {}^tv) \wedge$

$\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-C0)

<u>IH1:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor(\tau_1 + \tau_2)^\ell\ \sigma\rfloor_E^{\hat\beta}$

This means from Definition 3.40 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat\beta}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_s) \Downarrow_j (H'_{s1}, {}^s v_1) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat\beta'_1 \sqsupseteq \hat\beta.$
$(n - j, H'_{s1}, H'_{t1}) \overset{\hat\beta'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n - j, {}^s v_1, {}^t v_1) \in \lfloor\tau\ \sigma\rfloor_V^{\hat\beta'_1}$

Instantiating with H_s, H_t and since we know that $(H_s, \mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists j < i < n$ s.t $(H_{s1}, e_s) \Downarrow_j (H'_{s1}, {}^s v_1)$

Therefore we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat\beta'_1 \sqsupseteq \hat\beta.$
$(n - j, H'_{s1}, H'_{t1}) \overset{\hat\beta'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n - j, {}^s v_1, {}^t v_1) \in \lfloor(\tau_1 + \tau_2)^\ell\ \sigma\rfloor_V^{\hat\beta'_1}$ (F-C1)

Since from (F-C1) we have $({}^s\theta'_1, n - j, {}^s v_1, {}^t v_1) \in \lfloor(\tau_1 + \tau_2)^\ell\ \sigma\rfloor_V^{\hat\beta'_1}$ therefore from Definition 3.39 we know that

$\exists^t v_i.{}^t v_1 = \mathsf{Lb}({}^t v_i) \wedge ({}^s\theta'_1, n - j, {}^s v_1, {}^t v_i) \in \lfloor(\tau_1 + \tau_2)\ \sigma\rfloor_V^{\hat\beta'_1}$ (F-C1.1)

2 cases arise

(a) ${}^s v_1 = \mathsf{inl}({}^s v_{i1})$ and ${}^t v_i = \mathsf{inl}({}^t v_{i1})$:

Also from Lemma 3.46 and Definition 3.44 we know that
$({}^s\theta'_1, n - j, \delta^s \cup \{x \mapsto {}^s v_1\}, \delta^t \cup \{x \mapsto {}^t v_{i1}\}) \in \lfloor(\Gamma, \{x \mapsto {}^s v_1\})\ \sigma\rfloor_V^{\hat\beta'_1}$
<u>IH2:</u>
$({}^s\theta'_1, n - j, e_{s1}\ \delta^s \cup \{x \mapsto {}^s v_1\}, e_{t1}\ \delta^t \cup \{x \mapsto {}^t v_{i1}\}) \in \lfloor\tau\ \sigma\rfloor_E^{\hat\beta'_1}$

This means from Definition 3.40 we have

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat\beta'_1}{\triangleright} {}^s\theta'_1 \wedge \forall k < n - j, {}^s v_2.(H_{s2}, e_{s1}\ \delta^s \cup \{x \mapsto {}^s v_1\}) \Downarrow_j (H'_{s2}, {}^s v_2) \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t1}\ \delta^t \cup \{x \mapsto {}^t v_{i1}\}) \Downarrow^f (H'_{t2}, {}^t v_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat\beta'_2 \sqsupseteq \hat\beta'_1.$
$(n - j - k, H'_{s2}, H'_{t2}) \overset{\hat\beta'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n - j - k, {}^s v_2, {}^t v_2) \in \lfloor\tau\ \sigma\rfloor_V^{\hat\beta'_2}$

Instantiating with H'_{s1}, H'_{t1} and since we know that $(H_s, \mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s \cup \{x \mapsto {}^s v_1\}) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists k < i - j < n - j$ s.t $(H'_{s1}, e_{s1}) \Downarrow_k (H'_{s2}, {}^s v_2)$
Therefore we have
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t1}\ \delta^t \cup \{x \mapsto {}^t v_1\}) \Downarrow^f (H'_{t2}, {}^t v_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat\beta'_2 \sqsupseteq \hat\beta'_1.$
$(n - j - k, H'_{s2}, H'_{t2}) \overset{\hat\beta'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n - j - k, {}^s v_2, {}^t v_2) \in \lfloor\tau\ \sigma\rfloor_V^{\hat\beta'_2}$ (F-C2)

Let $\tau\ \sigma = \mathsf{A}_2^{\ell_i}$, since $\tau\ \sigma \searrow \ell\ \sigma$ therefore $\ell\ \sigma \sqsubseteq \ell_i$ and
$({}^s\theta'_2, n - j - k, {}^s v_2, {}^t v_2) \in \lfloor\tau\ \sigma\rfloor_V^{\hat\beta'_2}$
Therefore from Definition 3.39 we know that
$({}^s\theta'_2, n - j - k, {}^s v_2, \mathsf{Lb}^t v_{2i}) \in \lfloor\tau\ \sigma\rfloor_V^{\hat\beta'_2}$ (F-C2.1)

In order to prove (F-C0) we choose H'_t as H'_{t2} and ${}^t v$ as $\mathsf{Lb}^t v_{2i}$
And we need to prove:

i. $(H_t, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{t1}, y.e_{t2})))) \ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}\, {}^t v_{2i})$:

From Lemma 3.48 it suffices to prove that
$(H_t, (\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{t1}, y.e_{t2})))) \ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}\, {}^t v_{2i})$
From SLIO*-Sem-bind it suffices to prove that

- $(H_t, e_t \ \delta^t) \Downarrow^f (H'_{t11}, {}^t v_{t11})$:
From (F-C1) we know that $H'_{t11} = H'_{t1}$ and ${}^t v_{t11} = {}^t v_1$
- $(H'_{t1}, \mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{t1}, y.e_{t2}))[{}^t v_1/a] \ \delta^t) \Downarrow^f (H'_{t1}, \mathsf{Lb}\, {}^t v_{2i})$:
From SLIO*-Sem-bind it suffices to prove that
  – $(H'_{t1}, (\mathsf{unlabel}\ a)[{}^t v_1/a] \ \delta^t) \Downarrow^f (H'_{t21}, {}^t v_{t21})$:
  Since from (F-C1.1) we know that ${}^t v_1 = \mathsf{Lb}({}^t v_i)$ therefore from SLIO*-Sem-unlabel we know that
  $H'_{t21} = H'_{t1}$ and ${}^t v_{t21} = {}^t v_i$
  – $(\mathsf{case}(b, x.e_{t1}, y.e_{t2})[{}^t v_i/b] \ \delta^t) \Downarrow {}^t v_{t22}$:
  Since we know that in this case ${}^t v_i = \mathsf{inl}({}^t v_{i1})$
  Therefore from SLIO*-Sem-case we know that ${}^t v_{t22} = e_{t1}[{}^t v_{i1}/x] \ \delta^t$
  – $(H'_{t1}, e_{t1}[{}^t v_{i1}/x] \ \delta^t) \Downarrow (H'_{t2}, \mathsf{Lb}\, {}^t v_{2i})$:
  We get this from (F-C2) and (F-C2.1)

ii. $\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau \ \sigma \rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta'_2$ and $\hat{\beta}'$ as $\hat{\beta}'_2$. Since from fg-case we know that $i = j + k + 1$ and $H'_s = H'_{s2}$ therefore from (F-C2) and Lemma 3.47 we get
$(n-i, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2$

Now we need to prove $({}^s\theta'_2, n-i, {}^s v, {}^t v) \in \lfloor \tau \ \sigma \rfloor_V^{\hat{\beta}'_2}$
Since ${}^s v = {}^s v_2$ and ${}^t v = {}^t v_2$ and since from (F-C2) we know that
$({}^s\theta'_2, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau \ \sigma \rfloor_V^{\hat{\beta}'_2}$
Therefore from Lemma 3.45 and Definition 3.39 we get
$({}^s\theta'_2, n-i, {}^s v_2, {}^t v_2) \in \lfloor \tau \ \sigma \rfloor_V^{\hat{\beta}'_2}$

(b) ${}^s v_1 = \mathsf{inr}({}^s v_{i1})$ and ${}^t v_1 = \mathsf{inr}({}^t v_{i1})$:
Symmetric reasoning as in the previous case

10. FC-FI:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{\ell_e} e_s : \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash_{pc} \Lambda e_s : (\forall \alpha_g.(\ell_e, \tau))^\perp \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(e_t))))} \text{FI}$$

Also given is: $\mathcal{L} \models \Psi \ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \Lambda e_s \ \delta^s, \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(e_t)))) \ \delta^t) \in \lfloor \tau \ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, \Lambda e_s \ \delta^s) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(e_t)))) \ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor (\forall \alpha_g.(\ell_e, \tau))^\perp \ \sigma \rfloor_V^{\hat{\beta}'}$

This means given some H_s, H_t s.t $(n, H_s, H_t) \overset{\gamma,\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^s v$ s.t $(H_s, \Lambda e_s\ \delta^s) \Downarrow_i (H'_s, {}^s v)$

And we need to prove

$\exists H'_t, {}^t v.(H_t, \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(e_t))))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor (\forall \alpha_g.(\ell_e, \tau))^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$

From fg-val we know that ${}^s v = (\Lambda e_s)\ \delta^s$, $H'_s = H_s$ and $i = 0$. Also from SLIO*-Sem-ret we know that $H'_t = H_t$ and ${}^t v = (\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(e_t))))\ \delta^t$

It suffices to prove that

$\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor (\forall \alpha_g.(\ell_e, \tau))^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$

We choose ${}^s\theta'$ as ${}^s\theta$ and $\hat{\beta}'$ as $\hat{\beta}$

(a) $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$: Given

(b) $({}^s\theta, n, \Lambda e_s\ \delta^s, (\mathsf{Lb}(\Lambda\Lambda\Lambda(\nu(e_t))))\ \delta^t) \in \lfloor (\forall \alpha_g.(\ell_e, \tau))^\perp\ \sigma \rfloor_V^{\hat{\beta}}$:
From Definition 3.39 it suffices to prove that
$({}^s\theta, n, \Lambda e_s\ \delta^s, (\Lambda\Lambda\Lambda(\nu(e_t)))\ \delta^t) \in \lfloor (\forall \alpha_g.(\ell_e, \tau))\ \sigma \rfloor_V^{\hat{\beta}}$

Again from Definition 3.39 it suffices to prove that
$\forall {}^s\theta'_1 \sqsupseteq {}^s\theta, j < n, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}'_1.({}^s\theta'_1, j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau[\ell'/\alpha_g]\ \sigma \rfloor_E^{\hat{\beta}'_1}$

This further means that given ${}^s\theta'_1 \sqsupseteq {}^s\theta, j < n, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}'_1$
And we need to prove
$({}^s\theta'_1, j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau[\ell'/\alpha_g] \rfloor_E^{\hat{\beta}'_1}$ (F-FI0)

<u>IH</u>: $({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \cup \{\alpha_g \mapsto \ell'\} \rfloor_E^{\hat{\beta}'_1}$

We get (F-FI0) directly from IH

11. FC-FE:

$$\frac{\mathrm{FV}(\ell') \subseteq \Sigma \qquad \begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e_s : (\forall \alpha_g.(\ell_e, \tau))^\ell \rightsquigarrow e_t \\ \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e[\ell'/\alpha]\end{array} \qquad \Sigma; \Psi \vdash \tau[\ell'/\alpha] \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e_s[] : \tau \rightsquigarrow \mathsf{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.b[][][]\bullet)))} \text{ FE}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, e_s[]\ \delta^s, \mathsf{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.b[][][]\bullet)))\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, e_s[]) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.b[][][]\bullet)))) \Downarrow^f (H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$

This means given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^s v$ s.t $(H_s, e_s[]) \Downarrow_i (H'_s, {}^s v)$

And we need to prove

$\exists H'_t, {}^t v.(H_t, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.b[][][]\bullet)))) \Downarrow^f (H'_t, {}^t v) \wedge \exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$

$(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-FE0)

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\forall \alpha_g.(\ell_e, \tau))^\ell\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_s\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\forall \alpha_g.(\ell_e, \tau))^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$

Instantiating with H_s, H_t and since we know that $(H_s, e_s[]) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists j < i < n$ s.t $(H_s, e_s) \Downarrow_j (H'_{s1}, {}^s v_1)$

This means we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\forall \alpha_g.(\ell_e, \tau))^\ell\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-FE1)

Since from (F-FE1) we have $({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\forall \alpha_g.(\ell_e, \tau))^\ell\ \sigma \rfloor_V^{\hat{\beta}'}$ therefore from Definition 3.39 we know that

$\exists^t v_i.{}^t v_1 = \mathsf{Lb}({}^t v_i) \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_i) \in \lfloor (\forall \alpha_g.(\ell_e, \tau))\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-FE1.1)

Therefore from Definition 3.39 we have

${}^s v_1 = \Lambda e'_s$ and ${}^t v_i = \Lambda\Lambda\Lambda\nu e'_t$

$\forall^s\theta'_2 \sqsupseteq {}^s\theta'_1, \ell'' \in \mathcal{L}, k < n-j, \hat{\beta} \sqsubseteq \hat{\beta}'_1.({}^s\theta'_2, k, e'_s, e'_t) \in \lfloor \tau[\ell''/\alpha_g]\ \sigma \rfloor_E^{\hat{\beta}'_1}$ (F-FE1.2)

We instantiate with ${}^s\theta'_1, \ell', n-j-1, \hat{\beta}'$ we get $({}^s\theta'_1, n-j-1, e'_s, e'_t) \in \lfloor \tau[\ell'/\alpha_g]\ \sigma \rfloor_E^{\hat{\beta}'}$

From Definition 3.40 we have

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta'_1 \wedge \forall k < (n-j-1), {}^s v_2.(H_{s2}, e'_s) \Downarrow_k (H'_{s2}, {}^s v_2) \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e'_t) \Downarrow^f (H'_{t2}, {}^t v_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'' \sqsupseteq \hat{\beta}'.$
$(n-j-1-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n-j-1-k, {}^s v_2, {}^t v_2) \in \lfloor \tau[\ell'/\alpha_g]\ \sigma \rfloor_V^{\hat{\beta}''}$

Instantiating with H'_{s1}, H'_{t1} and since we know that $(H_s, e_s[]) \Downarrow_i (H'_s, {}^s v)$ and from fg-FE we know that $i = j+k+1 < n$ therefore we know that $k < n-j-1$ s.t $(H_{s2}, e'_s) \Downarrow_k (H'_{s2}, {}^s v_2)$. Therefore we have

$\exists H'_{t2}, {}^t v_2.(H'_{t1}, e'_t) \Downarrow^f (H'_{t2}, {}^t v_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'' \sqsupseteq \hat{\beta}'.$
$(n-j-1-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n-j-1-k, {}^s v_2, {}^t v_2) \in \lfloor \tau[\ell'/\alpha_g]\ \sigma \rfloor_V^{\hat{\beta}''}$ (F-FE1.3)

Let $\tau[\ell'/\alpha]\ \sigma = \mathsf{A}^{\ell_i}$, since $\tau[\ell'/\alpha]\ \sigma \searrow \ell\ \sigma$ therefore $\ell\ \sigma \sqsubseteq \ell_i$ and

$({}^s\theta'_2, n-j-1-k, {}^s v_2, {}^t v_2) \in \lfloor \tau[\ell'/\alpha_g]\ \sigma \rfloor_V^{\hat{\beta}''}$
Therefore from Definition 3.39 we know that
$({}^s\theta'_2, n-j-1-k, {}^s v_2, \mathsf{Lb}\, {}^t v_{2i}) \in \lfloor \tau[\ell'/\alpha_g]\ \sigma \rfloor_V^{\hat{\beta}''}$ (F-FE1.4)

In order to prove (F-FE0) we choose H'_t as H'_{t2} and ${}^t v$ as $\mathsf{Lb}\, {}^t v_{2i}$. We need to prove

(a) $(H_t, \mathsf{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.b[][][]\bullet)))) \Downarrow^f (H'_{t2}, \mathsf{Lb}\, {}^t v_{2i})$:

From Lemma 3.48 it suffices to prove that
$(H_t, (\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.b[][][]\bullet)))) \Downarrow^f (H'_{t2}, \mathsf{Lb}\, {}^t v_{2i})$
From SLIO*-Sem-bind it suffices to prove that

- $(H_t, e_t\ \delta^t) \Downarrow^f (H'_{t11}, {}^t v_{t11})$:
  From (F-FE1) we know that $H'_{t11} = H'_{t1}$ and ${}^t v_{t11} = {}^t v_1$
- $(H'_{t1}, \mathsf{bind}(\mathsf{unlabel}\ a, b.b[][][]\bullet)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}\, {}^t v_{2i})$:
  Again from SLIO*-Sem-bind it suffices to prove that
  - $(H'_{t1}, (\mathsf{unlabel}\ a)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t12}, {}^t v_{t12})$:
    From (F-FE1.1) we know that ${}^t v_1 = \mathsf{Lb}({}^t v_i)$
    Therefore from SLIO*-Sem-unlabel we have $H'_{t12} = H'_{t1}$ and ${}^t v_{t12} = {}^t v_i$
  - $(b[][][]\bullet)[{}^t v_i/b]\ \delta^t \Downarrow {}^t v_{t13}$:
    From (F-FE1.2) we know that ${}^s v_1 = \Lambda e'_s$ and ${}^t v_i = \Lambda\Lambda\Lambda\nu e'_t$

    Therefore from SLIO*-Sem-FE and SLIO*-Sem-CE we know that ${}^t v_{t13} = e'_t$
  - $(H'_{t1}, e'_t \Downarrow^f (H'_{t2}, \mathsf{Lb}\, {}^t v_{2i})$
    From (F-FE1.3) and (F-FE1.4) we get the desired.

(b) $\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau[\ell'/\alpha_g]\ \sigma \rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta'_2$ and $\hat{\beta}'$ as $\hat{\beta}''$. From fg-FE we know that $i = j+k+1$, ${}^s v = {}^s v'_2$, ${}^t v = {}^t v'_2$, $H'_s = H'_{s2}$ and $H'_t = H'_{t2}$.

Therefore from (F-FE1.3) we get the $(n-i, H'_{s2}, H'_{t2}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta'_2$

<u>To prove:</u> $({}^s\theta'_2, n-i, {}^s v'_2, {}^t v'_2) \in \lfloor \tau[\ell'/\alpha_g]\ \sigma \rfloor_V^{\hat{\beta}''}$

We get this directly from (F-FE1.3)

12. FC-CI:

$$\frac{\Sigma; \Psi, c; \Gamma \vdash_{\ell_e} e : \tau \rightsquigarrow e_c}{\Sigma; \Psi; \Gamma \vdash_{pc} \nu e : (c \overset{\ell_e}{\Rightarrow} \tau)^\perp \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda(\nu(e_c))))}\ \text{CI}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \nu e\ \delta^s, \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda(\nu(e_c))))\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, \nu e_s\ \delta^s) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda(\nu(e_c))))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$

This means given some H_s, H_t s.t $(n, H_s, H_t) \overset{\gamma,\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^s v$ s.t $(H_s, \nu e_s\ \delta^s) \Downarrow_i (H_s', {}^s v)$

And we need to prove

$\exists H_t', {}^t v.(H_t, \mathsf{ret}(\mathsf{Lb}(\Lambda\Lambda(\nu(e_c))))\ \delta^t) \Downarrow^f (H_t', {}^t v) \wedge \exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$

From fg-val we know that ${}^s v = (\nu e_s)\ \delta^s$, $H_s' = H_s$ and $i = 0$. Also from SLIO*-Sem-ret we know that $H_t' = H_t$ and ${}^t v = (\mathsf{Lb}(\Lambda\Lambda(\nu(e_c))))\ \delta^t$

It suffices to prove that

$\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$

We choose ${}^s\theta'$ as ${}^s\theta$ and $\hat{\beta}'$ as $\hat{\beta}$

(a) $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$: Given

(b) $({}^s\theta, n, \nu e_s\ \delta^s, (\mathsf{Lb}(\Lambda\Lambda(\nu(e_c))))\ \delta^t) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\perp\ \sigma \rfloor_V^{\hat{\beta}}$:
From Definition 3.39 it suffices to prove that
$({}^s\theta, n, \Lambda e_s\ \delta^s, (\mathsf{Lb}(\Lambda\Lambda(\nu(e_c))))\ \delta^t) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)\ \sigma \rfloor_V^{\hat{\beta}}$

Again from Definition 3.39 it suffices to prove that
$\mathcal{L} \models c\ \sigma \implies \forall^s\theta' \sqsupseteq {}^s\theta, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, e_s, e_t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'}$

This further means that given $\mathcal{L} \models c\ \sigma$ and ${}^s\theta' \sqsupseteq {}^s\theta, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'$
And we need to prove
$({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'}$ (F-CI0)

<u>IH</u>: $({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'}$

We get (F-CI0) directly from IH

13. FC-CE:

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e_s : (c \overset{\ell_e}{\Rightarrow} \tau))^\ell \leadsto e_t \qquad \Sigma;\Psi \vdash c \qquad \Sigma;\Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e \qquad \Sigma;\Psi \vdash \tau \searrow \ell}{\Sigma;\Psi;\Gamma \vdash_{pc} e_s\bullet : \tau \leadsto \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a.b.b[][]\bullet)))}\ \text{CE}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, e_s \bullet\ \delta^s, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.b[][]\bullet)))\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, e_s[]) \Downarrow_i (H_s', {}^s v) \implies$
$\exists H_t', {}^t v.(H_t, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.b[][]\bullet)))) \Downarrow^f (H_t', {}^t v) \wedge \exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$

This means given some H_s, H_t s.t $(n, H_s, H_t) \overset{\gamma,\hat{\beta}}{\rhd} {}^s\theta$. Also given some $i < n, {}^sv$ s.t $(H_s, e_s[]) \Downarrow_i (H'_s, {}^sv)$

And we need to prove

$\exists H'_t, {}^tv.(H_t, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.b[][]\bullet)))) \Downarrow^f (H'_t, {}^tv) \wedge \exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$

$(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\rhd} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-CE0)

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\ell\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\rhd} {}^s\theta \wedge \forall j < n, {}^sv_1.(H_{s1}, e_s\ \delta^s) \Downarrow_j (H'_{s1}, {}^sv_1) \implies$
$\exists H'_{t1}, {}^tv_1.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^tv_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\rhd} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^sv_1, {}^tv_1) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$

Instantiating with H_s, H_t and since we know that $(H_s, e_s[]) \Downarrow_i (H'_s, {}^sv)$ therefore $\exists j < i < n$ s.t $(H_s, e_s) \Downarrow_j (H'_{s1}, {}^sv_1)$

This means we have

$\exists H'_{t1}, {}^tv_1.(H_{t1}, e_t) \Downarrow^f (H'_{t1}, {}^tv_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'}{\rhd} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^sv_1, {}^tv_1) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\ell\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-CE1)

Since from (F-CE1) we have $({}^s\theta'_1, n-j, {}^sv_1, {}^tv_1) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\ell\ \sigma \rfloor_V^{\hat{\beta}'}$ therefore from Definition 3.39 we know that

$\exists^t v_i.{}^tv_1 = \mathsf{Lb}({}^tv_i) \wedge ({}^s\theta'_1, n-j, {}^sv_1, {}^tv_i) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-CE1.1)

Therefore from Definition 3.39 we have

${}^sv_1 = \Lambda e'_s$ and ${}^tv_i = \Lambda\Lambda\nu e'_t$

$\mathcal{L} \models c\ \sigma \implies \forall^s\theta'_2 \sqsupseteq {}^s\theta'_1, k < n-j, \hat{\beta} \sqsubseteq \hat{\beta}'_1.({}^s\theta'_2, k, e'_s, e'_t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'_1}$ (F-CE1.2)

Since we know that $\mathcal{L} \models c\ \sigma$, we instantiate with ${}^s\theta'_1, n-j-1, \hat{\beta}'$ to get

$({}^s\theta'_1, n-j-1, e'_s, e'_t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'}$

From Definition 3.40 we have

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}'}{\rhd} {}^s\theta'_1 \wedge \forall k < (n-j-1), {}^sv_2.(H_{s2}, e'_s) \Downarrow_k (H'_{s2}, {}^sv_2) \implies$
$\exists H'_{t2}, {}^tv_2.(H_{t2}, e'_t) \Downarrow^f (H'_{t2}, {}^tv_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'' \sqsupseteq \hat{\beta}'.$
$(n-j-1-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}''}{\rhd} {}^s\theta'_2 \wedge ({}^s\theta'_2, n-j-1-k, {}^sv_2, {}^tv_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$

Instantiating with H'_{s1}, H'_{t1} and since we know that $(H_s, e_s[]) \Downarrow_i (H'_s, {}^sv)$ and since from fg-CE we know that $i = j+k+1 < n$ therefore we know that $k < n-j-1$ s.t $(H_{s2}, e'_s) \Downarrow_k (H'_{s2}, {}^sv_2)$. Therefore we have

$\exists H'_{t2}, {}^tv_2.(H'_{t1}, e'_t) \Downarrow^f (H'_{t2}, {}^tv_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'' \sqsupseteq \hat{\beta}'.$
$(n-j-1-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}''}{\rhd} {}^s\theta'_2 \wedge ({}^s\theta'_2, n-j-1-k, {}^sv_2, {}^tv_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$ (F-CE1.3)

Let $\tau\ \sigma = \mathsf{A}^{\ell_i}$, since $\tau\ \sigma \searrow \ell\ \sigma$ therefore $\ell\ \sigma \sqsubseteq \ell_i$ and

$({}^s\theta'_2, n-j-1-k, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$

Therefore from Definition 3.39 we know that

$({}^s\theta'_2, n-j-1-k, {}^s v_2, \mathsf{Lb}\,{}^t v_{2i}) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$ (F-CE1.4)

In order to prove (F-CE0) we choose H'_t as H'_{t2} and ${}^t v$ as $\mathsf{Lb}\,{}^t v_{2i}$. We need to prove

(a) $(H_t, \mathsf{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.b[][]\bullet)))) \Downarrow^f (H'_{t2}, \mathsf{Lb}\,{}^t v_{2i})$:

From Lemma 3.48 it suffices to prove that
$(H_t, (\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.b[][]\bullet)))) \Downarrow^f (H'_{t2}, \mathsf{Lb}\,{}^t v_{2i})$
From SLIO*-Sem-bind it suffices to prove that

- $(H_t, e_t\ \delta^t) \Downarrow^f (H'_{t11}, {}^t v_{t11})$:
  From (F-CE1) we know that $H'_{t11} = H'_{t1}$ and ${}^t v_{t11} = {}^t v_1$
- $(H'_{t1}, \mathsf{bind}(\mathsf{unlabel}\ a, b.b[][]\bullet)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}\,{}^t v_{2i})$:
  Again from SLIO*-Sem-bind it suffices to prove that
  - $(H'_{t1}, (\mathsf{unlabel}\ a)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t12}, {}^t v_{t12})$:
    From (F-CE1.1) we know that ${}^t v_1 = \mathsf{Lb}({}^t v_i)$
    Therefore from SLIO*-Sem-unlabel we have $H'_{t12} = H'_{t1}$ and ${}^t v_{t12} = {}^t v_i$
  - $(b[][]\bullet)[{}^t v_i/b]\ \delta^t \Downarrow {}^t v_{t13}$:
    From (F-CE1.2) we know that ${}^s v_1 = \Lambda e'_s$ and ${}^t v_i = \Lambda\Lambda\nu e'_t$

    Therefore from SLIO*-Sem-FE and SLIO*-Sem-CE we know that ${}^t v_{t13} = e'_t$
  - $(H'_{t1}, e'_t \Downarrow^f (H'_{t2}, \mathsf{Lb}\,{}^t v_{2i})$
    We get the desired from From (F-CE1.3) and (F-CE1.4)

(b) $\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta'_2$ and $\hat{\beta}'$ as $\hat{\beta}''$. From fg-CE we know that $i = j+k+1$, ${}^s v = {}^s v'_2$, ${}^t v = {}^t v'_2$, $H'_s = H'_{s2}$ and $H'_t = H'_{t2}$.

Therefore from (F-CE1.3) we get the $(n-i, H'_{s2}, H'_{t2}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta'_2$

<u>To prove:</u> $({}^s\theta'_2, n-i, {}^s v'_2, {}^t v'_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$

From (F-CE1.3) we know that $({}^s\theta'_2, n-j-1-k, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$

14. FC-ref:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_s : \tau \rightsquigarrow e_t \qquad \Sigma; \Psi \vdash \tau \searrow pc}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{new}\ (e_s) : (\mathsf{ref}\ \tau)^{\perp} \rightsquigarrow \mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb} b)))}\ \text{ref}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{new}\ (e_s)\ \delta^s, \mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb}\ b))\ \delta^t)\ \delta^t) \in \lfloor (\mathsf{ref}\ \tau)^{\perp}\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we have

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, \mathsf{new}\ (e_s)\ \delta^s) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb}\ b)))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\rhd} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor (\mathsf{ref}\ \tau)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\gamma,\hat{\beta}}{\rhd} {}^s\theta$. Also given some $i < n, {}^s v$ s.t $(H_s, \mathsf{new}\ (e_s)\ \delta^s) \Downarrow_i (H'_s, {}^s v)$.

And we are required to prove

$\exists H'_t, {}^t v.(H_t, \mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb}\ b)))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\rhd} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor (\mathsf{ref}\ \tau)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-R0)

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\rhd} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_s\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n - j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\rhd} {}^s\theta'_1 \wedge ({}^s\theta'_1, n - j, {}^s v_1, {}^t v_1) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_1}$

Instantiating with H_s, H_t and since we know that $(H_s, \mathsf{new}\ (e_s)\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore we know that $\exists j < n$ s.t $(H_s, e_s\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1)$.

Therefore we have

$\exists H'_{t1}, {}^t v_1.(H_t, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n - j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\rhd} {}^s\theta'_1 \wedge ({}^s\theta'_1, n - j, {}^s v_1, {}^t v_1) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-R1)

In order to prove (F-R0) we choose H'_t as $H'_1 \cup \{a_t \mapsto {}^t v_1\}$, ${}^t v = \mathsf{Lb}(a_t)$, ${}^s\theta'$ as ${}^s\theta'_1 \cup \{a_s \mapsto \tau\ \sigma\}$ and $\hat{\beta}'$ as $\hat{\beta}'_1 \cup \{(a_s, a_t)\}$

And we need to prove:

(a) $(H_t, \mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb}\ b)))\ \delta^t) \Downarrow^f (H'_t, {}^t v)$:
From SLIO*-Sem-bind it suffices to prove that
- $(H_t, e_t\ \delta^t) \Downarrow^f (H'_{t11}, {}^t v_{t1})$:
From (F-R1) we know that $H'_{t11} = H'_{t1}$ and ${}^t v_{t1} = {}^t v_1$
- $(H'_1, \mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb}\ b))[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t2}, {}^t v_{t2})$:
From SLIO*-Sem-bind it suffices to prove that
  i. $(H'_1, \mathsf{new}\ (a)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t2}, {}^t v_{t2})$:
  From SLIO*-Sem-new we know that $H'_{t2} = H'_{t1} \cup \{a_t \mapsto {}^t v_1\}$ and ${}^t v_{t2} = a_t$
  ii. $(H'_1 \cup \{a_t \mapsto {}^t v_1\}, \mathsf{ret}(\mathsf{Lb}\ b))[{}^t v_1/a][a_t/b]\ \delta^t) \Downarrow^f (H'_t, {}^t v_t)$:
  From SLIO*-Sem-ret we know that $H'_t = H'_{t1} \cup \{a_t \mapsto {}^t v_1\}$ and ${}^t v_t = \mathsf{Lb}(a_t)$

(b) $\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\rhd} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor (\mathsf{ref}\ \tau)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$:

From (F-R1) we know that $(n - j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\rhd} {}^s\theta'_1$ and since $H'_s = H'_{s1} \cup \{a_s \mapsto {}^s v_1\}$, $H'_t = H'_{t1} \cup \{a_t \mapsto {}^t v_1\}$, ${}^s\theta' = {}^s\theta'_1 \cup \{a_s \mapsto \tau\ \sigma\}$

Therefore from Definition 3.41 and Lemma 3.47 we get $(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta'$

To prove: $({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor (\mathsf{ref}\ \tau)^{\perp}\ \sigma \rfloor_V^{\hat{\beta}'}$

Since we know that ${}^sv = a_s$ and ${}^tv = \mathsf{Lb}\ a_t$ therefore we need to prove

$({}^s\theta', n-i, a_s, \mathsf{Lb}(a_t)) \in \lfloor (\mathsf{ref}\ \tau)^{\perp}\ \sigma \rfloor_V^{\hat{\beta}'}$

From Definition 3.39 it suffices to prove that
$({}^s\theta', n-i, a_s, a_t) \in \lfloor (\mathsf{ref}\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'}$

Again from Definition 3.39 it suffices to prove that
${}^s\theta'(a_s) = \tau\ \sigma \wedge (a_s, a_t) \in \hat{\beta}'$
We get this by construction

15. FC-deref:

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_s : (\mathsf{ref}\ \tau)^{\ell} \rightsquigarrow e_t \qquad \Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \tau' \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} !e_s : \tau' \rightsquigarrow \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))} \text{deref}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, !e\ \delta^s, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))\ \delta^t) \in \lfloor \tau'\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv.(H_s, !e_s) \Downarrow_i (H'_s, {}^sv) \implies$
$\exists H'_t, {}^tv.(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))) \Downarrow^f (H'_t, {}^tv) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}'}$

This means that we are given some H_s, H_t s.t $(n, H_s, H_t) \overset{\gamma, \hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^sv$ s.t $(H_s, !e_s) \Downarrow_i (H'_s, {}^sv)$
And we need to prove
$\exists H'_t, {}^tv.(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))) \Downarrow^f (H'_t, {}^tv) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-DR0)

IH:

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\mathsf{ref}\ \tau)^{\ell}\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we need to prove

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^sv_1.(H_{s1}, e_s) \Downarrow_j (H'_{s1}, {}^sv_1) \implies$
$\exists H'_{t1}, {}^tv_1.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^tv_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^sv_1, {}^tv_1) \in \lfloor (\mathsf{ref}\ \tau)^{\ell}\ \sigma \rfloor_V^{\hat{\beta}'_1}$

Instantiating with H_s, H_t and since we know that $(H_s, !e_s) \Downarrow_i (H'_s, {}^sv)$ therefore $\exists j < n$ s.t $(H_{s1}, e_s) \Downarrow_j (H'_{s1}, {}^sv)$
Therefore we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s \theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n - j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n - j, {}^s v_1, {}^t v_1) \in \lfloor(\mathsf{ref}\ \tau)^\ell\ \sigma\rfloor_V^{\hat{\beta}'_1}$ (F-DR1)

From (F-DR1) we have $({}^s\theta'_1, n - j, {}^s v_1, {}^t v_1) \in \lfloor(\mathsf{ref}\ \tau)^\ell\ \sigma\rfloor_V^{\hat{\beta}'_1}$

From Definition 3.39 we have
$\exists^t v_i.{}^t v_1 = \mathsf{Lb}({}^t v_i) \wedge ({}^s\theta'_1, n - j, {}^s v_1, {}^t v_i) \in \lfloor(\mathsf{ref}\ \tau)\ \sigma\rfloor_V^{\hat{\beta}'_1}$ (F-DR1.1)

From Definition 3.39 we know that ${}^s v_1 = a_s$ and ${}^t v_i = a_t$
${}^s\theta'_1(a_s) = \tau \wedge (a_s, a_t) \in \hat{\beta}'_1$ (F-DR1.2)

Let $\tau'\ \sigma = \mathsf{A}^{\ell_i}$, since $\tau'\ \sigma \searrow \ell\ \sigma$ therefore $\ell\ \sigma \sqsubseteq \ell_i$ and
Let $v_g = H_t(a_t)$ therefore from Definition 5.27 we have
$({}^s\theta, n - 1, H_s(a_s), \mathsf{Lb}\, v_{gi}) \in \lfloor\tau'\rfloor_V^{\hat{\beta}}$ (F-DR1.3)

In order to prove (F-DR0) we choose H'_t as H'_{t1} and ${}^t v$ as $H'_{t1}(a_t) = v_g = \mathsf{Lb}\, v_{gi}$

(a) $(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))\ \delta^t) \Downarrow^f (H'_{t1}, \mathsf{Lb}\, v_{gi})$:

From Lemma 3.48 it suffices to prove that
$(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))\ \delta^t) \Downarrow^f (H'_{t1}, \mathsf{Lb}\, v_{gi})$
From SLIO*-Sem-bind it suffices to prove

i. $(H_t, e_t\ \delta^t) \Downarrow^f (H'_{t11}, {}^t v_{t1})$:
From (F-DR1) we know that $H'_{t11} = H'_{t1}$ and ${}^t v_{t1} = {}^t v_1$

ii. $(H'_{t1}, \mathsf{bind}(\mathsf{unlabel}\ a, b.!b)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t12}, {}^t v_{t2})$:
From SLIO*-Sem-bind it suffices to prove that

A. $(H'_{t1}, (\mathsf{unlabel}\ a)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t21}, {}^t v_{t21})$:
From (F-DR1.1) we know that ${}^t v_1 = \mathsf{Lb}({}^t v_i)$
Therefore from SLIO*-Sem-unlabel we know that $H'_{t21} = H'_{t1}$ and ${}^t v_{t21} = {}^t v_i$

B. $(H'_{t1}, (!b)[{}^t v_1/a][{}^t v_i/b]\ \delta^t) \Downarrow^f (H'_t, \mathsf{Lb}\, v_{gi})$:
Since from (F-DR1.2) we know that ${}^t v_i = a_t$ therefore from SLIO*-Sem-deref we know that $H'_t = H'_{t1}$ and ${}^t v = H'_{t1}(a_t) = v_g = \mathsf{Lb}\, v_{gi}$

(b) $\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor\tau'\ \sigma\rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta'_1$ and $\hat{\beta}'$ as $\hat{\beta}'_1$

Therefore from (F-DR1) we get $(n - j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1$ and snce $i = j + 1$ therefore from Lemma 3.47 we get $(n - i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1$

Since from (F-DR1.2) we know that $(a_s, a_t) \in \hat{\beta}'_1$ and ${}^s\theta'_1(a_s) = \tau$. Also from (F-DR1) we have $(n - j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1$. Therefore from Definition 3.40 we have $(n - j - 1, H'_{s1}(a_s), H'_{t1}(a_t)) \in \lfloor {}^s\theta'_1(a_s)\rfloor_V^{\hat{\beta}'_1}$

Since $i = j + 1$, ${}^s\theta'_1(a_s) = \tau\ \sigma$, $H'_{s1}(a_s) = {}^s v$ and $H'_{t1}(a_t) = {}^t v$
Therefore we get
$({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}'}$

Finally from Lemma 3.50 we get
$({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau' \ \sigma \rfloor_V^{\hat{\beta}'}$

16. FC-assign:

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e_{s1} : (\mathsf{ref}\ \tau)^{\ell} \rightsquigarrow e_{t1} \qquad \Sigma;\Psi;\Gamma \vdash_{pc} e_{s2} : \tau \rightsquigarrow e_{t2} \qquad \Sigma;\Psi \vdash \tau \searrow (pc \sqcup \ell)}{\begin{array}{c}\Sigma;\Psi;\Gamma \vdash_{pc} e_{s1} := e_{s2} : \mathsf{unit} \rightsquigarrow \\ \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())\end{array}} \text{assign}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$
To prove:
$({}^s\theta, n, (e_{s1} := e_{s2})\ \delta^s, \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())\ \delta^t) \in \lfloor \mathsf{unit}\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we are required to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, (e_{s1} := e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())\ \delta^t) \Downarrow^f$
$(H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}'}$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\gamma,\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^s v$ s.t $(H_s, (e_{s1} := e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$
And we need to prove
$\exists H'_t, {}^t v.(H_t, \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())\ \delta^t) \Downarrow^f$
$(H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}'}$ (F-AN0)

<u>IH1:</u>
$({}^s\theta, n, e_{s1}\ \delta^s, e_{t1}\ \delta^t) \in \lfloor (\mathsf{ref}\tau)^{\ell}\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we are required to prove

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\gamma,\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_{s1}\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\mathsf{ref}\ \tau)^{\ell}\ \sigma \rfloor_V^{\hat{\beta}'_1}$

Instantiating with H_s, H_t and since we know that $(H_s, (e_{s1} := e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists j < n$ s.t $(H_{s1}, e_{s1}\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1)$
Therefore we have
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\mathsf{ref}\ \tau)^{\ell}\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-AN1)

Since from (F-AN1) we know that $({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\mathsf{ref}\ \tau)^{\ell}\ \sigma \rfloor_V^{\hat{\beta}'_1}$ therefore from Definition 3.39 we have

$\exists^t v_i.^t v_1 = \mathsf{Lb}(^t v_i) \wedge (^s\theta'_1, n-j, ^s v_1, ^t v_i) \in \lfloor(\mathsf{ref}\ \tau)\ \sigma\rfloor_V^{\hat{\beta}'_1}$ (F-AN1.1)

From Definition 3.39 this further means that

$^s\theta'_1(a_s) = \tau \wedge (a_s, a_t) \in \hat{\beta}'_1$ where $^s v_1 = a_s$ and $^t v_1 = a_t$ (F-AN1.2)

IH2:

$(^s\theta'_1, n-j, e_{s2}\ \delta^s, e_{t2}\ \delta^t) \in \lfloor\tau\ \sigma\rfloor_E^{\hat{\beta}'_1}$

This means from Definition 3.40 we are required to prove

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge \forall k < n-j, ^s v_2.(H_{s2}, e_{s2}\ \delta^s) \Downarrow_k (H'_{s2}, ^s v_2) \implies$
$\exists H'_{t2}, ^t v_2.(H_{t2}, e_{t2}\ \delta^t) \Downarrow^f (H'_{t2}, ^t v_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_1.$
$(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge (^s\theta'_2, n-j-k, ^s v_2, ^t v_2) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}'_2}$

Instantiating with H'_{s1}, H'_{t1} and since we know that $(H_s, (e_{s2} := e_{s2})\ \delta^s) \Downarrow_i (H'_s, ^s v)$ therefore $\exists k < n-j$ s.t $(H_{s2}, e_{s2}\ \delta^s) \Downarrow_k (H'_{s2}, ^s v_2)$

Therefore we have

$\exists H'_{t2}, ^t v_2.(H_{t2}, e_{t2}\ \delta^t) \Downarrow^f (H'_{t2}, ^t v_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_1.$
$(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge (^s\theta'_2, n-j-k, ^s v_2, ^t v_2) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}'_2} \wedge$
(F-AN2)

In order to prove (F-AN0) we choose H'_t as $H'_{t2}[a_t \mapsto {}^s v_2]$, $^t v$ as ()

We need to prove

(a) $(H_t, \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())\ \delta^t) \Downarrow^f (H'_t, ^t v)$:
From SLIO*-Sem-bind it suffices to prove that
- $(H_t, (\mathsf{toLabeled}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())\ \delta^t) \Downarrow^f (H'_T, ^t v_T)$:

  From SLIO*-Sem-toLabeled it suffices to prove that
  $(H_t, \mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))\ \delta^t) \Downarrow^f (H'_T, ^t v_{Ti})$
  where $^t v_T = \mathsf{Lb}^t v_{Ti}$
  From SLIO*-Sem-bind it further suffices to prove that:
  - $(H_t, e_{t1}\ \delta^t) \Downarrow^f (H'_{t11}, ^t v_{t11})$:
    From (F-AN1) we know that $H'_{t11} = H'_{t1}$ and $^t v_{t11} = {}^t v_1$
  - $(H'_{t1}, \mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b))[^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t12}, ^t v_{t12})$:
    From SLIO*-Sem-bind it suffices to prove
    - $(H'_{t1}, e_{t2}\ \delta^t) \Downarrow^f (H'_{t13}, ^t v_{t13})$:
      From (F-AN2) we know that $H'_{t13} = H'_{t2}$ and $^t v_{t13} = {}^t v_2$
    - $(H'_{t1}, \mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)[^t v_1/a][^t v_2/b]\ \delta^t) \Downarrow^f (H'_t, ^t v)$:
      From SLIO*-Sem-bind it suffices to prove that
      * $(H'_{t1}, \mathsf{unlabel}\ a[^t v_1/a][^t v_2/b]\ \delta^t) \Downarrow^f (H'_{t21}, ^t v_{t21})$:
        From (F-AN1.1) we know that
        $^t v_1 = \mathsf{Lb}(^t v_i) \wedge (^s\theta'_1, n-j, ^s v_1, ^t v_i) \in \lfloor(\mathsf{ref}\ \tau)\ \sigma\rfloor_V^{\hat{\beta}'_1}$
        Therefore from SLIO*-Sem-unlabel we know that $H'_{t21} = H'_{t1}$ and $^t v_{t21} = {}^t v_i = a_t$

* $(H'_{t1}, (c := b)[{}^tv_1/a][{}^tv_2/b][{}^tv_i/c]\ \delta^t) \Downarrow^f (H'_T, {}^tv_{Ti})$:
  From SLIO*-Sem-assign we know that $H'_T = H'_{t1}[a_t \mapsto {}^tv_2]$ and ${}^tv_{Ti} = ()$

Since ${}^tv_{t12} = {}^tv_{Ti} = ()$ therefore ${}^tv_T = \mathsf{Lb}()$
- $(H'_T, \mathsf{ret}()[{}^tv_T/d])\ \delta^t) \Downarrow^f (H'_t, ())$:
From SLIO*-Sem-ret and SLIO*-Sem-val

(b) $\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta'_2$ and $\hat{\beta}'$ as $\hat{\beta}'_2$

In order to prove $(n-i, H'_s, H'_t) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2$ it suffices to prove

- $dom({}^s\theta'_2) \subseteq dom(H'_s)$:

  Since from (F-AN2) we know that $(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2$ therefore from Definition 3.41 we get $dom({}^s\theta'_2) \subseteq dom(H'_s)$
- $\hat{\beta}'_2 \subseteq (dom({}^s\theta'_2) \times dom(H'_t))$:

  Since from (F-AN2) we know that $(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2$ therefore from Definition 3.41 we get
  $\hat{\beta}'_2 \subseteq (dom({}^s\theta'_2) \times dom(H'_t))$
- $\forall (a_1, a_2) \in \hat{\beta}'_2.({}^s\theta'_2, n-i-1, H'_s(a_1), H'_t(a_2)) \in \lfloor {}^s\theta'_2(a_1) \rfloor_V^{\hat{\beta}}$:
  $\forall (a_1, a_2) \in \hat{\beta}'_2$.
  - $a_1 = a_s$ and $a_1 = a_t$:
    Since from (F-AN2) we know that $({}^s\theta'_2, n-j-k, {}^sv_2, {}^tv_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_2}$

    Also from (F-AN1.2) and Definition 3.37 we know that ${}^s\theta'_2(a_1) = \tau\ \sigma$
    Therefore from Lemma 3.45 we get
    $({}^s\theta'_2, n-i-1, {}^sv_2, {}^tv_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_2}$
  - $a_1 \neq a_s$ and $a_1 \neq a_t$:

    From (F-AN2) since we know that $(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2$ therefore from Definition 3.41 we get
    $({}^s\theta'_2, n-j-k-1, H'_{s2}(a_1), H'_{t2}(a_2)) \in \lfloor {}^s\theta'_2(a_1)\ \sigma \rfloor_V^{\hat{\beta}'_2}$

    Since $i = j+k+1$ therefore from Lemma 3.45 we get
    $({}^s\theta'_2, n-i-1, H'_{s2}(a_1), H'_{t2}(a_2)) \in \lfloor {}^s\theta'_2(a_1)\ \sigma \rfloor_V^{\hat{\beta}'_2}$
  - $a_1 = a_s$ and $a_1 \neq a_t$:
    This case cannot arise
  - $a_1 \neq a_s$ and $a_1 = a_t$:
    This case cannot arise

And in order to prove $({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}'}$
Since we know that ${}^sv = ()$ and ${}^tv = ()$ therefore from Definition 3.39 we get $({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}'}$

□

Lemma 3.50 (FG $\rightsquigarrow$ SLIO*: Semantic Subtyping lemma)**.** *The following holds:*
$\forall \Sigma, \Psi, \sigma, \mathcal{L}, \hat{\beta}$.

1. $\forall \mathsf{A}, \mathsf{A}'$.

   (a) $\Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor(\mathsf{A}\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor(\mathsf{A}'\ \sigma)\rfloor_V^{\hat{\beta}}$

2. $\forall \tau, \tau'$.

   (a) $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor(\tau\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor(\tau'\ \sigma)\rfloor_V^{\hat{\beta}}$

   (b) $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor(\tau\ \sigma)\rfloor_E^{\hat{\beta}} \subseteq \lfloor(\tau'\ \sigma)\rfloor_E^{\hat{\beta}}$

Proof. Proof by simultaneous induction on $\mathsf{A} <: \mathsf{A}'$ and $\tau <: \tau'$

Proof of statement 1(a)

We analyse the different cases of $\mathsf{A} <: \mathsf{A}'$ in the last step:

1. FGsub-arrow:

   Given:

$$\frac{\Sigma; \Psi \vdash \tau_1' <: \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2' \qquad \Sigma; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'} \text{FGsub-arrow}$$

   To prove: $\lfloor((\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor((\tau_1' \xrightarrow{\ell_e'} \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

   IH1: $\lfloor(\tau_1'\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor(\tau_1\ \sigma)\rfloor_V^{\hat{\beta}}$ (Statement 2(a))

   It suffices to prove: $\forall ({}^s\theta, m, \lambda x.e_s, \Lambda\Lambda\Lambda(\nu(\lambda x.e_t))) \in \lfloor((\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}}$.
   $({}^s\theta, m, \lambda x.e_s, \Lambda\Lambda\Lambda(\nu(\lambda x.e_t))) \in \lfloor((\tau_1' \xrightarrow{\ell_e'} \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

   This means that given some ${}^s\theta, m$ and $\lambda x.e_s, \Lambda\Lambda\Lambda(\nu(\lambda x.e_t))$ s.t
   $({}^s\theta, m, \lambda x.e_s, \Lambda\Lambda\Lambda(\nu(\lambda x.e_t))) \in \lfloor((\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}}$
   Therefore from Definition 3.39 we are given:
   $\forall {}^s\theta_1' \sqsupseteq {}^s\theta, {}^sv_1, {}^tv_1, j < m, \hat{\beta} \sqsubseteq \hat{\beta}_1'.({}^s\theta_1', j, {}^sv_1, {}^tv_1) \in \lfloor \tau_1\ \sigma\rfloor_V^{\hat{\beta}_1'} \implies$
   $({}^s\theta_1', j, e_s[{}^sv_1/x]\ \delta^s, e_t[{}^tv_1/x]\ \delta^t) \in \lfloor \tau_2\ \sigma\rfloor_E^{\hat{\beta}_1'}$ (S-L0)

   And it suffices to prove: $({}^s\theta, m, \lambda x.e_s, \Lambda\Lambda\Lambda(\nu(\lambda x.e_t))) \in \lfloor((\tau_1' \xrightarrow{\ell_e'} \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

   Again from Definition 3.39, it suffices to prove:
   $\forall {}^s\theta_2' \sqsupseteq {}^s\theta, {}^sv_2, {}^tv_2, k < m, \hat{\beta} \sqsubseteq \hat{\beta}_2'.({}^s\theta_2', k, {}^sv_2, {}^tv_2) \in \lfloor \tau_1'\ \sigma\rfloor_V^{\hat{\beta}_2'} \implies$
   $({}^s\theta_2', k, e_s[{}^sv_2/x]\ \delta^s, e_t[{}^tv_2/x]\ \delta^t) \in \lfloor \tau_2'\ \sigma\rfloor_E^{\hat{\beta}_2'}$ (S-L1)

   This means that given ${}^s\theta_2' \sqsupseteq {}^s\theta, {}^sv_2, {}^tv_2, k < m, \hat{\beta} \sqsubseteq \hat{\beta}_2'$ s.t $({}^s\theta_2', k, {}^sv_2, {}^tv_2) \in \lfloor \tau_1'\ \sigma\rfloor_V^{\hat{\beta}_2'}$
   And we need to prove

   $({}^s\theta_2', k, e_s[{}^sv_2/x]\ \delta^s, e_t[{}^tv_2/x]\ \delta^t) \in \lfloor \tau_2'\ \sigma\rfloor_E^{\hat{\beta}_2'}$ (S-L2)

   Instantiating (S-L0) with ${}^s\theta_2', {}^sv_2, {}^tv_2, k, \hat{\beta}_2'$. Since we have $({}^s\theta_2', k, {}^sv_2, {}^tv_2) \in \lfloor \tau_1'\ \sigma\rfloor_V^{\hat{\beta}_2'}$ therefore from IH1 we also have

$({}^s\theta'_2, k, {}^s v_2, {}^t v_2) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'_2}$

Therefore we get

$({}^s\theta'_2, k, e_s[{}^s v_2/x]\ \delta^s, e_t[{}^t v_2/x]\ \delta^t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}'_2}$

IH2: $\lfloor (\tau_2\ \sigma) \rfloor_E^{\hat{\beta}} \subseteq \lfloor (\tau'_2\ \sigma) \rfloor_E^{\hat{\beta}}$ (Statement 2(b))

Finally using IH2 we get

$({}^s\theta'_2, k, e_s[{}^s v_2/x]\ \delta^s, e_t[{}^t v_2/x]\ \delta^t) \in \lfloor \tau'_2\ \sigma \rfloor_E^{\hat{\beta}'_2}$

2. FGsub-prod:

Given:

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau'_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau'_2}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau'_1 \times \tau'_2} \text{ FGsub-prod}$$

To prove: $\lfloor ((\tau_1 \times \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor ((\tau'_1 \times \tau'_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

IH1: $\lfloor (\tau_1\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau'_1\ \sigma) \rfloor_V^{\hat{\beta}}$ (Statement 2(a))

IH2: $\lfloor (\tau_2\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau'_2\ \sigma) \rfloor_V^{\hat{\beta}}$ (Statement 2(a))

It suffices to prove:

$\forall ({}^s\theta, m, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \in \lfloor ((\tau_1 \times \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}.\ \ ({}^s\theta, m, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \in \lfloor ((\tau'_1 \times \tau'_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

This means that given some ${}^s\theta, n$ and ${}^s v_1, {}^s v_2, {}^t v_1, {}^t v_2$ s.t

$({}^s\theta, m, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \in \lfloor ((\tau_1 \times \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

Therefore from Definition 3.39 we are given:

$({}^s\theta, m, {}^s v_1, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}} \wedge ({}^s\theta, m, {}^s v_2, {}^t v_2) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}}$ (S-P0)

And it suffices to prove: $({}^s\theta, m, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \in \lfloor ((\tau'_1 \times \tau'_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

Again from Definition 3.39, it suffices to prove:

$({}^s\theta, m, {}^s v_1, {}^t v_1) \in \lfloor \tau'_1\ \sigma \rfloor_V^{\hat{\beta}} \wedge ({}^s\theta, m, {}^s v_2, {}^t v_2) \in \lfloor \tau'_2\ \sigma \rfloor_V^{\hat{\beta}}$ (S-P1)

Since from (S-P0) we know that $({}^s\theta, m, {}^s v_1, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}}$ therefore from IH1 we have $({}^s\theta, m, {}^s v_1, {}^t v_1) \in \lfloor \tau'_1\ \sigma \rfloor_V^{\hat{\beta}}$

Similarly since we have $({}^s\theta, m, {}^s v_2, {}^t v_2) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}}$ from (S-P0) therefore from IH2 we have $({}^s\theta, m, {}^s v_2, {}^t v_2) \in \lfloor \tau'_2\ \sigma \rfloor_V^{\hat{\beta}}$

3. FGsub-sum:

Given:

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'} \text{FGsub-sum}$$

To prove: $\lfloor((\tau_1 + \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor((\tau_1' + \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

IH1: $\lfloor(\tau_1\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor(\tau_1'\ \sigma)\rfloor_V^{\hat{\beta}}$ (Statement 2(a))

IH2: $\lfloor(\tau_2\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor(\tau_2'\ \sigma)\rfloor_V^{\hat{\beta}}$ (Statement 2(a))

It suffices to prove: $\forall ({}^s\theta, n, {}^s v, {}^t v) \in \lfloor((\tau_1 + \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, {}^s v, {}^t v) \in \lfloor((\tau_1' + \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

This means that given: $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor((\tau_1 + \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}}$

And it suffices to prove: $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor((\tau_1' + \tau_2')\ \sigma)\rfloor_V^{\hat{\beta}}$

2 cases arise

(a) ${}^s v = \mathsf{inl}\ {}^s v_i$ and ${}^t v = \mathsf{inl}\ {}^t v_i$:
From Definition 3.39 we are given:
$({}^s\theta, n, {}^s v_i, {}^t v_i) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}}$ (S-S0)
And we are required to prove that:
$({}^s\theta, n, {}^s v_i, {}^t v_i) \in \lfloor \tau_1'\ \sigma \rfloor_V^{\hat{\beta}}$
From (S-S0) and IH1 get this

(b) ${}^s v = \mathsf{inr}\ {}^s v_i$ and ${}^t v = \mathsf{inr}\ {}^t v_i$:
Symmetric reasoning as in the previous case

4. FGsub-forall:

Given:

$$\frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2 \qquad \Sigma, \alpha; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash \forall \alpha.(\ell_e, \tau_1) <: \forall \alpha.(\ell_e', \tau_2)} \text{FGsub-forall}$$

To prove: $\lfloor((\forall \alpha.(\ell_e, \tau_1))\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor(\forall \alpha.(\ell_e', \tau_2))\ \sigma\rfloor_V^{\hat{\beta}}$

It suffices to prove:

$\forall ({}^s\theta, n, \Lambda e_s, \Lambda\Lambda\Lambda(\nu(e_t))) \in \lfloor((\forall \alpha.(\ell_e, \tau_1))\ \sigma)\rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, \Lambda e_s, \Lambda\Lambda\Lambda(\nu(e_t))) \in \lfloor((\forall \alpha.(\ell_e', \tau_2))\ \sigma)\rfloor_V^{\hat{\beta}}$

This means that given $({}^s\theta, n, \Lambda e_s, \Lambda\Lambda\Lambda(\nu(e_t))) \in \lfloor((\forall \alpha.(\ell_e, \tau_1))\ \sigma)\rfloor_V^{\hat{\beta}}$

Therefore from Definition 3.39 we have:

$\forall {}^s\theta_1' \sqsupseteq {}^s\theta, j < n, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}_1'.({}^s\theta_1', j, e_s, e_t) \in \lfloor \tau_1[\ell'/\alpha]\ \sigma\rfloor_E^{\hat{\beta}_1'}$ (S-F0)

And we need to prove

$({}^s\theta, n, \Lambda e_s, \Lambda\Lambda\Lambda(\nu(e_t))) \in \lfloor((\forall \alpha.(\ell_e', \tau_2))\ \sigma)\rfloor_V^{\hat{\beta}}$

Again from Definition 3.39 it means we need to prove

$\forall^s\theta_2' \sqsupseteq {}^s\theta, k < n, \ell'' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}_2'.({}^s\theta_2', k, e_s, e_t) \in \lfloor \tau_2[\ell''/\alpha]\ \sigma \rfloor_E^{\hat{\beta}_2'}$

This means that given ${}^s\theta_2' \sqsupseteq {}^s\theta, k < n, \ell'' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}_2'$

And we need to prove

$({}^s\theta_2', k, e_s, e_t) \in \lfloor \tau_2[\ell''/\alpha] \rfloor_E^{\hat{\beta}_2'}$ (S-F1)

Instantiating (S-F0) with ${}^s\theta_2', k, \ell'', \hat{\beta}_2'$ and we get

$({}^s\theta_2', k, e_s, e_t) \in \lfloor \tau_1[\ell''/\alpha] \rfloor_E^{\hat{\beta}_2'}$

IH: $\lfloor (\tau_1\ \sigma \cup \{\alpha \mapsto \ell''\}) \rfloor_E^{\hat{\beta}_2'} \subseteq \lfloor (\tau_2\ \sigma \cup \{\alpha \mapsto \ell''\}) \rfloor_E^{\hat{\beta}_2'}$ (Statement 2(b))

Therefore from IH we get the desired

5. FGsub-constraint:

Given:

$$\frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi, c_2 \vdash \tau_1 <: \tau_2 \qquad \Sigma; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash c_1 \overset{\ell_e}{\Rightarrow} \tau_1 <: c_2 \overset{\ell_e'}{\Rightarrow} \tau_2} \text{ FGsub-constraint}$$

To prove: $\lfloor ((c_1 \overset{\ell_e}{\Rightarrow} \tau_1)\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor ((c_2 \overset{\ell_e'}{\Rightarrow} \tau_2))\ \sigma \rfloor_V^{\hat{\beta}}$

It suffices to prove:

$\forall ({}^s\theta, n, \nu e_s, \Lambda\Lambda(\nu(e_t))) \in \lfloor ((c_1 \overset{\ell_e}{\Rightarrow} \tau_1)\ \sigma) \rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, \nu e_s, \Lambda\Lambda(\nu(e_t))) \in \lfloor ((c_2 \overset{\ell_e'}{\Rightarrow} \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

This means that given: $({}^s\theta, n, \nu e_s, \Lambda\Lambda(\nu(e_t))) \in \lfloor ((c_1 \overset{\ell_e}{\Rightarrow} \tau_1)\ \sigma) \rfloor_V^{\hat{\beta}}$

Therefore from Definition 3.39 we are given:

$\mathcal{L} \models c_1\ \sigma \implies \forall^s\theta' \sqsupseteq {}^s\theta, j < n, \hat{\beta} \sqsubseteq \hat{\beta}_1'.({}^s\theta_1', j, e_s, e_t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}_1'}$ (S-C0)

And it suffices to prove:

$({}^s\theta, n, \nu e_s, \Lambda\Lambda(\nu(e_t))) \in \lfloor ((c_1 \overset{\ell_e'}{\Rightarrow} \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

Again from Definition 3.39 it means that we need to prove:

$\mathcal{L} \models c_2\ \sigma \implies \forall^s\theta_2' \sqsupseteq {}^s\theta, k < n, \hat{\beta} \sqsubseteq \hat{\beta}_2'.({}^s\theta_2', k, e_s, e_t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}_2'}$

This means that given that $\mathcal{L} \models c_2\ \sigma$ and ${}^s\theta_2' \sqsupseteq {}^s\theta, k < n, \hat{\beta} \sqsubseteq \hat{\beta}_2'$

And we need to prove

$({}^s\theta_2', k, e_s, e_t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}_2'}$ (S-C1)

Instantiating (S-C0) with ${}^s\theta_2', k, \hat{\beta}_2'$ we get $({}^s\theta_2', k, e_s, e_t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}_2'}$

IH: $\lfloor (\tau_1\ \sigma) \rfloor_E^{\hat{\beta}_2'} \subseteq \lfloor (\tau_2\ \sigma) \rfloor_E^{\hat{\beta}_2'}$ (Statement 2(b))

Finally from IH we get $({}^s\theta_2', k, e_s, e_t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}_2'}$

6. FGsub-ref:

   Given:

$$\frac{}{\Sigma; \Psi \vdash \mathsf{ref}\ \tau <: \mathsf{ref}\ \tau}\ \text{FGsub-ref}$$

   To prove: $\lfloor((\mathsf{ref}\ \tau)\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor((\mathsf{ref}\ \tau)\ \sigma)\rfloor_V^{\hat{\beta}}$

   It suffices to prove: $\forall({}^s\theta, n, a_s, a_t) \in \lfloor((\mathsf{ref}\ \tau)\ \sigma)\rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, a_s, a_t) \in \lfloor((\mathsf{ref}\ \tau)\ \sigma)\rfloor_V^{\hat{\beta}}$

   We get this directly from Definition 3.39

7. FGsub-base:

   Given:

$$\frac{}{\Sigma; \Psi \vdash \mathsf{b} <: \mathsf{b}}\ \text{FGsub-base}$$

   To prove: $\lfloor((\mathsf{b})\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor((\mathsf{b})\ \sigma)\rfloor_V^{\hat{\beta}}$

   Directly from Definition 3.39

8. FGsub-unit:

   Given:

$$\frac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}}\ \text{FGsub-unit}$$

   To prove: $\lfloor((\mathsf{unit})\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor((\mathsf{unit})\ \sigma)\rfloor_V^{\hat{\beta}}$

   Directly from Definition 3.39

Proof of statement 2(a)

Given:

$$\frac{\Sigma; \Psi \vdash \ell' \sqsubseteq \ell'' \qquad \Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}'}{\Sigma; \Psi \vdash \mathsf{A}^{\ell'} <: \mathsf{A}'^{\ell''}}\ \text{FGsub-label}$$

To prove: $\lfloor((\mathsf{A}^{\ell'})\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor((\mathsf{A}'^{\ell''}))\ \sigma\rfloor_V^{\hat{\beta}}$

This means from Definition 3.39 we need to prove

$\forall({}^s\theta, n, {}^s v, \mathsf{Lb}({}^t v_i)) \in \lfloor \mathsf{A}^{\ell'}\ \sigma\rfloor_V^{\hat{\beta}}.({}^s\theta, n, {}^s v, \mathsf{Lb}({}^t v_i)) \in \lfloor \mathsf{A}'^{\ell''}\ \sigma\rfloor_V^{\hat{\beta}}$

This means that given $({}^s\theta, n, {}^s v, \mathsf{Lb}({}^t v_i)) \in \lfloor \mathsf{A}^{\ell'}\ \sigma\rfloor_V^{\hat{\beta}}$

From Definition 3.39 it further means that we are given

$({}^s\theta, n, {}^s v, {}^t v_i) \in \lfloor \mathsf{A}\ \sigma\rfloor_V^{\hat{\beta}}$ (S-LB0)

And we need to prove

$({}^s\theta, n, {}^s v, \mathsf{Lb}({}^t v_i)) \in \lfloor \mathsf{A}'^{\ell''}\ \sigma\rfloor_V^{\hat{\beta}}$

Again from Definition 3.39 it suffices to prove that

$({}^s\theta, n, {}^s v, {}^t v_i) \in \lfloor \mathsf{A}'\ \sigma\rfloor_V^{\hat{\beta}}$

Since $\ell' \sqsubseteq \ell''$ and $\mathsf{A}' <: \mathsf{A}''$ therefore from IH (Statement 1(a)) and (S-LB0) we get the desired

Proof of statement 2(b)
Given: $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma$
To prove: $\lfloor(\tau\ \sigma)\rfloor_E^{\hat{\beta}} \subseteq \lfloor(\tau'\ \sigma)\rfloor_E^{\hat{\beta}}$
This means we need to prove that
$\forall({}^s\theta, n, e_s, e_t) \in \lfloor(\tau\ \sigma)\rfloor_E^{\hat{\beta}}.\ ({}^s\theta, n, e_s, e_t) \in \lfloor(\tau'\ \sigma)\rfloor_E^{\hat{\beta}}$

This means given $({}^s\theta, n, e_s, e_t) \in \lfloor(\tau\ \sigma)\rfloor_E^{\hat{\beta}}$

This means from Definition 3.40 we have

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, e_s) \Downarrow_i (H_s', {}^s v) \implies$
$\exists H_t', {}^t v.(H_t, e_t) \Downarrow^f (H_t', {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n - i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}'}$ (S-E0)

And it suffices to prove that $({}^s\theta, n, e_s, e_t) \in \lfloor(\tau'\ \sigma)\rfloor_E^{\hat{\beta}}$

Again from Definition 3.40 it means we need to prove

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_s) \Downarrow_j (H_{s1}', {}^s v_1) \implies$
$\exists H_{t1}', {}^t v_1.(H_{t1}, e_t) \Downarrow^f (H_{t1}', {}^t v_1) \wedge \exists {}^s\theta_1' \sqsupseteq {}^s\theta, \hat{\beta}_1' \sqsupseteq \hat{\beta}.$
$(n - j, H_{s1}', H_{t1}') \overset{\hat{\beta}_1'}{\triangleright} {}^s\theta_1' \wedge ({}^s\theta_1', n - j, {}^s v_1, {}^t v_1) \in \lfloor\tau'\ \sigma\rfloor_V^{\hat{\beta}_1'}$

This means that given some H_{s1}, H_{t1} s.t $(n, H_{s1}, H_{t1}) \overset{\ell_2, \hat{\beta}}{\triangleright} {}^s\theta$. Also given some $j < n, {}^s v_1$ s.t $(H_{s1}, e_s) \Downarrow_j (H_{s1}', {}^s v_1)$
And we need to prove
$\exists H_{t1}', {}^t v_1.(H_{t1}, e_t) \Downarrow^f (H_{t1}', {}^t v_1) \wedge \exists {}^s\theta_1' \sqsupseteq {}^s\theta, \hat{\beta}_1' \sqsupseteq \hat{\beta}.$
$(n - j, H_{s1}', H_{t1}') \overset{\hat{\beta}_1'}{\triangleright} {}^s\theta_1' \wedge ({}^s\theta_1', n - j, {}^s v_1, {}^t v_1) \in \lfloor\tau'\ \sigma\rfloor_V^{\hat{\beta}_1'}$ (S-E1)
Instantiating (S-E0) with H_{s1}, H_{t1} and with $j, {}^s v_1$. Then we get
$\exists H_t', {}^t v.(H_t, e_t) \Downarrow^f (H_t', {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n - j, H_{s1}', H_t') \overset{\hat{\beta}_1'}{\triangleright} {}^s\theta_1' \wedge ({}^s\theta_1', n - j, {}^s v_1, {}^t v_1) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}_1'}$
Since we have $\tau <: \tau'$. Therefore from IH (Statement 2(a)) we get
$\exists H_{t1}', {}^t v_1.(H_{t1}, e_t) \Downarrow^f (H_{t1}', {}^t v_1) \wedge \exists {}^s\theta_1' \sqsupseteq {}^s\theta, \hat{\beta}_1' \sqsupseteq \hat{\beta}.$
$(n - j, H_{s1}', H_{t1}') \overset{\hat{\beta}_1'}{\triangleright} {}^s\theta_1' \wedge ({}^s\theta_1', n - j, {}^s v_1, {}^t v_1) \in \lfloor\tau'\ \sigma\rfloor_V^{\hat{\beta}_1'}$

□

Theorem 3.51 (FG ⇝ SLIO*: Deriving FG NI via compilation)**.** $\forall e_s, {}^s v_1, {}^s v_2, n_1, n_2, H_{s1}', H_{s2}', pc.$
Let $\mathsf{bool} = (\mathsf{unit} + \mathsf{unit})$
$\emptyset, \emptyset, x : \mathsf{bool}^\top \vdash_{pc} e_s : \mathsf{bool}^\perp\ \wedge$
$\emptyset, \emptyset, \emptyset \vdash_{pc} {}^s v_1 : \mathsf{bool}^\top\ \wedge\ \emptyset, \emptyset, \emptyset \vdash_{pc} {}^s v_2 : \mathsf{bool}^\top\ \wedge$
$(\emptyset, e_s[{}^s v_1/x]) \Downarrow_{n_1} (H_{s1}', {}^s v_1')\ \wedge$
$(\emptyset, e_s[{}^s v_2/x]) \Downarrow_{n_2} (H_{s2}', {}^s v_2')\ \wedge$
$\implies$
${}^s v_1' = {}^s v_2'$

Proof. From the FG to CG translation we know that $\exists e_t$ s.t

$\emptyset, \emptyset, x : \mathsf{bool}^{\top} \vdash e_s : \mathsf{bool}^{\perp} \leadsto e_t$

Similarly we also know that $\exists^t v_1, {}^t v_2$ s.t

$\emptyset, \emptyset, \emptyset \vdash {}^s v_1 : \mathsf{bool}^{\top} \leadsto {}^t v_1$ and $\emptyset, \emptyset, \emptyset \vdash {}^s v_2 : \mathsf{bool}^{\top} \leadsto {}^t v_2$ (NI-0)

From type preservation theorem (choosing $\alpha = \gamma = \overline{\beta} = \perp$) we know that

$\emptyset, \emptyset, x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e_t : \mathbb{SLIO}\ \perp\ \perp\ \mathsf{Labeled}\ \perp\ \mathsf{bool}$

$\emptyset, \emptyset, \emptyset \vdash {}^t v_1 : \mathbb{SLIO}\ \perp\ \perp\ \mathsf{Labeled}\ \top\ \mathsf{bool}$

$\emptyset, \emptyset, \emptyset \vdash {}^t v_2 : \mathbb{SLIO}\ \perp\ \perp\ \mathsf{Labeled}\ \top\ \mathsf{bool}$ (NI-1)

Since we have $\emptyset, \emptyset, \emptyset \vdash {}^s v_1 : \mathsf{bool}^{\top} \leadsto {}^t v_1$

And since ${}^s v_1$ and ${}^t v_1$ are closed terms (from given and NI-1)

Therefore from Theorem 3.49 we have (we choose $n > n_1$ and $n > n_2$)

$(\emptyset, n, {}^s v_1, {}^t v_1) \in \lfloor \mathsf{bool}^{\top} \rfloor_E^{\emptyset}$ (NI-2)

Therefore from Definition 3.40 we have

$\forall H_s, H_t.(n, H_s, H_t) \overset{\emptyset}{\rhd} \emptyset \wedge \forall i < n, {}^s v.(H_s, {}^s v_1) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v_{11}.(H_t, {}^t v_1) \Downarrow^f (H'_t, {}^t v_{11}) \wedge \exists^s \theta' \sqsupseteq \emptyset, \hat{\beta}' \sqsupseteq \emptyset.$
$(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\rhd} {}^s \theta' \wedge ({}^s \theta', n - i, {}^s v, {}^t v_{11}) \in \lfloor \mathsf{bool}^{\top}\ \sigma \rfloor_V^{\hat{\beta}'}$

Instantiating with $\emptyset, \emptyset$ and from fg-val we know that $H'_s = H_s = \emptyset$, ${}^s v = {}^s v_1$. Therefore we have

$\exists H'_t, {}^t v_{11}.(H_t, {}^t v_1) \Downarrow^f (H'_t, {}^t v_{11}) \wedge \exists^s \theta' \sqsupseteq \emptyset, \hat{\beta}' \sqsupseteq \emptyset.$
$(n, H'_s, H'_t) \overset{\hat{\beta}'}{\rhd} {}^s \theta' \wedge ({}^s \theta', n, {}^s v_1, {}^t v_{11}) \in \lfloor \mathsf{bool}^{\top}\ \sigma \rfloor_V^{\hat{\beta}'}$ (NI-2.1)

From Definition 3.39 we know that

${}^t v_{11} = \mathsf{Lb}({}^t v_{i11}) \wedge ({}^s \theta', n, {}^s v_1, {}^t v_{i11}) \in \lfloor (\mathsf{unit} + \mathsf{unit})\ \sigma \rfloor_V^{\hat{\beta}'}$

Again from Definition 3.39 we know that

Either a) ${}^s v_1 = \mathsf{inl}()$ and ${}^t v_{i11} = \mathsf{inl}()$ or b)${}^s v_1 = \mathsf{inr}()$ and ${}^t v_{i11} = \mathsf{inr}()$

But in either case we have that $\emptyset, \emptyset, \emptyset \vdash {}^t v_{i11} : (\mathsf{unit} + \mathsf{unit})$ (NI-2.2)

As a result we have $\emptyset, \emptyset, \emptyset \vdash {}^t v_{11} : \mathsf{Labeled}\ \top\ (\mathsf{unit} + \mathsf{unit})$ (NI-2.3)

We give it typing derivation

$$\dfrac{\dfrac{}{\emptyset, \emptyset, \emptyset \vdash {}^t v_{i11} : (\mathsf{unit} + \mathsf{unit})}\ \text{(NI-2.2)}}{\emptyset, \emptyset, \emptyset \vdash \mathsf{Lb}({}^t v_{i11}) : \mathsf{Labeled}\ \top\ (\mathsf{unit} + \mathsf{unit})}$$

From Definition 3.44 and (NI-2.1) we know that

$(\emptyset, n, (x \mapsto {}^s v_1), (x \mapsto {}^t v_{11})) \in \lfloor x \mapsto \mathsf{bool}^{\top} \rfloor_V^{\hat{\beta}'}$

Therefore we can apply Theorem 3.49 to get

$(\emptyset, n, e_s[{}^s v_1/x], e_t[{}^t v_{11}/x]) \in \lfloor \mathsf{bool}^{\perp} \rfloor_E^{\hat{\beta}'}$ (NI-2.4)

From Definition 3.40 we get

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}'}{\rhd} \emptyset \wedge \forall i < n, {}^s v''_1.(H_s, e_s[{}^s v_1/x]) \Downarrow_i (H'_{s1}, {}^s v''_1) \implies$
$\exists H'_{t1}, {}^t v''_1.(H_t, e_t[{}^t v_{11}/x]) \Downarrow^f (H'_{t1}, {}^t v''_1) \wedge \exists^s \theta' \sqsupseteq \emptyset, \hat{\beta}'' \sqsupseteq \hat{\beta}'.$
$(n - i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\rhd} {}^s \theta' \wedge ({}^s \theta', n - i, {}^s v''_1, {}^t v''_1) \in \lfloor \mathsf{bool}^{\perp}\ \sigma \rfloor_V^{\hat{\beta}''}$

Instantiating with $\emptyset, \emptyset, n_1, {}^s v'_1$ we get

$\exists H'_{t1}, {}^t v''_1.(H_t, e_t[{}^t v_{11}/x]) \Downarrow^f (H'_{t1}, {}^t v''_1) \wedge \exists^s \theta' \sqsupseteq {}^s\theta, \hat{\beta}'' \sqsupseteq \hat{\beta}'.$
$(n - n_1, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\rhd} {}^s\theta' \wedge ({}^s\theta', n - n_1, {}^s v'_1, {}^t v''_1) \in \lfloor \mathsf{bool}^{\perp}\ \sigma \rfloor_V^{\hat{\beta}''}$ (NI-2.5)

Since we have $({}^s\theta', n - n_1, {}^s v'_1, {}^t v''_1) \in \lfloor \mathsf{bool}^{\perp}\ \sigma \rfloor_V^{\hat{\beta}''}$ therefore from Definition 3.39 we have
$\exists^t v_{i1}.{}^t v'' = \mathsf{Lb}({}^t v_{i1}) \wedge ({}^s\theta', n - n_1, {}^s v'_1, {}^t v_{i1}) \in \lfloor \mathsf{bool}\ \sigma \rfloor_V^{\hat{\beta}''}$
Since $({}^s\theta', n - n_1, {}^s v'_1, {}^t v_{i1}) \in \lfloor (\mathsf{unit} + \mathsf{unit}) \rfloor_V^{\hat{\beta}''}$ therefore from Definition 3.39 two cases arise

- ${}^s v'_1 = \mathsf{inl}\ {}^s v_{i11}$ and ${}^t v_{i1} = \mathsf{inl}^t v_{i11}$:
  From Definition 3.39 we have
  $({}^s\theta', n - n_1, {}^s v_{i11}, {}^t v_{i11}) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}''}$
  which means we have ${}^s v_{i11} = {}^t v_{i11}$
- ${}^s v'_1 = \mathsf{inr}\ {}^s v_{i11}$ and ${}^t v_{i1} = \mathsf{inr}^t v_{i11}$:
  Symmetric reasoning as in the previous case

So no matter which case arise we have ${}^s v'_1 = {}^t v_{i1}$

Similarly with other substitution we have $(\emptyset, n, {}^s v_2, {}^t v_2) \in \lfloor \mathsf{bool}^{\top} \rfloor_E^{\emptyset}$ (NI-3)

Therefore from Definition 3.40 we have
$\forall H_s, H_t.(n, H_s, H_t) \overset{\emptyset}{\rhd} \emptyset \wedge \forall i < n, {}^s v.(H_s, {}^s v_2) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v_{22}.(H_t, {}^t v_2) \Downarrow^f (H'_t, {}^t v_{22}) \wedge \exists^s \theta' \sqsupseteq \emptyset, \hat{\beta}' \sqsupseteq \emptyset.$
$(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\rhd} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v_{22}) \in \lfloor \mathsf{bool}^{\top}\ \sigma \rfloor_V^{\hat{\beta}'}$

Instantiating with $\emptyset, \emptyset$ and from fg-val we know that $H'_s = H_s = \emptyset$, ${}^s v = {}^s v_1$. Therefore we have
$\exists H'_t, {}^t v_{22}.(H_t, {}^t v_2) \Downarrow^f (H'_t, {}^t v_{22}) \wedge \exists^s \theta' \sqsupseteq \emptyset, \hat{\beta}' \sqsupseteq \emptyset.$
$(n, H'_s, H'_t) \overset{\hat{\beta}'}{\rhd} {}^s\theta' \wedge ({}^s\theta', n, {}^s v_1, {}^t v_{22}) \in \lfloor \mathsf{bool}^{\top}\ \sigma \rfloor_V^{\hat{\beta}'}$ (NI-3.1)

From Definition 3.39 we know that
${}^t v_2 = \mathsf{Lb}({}^t v_{i22}) \wedge ({}^s\theta', n, {}^s v_1, {}^t v_{i22}) \in \lfloor (\mathsf{unit} + \mathsf{unit})\ \sigma \rfloor_V^{\hat{\beta}'}$

Again from Definition 3.39 we know that
Either a) ${}^s v_2 = \mathsf{inl}()$ and ${}^t v_{i22} = \mathsf{inl}()$ or b)${}^s v_2 = \mathsf{inr}()$ and ${}^t v_{i22} = \mathsf{inr}()$
But in either case we have that $\emptyset, \emptyset, \emptyset \vdash {}^t v_{i22} : (\mathsf{unit} + \mathsf{unit})$ (NI-3.2)

As a result we have $\emptyset, \emptyset, \emptyset \vdash {}^t v_{22} : \mathsf{Labeled}\ \top\ (\mathsf{unit} + \mathsf{unit})$ (NI-3.3)
We give it typing derivation

$$\dfrac{\dfrac{}{\emptyset, \emptyset, \emptyset \vdash {}^t v_{i22} : (\mathsf{unit} + \mathsf{unit})}\ \text{(NI-3.2)}}{\emptyset, \emptyset, \emptyset \vdash \mathsf{Lb}({}^t v_{i22}) : \mathsf{Labeled}\ \top\ (\mathsf{unit} + \mathsf{unit})}$$

From Definition 3.44 and (NI-3.1) we know that
$(\emptyset, n, (x \mapsto {}^s v_2), (x \mapsto {}^t v_{22})) \in \lfloor x \mapsto \mathsf{bool}^{\top} \rfloor_V^{\hat{\beta}'}$

Therefore we can apply Theorem 3.49 to get
$(\emptyset, n, e_s[{}^s v_2/x], e_t[{}^t v_{22}/x]) \in \lfloor \mathsf{bool}^{\perp} \rfloor_E^{\hat{\beta}'}$ (NI-3.4)

From Definition 3.40 we get

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}'}{\triangleright} \emptyset \wedge \forall i < n, {}^s v_2''.(H_s, e_s[{}^s v_2/x]) \Downarrow_i (H_{s2}', {}^s v_2'') \implies$
$\exists H_{t2}', {}^t v_2''.(H_t, e_t[{}^t v_{22}/x]) \Downarrow^f (H_{t2}', {}^t v_2'') \wedge \exists^s \theta' \sqsupseteq \emptyset, \hat{\beta}'' \sqsupseteq \hat{\beta}'.$
$(n - i, H_{s2}', H_{t2}') \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v_2'', {}^t v_2'') \in \lfloor \mathsf{bool}^{\perp}\ \sigma \rfloor_V^{\hat{\beta}''}$

Instantiating with $\emptyset, \emptyset, n_2, {}^s v_2'$ we get
$\exists H_{t2}', {}^t v_2''.(H_t, e_t[{}^t v_{22}/x]) \Downarrow^f (H_{t2}', {}^t v_2'') \wedge \exists^s \theta' \sqsupseteq {}^s\theta, \hat{\beta}'' \sqsupseteq \hat{\beta}'.$
$(n - n_1, H_s', H_{t2}') \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - n_1, {}^s v_2', {}^t v_2'') \in \lfloor \mathsf{bool}^{\perp}\ \sigma \rfloor_V^{\hat{\beta}''}$ (NI-3.5)

Since we have $({}^s\theta', n - n_2, {}^s v_2', {}^t v_2'') \in \lfloor \mathsf{bool}^{\perp}\ \sigma \rfloor_V^{\hat{\beta}''}$ therefore from Definition 3.39 we have
$\exists^t v_{i2}.{}^t v_2'' = \mathsf{Lb}({}^t v_{i2}) \wedge ({}^s\theta', n - n_2, {}^s v_2', {}^t v_{i2}) \in \lfloor \mathsf{bool}\ \sigma \rfloor_V^{\hat{\beta}''}$
Since $({}^s\theta', n - n_2, {}^s v_2', {}^t v_{i2}) \in \lfloor (\mathsf{unit} + \mathsf{unit}) \rfloor_V^{\hat{\beta}''}$ therefore from Definition 3.39 two cases arise

- ${}^s v_2' = \mathsf{inl}\ {}^s v_{i22}$ and ${}^t v_{i2} = \mathsf{inl}^t v_{i22}$:
  From Definition 3.39 we have
  $({}^s\theta', n - n_2, {}^s v_{i22}, {}^t v_{i22}) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}''}$
  which means we have ${}^s v_{i22} = {}^t v_{i22}$
- ${}^s v_1' = \mathsf{inr}\ {}^s v_{i22}$ and ${}^t v_{i2} = \mathsf{inr}^t v_{i22}$:
  Symmetric reasoning as in the previous case

So no matter which case arise we have ${}^s v_2' = {}^t v_{i2}$

We know that $\emptyset, \emptyset, \emptyset \vdash {}^t v_{11} : \mathsf{Labeled}\ \top\ \mathsf{bool}$ (NI-2.3)

Also we have $\emptyset, \emptyset, \emptyset \vdash {}^t v_{22} : \mathsf{Labeled}\ \top\ \mathsf{bool}$ (NI-3.3)

Let $e_T = \mathsf{bind}(e_t, y.\mathsf{unlabel}(y))$
We show that $\emptyset, \emptyset, x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e_T : \mathbb{SLIO}\ \perp\ \perp\ \mathsf{bool}$ by giving a typing derivation
P2:

$$\dfrac{\dfrac{}{\emptyset, \emptyset, x : \mathsf{Labeled}\ \top\ \mathsf{bool}, y : \mathsf{Labeled}\ \perp\ \mathsf{bool} \vdash y : \mathsf{Labeled}\ \perp\ \mathsf{bool}}\ \text{SLIO}^*\text{-var}}{\emptyset, \emptyset, x : \mathsf{Labeled}\ \top\ \mathsf{bool}, y : \mathsf{Labeled}\ \perp\ \mathsf{bool} \vdash \mathsf{unlabel}(y) : \mathbb{SLIO}\ \perp\ \perp\ \mathsf{bool}}\ \text{SLIO}^*\text{-unlabel}$$

P1:

$$\dfrac{}{\emptyset, \emptyset, x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e_t : \mathbb{SLIO}\ \perp\ \perp\ \mathsf{Labeled}\ \perp\ \mathsf{bool}}\ \text{From (NI-1)}$$

Main derivation:

$$\dfrac{P1 \qquad P2}{\emptyset, \emptyset, x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash \mathsf{bind}(e_t, y.\mathsf{unlabel}(y)) : \mathbb{SLIO}\ \perp\ \perp\ \mathsf{bool}}$$

Say $e_t[{}^t v_{11}/x]$ reduces in n_{t1} steps in (NI-2.5) and $e_t[{}^t v_{22}/x]$ reduces in n_{t2} steps in (NI-3.5)
We instantiate Theorem 2.28 with $e_T, {}^t v_{11}, {}^t v_{22}, {}^t v_{i1}, {}^t v_{i2}, n_{t1} + 2, n_{t2} + 2, H_{t1}', H_{t2}'$ and from (NI-2.5) and (NI-3.5) we have ${}^t v_{i1} = {}^t v_{i2}$ and thus ${}^s v_1' = {}^s v_2'$

□

4 New coarse-grained IFC enforcement (CG)

4.1 CG type system

Term, type, constraint syntax:

Expressions	e	$::=$	$x \mid \lambda x.e \mid e\ e \mid (e,e) \mid \mathsf{fst}(e) \mid \mathsf{snd}(e) \mid \mathsf{inl}(e) \mid \mathsf{inr}(e) \mid \mathsf{case}(e, x.e, y.e) \mid \mathsf{new}\ e \mid !e \mid e := e \mid () \mid \Lambda e \mid e\ [] \mid \nu\ e \mid e\ \bullet \mid \mathsf{Lb}(e) \mid \mathsf{unlabel}(e) \mid \mathsf{toLabeled}(e) \mid \mathsf{ret}(e) \mid \mathsf{bind}(e, x.e)$
Labels	ℓ	$::=$	$\bot \mid \top \mid l \mid \ell \sqcup \ell \mid \ell \sqcap \ell$
Types	τ	$::=$	$\mathsf{b} \mid \mathsf{unit} \mid \tau \to \tau \mid \tau \times \tau \mid \tau + \tau \mid \mathsf{ref}\ \ell\ \tau \mid \mathsf{Labeled}\ \ell\ \tau \mid \mathbb{C}\ \ell_1\ \ell_2\ \tau \mid \forall \alpha.\tau \mid c \Rightarrow \tau$

Type system: $\boxed{\Gamma \vdash e : \tau}$

(All rules of the simply typed lambda-calculus pertaining to the types $\mathsf{b}, \tau \to \tau, \tau \times \tau, \tau + \tau, \mathsf{unit}$ are included.)

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{Lb}(e) : \mathsf{Labeled}\ \ell\ \tau}\ \text{CG-label} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{Labeled}\ \ell\ \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{unlabel}(e) : \mathbb{C}\ \top\ \ell\ \tau}\ \text{CG-unlabel}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathbb{C}\ \ell\ \ell'\ \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{toLabeled}(e) : \mathbb{C}\ \ell\ \bot\ (\mathsf{Labeled}\ \ell'\ \tau)}\ \text{CG-toLabeled} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{ret}(e) : \mathbb{C}\ \ell\ \ell'\ \tau}\ \text{CG-ret}$$

$$\frac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash e_1 : \mathbb{C}\ \ell_1\ \ell_2\ \tau \qquad \Sigma; \Psi; \Gamma, x : \tau \vdash e_2 : \mathbb{C}\ \ell_3\ \ell_4\ \tau' \\ \Sigma; \Psi \vdash \ell \sqsubseteq \ell_1 \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell_3 \qquad \Sigma; \Psi \vdash \ell_2 \sqsubseteq \ell_3 \qquad \Sigma; \Psi \vdash \ell_2 \sqsubseteq \ell_4 \qquad \Sigma; \Psi \vdash \ell_4 \sqsubseteq \ell'\end{array}}{\Sigma; \Psi; \Gamma \vdash \mathsf{bind}(e_1, x.e_2) : \mathbb{C}\ \ell\ \ell'\ \tau'}\ \text{CG-bind}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau' \qquad \Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi; \Gamma \vdash e : \tau}\ \text{CG-sub} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{Labeled}\ \ell'\ \tau \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash \mathsf{new}\ e : \mathbb{C}\ \ell\ \bot\ (\mathsf{ref}\ \ell'\ \tau)}\ \text{CG-ref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{ref}\ \ell'\ \tau}{\Sigma; \Psi; \Gamma \vdash !e : \mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell'\tau)}\ \text{CG-deref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \mathsf{ref}\ \ell'\ \tau \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \mathsf{Labeled}\ \ell'\ \tau \qquad \mathcal{L} \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash e_1 := e_2 : \mathbb{C}\ \ell\ \bot\ \mathsf{unit}}\ \text{CG-assign}$$

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash e : \tau}{\Sigma; \Gamma \vdash \Lambda e : \forall \alpha.\tau}\ \text{CG-FI} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : \forall \alpha.\tau \qquad \mathrm{FV}(\ell) \in \Sigma}{\Sigma; \Psi; \Gamma \vdash e\ [] : \tau[\ell/\alpha]}\ \text{CG-FE}$$

$$\frac{\Sigma; \Psi, c; \Gamma \vdash e : \tau}{\Sigma; \Gamma \vdash \nu\ e : c \Rightarrow \tau}\ \text{CG-CI} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : c \Rightarrow \tau \qquad \Sigma; \Psi \vdash c}{\Sigma; \Psi; \Gamma \vdash e\ \bullet : \tau}\ \text{CG-CE}$$

Figure 10: Type system of CG.

4.2 CG semantics

Judgement: $e \Downarrow_i v$ and $(H, e) \Downarrow_i^f (H', v)$

$$\frac{}{\Sigma; \Psi \vdash \tau <: \tau}\ \text{CGsub-refl} \qquad \frac{\Sigma; \Psi \vdash \tau_1' <: \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 \to \tau_2 <: \tau_1' \to \tau_2'}\ \text{CGsub-arrow}$$

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}\ \text{CGsub-prod}$$

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'}\ \text{CGsub-sum}$$

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi \vdash \mathsf{Labeled}\ \ell\ \tau <: \mathsf{Labeled}\ \ell'\ \tau'}\ \text{CGsub-labeled}$$

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell_i' \sqsubseteq \ell_i \qquad \Sigma; \Psi \vdash \ell_o \sqsubseteq \ell_o'}{\Sigma; \Psi \vdash \mathbb{C}\ \ell_i\ \ell_o\ \tau <: \mathbb{C}\ \ell_i'\ \ell_o'\ \tau'}\ \text{CGsub-monad}$$

$$\frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash \forall \alpha.\tau_1 <: \forall \alpha.\tau_2}\ \text{CGsub-forall} \qquad \frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash c_1 \Rightarrow \tau_1 <: c_2 \Rightarrow \tau_2}\ \text{CGsub-constraint}$$

Figure 11: CG subtyping

$$\frac{}{\Sigma; \Psi \vdash \mathsf{b}\ WF}\ \text{CG-wff-base} \qquad \frac{}{\Sigma; \Psi \vdash \mathsf{unit}\ WF}\ \text{CG-wff-unit}$$

$$\frac{\Sigma; \Psi \vdash \tau_1\ WF \qquad \Sigma; \Psi \vdash \tau_2\ WF}{\Sigma; \Psi \vdash (\tau_1 \to \tau_2)\ WF}\ \text{CG-wff-arrow}$$

$$\frac{\Sigma; \Psi \vdash \tau_1\ WF \qquad \Sigma; \Psi \vdash \tau_2\ WF}{\Sigma; \Psi \vdash (\tau_1 \times \tau_2)\ WF}\ \text{CG-wff-times} \qquad \frac{\Sigma; \Psi \vdash \tau_1\ WF \qquad \Sigma; \Psi \vdash \tau_2\ WF}{\Sigma; \Psi \vdash (\tau_1 + \tau_2)\ WF}\ \text{CG-wff-sum}$$

$$\frac{\mathrm{FV}(\ell) = \emptyset \qquad \mathrm{FV}(\tau) = \emptyset}{\Sigma; \Psi \vdash (\mathsf{ref}\ \ell\ \tau)\ WF}\ \text{CG-wff-ref} \qquad \frac{\Sigma, \alpha; \Psi \vdash \tau\ WF}{\Sigma; \Psi \vdash (\forall \alpha.\ \tau)\ WF}\ \text{CG-wff-forall}$$

$$\frac{\Sigma; \Psi, c \vdash \tau\ WF}{\Sigma; \Psi \vdash (c \Rightarrow \tau)\ WF}\ \text{CG-wff-constraint} \qquad \frac{\Sigma; \Psi \vdash \tau\ WF \qquad \mathrm{FV}(\ell) \in \Sigma}{\Sigma; \Psi \vdash (\mathsf{Labeled}\ \ell\ \tau)\ WF}\ \text{CG-wff-labeled}$$

$$\frac{\Sigma; \Psi \vdash \tau\ WF \qquad \mathrm{FV}(\ell_i) \in \Sigma \qquad \mathrm{FV}(\ell_o) \in \Sigma}{\Sigma; \Psi \vdash (\mathbb{SLIO}\ \ell_i\ \ell_o\ \tau)\ WF}\ \text{CG-wff-monad}$$

Figure 12: Well-formedness relation for CG

$$\frac{e_1 \Downarrow_i \lambda x.e_i \qquad e_2 \Downarrow_j v_2 \qquad e_i[v_2/x] \Downarrow_k v_3}{e_1\ e_2 \Downarrow_{i+j+k+1} v_3} \text{ cg-app} \qquad \frac{e_1 \Downarrow_i v_1 \qquad e_2 \Downarrow_j v_2}{(e_1, e_2) \Downarrow_{i+j+1} (v_1, v_2)} \text{ cg-prod}$$

$$\frac{e \Downarrow_i (v_1, v_2)}{\mathsf{fst}(e) \Downarrow_{i+1} v_1} \text{ cg-fst} \qquad \frac{e \Downarrow_i (v_1, v_2)}{\mathsf{snd}(e) \Downarrow_{i+1} v_2} \text{ cg-snd} \qquad \frac{e \Downarrow_i v}{\mathsf{inl}(e) \Downarrow_{i+1} \mathsf{inl}(v)} \text{ cg-inl}$$

$$\frac{e \Downarrow_i v}{\mathsf{inr}(e) \Downarrow_{i+1} \mathsf{inr}(v)} \text{ cg-inr} \qquad \frac{e \Downarrow_i \mathsf{inl}\ v \qquad e_1[v/x] \Downarrow_j v_1}{\mathsf{case}(e, x.e_1, y.e_2) \Downarrow_{i+j+1} v_1} \text{ cg-case1}$$

$$\frac{e \Downarrow_i \mathsf{inr}\ v \qquad e_2[v/x] \Downarrow_j v_2}{\mathsf{case}(e, x.e_1, y.e_2) \Downarrow_{i+j+1} v_2} \text{ cg-case2} \qquad \frac{e \Downarrow_i v}{\mathsf{Lb}(e) \Downarrow_{i+1} \mathsf{Lb}(v)} \text{ cg-Lb}$$

$$\frac{e \Downarrow_i \Lambda\ e_i \qquad e_i \Downarrow_j v}{e[] \Downarrow_{i+j+1} v} \text{ SLIO}^*\text{-Sem-FE} \qquad \frac{e \Downarrow_i \nu\ e_i \qquad e_i \Downarrow_j v}{e\bullet \Downarrow_{i+j+1} v} \text{ SLIO}^*\text{-Sem-CE}$$

$$\frac{e \Downarrow_i v}{(H, \mathsf{ret}(e)) \Downarrow^f_{i+1} (H, v)} \text{ cg-ret}$$

$$\frac{e_1 \Downarrow_i v_1 \qquad (H, v_1) \Downarrow^f_j (H', v_1') \qquad e_2[v_1'/x] \Downarrow_k v_2 \qquad (H', v_2) \Downarrow^f_l (H'', v_2')}{(H, \mathsf{bind}(e_1, x.e_2)) \Downarrow^f_{i+j+k+l+1} (H'', v_2')} \text{ cg-bind}$$

$$\frac{e \Downarrow_i \mathsf{Lb}(v)}{(H, \mathsf{unlabel}(e)) \Downarrow^f_{i+1} (H, v)} \text{ cg-unlabel} \qquad \frac{e \Downarrow_i v \qquad (H, v) \Downarrow^f_j (H', v')}{(H, \mathsf{toLabeled}(e)) \Downarrow^f_{i+j+1} (H', \mathsf{Lb}(v'))} \text{ cg-toLabeled}$$

$$\frac{e \Downarrow_i \mathsf{Lb} v \qquad a \notin dom(H)}{(H, \mathsf{new}\ (e)) \Downarrow^f_{i+1} (H[a \mapsto \mathsf{Lb} v], a)} \text{ cg-ref} \qquad \frac{e \Downarrow_i a}{(H, !e) \Downarrow^f_{i+1} (H, H(a))} \text{ cg-deref}$$

$$\frac{e_1 \Downarrow_i a \qquad e_2 \Downarrow_j \mathsf{Lb} v}{(H, e_1 := e_2) \Downarrow^f_{i+j+1} (H[a \mapsto \mathsf{Lb} v], ())} \text{ cg-assign}$$

$$\frac{e \in \{x, \lambda y.-, \Lambda, \nu, \mathsf{ret}-, \mathsf{bind}(-,-.-), \mathsf{unlabel}(-), \mathsf{toLabeled}(-), \mathsf{new}\ (-), !-, - := -\}}{e \Downarrow_0 e} \text{ cg-val}$$

Figure 13: CG semantics

4.3 Model for CG

$W : ((Loc \mapsto Type) \times (Loc \mapsto Type) \times (Loc \leftrightarrow Loc))$

Definition 4.1 (θ_2 extends θ_1)**.** $\theta_1 \sqsubseteq \theta_2 \triangleq$
$\forall a \in \theta_1.\theta_1(a) = \tau \implies \theta_2(a) = \tau$

Definition 4.2 (W_2 extends W_1)**.** $W_1 \sqsubseteq W_2 \triangleq$

1. $\forall i \in \{1, 2\}.\ W_1.\theta_i \sqsubseteq W_2.\theta_i$
2. $\forall p \in (W_1.\hat{\beta}).p \in (W_2.\hat{\beta})$

Definition 4.3 (Value Equivalence)**.**

$$ValEq(\mathcal{A}, W, \ell, n, v_1, v_2, \tau) \triangleq \begin{cases} (W, n, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}} & \ell \sqsubseteq \mathcal{A} \\ \\ \forall j.(W.\theta_1, j, v_1) \in \lfloor \tau \rfloor_V \wedge & \ell \not\sqsubseteq \mathcal{A} \\ (W.\theta_2, j, v_2) \in \lfloor \tau \rfloor_V & \end{cases}$$

Definition 4.4 (Binary value relation).

$$
\begin{array}{lll}
\lceil \mathsf{b} \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, v_1, v_2) \mid v_1 = v_2 \wedge \{v_1, v_2\} \in [\![\mathsf{b}]\!]\} \\
\lceil \mathsf{unit} \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, (), ()) \mid () \in [\![\mathsf{unit}]\!]\} \\
\lceil \tau_1 \times \tau_2 \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, (v_1, v_2), (v_1', v_2')) \mid (W, n, v_1, v_1') \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \wedge (W, n, v_2, v_2') \in \lceil \tau_2 \rceil_V^{\mathcal{A}}\} \\
\lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, \mathsf{inl}\ v, \mathsf{inl}\ v') \mid (W, n, v, v') \in \lceil \tau_1 \rceil_V^{\mathcal{A}}\} \cup \\
& & \{(W, n, \mathsf{inr}\ v, \mathsf{inr}\ v') \mid (W, n, v, v') \in \lceil \tau_2 \rceil_V^{\mathcal{A}}\} \\
\lceil \tau_1 \to \tau_2 \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, \lambda x.e_1, \lambda x.e_2) \mid \\
& & \forall W' \sqsupseteq W, j < n, v_1, v_2. \\
& & ((W', j, v_1, v_2) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \implies (W', j, e_1[v_1/x], e_2[v_2/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}}) \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_1, v_c, j. \\
& & ((\theta_l, j, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, j, e_1[v_c/x]) \in \lfloor \tau_2 \rfloor_E) \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_2, v_c, j. \\
& & ((\theta_l, j, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, j, e_2[v_c/x]) \in \lfloor \tau_2 \rfloor_E)\} \\
\lceil \forall \alpha.\tau \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, \Lambda e_1, \Lambda e_2) \mid \\
& & \forall W' \sqsupseteq W, j < n, \ell' \in \mathcal{L}. \\
& & ((W', j, e_1, e_2) \in \lceil \tau[\ell'/\alpha] \rceil_E^{\mathcal{A}}) \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_1, \ell'' \in \mathcal{L}, j.(\theta_l, j, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_2, \ell'' \in \mathcal{L}, j.(\theta_l, j, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E\} \\
\lceil c \Rightarrow \tau \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, \nu e_1, \nu e_2) \mid \\
& & \forall W' \sqsupseteq W, j < n. \\
& & \mathcal{L} \models c \implies (W', j, e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}} \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c \implies (\theta_l, j, e_1) \in \lfloor \tau \rfloor_E \wedge \\
& & \forall \theta_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c \implies (\theta_l, j, e_2) \in \lfloor \tau \rfloor_E\} \\
\lceil \mathsf{ref}\ \ell\ \tau \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, a_1, a_2) \mid \\
& & (a_1, a_2) \in W.\hat{\beta} \wedge W.\theta_1(a_1) = W.\theta_2(a_2) = \mathsf{Labeled}\ \ell\ \tau\} \\
\lceil \mathsf{Labeled}\ \ell\ \tau \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, \mathsf{Lb}(v_1), \mathsf{Lb}(v_2)) \mid \mathit{ValEq}(\mathcal{A}, W, \ell, n, v_1, v_2, \tau)\} \\
\lceil \mathbb{C}\ \ell_1\ \ell_2\ \tau \rceil_V^{\mathcal{A}} & \triangleq & \{(W, n, v_1, v_2) \mid \\
& & \Big(\forall k \leq n, W_e \sqsupseteq W, H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \\
& & \forall v_1', v_2', j.(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies \\
& & \exists W' \sqsupseteq W_e.(k - j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k - j, \ell_2, v_1', v_2', \tau)\Big) \wedge \\
& & \forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies \\
& & \exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v_l') \in \lfloor \tau \rfloor_V \wedge \\
& & (\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge \\
& & (\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_1)\Big)\}
\end{array}
$$

Definition 4.5 (Binary expression relation).

$$
\lceil \tau \rceil_E^{\mathcal{A}} \triangleq \{(W, n, e_1, e_2) \mid \forall i < n.e_1 \Downarrow_i v_1 \wedge e_2 \Downarrow v_2 \implies (W, n - i, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}\}
$$

Definition 4.6 (Unary value relation).

$$
\begin{array}{lll}
\lfloor \mathsf{b} \rfloor_V & \triangleq & \{(\theta, m, v) \mid v \in [\![\mathsf{b}]\!]\} \\
\lfloor \mathsf{unit} \rfloor_V & \triangleq & \{(\theta, m, v \mid v \in [\![\mathsf{unit}]\!]\} \\
\lfloor \tau_1 \times \tau_2 \rfloor_V & \triangleq & \{(\theta, m, (v_1, v_2)) \mid (\theta, m, v_1) \in \lfloor \tau_1 \rfloor_V \wedge (\theta, m, v_2) \in \lfloor \tau_2 \rfloor_V\} \\
\lfloor \tau_1 + \tau_2 \rfloor_V & \triangleq & \{(\theta, m, \mathsf{inl}\ v) \mid (\theta, m, v) \in \lfloor \tau_1 \rfloor_V\} \cup \{(\theta, m, \mathsf{inr}\ v) \mid (\theta, m, v) \in \lfloor \tau_2 \rfloor_V\} \\
\lfloor \tau_1 \to \tau_2 \rfloor_V & \triangleq & \{(\theta, m, \lambda x.e) \mid \forall \theta' \sqsupseteq \theta, v, j < m.(\theta', j, v) \in \lfloor \tau_1 \rfloor_V \implies (\theta', j, e[v/x]) \in \lfloor \tau_2 \rfloor_E\} \\
\lfloor \forall \alpha.\tau \rfloor_V & \triangleq & \{(\theta, m, \Lambda e) \mid \forall \theta'.\theta \sqsubseteq \theta', j < m.\forall \ell' \in \mathcal{L}.(\theta', j, e) \in \lfloor \tau[\ell'/\alpha] \rfloor_E\} \\
\lfloor c \Rightarrow \tau) \rfloor_V & \triangleq & \{(\theta, m, \nu e) \mid \mathcal{L} \models c \implies \forall \theta'.\theta \sqsubseteq \theta', j < m.(\theta', j, e) \in \lfloor \tau \rfloor_E\} \\
\lfloor \mathsf{ref}\ \ell\ \tau \rfloor_V & \triangleq & \{(\theta, m, a) \mid \theta(a) = \mathsf{Labeled}\ \ell\ \tau\} \\
\lfloor \mathsf{Labeled}\ \ell\ \tau \rfloor_V & \triangleq & \{(\theta, m, \mathsf{Lb}(v) \mid (\theta, m, v) \in \lfloor \tau \rfloor_V\} \\
\lfloor \mathbb{C}\ \ell_1\ \ell_2\ \tau \rfloor_V & \triangleq & \{(\theta, m, e) \mid \\
& & \forall k \leq m, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v) \Downarrow_j^f (H', v') \wedge j < k \implies \\
& & \exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor \tau \rfloor_V \wedge \\
& & (\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge \\
& & (\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_1)\}
\end{array}
$$

Definition 4.7 (Unary expression relation).

$$\lfloor \tau \rfloor_E \triangleq \{(\theta, n, e) \mid \forall i < n.e \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor \tau \rfloor_V\}$$

Definition 4.8 (Unary heap well formedness).

$$(n, H) \triangleright \theta \triangleq dom(\theta) \subseteq dom(H) \wedge \forall a \in dom(\theta).(\theta, n - 1, H(a)) \in \lfloor \theta(a) \rfloor_V$$

Definition 4.9 (Binary heap well formedness).

$$
\begin{array}{lll}
(n, H_1, H_2) \overset{\mathcal{A}}{\triangleright} W & \triangleq & dom(W.\theta_1) \subseteq dom(H_1) \wedge dom(W.\theta_2) \subseteq dom(H_2) \wedge \\
& & (W.\hat{\beta}) \subseteq (dom(W.\theta_1) \times dom(W.\theta_2)) \wedge \\
& & \forall (a_1, a_2) \in (W.\hat{\beta}).(W.\theta_1(a_1) = W.\theta_2(a_2) \wedge \\
& & (W, n - 1, H_1(a_1), H_2(a_2)) \in \lceil W.\theta_1(a_1) \rceil_V^{\mathcal{A}}) \wedge \\
& & \forall i \in \{1, 2\}.\forall m.\forall a_i \in dom(W.\theta_i).(W.\theta_i, m, H_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V
\end{array}
$$

Definition 4.10 (Binary substitution). $\gamma : Var \mapsto (Val, Val)$

Definition 4.11 (Unary substitution). $\delta : Var \mapsto Val$

Definition 4.12 (Unary interpretation of Γ).

$$\lfloor \Gamma \rfloor_V \triangleq \{(\theta, n, \delta) \mid dom(\Gamma) \subseteq dom(\delta) \wedge \forall x \in dom(\Gamma).(\theta, n, \delta(x)) \in \lfloor \Gamma(x) \rfloor_V\}$$

Definition 4.13 (Binary interpretation of Γ).

$$\lceil \Gamma \rceil_V^{\mathcal{A}} \triangleq \{(W, n, \gamma) \mid dom(\Gamma) \subseteq dom(\gamma) \wedge \forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}\}$$

4.4 Soundness proof for CG

Lemma 4.14 (Binary value relation subsumes unary value relation). $\forall W, v_1, v_2, \mathcal{A}, n, \tau.$
$(W, n, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}} \implies \forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, v_i) \in \lfloor \tau \rfloor_V$

Proof. Proof by induction on τ

1. Case $\mathsf{b}, \mathsf{unit}$:

   From Definition 4.6

2. Case $\tau_1 \times \tau_2$:

   <u>Given</u>: $(W, n, (v_{i1}, v_{i2}), (v_{j1}, v_{j2})) \in \lceil \tau_1 \times \tau_2 \rceil_V^{\mathcal{A}}$

   <u>To prove</u>:

   $\forall m.\ (W.\theta_1, m, (v_{i1}, v_{i2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$ (P01)

   and

   $\forall m.\ (W.\theta_2, m, (v_{j1}, v_{j2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$ (P02)

   From Definition 4.4 we know that we are given

   $(W, n, v_{i1}, v_{j1}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \wedge (W, n, v_{i2}, v_{j2}) \in \lceil \tau_2 \rceil_V^{\mathcal{A}}$ (P1)

   IH1a: $\forall m_1.\ (W.\theta_1, m_1, v_{i1}) \in \lfloor \tau_1 \rfloor_V$ and

   IH1b: $\forall m_1.\ (W.\theta_2, m_1, v_{j1}) \in \lfloor \tau_1 \rfloor_V$

   IH2a: $\forall m_2.\ (W.\theta_1, m_2, v_{i2}) \in \lfloor \tau_2 \rfloor_V$ and

   IH2b: $\forall m_2.\ (W.\theta_2, m_2, v_{j2}) \in \lfloor \tau_2 \rfloor_V$

   From (P01) we know that given some m we need to prove

   $(W.\theta_1, m, (v_{i1}, v_{i2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

   Similarly from (P02) we know that given some m we need to prove

   $(W.\theta_2, m, (v_{j1}, v_{j2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

   We instantiate IH1a and IH2a with the given m from (P01) to get

   $(W.\theta_1, m, v_{i1}) \in \lfloor \tau_1 \rfloor_V$ and $(W.\theta_1, m, v_{i2}) \in \lfloor \tau_2 \rfloor_V$

   Then from Definition 4.6, we get

   $(W.\theta_1, m, (v_{i1}, v_{i2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

   Similarly we instantiate IH1b and IH2b with the given m from (P02) to get

   $(W.\theta_2, m, v_{j1}) \in \lfloor \tau_1 \rfloor_V$ and $(W.\theta_2, m, v_{j2}) \in \lfloor \tau_2 \rfloor_V$

   Then from Definition 4.6, we get

   $(W.\theta_2, m, (v_{j1}, v_{j2})) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$

3. Case $\tau_1 + \tau_2$:

   2 cases arise:

   (a) $v_1 = \mathsf{inl}(v_{i1})$ and $v_2 = \mathsf{inl}(v_{j1})$

   <u>Given</u>: $(W, n, \mathsf{inl}(v_{i1}), \mathsf{inl}(v_{j1})) \in \lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}}$

   <u>To prove</u>:

   $\forall m.\ (W.\theta_1, m, \mathsf{inl}(v_{i1})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$ (S01)

   and

   $\forall m.\ (W.\theta_2, m, \mathsf{inl}(v_{i2})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$ (S02)

From Definition 4.4 we know that we are given
$(W, n, v_{i1}, v_{j1}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$ (S0)
IH1: $\forall m_1.\ (W.\theta_1, m_1, v_{i1}) \in \lfloor \tau_1 \rfloor_V$ and
IH2: $\forall m_2.\ (W.\theta_2, m_2, v_{j1}) \in \lfloor \tau_1 \rfloor_V$

From (S01) we know that given some m and we are required to prove:
$(W.\theta_1, m, \mathsf{inl}(v_{i1})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$
Also from (S02) we know that given some m and we are required to prove:
$(W.\theta_2, m, \mathsf{inl}(v_{i2})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$

We instantiate IH1 with m from (S01) to get
$(W.\theta_1, m, v_{i1}) \in \lfloor \tau_1 \rfloor_V$
Therefore from Definition 4.6, we get
$(W.\theta_1, m, \mathsf{inl}(v_{i1})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$

We instantiate IH2 with m from (S02) to get
$(W.\theta_2, m, v_{j1}) \in \lfloor \tau_1 \rfloor_V$
Therefore from Definition 4.6, we get
$(W.\theta_2, m, \mathsf{inl}(v_{j1})) \in \lfloor \tau_1 + \tau_2 \rfloor_V$

(b) $v_1 = \mathsf{inr}(v_{i2})$ and $v_2 = \mathsf{inr}(v_{j2})$
Symmetric reasoning as in the (a) case above

4. Case $\tau_1 \to \tau_2$:
Given: $(W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil \tau_1 \to \tau_2 \rceil_V^{\mathcal{A}}$
This means from Definition 4.4 we know that
$\forall W' \sqsupseteq W, j < n, v_1, v_2.((W', j, v_1, v_2) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \implies (W', j, e_1[v_1/x], e_2[v_2/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}})$
$\wedge\ \forall \theta_l \sqsupseteq W.\theta_1, i, v_c.((\theta_l, i, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, i, e_1[v_c/x]) \in \lfloor \tau_2 \rfloor_E)$
$\wedge\ \forall \theta_l \sqsupseteq W.\theta_2, k, v_c.((\theta_l, k, v_2) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, k, e_2[v_c/x]) \in \lfloor \tau_2 \rfloor_E)$ (L0)

To prove:

(a) $\forall m.\ (W.\theta_1, m, \lambda x.e_1) \in \lfloor \tau_1 \to \tau_2 \rfloor_V$:
This means from Definition 4.6 we need to prove:
$\forall \theta'. W.\theta_1 \sqsubseteq \theta' \wedge \forall j < m. \forall v.(\theta', j, v) \in \lfloor \tau_1 \rfloor_V \implies (\theta', j, e_1[v/x]) \in \lfloor \tau_2 \rfloor_E$
This further means that we have some θ', j and v s.t
$W.\theta_1 \sqsubseteq \theta' \wedge j < m \wedge (\theta', j, v) \in \lfloor \tau_1 \rfloor_V$
And we need to prove: $(\theta', j, e_1[v/x]) \in \lfloor \tau_2 \rfloor_E$

Instantiating θ_l, i and v_c in the second conjunct of L0 with θ', j and v respectively and since we know that $W.\theta_1 \sqsubseteq \theta'$ and $(\theta', j, v) \in \lfloor \tau_1 \rfloor_V$

Therefore we get $(\theta', j, e_1[v/x]) \in \lfloor \tau_2 \rfloor_E$

(b) $\forall m.\ (W.\theta_2, m, \lambda x.e_2) \in \lfloor \tau_1 \to \tau_2 \rfloor_V$:
Similar reasoning with e_2

5. Case $\forall \alpha.\tau$:

   Given: $(W, n, \Lambda e_1, \Lambda e_2) \in \lceil \forall \alpha.\tau \rceil_V^{\mathcal{A}}$

   This means from Definition 4.4 we know that

   $\forall W_b \sqsupseteq W, n_b < n, \ell' \in \mathcal{L}.((W_b, n_b, e_1, e_2) \in \lceil \tau[\ell'/\alpha] \rceil_E^{\mathcal{A}})$
   $\wedge\ \forall \theta_l \sqsupseteq W.\theta_1, i, \ell'' \in \mathcal{L}.((\theta_l, i, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$
   $\wedge\ \forall \theta_l \sqsupseteq W.\theta_2, i, \ell'' \in \mathcal{L}.((\theta_l, i, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$ (F0)

   To prove:

   (a) $\forall m.\ (W.\theta_1, m, \Lambda e_1) \in \lfloor \forall \alpha.\tau \rfloor_V$:
      This means from Definition 2.6 we need to prove:
      $\forall \theta'. W.\theta_1 \sqsubseteq \theta'. \forall m' < m. \forall \ell_u \in \mathcal{L}.(\theta', m', e_1) \in \lfloor \tau[\ell_u/\alpha] \rfloor_E$
      This further means that we are given some θ', m' and ℓ_u s.t $W.\theta_1 \sqsubseteq \theta'$, $m' < m$ and $\ell_u \in \mathcal{L}$
      And we need to prove: $(\theta', m', e_1) \in \lfloor \tau[\ell_u/\alpha] \rfloor_E$

      Instantiating θ_l, i and ℓ'' in the second conjunct of F0 with θ', m' and ℓ_u respectively and since we know that $W.\theta_1 \sqsubseteq \theta'$ and $\ell_u \in \mathcal{L}$

      Therefore we get $(\theta', m', e_1) \in \lfloor \tau[\ell_u/\alpha] \rfloor_E$

   (b) $\forall m.\ (W.\theta_2, m, \Lambda e_2) \in \lfloor \forall \alpha.\tau \rfloor_V$:
      Symmetric reasoning for e_2

6. Case $c \Rightarrow \tau$:

   Given: $(W, n, \nu e_1, \nu e_2) \in \lceil c \Rightarrow \tau \rceil_V^{\mathcal{A}}$

   This means from Definition 4.4 we know that

   $\forall W_b \sqsupseteq W, n' < n. \mathcal{L} \models c \implies (W_b, n', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$
   $\wedge \forall \theta_l \sqsupseteq W.\theta_1, j. \mathcal{L} \models c \implies (\theta_l, j, e_1) \in \lfloor \tau \rfloor_E)$
   $\wedge \forall \theta_l \sqsupseteq W.\theta_2, j. \mathcal{L} \models c \implies (\theta_l, j, e_2) \in \lfloor \tau \rfloor_E)$ (C0)

   To prove:

   (a) $\forall m.\ (W.\theta_1, m, \nu e_1) \in \lfloor c \Rightarrow \tau \rfloor_V$:
      This means from Definition 4.6 we need to prove:
      $\forall \theta'. W.\theta_1 \sqsubseteq \theta'. \forall m' < m. \mathcal{L} \models c \implies (\theta', m', e_1) \in \lfloor \tau \rfloor_E$
      This further means that we are given some θ' and m' s.t $W.\theta_1 \sqsubseteq \theta'$, $m' < m$ and $\mathcal{L} \models c$
      And we need to prove: $(\theta', m', e_1) \in \lfloor \tau \rfloor_E$

      Instantiating θ_l, j in the second conjunct of C0 with θ', m' respectively and since we know that $W.\theta_1 \sqsubseteq \theta'$ and $\mathcal{L} \models c$

      Therefore we get $(\theta', m', e_1) \in \lfloor \tau \rfloor_E$

   (b) $\forall m.\ (W.\theta_2, m, \nu e_2) \in \lfloor c \Rightarrow \tau \rfloor_V$:
      Symmetric reasoning for e_2

7. Case $\mathsf{ref}\ \ell\ \tau$:

   From Definition 4.4 and 4.6

8. Case $\mathsf{Labeled}\ \ell\ \tau$:

   Given $(W, n, \mathsf{Lb} v_1, \mathsf{Lb} v_2) \in \lceil \mathsf{Labeled}\ \ell\ \tau \rceil_V^{\mathcal{A}}$

   2 cases arise:

   (a) $\ell \sqsubseteq \mathcal{A}$:

   From Definition 4.3 we know that
   $(W, n, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$

   Therefore from IH we get $\forall m.(W.\theta_1, m, v_1) \in \lfloor \tau \rfloor_V$ and $\forall m.(W.\theta_2, m, v_2) \in \lfloor \tau \rfloor_V$

   (b) $\ell \not\sqsubseteq \mathcal{A}$:

   Directly from Definition 4.3

9. Case $\mathbb{C}\ \ell_1\ \ell_2\ \tau$:

   Given: $(W, n, v_1, v_2) \in \lceil \mathbb{C}\ \ell_1\ \ell_2\ \tau \rceil_V^{\mathcal{A}}$

   This means from Definition 4.4 we know that

   $\Big(\forall k \leq n, W_e \sqsupseteq W, H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v_1', v_2', j.$
   $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
   $\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_2, v_1', v_2', \tau)\Big) \wedge$
   $\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
   $\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau \rfloor_V \wedge$
   $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
   $(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_1)\Big)$ (CG0)

   To prove: $\forall i \in \{1,2\}.\ \forall m.\ (W.\theta_i, m, v_i) \in \lfloor \mathbb{C}\ \ell_1\ \ell_2\ \tau \rfloor_V$

   This means from Definition 4.6 we need to prove

   $\forall l \in \{1,2\}.\forall m.\Big(\forall k \leq m, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
   $\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau \rfloor_V \wedge$
   $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
   $(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_1)\Big)$

   <u>Case $l = 1$</u>

   And given some m and $k \leq m, \theta_e \sqsupseteq W.\theta_l, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k$

   We need to prove that

   $\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau \rfloor_V \wedge$
   $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
   $(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_1)$

   Instantiating (CG0) with $l = 1$ and the given $k \leq m, \theta_e \sqsupseteq W.\theta_l, H, j$ we get the desired.

   <u>Case $l = 2$</u>

   Symmetric reasoning as in the previous case above

□

Lemma 4.15 (Monotonicity Unary)**.** *The following holds:*
$\forall \theta, \theta', v, m, m', \tau.$
$(\theta, m, v) \in \lfloor \tau \rfloor_V \wedge m' < m \wedge \theta \sqsubseteq \theta' \implies (\theta', m', v) \in \lfloor \tau \rfloor_V$

Proof. Proof by induction on τ

1. case $\mathsf{b}, \mathsf{unit}$:
   Directly from Definition 4.6

2. case $\tau_1 \times \tau_2$:
   Given: $(\theta, m, (v_1, v_2)) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$
   To prove: $(\theta', m', (v_1, v_2)) \in \lfloor \tau_1 \times \tau_2 \rfloor_V$
   This means from Definition 4.6 we know that
   $(\theta, m, v_1) \in \lfloor \tau_1 \rfloor_V \wedge (\theta, m, v_2) \in \lfloor \tau_2 \rfloor_V$

   IH1 : $(\theta', m', v_1) \in \lfloor \tau_1 \rfloor_V$
   IH2 : $(\theta', m', v_2) \in \lfloor \tau_2 \rfloor_V$

   We get the desired from IH1, IH2 and Definition 4.6

3. case $\tau_1 + \tau_2$:
   2 cases arise:

   (a) $v = \mathsf{inl}(v_1)$:
   Given: $(\theta, m, (\mathsf{inl}\ v_1)) \in \lfloor \tau_1 + \tau_2 \rfloor_V$
   To prove: $(\theta', m', \mathsf{inl}\ v_1) \in \lfloor \tau_1 + \tau_2 \rfloor_V$
   This means from Definition 4.6 we know that
   $(\theta, m, v_1) \in \lfloor \tau_1 \rfloor_V$
   IH : $(\theta', m', v_1) \in \lfloor \tau_1 \rfloor_V$
   Therefore from IH and Definition 4.6 we get the desired

   (b) $v = \mathsf{inr}(v_2)$
   Symmetric case

4. case $\tau_1 \to \tau_2$:
   Given: $(\theta, m, (\lambda x.e_1)) \in \lfloor \tau_1 \to \tau_2 \rfloor_V$
   To prove: $(\theta', m', (\lambda x.e_1)) \in \lfloor \tau_1 \to \tau_2 \rfloor_V$
   This means from Definition 4.6 we know that

   $$\forall \theta''.\theta \sqsubseteq \theta'' \wedge \forall j < m. \forall v.(\theta'', j, v) \in \lfloor \tau_1 \rfloor_V \implies (\theta'', j, e_1[v/x]) \in \lfloor \tau_2 \rfloor_E \tag{91}$$

   Similarly from Definition 4.6 we know that we are required to prove
   $\forall \theta'''.\theta' \sqsubseteq \theta''' \wedge \forall k < m'. \forall v_1.(\theta''', k, v_1) \in \lfloor \tau_1 \rfloor_V \implies (\theta''', k, e_1[v_1/x]) \in \lfloor \tau_2 \rfloor_E$

   This means that given some θ''', k and v_1 such that $\theta' \sqsubseteq \theta''' \wedge k < m' \wedge (\theta''', k, v_1) \in \lfloor \tau_1 \rfloor_V$

   And we are required to prove $(\theta''', k, e_1[v_1/x]) \in \lfloor \tau_2 \rfloor_E$

Instantiating Equation 91 with θ''', k and v_1 and since we know that $\theta' \sqsubseteq \theta'''$ and $\theta \sqsubseteq \theta'$ therefore we have $\theta \sqsubseteq \theta'''$. Also, we know that $k < m' < m$ and $(\theta''', k, v_1) \in \lfloor \tau_1 \rfloor_V$

Therefore we get $(\theta''', k, e_1[v_1/x]) \in \lfloor \tau_2 \rfloor_E$

5. case $\mathsf{ref}\ \ell\ \tau$:

   From Definition 4.6 and Definition 4.1

6. case $\forall \alpha.\tau$:

   Given: $(\theta, m, (\Lambda e_1)) \in \lfloor \forall \alpha.\tau \rfloor_V$

   To prove: $(\theta', m', (\Lambda e_1)) \in \lfloor \forall \alpha.\tau \rfloor_V$

   This means from Definition 4.6 we know that

   $$\forall \theta''.\theta \sqsubseteq \theta'' \land \forall j < m.\forall \ell_i \in \mathcal{L}.(\theta'', j, e_1) \in \lfloor \tau[\ell_i/\alpha] \rfloor_E \tag{92}$$

   Similarly from Definition 4.6 we know that we are required to prove
   $\forall \theta'''.\theta' \sqsubseteq \theta''' \land \forall k < m'.\forall \ell_j \in \mathcal{L}.(\theta''', k, e_1) \in \lfloor \tau[\ell_j/\alpha] \rfloor_E$

   This means that given some θ''', k and ℓ_j such that $\theta' \sqsubseteq \theta''' \land k < m' \land \ell_j \in \mathcal{L}$

   And we are required to prove $(\theta''', k, e_1) \in \lfloor \tau[\ell_j/\alpha] \rfloor_E$

   Instantiating Equation 92 with θ''', k and ℓ_j and since we know that $\theta' \sqsubseteq \theta'''$ and $\theta \sqsubseteq \theta'$ therefore we have $\theta \sqsubseteq \theta'''$. Also, we know that $k < m' < m$ and $\ell_j \in \mathcal{L}$

   Therefore we get $(\theta''', k, e_1) \in \lfloor \tau[\ell_j/\alpha] \rfloor_E$

7. case $c \Rightarrow \tau$:

   Given: $(\theta, m, (\nu e_1)) \in \lfloor c \Rightarrow \tau \rfloor_V$

   To prove: $(\theta', m', (\nu e_1)) \in \lfloor c \Rightarrow \tau \rfloor_V$

   This means from Definition 4.6 we know that

   $$\forall \theta''.\theta \sqsubseteq \theta'' \land \forall j < m.\mathcal{L} \models c \implies (\theta'', j, e_1) \in \lfloor \tau \rfloor_E \tag{93}$$

   Similarly from Definition 4.6 we know that we are required to prove
   $\forall \theta'''.\theta' \sqsubseteq \theta''' \land \forall k < m'.\mathcal{L} \models c \implies (\theta''', k, e_1) \in \lfloor \tau \rfloor_E$

   This means that given some θ''', k and ℓ_j such that $\theta' \sqsubseteq \theta''' \land k < m' \land \ell_j \in \mathcal{L}$

   And we are required to prove $(\theta''', k, e_1) \in \lfloor \tau \rfloor_E$

   Instantiating Equation 93 with θ''', k and since we know that $\theta' \sqsubseteq \theta'''$ and $\theta \sqsubseteq \theta'$ therefore we have $\theta \sqsubseteq \theta'''$. Also, we know that $k < m' < m$ and $\mathcal{L} \models c$

   Therefore we get $(\theta''', k, e_1) \in \lfloor \tau \rfloor_E$

8. case $\mathsf{Labeled}\ \ell\ \tau$:

   Given: $(\theta, m, (\mathsf{Lb}\, v)) \in \lfloor \mathsf{Labeled}\ \ell\ \tau \rfloor_V$

   To prove: $(\theta', m', (\mathsf{Lb}\, v)) \in \lfloor \mathsf{Labeled}\ \ell\ \tau \rfloor_V$

   This means from Definition 4.6 we know that $(\theta, m, v) \in \lfloor \tau \rfloor_V$

   IH: $(\theta', m', v) \in \lfloor \tau \rfloor_V$

   Therefore from IH and Definition 4.6 we get the desired

9. case $\mathbb{C}\ \ell_1\ \ell_2\ \tau$:

   Given: $(\theta, m, e) \in \lfloor \mathbb{C}\ \ell_1\ \ell_2\ \tau \rfloor_V$

   To prove: $(\theta', m', e) \in \lfloor \mathbb{C}\ \ell_1\ \ell_2\ \tau \rfloor_V$

   This means from Definition 4.6 we know that

   $\forall k \leq m, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v) \Downarrow_j^f (H', v') \wedge j < k \implies$
   $\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor \tau \rfloor_V \wedge$
   $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell_1 \sqsubseteq \ell') \wedge$
   $(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_1)$ (LB0)

   Similarly from Definition 4.6 we are required to prove

   $\forall k_1 \leq m', \theta_{e1} \sqsupseteq \theta', H_1, j_1.(k_1, H_1) \triangleright \theta_{e1} \wedge (H_1, v_1) \Downarrow_{j_1}^f (H_1', v_1') \wedge j_1 < k_1 \implies$
   $\exists \theta' \sqsupseteq \theta_e.(k_1 - j_1, H') \triangleright \theta' \wedge (\theta_1', k_1 - j_1, v') \in \lfloor \tau \rfloor_V \wedge$
   $(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta_{e1}(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell_1 \sqsubseteq \ell') \wedge$
   $(\forall a \in dom(\theta_1') \backslash dom(\theta_{e1}).\theta_1'(a) \searrow \ell_1)$

   This means we are given

   $k_1 \leq m', \theta_{e1} \sqsupseteq \theta', H_1, j_1$ s.t $(k_1, H) \triangleright \theta_{e1} \wedge (H_1, v_1) \Downarrow_{j_1}^f (H_1', v_1') \wedge j_1 < k_1$

   And we are required to prove:

   $\exists \theta' \sqsupseteq \theta_e.(k_1 - j_1, H') \triangleright \theta' \wedge (\theta_1', k_1 - j_1, v') \in \lfloor \tau \rfloor_V \wedge$
   $(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta_{e1}(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell_1 \sqsubseteq \ell') \wedge$
   $(\forall a \in dom(\theta_1') \backslash dom(\theta_{e1}).\theta_1'(a) \searrow \ell_1)$

   Instantiating (LB0), k with k_1, θ_e with θ_{e1}, H with H_1 and j with j_1. We know that $k_1 < m' < m$, $\theta \sqsubseteq \theta' \sqsubseteq \theta_{e1}$, $(k_1, H_1) \triangleright \theta_{e1}$, $(H_1, v_1) \Downarrow_{j_1}^f (H_1', v_1')$ and $i_1 + j_1 < k_1$. Therefore we get

   $\exists \theta' \sqsupseteq \theta_e.(k_1 - j_1, H') \triangleright \theta' \wedge (\theta_1', k_1 - j_1, v') \in \lfloor \tau \rfloor_V \wedge$
   $(\forall a.H_1(a) \neq H_1'(a) \implies \exists \ell'.\theta_{e1}(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell_1 \sqsubseteq \ell') \wedge$
   $(\forall a \in dom(\theta_1') \backslash dom(\theta_{e1}).\theta_1'(a) \searrow \ell_1)$

□

Lemma 4.16 (Monotonicity binary). *The following holds:*
$\forall W, W', v_1, v_2, \mathcal{A}, n, n', \tau.$
$(W, n, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}} \wedge n' < n \wedge W \sqsubseteq W' \implies (W', n', v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$

Proof. Proof by induction on τ

1. Case b, unit:

   From Definition 4.4

2. Case $\tau_1 \times \tau_2$:

   Given: $(W, n, (v_{i1}, v_{i2}), (v_{j1}, v_{j2})) \in \lceil \tau_1 \times \tau_2 \rceil_V^{\mathcal{A}}$

   To prove: $(W', n', (v_{i1}, v_{i2}), (v_{j1}, v_{j2})) \in \lceil \tau_1 \times \tau_2 \rceil_V^{\mathcal{A}}$

   From Definition 4.4 we know that we are given

   $(W, n, v_{i1}, v_{j1}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \wedge (W, n, v_{i2}, v_{j2}) \in \lceil \tau_2 \rceil_V^{\mathcal{A}}$

   IH1 : $(W', n', v_{i1}, v_{j1}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$

   IH2 : $(W', n', v_{i2}, v_{j2}) \in \lceil \tau_2 \rceil_V^{\mathcal{A}}$

   From IH1, IH2 and Definition 4.4 we get the desired.

3. Case $\tau_1 + \tau_2$:

   2 cases arise:

   (a) $v_1 = \mathsf{inl}\ v_{i1}$ and $v_2 = \mathsf{inl}\ v_{i2}$:
   Given: $(W, n, (\mathsf{inl}\ v_{i1}, \mathsf{inl}\ v_{i2})) \in \lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}}$
   To prove: $(W', n', (\mathsf{inl}\ v_{i1}, \mathsf{inl}\ v_{i2})) \in \lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}}$

   From Definition 4.4 we know that we are given
   $(W, n, v_{i1}, v_{i2}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$
   IH : $(W', n', v_{i1}, v_{i2}) \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$
   Therefore from Definition 4.4 we get
   $(W', n', \mathsf{inl}\ v_{i1}, \mathsf{inl}\ v_{i2}) \in \lceil \tau_1 + \tau_2 \rceil_V^{\mathcal{A}}$

   (b) $v_1 = \mathsf{inr}(v_{12})$ and $v_2 = \mathsf{inr}(v_{22})$:
   Symmetric case

4. Case $\tau_1 \to \tau_2$:

   Given: $(W, n, (\lambda x.e_1), (\lambda x.e_2)) \in \lceil \tau_1 \to \tau_2 \rceil_V^{\mathcal{A}}$

   To prove: $(\theta', n', (\lambda x.e_1), (\lambda x.e_1)) \in \lceil \tau_1 \to \tau_2 \rceil_V^{\mathcal{A}}$

   This means from Definition 4.4 we know that the following holds

   $\forall W' \sqsupseteq W, j < n, v_1, v_2.((W', j, v_1, v_2) \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \implies (W', j, e_1[v_1/x], e_2[v_2/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}})$ (BM-A0)

   $\forall \theta_l \sqsupseteq W.\theta_1, j, v_c.((\theta_l, j, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, j, e_1[v_c/x]) \in \lfloor \tau_2 \rfloor_E)$ (BM-A1)

   $\forall \theta_l \sqsupseteq W.\theta_2, j, v_c.((\theta_l, j, v_c) \in \lfloor \tau_1 \rfloor_V \implies (\theta_l, j, e_2[v_c/x]) \in \lfloor \tau_2 \rfloor_E)$ (BM-A2)

   Similarly from Definition 4.4 we know that we are required to prove

   (a) $\forall W'' \sqsupseteq W', k < n', v_1', v_2'.((W'', k, v_1', v_2') \in \lceil \tau_1 \rceil_V^{\mathcal{A}} \implies (W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}})$:
   This means that we are given some $W'' \sqsupseteq W'$, $k < n'$ and v_1', v_2' s.t
   $(W'', k, v_1', v_2') \in \lceil \tau_1 \rceil_V^{\mathcal{A}}$
   And we a required to prove: $(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}}$

   Instantiating BM-A0 with W'', k and v_1', v_2' we get
   $(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil \tau_2 \rceil_E^{\mathcal{A}}$

(b) $\forall \theta_l' \sqsupseteq W'.\theta_1, k, v_c'.((\theta_l', k, v_c') \in \lfloor \tau_1 \rfloor_V \implies (\theta_l', k, e_1[v_c'/x]) \in \lfloor \tau_2 \rfloor_E)$:
This means that we are given some $\theta_l' \sqsupseteq W'.\theta_1$, k and v_c' s.t
$(\theta_l', k, v_c') \in \lfloor \tau_1 \rfloor_V$
And we a required to prove: $(\theta_l', k, e_1[v_c'/x]) \in \lfloor \tau_2 \rfloor_E$

Instantiating BM-A1 with θ_l', k and v_c' we get
$(\theta_l', k, e_1[v_c'/x]) \in \lfloor \tau_2 \rfloor_E$

(c) $\forall \theta_l' \sqsupseteq W.\theta_2, k, v_c'.((\theta_l', k, v_c') \in \lfloor \tau_1 \rfloor_V \implies (\theta_l', k, e_2[v_c'/x]) \in \lfloor \tau_2 \rfloor_E)$:
This means that we are given some $\theta_l' \sqsupseteq W'.\theta_2$, k and v_c' s.t
$(\theta_l', k, v_c') \in \lfloor \tau_1 \rfloor_V$
And we a required to prove: $(\theta_l', k, e_2[v_c'/x]) \in \lfloor \tau_2 \rfloor_E$

Instantiating BM-A1 with θ_l', k and v_c' we get
$(\theta_l', k, e_2[v_c'/x]) \in \lfloor \tau_2 \rfloor_E$

5. Case $\mathsf{ref}\ \ell\ \tau$:

From Definition 4.4 and Definition 4.2

6. Case $\forall \alpha.\tau$:

Given: $(W, n, (\Lambda e_1), (\Lambda e_2)) \in \lceil \forall \alpha.\tau \rceil_V^{\mathcal{A}}$

To prove: $(\theta', n', (\Lambda e_1), (\Lambda e_1)) \in \lceil \forall \alpha.\tau \rceil_V^{\mathcal{A}}$

This means from Definition 4.4 we know that the following holds

$\forall W' \sqsupseteq W, n' < n, \ell' \in \mathcal{L}.((W', n', e_1, e_2) \in \lceil \tau[\ell'/\alpha] \rceil_E^{\mathcal{A}})$ (BM-F0)

$\forall \theta_l \sqsupseteq W.\theta_1, j, \ell' \in \mathcal{L}.((\theta_l, j, e_1) \in \lfloor \tau[\ell'/\alpha] \rfloor_E)$ (BM-F1)

$\forall \theta_l \sqsupseteq W.\theta_2, j, \ell' \in \mathcal{L}.((\theta_l, j, e_2) \in \lfloor \tau[\ell'/\alpha] \rfloor_E)$ (BM-F2)

Similarly from Definition 4.4 we know that we are required to prove

(a) $\forall W'' \sqsupseteq W', n'' < n', \ell'' \in \mathcal{L}.((W'', n'', e_1, e_2) \in \lceil \tau[\ell''/\alpha] \rceil_E^{\mathcal{A}})$:
This means that we are given some $W'' \sqsupseteq W'$, $n'' < n'$ and $\ell'' \in \mathcal{L}$
And we a required to prove: $((W'', n'', e_1, e_2) \in \lceil \tau[\ell''/\alpha] \rceil_E^{\mathcal{A}})$

Instantiating BM-F0 with W'', n'' and ℓ''. And since $W'' \sqsupseteq W'$ and $W' \sqsupseteq W$ therefore $W'' \sqsupseteq W$. Also since $n'' < n'$ and $n' < n$ therefore $n'' < n$. And finally since $\ell'' \in \mathcal{L}$ therefore we get
$((W'', n'', e_1, e_2) \in \lceil \tau[\ell''/\alpha] \rceil_E^{\mathcal{A}})$

(b) $\forall \theta_l' \sqsupseteq W'.\theta_1, k, \ell'' \in \mathcal{L}.((\theta_l', k, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$:
This means that we are given some $\theta_l' \sqsupseteq W'.\theta_1$, k and $\ell'' \in \mathcal{L}$
And we a required to prove: $((\theta_l', k, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$

Instantiating BM-F1 with θ_l', k and ℓ''. And since $\theta_l' \sqsupseteq W'.\theta_1$ and $W' \sqsupseteq W$ therefore $\theta_1' \sqsupseteq W.\theta_1$. And since $\ell'' \in \mathcal{L}$ therefore we get
$((\theta_l', k, e_1) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$

(c) $\forall \theta_l \sqsupseteq W.\theta_2, j, \ell'' \in \mathcal{L}.((\theta_l', k, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$:
This means that we are given some $\theta_l' \sqsupseteq W'.\theta_2$, k and $\ell'' \in \mathcal{L}$
And we a required to prove: $((\theta_l', k, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$

Instantiating BM-F1 with θ_l', k and ℓ''. And since $\theta_l' \sqsupseteq W'.\theta_2$ and $W' \sqsupseteq W$ therefore $\theta_2' \sqsupseteq W.\theta_2$. And since $\ell'' \in \mathcal{L}$ therefore we get
$((\theta_l', k, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E)$

7. Case $c \Rightarrow \tau$:

Given: $(W, n, (\nu e_1), (\nu e_2)) \in \lceil c \Rightarrow \tau \rceil_V^{\mathcal{A}}$

To prove: $(\theta', n', (\nu e_1), (\nu e_1)) \in \lceil c \Rightarrow \tau \rceil_V^{\mathcal{A}}$

This means from Definition 4.4 we know that the following holds

$\forall W' \sqsupseteq W, n' < n.\mathcal{L} \models c \implies (W', n', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$ (BM-C0)

$\forall \theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c \implies (\theta_l, j, e_1) \in \lfloor \tau \rfloor_E$ (BM-C1)

$\forall \theta_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c \implies (\theta_l, j, e_2) \in \lfloor \tau \rfloor_E$ (BM-C2)

Similarly from Definition 4.4 we know that we are required to prove

(a) $\forall W'' \sqsupseteq W', n'' < n.\mathcal{L} \models c \implies (W'', n'', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$:
This means that we are given some $W'' \sqsupseteq W'$, $n'' < n'$ and $\mathcal{L} \models c$
And we a required to prove: $(W'', n'', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$

Instantiating BM-C0 with W'', n''. And since $W'' \sqsupseteq W'$ and $W' \sqsupseteq W$ therefore $W'' \sqsupseteq W$. And since $\mathcal{L} \models c$ therefore we get
$(W'', n'', e_1, e_2) \in \lceil \tau \rceil_E^{\mathcal{A}}$

(b) $\forall \theta_l' \sqsupseteq W'.\theta_1, k.\mathcal{L} \models c \implies (\theta_l', k, e_1) \in \lfloor \tau \rfloor_E$:
This means that we are given some $\theta_l' \sqsupseteq W'.\theta_1$, k and $\mathcal{L} \models c$
And we a required to prove: $(\theta_l', k, e_1) \in \lfloor \tau \rfloor_E$

Instantiating BM-F1 with θ_l', k. And since $\theta_l' \sqsupseteq W'.\theta_1$ and $W' \sqsupseteq W$ therefore $\theta_1' \sqsupseteq W.\theta_1$. And since $\mathcal{L} \models c$ therefore we get
$(\theta_l', k, e_1) \in \lfloor \tau \rfloor_E$

(c) $\forall \theta_l' \sqsupseteq W'.\theta_2, k.\mathcal{L} \models c \implies (\theta_l, k, e_2) \in \lfloor \tau \rfloor_E$:
This means that we are given some $\theta_l' \sqsupseteq W'.\theta_2$, k and $\mathcal{L} \models c$
And we a required to prove: $(\theta_l', k, e_2) \in \lfloor \tau \rfloor_E$

Instantiating BM-F1 with θ_l', k. And since $\theta_l' \sqsupseteq W'.\theta_2$ and $W' \sqsupseteq W$ therefore $\theta_2' \sqsupseteq W.\theta_2$. And since $\mathcal{L} \models c$ therefore we get
$(\theta_l', k, e_2) \in \lfloor \tau \rfloor_E$

8. Case $\mathsf{Labeled}\ \ell\ \tau$:

Given: $(W, n, (\mathsf{Lb}\, v_1), (\mathsf{Lb}\, v_2)) \in \lceil \mathsf{Labeled}\ \ell\ \tau \rceil_V^{\mathcal{A}}$

To prove: $(W', n', (\mathsf{Lb}\, v_1), (\mathsf{Lb}\, v_2)) \in \lceil \mathsf{Labeled}\ \ell\ \tau \rceil_V^{\mathcal{A}}$

From Definition 4.4 2 cases arise:

(a) $\ell \sqsubseteq \mathcal{A}$:

In this case we know that $(W, n, v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$

Therefore from IH we know that $(W', n', v_1, v_2) \in \lceil \tau \rceil_V^{\mathcal{A}}$

Hence from Definition 4.4 we get $(W', n', (\mathsf{Lb}\, v_1), (\mathsf{Lb}\, v_2)) \in \lceil \mathsf{Labeled}\ \ell\ \tau \rceil_V^{\mathcal{A}}$

(b) $\ell \not\sqsubseteq \mathcal{A}$:

In this case we know that $\forall m.\ (W.\theta_1, m, v_1) \in \lfloor \tau \rfloor_V$ and $(W.\theta_2, m, v_2) \in \lfloor \tau \rfloor_V$

Since $W.\theta_1 \sqsubseteq W'.\theta_1$ (from Definition 4.2). Therefore from Lemma 4.15 we know that $\forall m' < m.\ (W'.\theta_1, m', v_1) \in \lfloor \tau \rfloor_V$

Similarly since $W.\theta_2 \sqsubseteq W'.\theta_2$ (from Definition 4.2). Therefore from Lemma 4.15 we know that

$\forall m' < m.\ (W'.\theta_2, m', v_2) \in \lfloor \tau \rfloor_V$

Finally from Definition 4.4 we get $(W', n', (\mathsf{Lb}\, v_1), (\mathsf{Lb}\, v_2)) \in \lceil \mathsf{Labeled}\ \ell\ \tau \rceil_V^{\mathcal{A}}$

9. Case $\mathbb{C}\ \ell_1\ \ell_2\ \tau$:

Given: $(W, n, v_1, v_2) \in \lceil \mathbb{C}\ \ell_1\ \ell_2\ \tau \rceil_V^{\mathcal{A}}$

To prove: $(W', n', v_1, v_2) \in \lceil \mathbb{C}\ \ell_1\ \ell_2\ \tau \rceil_V^{\mathcal{A}}$

From Definition 4.4 we are given that

$\Big(\forall k \leq n, W_e \sqsupseteq W, H_1, H_2.(k, H_1, H_2) \rhd W_e \wedge$
$\forall v_1', v_2', j.(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H_1', H_2') \rhd W' \wedge \mathit{ValEq}(\mathcal{A}, W', k - j, \ell_2, v_1', v_2', \tau)\Big) \wedge$
$\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \rhd \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \rhd \theta' \wedge (\theta', k - j, v_l') \in \lfloor \tau \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_1)\Big)$ (BM-M0)

Similarly from Definition 4.4 it suffices to prove that

(a) $\Big(\forall k \leq n, W_e \sqsupseteq W, H_1, H_2.(k, H_1, H_2) \rhd W_e \wedge$
$\forall v_1', v_2', j.(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H_1', H_2') \rhd W' \wedge \mathit{ValEq}(\mathcal{A}, W', k - j, \ell_2, v_1', v_2', \tau)\Big)$:

This means that given some $k \leq n$, $W_e \sqsupseteq W, H_1, H_2, v_1', v_2', j$ s.t
$(k, H_1, H_2) \rhd W_e \wedge (H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2') \wedge j < k$

It suffices to prove that
$\exists W' \sqsupseteq W_e.(k - j, H_1', H_2') \rhd W' \wedge \mathit{ValEq}(\mathcal{A}, W', k - j, \ell_2, v_1', v_2', \tau)$

Instantiating the first conjunct of (BM-M0) with the given k, $W_e \sqsupseteq W, H_1, H_2, v_1', v_2', j$ and since we know that $n' \leq n$ and $W \sqsubseteq W'$ we get the desired

(b) $\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \rhd \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \rhd \theta' \wedge (\theta', k - j, v_l') \in \lfloor \tau \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_1)\Big)$:

Similar reasoning as in the previous case but using Lemma 4.15

□

Lemma 4.17 (Unary monotonicity for Γ)**.** $\forall \theta, \theta', \delta, \Gamma, n, n'$.
$(\theta, n, \delta) \in \lfloor \Gamma \rfloor_V \wedge n' < n \wedge \theta \sqsubseteq \theta' \implies (\theta', n', \delta) \in \lfloor \Gamma \rfloor_V$

Proof. Given: $(\theta, n, \delta) \in \lfloor \Gamma \rfloor_V \wedge n' < n \wedge \theta \sqsubseteq \theta'$
To prove: $(\theta', n', \delta) \in \lfloor \Gamma \rfloor_V$

From Definition 4.12 it is given that
$dom(\Gamma) \subseteq dom(\delta) \wedge \forall x \in dom(\Gamma).(\theta, n, \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$

And again from Definition 4.12 we are required to prove that
$dom(\Gamma) \subseteq dom(\delta) \wedge \forall x \in dom(\Gamma).(\theta', n', \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$

- $dom(\Gamma) \subseteq dom(\delta)$:

  Given

- $\forall x \in dom(\Gamma).(\theta', n', \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$:

  Since we know that $\forall x \in dom(\Gamma).(\theta, n, \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$ (given)

  Therefore from Lemma 4.15 we get

  $\forall x \in dom(\Gamma).(\theta', n', \delta(x)) \in \lfloor \Gamma(x) \rfloor_V$

□

Lemma 4.18 (Binary monotonicity for Γ)**.** $\forall W, W', \delta, \Gamma, n, n'$.
$(W, n, \gamma) \in \lfloor \Gamma \rfloor_V \wedge n' < n \wedge W \sqsubseteq W' \implies (W', n', \gamma) \in \lfloor \Gamma \rfloor_V$

Proof. Given: $(W, n, \gamma) \in \lfloor \Gamma \rfloor_V \wedge n' < n \wedge W \sqsubseteq W'$
To prove: $(W', n', \gamma) \in \lfloor \Gamma \rfloor_V$

From Definition 4.13 it is given that
$dom(\Gamma) \subseteq dom(\gamma) \wedge \forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$

And again from Definition 4.12 we are required to prove that
$dom(\Gamma) \subseteq dom(\gamma) \wedge \forall x \in dom(\Gamma).(W', n', \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$

- $dom(\Gamma) \subseteq dom(\gamma)$:

  Given

- $\forall x \in dom(\Gamma).(W', n', \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$:

  Since we know that $\forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$ (given)

  Therefore from Lemma 4.16 we get

  $\forall x \in dom(\Gamma).(W', n', \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$

□

Lemma 4.19 (Unary monotonicity for H)**.** $\forall \theta, H, n, n'$.
$(n, H) \triangleright \theta \wedge n' < n \implies (n', H) \triangleright \theta$

Proof. Given: $(n, H) \triangleright \theta \wedge n' < n$
To prove: $(n', H) \triangleright \theta$

From Definition 4.8 it is given that
$dom(\theta) \subseteq dom(H) \wedge \forall a \in dom(\theta).(\theta, n-1, H(a)) \in \lfloor \theta(a) \rfloor_V$

And again from Definition 4.12 we are required to prove that
$dom(\theta) \subseteq dom(H) \wedge \forall a \in dom(\theta).(\theta, n'-1, H(a)) \in \lfloor \theta'(a) \rfloor_V$

- $dom(\theta) \subseteq dom(H)$:
  Given
- $\forall a \in dom(\theta).(\theta, n'-1, H(a)) \in \lfloor \theta'(a) \rfloor_V$:
  Since we know that $\forall a \in dom(\theta).(\theta, n-1, H(a)) \in \lfloor \theta(a) \rfloor_V$ (given)
  Therefore from Lemma 4.15 we get
  $\forall a \in dom(\theta).(\theta, n'-1, H(a)) \in \lfloor \theta'(a) \rfloor_V$

□

Lemma 4.20 (Binary monotonicity for heaps)**.** $\forall W, H_1, H_2, n, n'.$
$(n, H_1, H_2) \triangleright W \wedge n' < n \implies (n', H_1, H_2) \triangleright W$

Proof. Given: $(n, H_1, H_2) \triangleright W \wedge n' < n \wedge W \sqsubseteq W'$
To prove: $(n', H_1, H_2) \triangleright W$

From Definition 4.9 it is given that
$dom(W.\theta_1) \subseteq dom(H_1) \wedge dom(W.\theta_2) \subseteq dom(H_2) \wedge$
$(W.\hat{\beta}) \subseteq (dom(W.\theta_1) \times dom(W.\theta_2)) \wedge$
$\forall (a_1, a_2) \in (W.\hat{\beta}).(W.\theta_1(a_1) = W.\theta_2(a_2) \wedge$
$(W, n-1, H_1(a_1), H_2(a_2)) \in \lceil W.\theta_1(a_1) \rceil_V^{\mathcal{A}}) \wedge$
$\forall i \in \{1, 2\}.\forall m.\forall a_i \in dom(W.\theta_i).(W.\theta_i, m, H_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$

And again from Definition 4.9 we are required to prove:

- $dom(W.\theta_1) \subseteq dom(H_1) \wedge dom(W.\theta_2) \subseteq dom(H_2)$:
  Given
- $(W.\hat{\beta}) \subseteq (dom(W.\theta_1) \times dom(W.\theta_2))$:
  Given
- $\forall (a_1, a_2) \in (W.\hat{\beta}).(W.\theta_1(a_1) = W.\theta_2(a_2)$ and $(W, n'-1, H_1(a_1), H_2(a_2)) \in \lceil W.\theta_1(a_1) \rceil_V^{\mathcal{A}})$:
  $\forall (a_1, a_2) \in (W.\hat{\beta}).$
  - $(W.\theta_1(a_1) = W.\theta_2(a_2)$: Given
  - $(W, n'-1, H_1(a_1), H_2(a_2)) \in \lceil W.\theta_1(a_1) \rceil_V^{\mathcal{A}})$:
    Given and from Lemma 4.16
- $\forall i \in \{1, 2\}.\forall m.\forall a_i \in dom(W.\theta_i).(W.\theta_i, m, H_i(a_i)) \in \lfloor W.\theta_i(a_i) \rfloor_V$:
  Given

□

Theorem 4.21 (Fundamental theorem unary)**.** $\forall \Sigma, \Psi, \Gamma, \theta, \mathcal{L}, e, \tau, \sigma, \delta, n.$
$\Sigma; \Psi; \Gamma \vdash e : \tau \wedge$
$\mathcal{L} \models \Psi\ \sigma \wedge$
$(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V \implies$
$(\theta, n, e\ \delta) \in \lfloor \tau\ \sigma \rfloor_E$

Proof. Proof by induction on CG typing derivation

1. CG-var:

$$\frac{}{\Gamma, x : \tau \vdash x : \tau}\ \text{CG-var}$$

Also given is $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, x\ \delta) \in \lfloor \tau\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.x\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor \tau\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $x\ \delta \Downarrow_i v$

(from cg-val we know that $v = x\ \delta$ and $i = 0$)

<u>It suffices to prove</u> $(\theta, n, x\ \delta) \in \lfloor \tau\ \sigma \rfloor_V$ (FU-V0)

Since $(\theta, n, \delta) \in \lfloor \Gamma' \rfloor_V$ where $\Gamma' = \Gamma \cup \{x : \tau\}$. Therefore from Definition 4.12 we know that $(\theta, n, \delta(x)) \in \lfloor \Gamma'(x) \rfloor_V$

So we are done.

2. CG-lam:

$$\frac{\Gamma, x : \tau_1 \vdash e' : \tau_2}{\Gamma \vdash \lambda x.e' : (\tau_1 \to \tau_2)}$$

Also given is $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \lambda x.e_i\ \delta) \in \lfloor (\tau_1 \to \tau_2)\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.\lambda x.e'\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor (\tau_1 \to \tau_2)\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $\lambda x.e'\ \delta \Downarrow_i v$

(from cg-val we know that $v = \lambda x.e'\ \delta$ and $i = 0$)

<u>It suffices to prove</u>

$(\theta, n, \lambda x.e'\ \delta) \in \lfloor (\tau_1 \to \tau_2)\ \sigma \rfloor_V$ (FU-L0)

From Definition 4.6 it further suffices to prove

$\forall \theta'' \sqsupseteq \theta, v', j < n.(\theta'', j, v') \in \lfloor \tau_1 \rfloor_V \implies (\theta'', j, (e'\ \delta)[v'/x]) \in \lfloor \tau_2 \rfloor_E$

This means given some θ'', v', j s.t $\theta'' \sqsupseteq \theta$, $j < n$ and $(\theta'', j, v') \in \lfloor \tau_1 \rfloor_V$ (FU-L1)

<u>We are required to prove</u>

$(\theta'', j, (e' \ \delta)[v'/x]) \in \lfloor \tau_2 \rfloor_E$

Since $(\theta, n, \delta) \in \lfloor \Gamma \ \sigma \rfloor_V$ therefore from Lemma 4.17 we know that $(\theta, j, \delta) \in \lfloor \Gamma \ \sigma \rfloor_V$ where $j < n$ (from FU-L1)

IH:

$\forall \theta_h, v_x. \ (\theta_h, j, e' \ \delta \cup \{x \mapsto v_x\}) \in \lfloor \tau_2 \rfloor_E$, s.t $(\theta_i, j, v_x) \in \lfloor \tau_1 \rfloor_V$

Instantiating IH with θ'' and v' from (FU-L1) we get $(\theta'', j, (e' \ \delta)[v'/x]) \in \lfloor \tau_2 \rfloor_E$

3. CG-app:

$$\frac{\Gamma \vdash e_1 : (\tau_1 \to \tau_2) \qquad \Gamma \vdash e_2 : \tau_1}{\Gamma \vdash e_1 \ e_2 : \tau_2}$$

Also given is $(\theta, n, \delta) \in \lfloor \Gamma \ \sigma \rfloor_V$

To prove: $(\theta, n, (e_1 \ e_2) \ \delta) \in \lfloor \tau_2 \ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.(e_1 \ e_2) \ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor \tau_2 \ \sigma \rfloor_V$

This means that given some $i < n$ s.t $(e_1 \ e_2) \ \delta \Downarrow_i v$

It suffices to prove

$(\theta, n - i, v) \in \lfloor \tau_2 \ \sigma \rfloor_V$ (FU-P0)

IH1:

$\forall j < n.e_1 \ \delta \Downarrow_j v_1 \implies (\theta, n - j, v_1) \in \lfloor (\tau_1 \to \tau_2) \ \sigma \rfloor_V$

Since we know that $(e_1 \ e_2) \ \delta \Downarrow_i v$ therefore $\exists j < i < n$ s.t $e_1 \ \delta \Downarrow_j v_1$. This means we have $(\theta, n - j, v_1) \in \lfloor (\tau_1 \to \tau_2) \ \sigma \rfloor_V$

From cg-app we know that $v_1 = \lambda x.e'$.Therefore we have

$(\theta, n - j, \lambda x.e') \in \lfloor (\tau_1 \to \tau_2) \ \sigma \rfloor_V$ (FU-P1)

This means from Definition 4.6 we have

$$\forall \theta'' \sqsupseteq \theta \wedge I < (n - j), v.(\theta'', I, v) \in \lfloor \tau_1 \rfloor_V \implies (\theta'', I, e'[v/x]) \in \lfloor \tau_2 \ \sigma \rfloor_E \quad (94)$$

IH2:

$\forall k < (n - j).e_2 \ \delta \Downarrow_k v_2 \implies (\theta, n - j - k, v_2) \in \lfloor \tau_1 \rfloor_V$

Since we know that $(e_1 \ e_2) \ \delta \Downarrow_i v$ therefore $\exists k < i - j$ (since $i < n$ therefore $i - j < n - j$) s.t $e_2 \ \delta \Downarrow_k v_2$. This means we have

$(\theta, n - j - k, v_2) \in \lfloor \tau_1 \rfloor_V$ (FU-P2)

Instantiating Equation 94 with $\theta, (n-j-k), v_2$ and since we know that $(\theta, n-j-k, v_2) \in \lfloor \tau_1 \rfloor_V$ therefore we get

$(\theta, n-j-k, e'[v_2/x]) \in \lfloor \tau_2\ \sigma \rfloor_E$

This means from Definition 4.7 we have

$\forall J < n-j-k.e'[v_2/x] \Downarrow_J v_f \implies (\theta, n-j-k-J, v_J) \in \lfloor \tau_2\ \sigma \rfloor_E$

Since we know that $(e_1\ e_2)\ \delta \Downarrow_i v$ therefore we know that $\exists J < i < n$ s.t $i = j+k+J$ (since $j+k+J < n$ therefore $J < n-j-k$) and $e'[v_2/x] \Downarrow_J v_f$

Therefore we have $(\theta, n-j-k-J, v_J) \in \lfloor \tau_2\ \sigma \rfloor_E$

Since we know that $i = j+k+J$ and $v = v_J$ therefore we get $(\theta, n-i, v_J) \in \lfloor \tau_2\ \sigma \rfloor_E$ (so FU-P0 is proved)

4. CG-prod:

$$\frac{\Gamma \vdash e_1 : \tau_1 \qquad \Gamma \vdash e_2 : \tau_2}{\Gamma \vdash (e_1, e_2) : (\tau_1 \times \tau_2)}$$

Also given is $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, (e_1, e_2)\ \delta) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.(e_1, e_2)\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $(e_1, e_2)\ \delta \Downarrow_i v$

It suffices to prove

$(\theta, n-i, v) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V$ (FU-PA0)

IH1:

$\forall j < n.e_1\ \delta \Downarrow_j v_1 \implies (\theta, n-j, v_1) \in \lfloor \tau_1 \rfloor_V$

Since we know that $(e_1, e_2)\ \delta \Downarrow_i v$ therefore $\exists j < i < n$ s.t $e_1\ \delta \Downarrow_j v_1$. This means we have

$(\theta, n-j, v_1) \in \lfloor \tau_1 \rfloor_V$ (FU-PA1)

IH2:

$\forall k < (n-j).e_2\ \delta \Downarrow_k v_2 \implies (\theta, n-j-k, v_2) \in \lfloor \tau_2\ \sigma \rfloor_V$

Since we know that $(e_1\ e_2)\ \delta \Downarrow_i v$ therefore $\exists k < i-j$ (since $i < n$ therefore $i-j < n-j$) s.t $e_2\ \delta \Downarrow_k v_2$. This means we have

$(\theta, n-j-k, v_2) \in \lfloor \tau_2\ \sigma \rfloor_V$ (FU-PA2)

In order to prove (FU-PA0) from cg-prod we know that $i = j+k+1$ and $v = (v_1, v_2)$ therefore from Definition 4.6 it suffices to prove

$(\theta, n-j-k-1, v_1) \in \lfloor \tau_1 \rfloor_V$ and $(\theta, n-j-k-1, v_2) \in \lfloor \tau_2\ \sigma \rfloor_V$

We get this from (FU-PA1) and Lemma 4.15 and from (FU-PA2) and Lemma 4.15

5. CG-fst:

$$\frac{\Gamma \vdash e' : (\tau_1 \times \tau_2)}{\Gamma \vdash \mathsf{fst}(e') : \tau_1}$$

Also given is $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \mathsf{fst}(e')\ \delta) \in \lfloor \tau_1\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.\mathsf{fst}(e')\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor \tau_1\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $\mathsf{fst}(e')\ \delta \Downarrow_i v$

<u>It suffices to prove</u>

$(\theta, n - i, v) \in \lfloor \tau_1\ \sigma \rfloor_V$ (FU-F0)

<u>IH1</u>:

$\forall j < n.e'\ \delta \Downarrow_j (v_1, v_2) \implies (\theta, n - j, (v_1, v_2)) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V$

Since we know that $\mathsf{fst}(e')\ \delta \Downarrow_i v$ therefore $\exists j < i < n$ s.t $e'\ \delta \Downarrow_j (v_1, v_2)$. This means we have

$(\theta, n - j, (v_1, v_2)) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V$

From Definition 4.6 we know the following holds

$(\theta, n - j, v_1) \in \lfloor \tau_1\ \sigma \rfloor_V$ and $(\theta, n - j, v_2) \in \lfloor \tau_2\ \sigma \rfloor_V$ (FU-F1)

From cg-fst we know that $v = v_1$ and $i = j + 1$. Therefore from (FU-F0), we are required to prove

$(\theta, n - j - 1, v_1) \in \lfloor \tau_1\ \sigma \rfloor_V$

We get this from (FU-F1) and Lemma 4.15

6. CG-snd:

   Symmetric reasoning as in the CG-fst case above

7. CG-inl:

$$\frac{\Gamma \vdash e' : \tau_1}{\Gamma \vdash \mathsf{inl}(e') : (\tau_1 + \tau_2)}$$

Also given is $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \mathsf{inl}(e')\ \delta) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.\mathsf{inl}(e')\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $\mathsf{inl}(e')\ \delta \Downarrow_i v$

<u>It suffices to prove</u>

$(\theta, n-i, v) \in \lfloor(\tau_1 + \tau_2)\ \sigma\rfloor_V$ (FU-LE0)

<u>IH1</u>:

$\forall j < n.e'\ \delta \Downarrow_j v_1 \implies (\theta, n-j, v_1) \in \lfloor\tau_1\ \sigma\rfloor_V$

Since we know that $\mathsf{inl}(e')\ \delta \Downarrow_i v$ therefore $\exists j < i < n$ s.t $e'\ \delta \Downarrow_j v_1$. This means we have

$(\theta, n-j, v_1) \in \lfloor\tau_1\ \sigma\rfloor_V$ (FU-LE1)

From cg-inl we know that $v = v_1$ and $i = j+1$. Therefore from (FU-LE0) w we are required to prove

$(\theta, n-j-1, v_1) \in \lfloor(\tau_1 + \tau_2)\ \sigma\rfloor_V$

From Definition 4.6 it suffices to prove

$(\theta, n-j-1, v_1) \in \lfloor\tau_1\ \sigma\rfloor_V$

We get this from (FU-LE1) and Lemma 4.15

8. CG-inr:

   Symmetric reasoning as in the CG-inl case above

9. CG-case:

$$\frac{\Gamma \vdash e_c : (\tau_1 + \tau_2) \qquad \Gamma, x : \tau_1 \vdash e_1 : \tau \qquad \Gamma, y : \tau_2 \vdash e_2 : \tau}{\Gamma \vdash \mathsf{case}(e, x.e_1, y.e_2) : \tau}$$

Also given is $(\theta, n, \delta) \in \lfloor\Gamma\ \sigma\rfloor_V$

To prove: $(\theta, n, (\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta) \in \lfloor\tau\ \sigma\rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.(\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor\tau\ \sigma\rfloor_V$

This means that given some $i < n$ s.t $(\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta \Downarrow_i v$

<u>It suffices to prove</u>

$(\theta, n-i, v) \in \lfloor\tau\ \sigma\rfloor_V$ (FU-C0)

<u>IH1</u>:

$\forall j < n.e_c\ \delta \Downarrow_j v_c \implies (\theta, n-j, v_1) \in \lfloor(\tau_1 + \tau_2)\ \sigma\rfloor_V$

Since we know that $(\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta \Downarrow_i v$ therefore $\exists j < i < n$ s.t $e_c\ \delta \Downarrow_j v_c$. This means we have

$(\theta, n-j, v_c) \in \lfloor(\tau_1 + \tau_2)\ \sigma\rfloor_V$ (FU-C1)

2 cases arise:

(a) $v_c = \mathsf{inl}(v_l)$:
<u>IH2</u>:
$\forall k < (n-j).e_1\ \delta \cup \{x \mapsto v_l\} \Downarrow_k v_1 \implies (\theta, n-j-k, v_1) \in \lfloor \tau\ \sigma \rfloor_V$

Since we know that $(\mathsf{case}\ e_c, x.e_1, y.e_2)\ \delta \Downarrow_i v$ therefore $\exists k < i-j$ (since $i < n$ therefore $i-j < n-j$) s.t $e_1\ \delta \cup \{x \mapsto v_l\} \Downarrow_k v_1$. This means we have
$(\theta, n-j-k, v_1) \in \lfloor \tau\ \sigma \rfloor_V$ (FU-C2)

From cg-case1 we know that $i = j+k+1$ and $v = v_1$. Therefore from (FU-C0) it suffices to prove
$(\theta, n-j-k-1, v_1) \in \lfloor \tau\ \sigma \rfloor_V$

We get this from (FU-C2) and Lemma 4.15

(b) $v_c = \mathsf{inr}(v_r)$:
Symmetric reasoning as in the previous case

10. CG-FI:

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash e' : \tau}{\Sigma; \Gamma \vdash \Lambda e' : \forall \alpha.\tau}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \Lambda e'\ \delta) \in \lfloor (\forall \alpha.(\ell_e, \tau))\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.\Lambda e'\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $\lambda x.e'\ \delta \Downarrow_i v$

(from CG-Sem-val we know that $v = \Lambda e'\ \delta$ and $i = 0$)

<u>It suffices to prove</u>

$(\theta, n, \Lambda e'\ \delta) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V$ (FU-FI0)

From Definition 4.6 it further suffices to prove

$\forall \theta'.\theta \sqsubseteq \theta', j < n.\forall \ell' \in \mathcal{L}.(\theta', j, e'\ \delta) \in \lfloor \tau[\ell'/\alpha] \rfloor_E$

This means given some $\theta', j, \ell' \in \mathcal{L}$ s.t $\theta' \sqsupseteq \theta$, $j < n$ (FU-FI1)

<u>We are required to prove</u>

$(\theta', j, (e'\ \delta)) \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_E$ (FU-FI2)

Since $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$ therefore from Lemma 4.17 we know that $(\theta, j, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$ where $j < n$ (from FU-L1)

<u>IH</u>: $(\theta', j, e'\ \delta) \in \lfloor \tau\ \sigma \cup \{\alpha \mapsto \ell'\} \rfloor_E$

(FU-FI2) is obtained directly from IH

11. CG-CI:

$$\frac{\Sigma; \Psi, c; \Gamma \vdash e' : \tau}{\Sigma; \Gamma \vdash \nu\ e' : c \Rightarrow \tau}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \nu e'\ \delta) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.\nu e'\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $\nu e'\ \delta \Downarrow_i v$

(from CG-Sem-val we know that $v = \nu e'\ \delta$ and $i = 0$)

<u>It suffices to prove</u>

$(\theta, n, \nu e'\ \delta) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_V$ (FU-CI0)

From Definition 4.6 it further suffices to prove

$\mathcal{L} \models c \implies \forall \theta'.\theta \sqsubseteq \theta', j < n.(\theta', j, e'\ \delta) \in \lfloor \tau \rfloor_E$

This means given $\mathcal{L} \models c$ and some θ', j s.t $\theta' \sqsupseteq \theta$, $j < n$ (FU-CI1)

<u>We are required to prove</u>

$(\theta', j, (e'\ \delta)) \in \lfloor \tau\ \sigma \rfloor_E$ (FU-CI2)

Since $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$ therefore from Lemma 4.17 we know that $(\theta, j, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$ where $j < n$ (from FU-L1). Also we know that $\mathcal{L} \models c\ \sigma$ therefore $\mathcal{L} \models (\Sigma \cup \{c\})\ \sigma$

<u>IH</u>: $(\theta', j, e'\ \delta) \in \lfloor \tau\ \sigma \rfloor_E$

(FU-CI2) is obtained directly from IH

12. CG-FE:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \forall \alpha.\tau \qquad \mathrm{FV}(\ell) \in \Sigma}{\Sigma; \Psi; \Gamma \vdash e'\ [] : \tau[\ell/\alpha]}$$

Also given is $\mathcal{L} \models \Psi\ \sigma \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, e'[]\ \delta) \in \lfloor \tau[\ell/\alpha]\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.e'[]\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor \tau[\ell/\alpha]\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $e'[]\ \delta \Downarrow_i v$

<u>It suffices to prove</u>

$(\theta, n-i, v) \in \lfloor \tau[\ell/\alpha]\ \sigma \rfloor_V$ (FU-FE0)

<u>IH</u>: $(\theta, n, e'\ \delta) \in \lfloor \forall \alpha.\tau \rfloor_E$

From Definition 4.7 we know that

$\forall h_1 < n.e'\ \delta \Downarrow_{h_1} \Lambda e_{h1} \implies (\theta, n-h_1, \Lambda e_{h1}) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V$

Since $e'[]\ \delta$ reduces therefore we know that $\exists h_1 < i < n$ such that $e'\ \delta \Downarrow_{h_1} \Lambda e_i$

Therefore we know that $(\theta, n-h_1, \Lambda e_{h1}) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V$

From Definition 4.6 we know that

$\forall \theta'' \sqsupseteq \theta, x < (n - h_1), \ell_h \in \mathcal{L}.(\theta'', x, e_{h1}) \in \lfloor (\tau[\ell_h/\alpha]) \ \sigma \rfloor_E$

Instantiating θ'' with θ, x with $n - h_1 - 1$ and ℓ_h with ℓ. So, we get
$(\theta, n - h_1 - 1, e_{h1}) \in \lfloor (\tau[\ell/\alpha]) \ \sigma \rfloor_E$

From Definition 4.7 we know that the following holds
$\forall h_2 < n - h_1 - 1.e_{h1} \ \delta \Downarrow_{h_2} v \implies (\theta, n - h_1 - 1 - h_2, v) \in \lfloor (\tau[\ell/\alpha]) \ \sigma \rfloor_V$
Since $e'[] \ \delta$ reduces in i steps therefore from CG-Sem-FE we know that $(i = h_1 + h_2 + 1)$ and since we know that $i < n$ therefore we have $h_2 < n - h_1 - 1$ such that $e_{h1} \ \delta \Downarrow_{h_2} v$. Therefore we get
$(\theta, n - h_1 - 1 - h_2, v) \in \lfloor (\tau[\ell/\alpha]) \ \sigma \rfloor_V$
Since $i = h_1 + h_2 + 1$ therefore we get
$(\theta, n - i, v) \in \lfloor (\tau[\ell/\alpha]) \ \sigma \rfloor_V$

13. CG-CE:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : c \Rightarrow \tau \qquad \Sigma; \Psi \vdash c}{\Sigma; \Psi; \Gamma \vdash e' \bullet : \tau}$$

Also given is $\mathcal{L} \models \Psi \ \sigma \ \wedge$ and $(\theta, n, \delta) \in \lfloor \Gamma \ \sigma \rfloor_V$
To prove: $(\theta, n, e' \bullet \ \delta) \in \lfloor \tau \ \sigma \rfloor_E$
This means that from Definition 4.7 we need to prove
$\forall i < n.e' \bullet \ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor \tau \ \sigma \rfloor_V$
This means that given some $i < n$ s.t $e' \bullet \ \delta \Downarrow_i v$
<u>It suffices to prove</u>
$(\theta, n - i, v) \in \lfloor \tau \ \sigma \rfloor_V$ (FU-CE0)

<u>IH</u>: $(\theta, n, e' \ \delta) \in \lfloor c \Rightarrow \tau \ \sigma \rfloor_E$

From Definition 4.7 we know that
$\forall h_1 < n.e' \ \delta \Downarrow_{h_1} \nu e_{h1} \implies (\theta, n - h_1, \nu e_{h1}) \in \lfloor c \Rightarrow \tau \ \sigma \rfloor_V$

Since $e' \bullet \ \delta$ reduces therefore we know that $\exists h_1 < i < n$ such that $e' \ \delta \Downarrow_{h_1} \nu e_{h_1}$

Therefore we know that $(\theta, n - h_1, \nu e_{h1}) \in \lfloor c \Rightarrow \tau \ \sigma \rfloor_V$

From Definition 4.6 we know that
$\mathcal{L} \models c \ \sigma \implies \forall \theta'' \sqsupseteq \theta, x < (n - h_1).(\theta'', x, e_{h1}) \in \lfloor \tau \ \sigma \rfloor_E$

Since we know that $\mathcal{L} \models c \ \sigma$ and then we instantiate θ'' with θ, x with $n - h_1 - 1$. So, we get
$(\theta, n - h_1 - 1, e_{h1}) \in \lfloor \tau \ \sigma \rfloor_E$

From Definition 4.7 we know that the following holds
$\forall h_2 < n - h_1 - 1.e_{h1} \ \delta \Downarrow_{h_2} v \implies (\theta, n - h_1 - 1 - h_2, v) \in \lfloor \tau \ \sigma \rfloor_V$

Since $e' \bullet\ \delta$ reduces in i steps therefore from CG-Sem-CE we know that $(i = h_1 + h_2 + 1)$ and since we know that $i < n$ therefore we have $h_2 < n - h_1 - 1$ such that $e_{h1}\ \delta \Downarrow_{h_2} v$. Therefore we get

$(\theta, n - h_1 - 1 - h_2, v) \in \lfloor \tau\ \sigma \rfloor_V$

Since we know that $i = h_1 + h_2 + 1$ therefore we get

$(\theta, n - i, v) \in \lfloor \tau\ \sigma \rfloor_V$

14. CG-ref:

$$\frac{\Gamma \vdash e' : \mathsf{Labeled}\ \ell'\ \tau \qquad \mathcal{L} \vdash \ell \sqsubseteq \ell'}{\Gamma \vdash \mathsf{new}\ (e') : \mathbb{C}\ \ell\ \bot\ (\mathsf{ref}\ \ell'\ \tau)}$$

Also given is $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \mathsf{new}\ (e')\ \delta) \in \lfloor \mathbb{C}\ \ell\ \bot\ (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.\mathsf{new}\ (e')\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor \mathbb{C}\ \ell\ \bot\ (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $\mathsf{new}\ (e')\ \delta \Downarrow_i v$

(from cg-val we know that $v = \mathsf{new}\ (e')\ \delta$ and $i = 0$)

<u>It suffices to prove</u>

$(\theta, n, \mathsf{new}\ (e')\ \delta) \in \lfloor \mathbb{C}\ \ell\ \bot\ (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V$

From Definition 4.6 it suffices to prove

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, \mathsf{new}\ (e')\ \delta) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor (\mathsf{ref}\ \ell'\ \tau\ \sigma) \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$

This means given some $k \leq n, \theta_e \sqsupseteq \theta, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, \mathsf{new}\ (e')\ \delta) \Downarrow_j^f (H', v') \wedge j < k$. Also from cg-ref we know that $v' = a$

It suffices to prove

$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, a) \in \lfloor (\mathsf{ref}\ \ell'\ \tau) \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$ (FU-R0)

<u>IH</u>:

$(\theta_e, k, e'\ \delta) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_E$

From Definition 4.7 this means we have

$\forall l < k.e'\ \delta \Downarrow_l v_h \implies (\theta_e, n - l, v_h) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V$

Since we know that $(H, \mathsf{new}\ (e')) \Downarrow_j^f (H', a)$ therefore from cg-ref we know that

$\exists l < j < k$ s.t $e'\ \delta \Downarrow_l v_h$

Therefore we have

$(\theta_e, n-l, v_h) \in \lfloor(\mathsf{Labeled}\ \ell'\ \tau)\ \sigma\rfloor_V$ (FU-R2)

In order to prove (FU-R0) we choose θ' as $\theta_n = \theta_e \cup \{a \mapsto \mathsf{Labeled}\ \ell'\ \tau\}$

Now we need to prove:

(a) $(k-j, H') \triangleright \theta_n$:
From Definition 4.8 it suffices to prove that
$dom(\theta_n) \subseteq dom(H') \wedge \forall a \in dom(\theta_n).(\theta_n, (k-j)-1, H'(a)) \in \lfloor \theta_n(a) \rfloor_V$

- $dom(\theta_n) \subseteq dom(H')$:
  We know that $dom(H') = dom(H) \cup \{a\}$
  We know that $dom(\theta_n) = dom(\theta_e) \cup \{a\}$
  And $(k, H) \triangleright \theta_e$ therefore from Definition 4.8 we know that $dom(\theta_e) \subseteq dom(H)$
  So we are done
- $\forall a \in dom(\theta_n).(\theta_n, (k-j)-1, H'(a)) \in \lfloor \theta_n(a) \rfloor_V$:
  Since from (FU-R2) we know that $(\theta_h, n-l, v_h) \in \lfloor(\mathsf{Labeled}\ \ell'\ \tau)\ \sigma\rfloor_V$
  Since $\theta_h \sqsubseteq \theta_n$ and $k-j-1 < n-l$ (since $k < n$ and $l < j$) therefore from Lemma 4.15 we know that $(\theta_n, k-j-1, v_h) \in \lfloor(\mathsf{Labeled}\ \ell'\ \tau)\ \sigma\rfloor_V$

(b) $(\theta_n, k-j-1, a) \in \lfloor(\mathsf{ref}\ \ell'\ \tau)\ \sigma\rfloor_V$:
From Definition 4.6 it suffices to prove that $\theta_n(a) = \mathsf{Labeled}\ \ell'\ \tau$
We get this by construction of θ_n

(c) $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell')$:
Holds vacuously

(d) $(\forall a \in dom(\theta_n) \backslash dom(\theta_e).\theta_n(a) \searrow \ell)$:
From CG-ref we know that $\ell \sqsubseteq \ell'$

15. CG-deref:

$$\frac{\Gamma \vdash e' : \mathsf{ref}\ \ell\ \tau}{\Gamma \vdash !e' : \mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau)}$$

Also given is $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, (!e')\ \delta) \in \lfloor \mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.!(e')\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor \mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V$

(From cg-val we know that $v = !e'\ \delta$ and $i = 0$)

This means that given some $i < n$ s.t $!e'\ \delta \Downarrow_i !e'\ \delta$

<u>It suffices to prove</u>

$(\theta, n, !e'\ \delta) \in \lfloor \mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V$

From Definition 4.6 it suffices to prove

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, (!e'\ \delta)) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell''.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau' \wedge \top \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \top)$

This means given some $k \leq n, \theta_e \sqsupseteq \theta, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, (!e'\ \delta)) \Downarrow_j^f (H', v') \wedge j < k$.

It suffices to prove

$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell''.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau' \wedge \top \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \top)$ (FU-D0)

<u>IH</u>:

$(\theta_e, k, e'\ \delta) \in \lfloor(\mathsf{ref}\ \ell\ \tau)\ \sigma\rfloor_E$

From Definition 4.7 this means we have

$\forall l < k.e'\ \delta \Downarrow_l v_h \implies (\theta_e, k-l, v_h) \in \lfloor(\mathsf{ref}\ \ell\ \tau)\ \sigma\rfloor_V$

Since we know that $(H, !(e')) \Downarrow_j^f (H', a)$ therefore from cg-deref we know that

$\exists l < j < k$ s.t $e'\ \delta \Downarrow_l v_h,\ v_h = a$

Therefore we have

$(\theta_e, k-l, a) \in \lfloor(\mathsf{ref}\ \ell\ \tau)\ \sigma\rfloor_V$ (FU-D1)

In order to prove (FU-D0) we choose θ' as θ_e

Now we need to prove:

(a) $(k-j, H') \triangleright \theta_e$:
From Definition 4.8 it suffices to prove that
$dom(\theta_e) \subseteq dom(H') \wedge \forall a \in dom(\theta_e).(\theta_e, (k-j)-1, H'(a)) \in \lfloor\theta_e(a)\rfloor_V$
- $dom(\theta_e) \subseteq dom(H')$:
And $(k, H) \triangleright \theta_e$ therefore from Definition 4.8 we know that $dom(\theta_e) \subseteq dom(H)$
And since $H' = H$ (from cg-deref) so we are done
- $\forall a \in dom(\theta_e).(\theta_e, (k-j)-1, H'(a)) \in \lfloor\theta_e(a)\rfloor_V$:
Since we know that $(k, H) \triangleright \theta_e$ therefore from Definition 4.8 we know that
$\forall a \in dom(\theta_e).(\theta_e, k-1, H(a)) \in \lfloor\theta_e(a)\rfloor_V$
Since $H' = H$ and from Lemma 4.15 we get
$\forall a \in dom(\theta_e).(\theta_e, (k-j)-1, H'(a)) \in \lfloor\theta_e(a)\rfloor_V$

(b) $(\theta_e, k-j, v') \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_V$:
From cg-deref we know that $H = H'$ and $v' = H(a)$
From (FU-D1) and Definition 4.6 we know that $\theta_e(a) = \mathsf{Labeled}\ \ell\ \tau$
Since we know that $(k, H) \triangleright \theta_e$ therefore from Definition 4.8 we know that
$\forall a \in dom(\theta_e).(\theta_e, k-1, H(a)) \in \lfloor\theta_e(a)\rfloor_V$
Since from cg-deref we know that $j \geq 1$. Therefore from Lemma 4.15 we get $(\theta_e, k-j, H(a)) \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rfloor_V$

(c) $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \top \sqsubseteq \ell')$:
Holds vacuously

(d) $(\forall a \in dom(\theta_e) \backslash dom(\theta_e).\theta_e(a) \searrow \top)$:
Holds vacuously

16. CG-assign:

$$\frac{\Gamma \vdash e_1 : \mathsf{ref}\ \ell'\ \tau \qquad \Gamma \vdash e_2 : \mathsf{Labeled}\ \ell'\ \tau \qquad \mathcal{L} \vdash \ell \sqsubseteq \ell'}{\Gamma \vdash e_1 := e_2 : \mathbb{C}\ \ell\ \bot\ \mathsf{unit}}$$

Also given is $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, (e_1 := e_2)\ \delta) \in \lfloor (\mathbb{C}\ \ell\ \bot\ \mathsf{unit}) \rfloor_E^{pc}$

This means that from Definition 4.7 we need to prove

$\forall i < n.(e_1 := e_2)\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor (\mathbb{C}\ \ell\ \bot\ \mathsf{unit}) \rfloor_V$

This means that given some $i < n$ s.t $(e_1 := e_2)\ \delta \Downarrow_i v$.

<u>It suffices to prove</u>

$(\theta, n - i, ()) \in \lfloor (\mathbb{C}\ \ell\ \bot\ \mathsf{unit}) \rfloor_V$

From Definition 4.6 it suffices to prove

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, (e_1 := e_2)\ \delta) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor (\mathsf{ref}\ \ell'\ \tau) \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$

This means given some $k \leq n, \theta_e \sqsupseteq \theta, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, (e_1 := e_2)\ \delta) \Downarrow_j^f (H', v') \wedge j < k$. Also from cg-assign we know that $v' = ()$

It suffices to prove

$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, ()) \in \lfloor \mathsf{unit} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$ (FU-A0)

<u>IH1</u>:

$\forall l < k.e_1\ \delta \Downarrow_l v_1 \implies (\theta, k - l, a) \in \lfloor (\mathsf{ref}\ \ell'\ \tau) \rfloor_V$

Since we know that $(e_1 := e_2)\ \delta \Downarrow_j^f v$ therefore $\exists l < j < k$ s.t $e_1\ \delta \Downarrow_l a$. This means we have

$(\theta, k - l, a) \in \lfloor (\mathsf{ref}\ \ell'\ \tau) \rfloor_V$ (FU-A1)

<u>IH2</u>:

$\forall m < (k - l).e_2\ \delta \Downarrow_m v_2 \implies (\theta, k - l - m, v_2) \in \lfloor \mathsf{Labeled}\ \ell'\ \tau \rfloor_V$

Since we know that $(e_1 := e_2)\ \delta \Downarrow_j^f v$ therefore $\exists m < j - l$ (since $j < k$ therefore $j - l < k - l$) s.t $e_2\ \delta \Downarrow_k v_2$. This means we have

$(\theta, k - l - m, v_2) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau) \rfloor_V$ (FU-A2)

In order to prove (FU-A0) we choose θ' as θ_e

Now we need to prove:

(a) $(k-j, H') \triangleright \theta_e$:
From Definition 4.8 it suffices to prove that
$dom(\theta_e) \subseteq dom(H') \wedge \forall a \in dom(\theta_e).(\theta_e, (k-j)-1, H'(a)) \in \lfloor \theta_e(a) \rfloor_V$

- $dom(\theta_e) \subseteq dom(H')$:
We know that $dom(H') = dom(H)$
And $(k, H) \triangleright \theta_e$ therefore from Definition 4.8 we know that $dom(\theta_e) \subseteq dom(H)$
So we are done
- $\forall a \in dom(\theta_e).(\theta_e, (k-j)-1, H'(a)) \in \lfloor \theta_e(a) \rfloor_V$:
$\forall a \in dom(\theta_e)$.
  i. $H(a) = H'(a)$:
  Since $(k, H) \triangleright \theta_e$ therefore from Definition 4.8 we know that
  $(\theta_e, k-1, H(a)) \in \lfloor \theta_e(a) \rfloor_V$
  Therefore from Lemma 4.15 we get
  $(\theta_e, k-1-j, H(a)) \in \lfloor \theta_e(a) \rfloor_V$
  ii. $H(a) \neq H'(a)$:
  From cg-assign we know that $H'(a) = v_2$
  From (FU-A1) we know that $\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau$
  Also we know that $j = l + m + 1$
  Since from (FU-A2) we know that
  $(\theta, k-l-m, v_2) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau) \rfloor_V$
  Therefore we get
  $(\theta, k-j+1, v_2) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau) \rfloor_V$
  Therefore from Lemma 4.15 we get
  $(\theta, k-j-1, v_2) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau) \rfloor_V$

(b) $(\theta_e, k-j-1, ()) \in \lfloor \mathsf{unit} \rfloor_V$:
From Definition 4.6

(c) $(\forall a. H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell \sqsubseteq \ell')$:
From CG-assign we know that $\ell \sqsubseteq \ell'$

(d) $(\forall a \in dom(\theta_e) \backslash dom(\theta_e).\theta_e(a) \searrow \ell)$:
Holds vacuously

17. CG-label:

$$\frac{\Gamma \vdash e' : \tau}{\Gamma \vdash \mathsf{Lb}(e') : \mathsf{Labeled}\ \ell\ \tau}$$

Also given is $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \mathsf{Lb}(e')\ \delta) \in \lfloor \mathsf{Labeled}\ \ell\ \tau\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.\mathsf{Lb}(e')\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor \mathsf{Labeled}\ \ell\ \tau\ \sigma \rfloor_V$

This means we are given some $i < n$ s.t $\mathsf{Lb}(e')\ \delta \Downarrow_i v$ and we are required to prove $(\theta, n-i, v) \in \lfloor \mathsf{Labeled}\ \ell\ \tau\ \sigma \rfloor_V$

Let $v = \mathsf{Lb}(v_i)$. This means from Definition 4.6 we are required to prove $(\theta, n-i, v_i) \in \lfloor \tau\ \sigma \rfloor_V$

IH: $(\theta, n, e' \; \delta) \in \lfloor \tau \; \sigma \rfloor_E$

This means from Definition 4.7 we have
$\forall j < n.e' \; \delta \Downarrow_j v_i \implies (\theta, n-j, v_i) \in \lfloor \tau \rfloor_V$

Since we know that $\mathsf{Lb}(e') \; \delta \Downarrow_i v$ therefore $\exists j < i < n$ s.t $e' \; \delta \Downarrow_j v_i$
Therefore we have $(\theta, n-j, v_i) \in \lfloor \tau \; \sigma \rfloor_V$

From cg-label we know that $i = j + 1$ therefore from Lemma 4.15 we have
$(\theta, n-i, v_i) \in \lfloor \tau \; \sigma \rfloor_V$

18. CG-unlabel:

$$\frac{\Gamma \vdash e' : \mathsf{Labeled} \; \ell \; \tau}{\Gamma \vdash \mathsf{unlabel}(e') : \mathbb{C} \; \top \; \ell \; \tau}$$

Also given is $(\theta, n, \delta) \in \lfloor \Gamma \; \sigma \rfloor_V$
To prove: $(\theta, n, \mathsf{unlabel}(e') \; \delta) \in \lfloor (\mathbb{C} \; \top \; \ell \; \tau) \; \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove
$\forall i < n.\mathsf{unlabel}(e') \; \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor (\mathbb{C} \; \top \; \ell \; \tau) \; \sigma \rfloor_V$
This means that given some $i < n$ s.t $\mathsf{unlabel}(e') \; \delta \Downarrow_i v$
(from cg-val we know that $v = \mathsf{unlabel}(e') \; \delta$ and $i = 0$)
It suffices to prove
$(\theta, n, \mathsf{unlabel}(e') \; \delta) \in \lfloor (\mathbb{C} \; \top \; \ell \; \tau) \; \sigma \rfloor_V$

From Definition 4.6 it suffices to prove
$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \rhd \theta_e \wedge (H, \mathsf{unlabel}(e') \; \delta) \Downarrow^f_j (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \rhd \theta' \wedge (\theta', k-j, v') \in \lfloor \tau \; \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled} \; \ell' \; \tau' \wedge \top \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \top)$

This means given some $k \leq n, \theta_e \sqsupseteq \theta, H, j$ s.t $(k, H) \rhd \theta_e \wedge (H, \mathsf{unlabel}(e') \; \delta) \Downarrow^f_j (H', v') \wedge j < k$. Also from cg-unlabel we know that $H' = H$
It suffices to prove
$\exists \theta' \sqsupseteq \theta_e.(k-j, H) \rhd \theta' \wedge (\theta', k-j, v') \in \lfloor \tau \; \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled} \; \ell' \; \tau' \wedge \top \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \top)$ (FU-U0)

IH:
$(\theta_e, k, e' \; \delta) \in \lfloor (\mathsf{Labeled} \; \ell \; \tau) \; \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove
$\forall h_1 < k.e' \; \delta \Downarrow_{h_1} v_h \implies (\theta_e, k - h_1, v_h) \in \lfloor (\mathsf{Labeled} \; \ell \; \tau) \; \sigma \rfloor_V$

Since we know that $(H, \mathsf{unlabel}(e')) \Downarrow^f_j (H, v')$ therefore from cg-unlabel we know that

$\exists h_1 < j < k$ s.t $e' \ \delta \Downarrow_{h_1} \mathsf{Lb}\, v'$

This means we have

$(\theta_e, k - h_1, \mathsf{Lb}\, v') \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V$

This means from Definition 4.6 we have

$(\theta_e, k - h_1, v') \in \lfloor \tau\ \sigma \rfloor_V$ (FU-U1)

In order to prove (FU-U0) we choose θ' as θ_e. And we a required to prove:

(a) $(k - j, H) \triangleright \theta_e$:
Since have $(k, H) \triangleright \theta_e$ therefore from Lemma 4.19 we get $(k - j, H) \triangleright \theta_e$

(b) $(\theta', k - j, v') \in \lfloor \tau\ \sigma \rfloor_V$:
Since from (FU-U1) we know that $(\theta_e, k - h_1, v') \in \lfloor \tau\ \sigma \rfloor_V$
And since $j = h_1 + 1$, therefore from Lemma 4.15 we get $(\theta_e, k - j, v') \in \lfloor \tau\ \sigma \rfloor_V$

(c) $(\forall a. H(a) \neq H'(a) \implies \exists \ell'. \theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \top \sqsubseteq \ell')$:
Holds vacuously

(d) $(\forall a \in dom(\theta') \backslash dom(\theta_e). \theta'(a) \searrow \top)$:
Holds vacuously

19. CG-ret:

$$\frac{\Gamma \vdash e' : \tau}{\Gamma \vdash \mathsf{ret}(e') : \mathbb{C}\ \ell\ \ell'\ \tau}$$

Also given is $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \mathsf{ret}(e')\ \delta) \in \lfloor \mathbb{C}\ \ell\ \ell'\ \tau\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n. \mathsf{ret}(e')\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor \mathbb{C}\ \ell\ \ell'\ \tau\ \sigma \rfloor_V$

This means we are given some $i < n$ s.t $\mathsf{ret}(e')\ \delta \Downarrow_i v$ and we are required to prove

$(\theta, n - i, v) \in \lfloor \mathbb{C}\ \ell\ \ell'\ \tau\ \sigma \rfloor_V$

(from cg-val we know that $v = \mathsf{ret}(e')\ \delta$ and $i = 0$)

<u>It suffices to prove</u>

$(\theta, n, \mathsf{ret}(e')\ \delta) \in \lfloor \mathbb{C}\ \ell\ \ell'\ \tau\ \sigma \rfloor_V$

From Definition 4.6 it suffices to prove

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, \mathsf{ret}(e')\ \delta) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a. H(a) \neq H'(a) \implies \exists \ell''. \theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau' \wedge \ell \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e). \theta'(a) \searrow \ell)$

This means given some $k \leq n, \theta_e \sqsupseteq \theta, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, \mathsf{ret}(e')\delta) \Downarrow_j^f (H', v') \wedge j < k$.
Also from cg-ret we know that $H' = H$

It suffices to prove

$\exists \theta' \sqsupseteq \theta_e.(k-j, H) \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell''.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau' \wedge \ell \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$ (FU-R0)

<u>IH</u>:

$(\theta_e, k, e'\ \delta) \in \lfloor \tau\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall h_1 < k.e'\ \delta \Downarrow_{h_1} v_h \implies (\theta_e, k-h_1, v_h) \in \lfloor \tau\ \sigma \rfloor_V$

Since we know that $(H, \mathsf{unlabel}(e')) \Downarrow_j^f (H, v')$ therefore from cg-ret we know that

$\exists h_1 < j < k$ s.t $e'\ \delta \Downarrow_{h_1} v'$

This means we have

$(\theta_e, k-h_1, v') \in \lfloor \tau\ \sigma \rfloor_V$ (FU-R1)

In order to prove (FU-U0) we choose θ' as θ_e. And we a required to prove:

(a) $(k-j, H) \triangleright \theta_e$:
Since have $(k, H) \triangleright \theta_e$ therefore from Lemma 4.19 we get $(k-j, H) \triangleright \theta_e$

(b) $(\theta', k-j, v') \in \lfloor \tau\ \sigma \rfloor_V$:
Since from (FU-R1) we know that $(\theta_e, k-h_1, v') \in \lfloor \tau\ \sigma \rfloor_V$
And since $j = h_1 + 1$, therefore from Lemma 4.15 we get $(\theta_e, k-j, v') \in \lfloor \tau\ \sigma \rfloor_V$

(c) $(\forall a.H(a) \neq H'(a) \implies \exists \ell''.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau' \wedge \ell \sqsubseteq \ell'')$:
Holds vacuously

(d) $(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$:
Holds vacuously

20. CG-bind:

$$\frac{\Gamma \vdash e_1 : \mathbb{C}\ \ell_1\ \ell_2\ \tau \qquad \Gamma, x:\tau \vdash e_2 : \mathbb{C}\ \ell_3\ \ell_4\ \tau' \qquad \ell \sqsubseteq \ell_1 \qquad \ell \sqsubseteq \ell_3 \qquad \ell_2 \sqsubseteq \ell_3 \qquad \ell_2 \sqsubseteq \ell_4 \qquad \ell_4 \sqsubseteq \ell'}{\Gamma \vdash \mathsf{bind}(e_1, x.e_2) : \mathbb{C}\ \ell\ \ell'\ \tau'}$$

Also given is $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \mathsf{bind}(e_1, x.e_2)\ \delta) \in \lfloor \mathbb{C}\ \ell\ \ell'\ \tau'\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.\mathsf{bind}(e_1, x.e_2)\ \delta \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor \mathbb{C}\ \ell\ \ell'\ \tau'\ \sigma \rfloor_V$

This means we are given some $i < n$ s.t $\mathsf{bind}(e_1, x.e_2)\ \delta \Downarrow_i v$ and we are required to prove

$(\theta, n-i, v) \in \lfloor \mathbb{C}\ \ell\ \ell'\ \tau'\ \sigma \rfloor_V$

(from cg-val we know that $v = \mathsf{bind}(e_1, x.e_2)\ \delta$ and $i = 0$)

Therefore we need to prove

$(\theta, n, v) \in \lfloor \mathbb{C}\ \ell\ \ell'\ \tau'\ \sigma \rfloor_V$

From Definition 4.6 it suffices to prove

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, \mathsf{bind}(e_1, x.e_2)\ \delta) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor \tau'\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau'' \wedge \ell \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$

This means we are given some $k \leq n, \theta_e \sqsupseteq \theta, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, \mathsf{bind}(e_1, x.e_2)\ \delta) \Downarrow_j^f (H', v') \wedge j < k$.

It suffices to prove

$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor \tau'\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau'' \wedge \ell \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$ (FU-B0)

IH1:

$(\theta_e, k, e_1\ \delta) \in \lfloor (\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall h_1 < k.e_1\ \delta \Downarrow_{h_1} v_1 \implies (\theta_e, k-h_1, v_1) \in \lfloor (\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma \rfloor_V$

Since we know that $(H, \mathsf{bind}(e_1, x.e_2)) \Downarrow_j^f (H_1, v_1)$ therefore from cg-bind we know that $\exists h_1 < j < k$ s.t $e_1\ \delta \Downarrow_{h_1} v_1$

This means we have

$(\theta_e, k-h_1, v_1) \in \lfloor (\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma \rfloor_V$

From Definition 4.6 we know that

$\forall k_{h1} \leq (k-h_1), \theta'_e \sqsupseteq \theta_e, H, J.(k_{h1}, H) \triangleright \theta'_e \wedge (H, v_1) \Downarrow_J^f (H', v'_{h1}) \wedge J < k_{h1} \implies$
$\exists \theta'' \sqsupseteq \theta'_e.(k_{h1}-J, H') \triangleright \theta'' \wedge (\theta'', k_{h1}-J, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell''.\theta'_e(a) = \mathsf{Labeled}\ \ell''\ \tau'' \wedge \ell_1 \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta'') \backslash dom(\theta'_e).\theta''(a) \searrow \ell_1)$

Instantiating k_{h1} with $k-h_1$, θ'_e with θ_e. Since we know that $(H, \mathsf{bind}(e_1, x.e_2)) \Downarrow_j^f (H_1, v_1)$ therefore $\exists J < j - h_1 < k - h_1$ s.t $(H, v_1) \Downarrow_J^f (H', v'_{h1})$. And since we already knwo that $(k, H) \triangleright \theta_e$ therefore from Lemma 4.19 we get $(k-h_1, H) \triangleright \theta_e$

This means we have

$\exists \theta'' \sqsupseteq \theta_e.(k_{h1}-J, H') \triangleright \theta'' \wedge (\theta'', k_{h1}-J, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell''.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau'' \wedge \ell_1 \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta'') \backslash dom(\theta_e).\theta''(a) \searrow \ell_1)$ (FU-B1)

IH2:

$(\theta'', k-h_1-J, e_2\ \delta \cup \{x \mapsto v'\}) \in \lfloor (\mathbb{C}\ \ell_3\ \ell_4\ \tau') \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall h_2 < k - h_1 - J.e_2\ \delta \cup \{x \mapsto v'\} \Downarrow_{h_2} v'' \implies (\theta'', k - h_1 - J - h_2, v'') \in \lfloor (\mathbb{C}\ \ell_3\ \ell_4\ \tau') \rfloor_V$

Since we know that $(H, \mathsf{bind}(e_1, x.e_2)) \Downarrow_j^f (H, v_1)$ therefore from cg-bind we know that $\exists h_2 < j - h_1 - J < k - h_1 - J$ s.t $e_2\ \delta \cup \{x \mapsto v'\} \Downarrow_{h_2} v''$

This means we have

$(\theta'', k - h_1 - J - h_2, v'') \in \lfloor (\mathbb{C}\ \ell_3\ \ell_4\ \tau') \rfloor_V$

From Definition 4.6 we know that

$\forall k_{h2} \leq (k - h_1 - J - h_2), \theta'_e \sqsupseteq \theta'', H, J'.(k_{h2}, H) \triangleright \theta'_e \wedge (H, v'') \Downarrow_{J'}^f (H'', v'_{h2}) \wedge J' < k_{h2} \implies$
$\exists \theta''' \sqsupseteq \theta'_e.(k_{h2} - J', H'') \triangleright \theta''' \wedge (\theta''', k_{h2} - J', v') \in \lfloor \tau' \rfloor_V \wedge$
$(\forall a.H(a) \neq H''(a) \implies \exists \ell''.\theta'_e(a) = \mathsf{Labeled}\ \ell''\ \tau'' \wedge \ell_3 \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta''') \backslash dom(\theta'_e).\theta'''(a) \searrow \ell_3)$

Since we know that $(H, \mathsf{bind}(e_1, x.e_2)) \Downarrow_j^f (H_1, v_1)$ therefore $\exists v_{h2}, i$ s.t $(v'' \Downarrow_i v_{h2})$. From cg-val we know that $v_{h2} = v''$ and $i = 0$. Instantiating k_{h2} with $k - h_1 - J - h_2$, θ'_e with θ'', H with H' (from FU-B1) and $\exists J' < j - h_1 - J - h_2 < k - h_1 - J - h_2$ s.t $(H', v_{h2}) \Downarrow_J^f (H'', v'_{h2})$. And since we already know that $(k - h_1, H') \triangleright \theta''$ therefore from Lemma 4.19 we get $(k - h_1 - J - h_2, H') \triangleright \theta''$

This means we have

$\exists \theta''' \sqsupseteq \theta'_e.(k_{h2} - J', H'') \triangleright \theta''' \wedge (\theta''', k_{h2} - J', v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H''(a) \implies \exists \ell''.\theta'_e(a) = \mathsf{Labeled}\ \ell''\ \tau' \wedge \ell_3 \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta''') \backslash dom(\theta'_e).\theta'''(a) \searrow \ell_3)$ (FU-B2)

We get (FU-B0) by choosing θ' as θ''' (from FU-B2)

21. CG-toLabeled:

$$\frac{\Gamma \vdash e' : \mathbb{C}\ \ell_1\ \ell_2\ \tau}{\Gamma \vdash \mathsf{toLabeled}(e') : \mathbb{C}\ \ell_1\ \bot\ (\mathsf{Labeled}\ \ell_2\ \tau)}$$

Also given is $(\theta, n, \delta) \in \lfloor \Gamma\ \sigma \rfloor_V$

To prove: $(\theta, n, \mathsf{toLabeled}(e')\ \delta) \in \lfloor (\mathbb{C}\ \ell_1\ \bot\ \mathsf{Labeled}\ \ell_2\ \tau)\ \sigma \rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall i < n.\mathsf{toLabeled}(e')\ \delta \Downarrow_i v \implies (\theta, n - i, v) \in \lfloor (\mathbb{C}\ \ell_1\ \bot\ \mathsf{Labeled}\ \ell_2\ \tau)\ \sigma \rfloor_V$

This means that given some $i < n$ s.t $\mathsf{toLabeled}(e')\ \delta \Downarrow_i v$

(from cg-val we know that $v = \mathsf{toLabeled}(e')\ \delta$ and $i = 0$)

<u>It suffices to prove</u>

$(\theta, n, \mathsf{toLabeled}(e')\ \delta) \in \lfloor (\mathbb{C}\ \ell_1\ \bot\ \mathsf{Labeled}\ \ell_2\ \tau)\ \sigma \rfloor_V$

From Definition 4.6 it suffices to prove

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, \mathsf{toLabeled}(e')\ \delta) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor (\mathsf{Labeled}\ \ell_2\ \tau) \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_1)$

And given some $k \leq n, \theta_e \sqsupseteq \theta, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, \mathsf{toLabeled}(e')\ \delta) \Downarrow_j^f (H', v') \wedge j < k$. Also from cg-tolabeled we know that $H' = H$

It suffices to prove

$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor(\mathsf{Labeled}\ \ell_2\ \tau)\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_1)$ (FU-TL0)

<u>IH</u>:

$(\theta_e, k, e'\ \delta) \in \lfloor(\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma\rfloor_E$

This means that from Definition 4.7 we need to prove

$\forall h_1 < k.e'\ \delta \Downarrow_{h_1} v_1 \implies (\theta, k - h_1, v_1) \in \lfloor(\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma\rfloor_V$

Since $H, \mathsf{toLabeled}(e') \Downarrow_j^f H', v'$ therefore from cg-tolabeled we know that $\exists h_1 < j < k$ s.t $e'\ \delta \Downarrow_{h_1} v_1$

Therefore we get $(\theta, k - h_1, v_1) \in \lfloor(\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma\rfloor_V$

From Definition 4.6 we know that

$\forall k_{h1} \leq (k - h_1), \theta'_e \sqsupseteq \theta_e, H_h, J.(k_{h1}, H_h) \triangleright \theta'_e \wedge (H_h, v_1) \Downarrow_J^f (H', v'_{h1}) \wedge J < k_{h1} \implies$
$\exists \theta'' \sqsupseteq \theta'_e.(k_{h1} - J, H') \triangleright \theta'' \wedge (\theta'', k_{h1} - J, v_1) \in \lfloor\tau\ \sigma\rfloor_V \wedge$
$(\forall a.H_h(a) \neq H'(a) \implies \exists \ell'.\theta'_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'') \backslash dom(\theta'_e).\theta''(a) \searrow \ell_1)$

Instantiating k_{h1} with $k - h_1$, H_h with H, θ'_e with θ_e. Since we know that $(H, \mathsf{toLabeled}(e')) \Downarrow_j^f (H', v_1)$ therefore $\exists J < j - h_1 < k - h_1$ s.t $(H, v_1) \Downarrow_J^f (H', v'_{h1})$. And since we already knwo that $(k, H) \triangleright \theta_e$ therefore from Lemma 4.19 we get $(k - h_1, H) \triangleright \theta_e$

This means we have

$\exists \theta'' \sqsupseteq \theta'_e.(k - h_1 - J, H') \triangleright \theta'' \wedge (\theta'', k - h1 - J, v_1) \in \lfloor\tau\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta'_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta'') \backslash dom(\theta'_e).\theta''(a) \searrow \ell_1)$ (FU-TL1)

In order to prove (FU-TL0) we choose θ' as θ''. Now we need to prove the following

(a) $(k - j, H') \triangleright \theta''$:
Since $(k - h_1 - J, H') \triangleright \theta''$ and $j = h_1 + J + 1$ therefore from Lemma 4.19 we get $(k - j, H') \triangleright \theta''$

(b) $(\theta'', k - j - 1, v') \in \lfloor(\mathsf{Labeled}\ \ell_o\ \tau)\rfloor_V$:
From cg-tolabeled we know that $v' = \mathsf{toLabeled}(v_1)$
From Definition 4.4 it suffices to prove that $(\theta'', k - j - 1, v_1) \in \lfloor\tau\ \sigma\rfloor_V$

We get this from (FU-TL1) and Lemma 4.15

(c) $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell')$:
Directly from (FU-TL1)

(d) $(\forall a \in dom(\theta_n) \backslash dom(\theta_e).\theta_n(a) \searrow \ell)$:
Directly from (FU-TL1)

□

Lemma 4.22 (Subtyping unary). *The following holds:*
$\forall \mathcal{L}, \tau, \tau'$.

1. $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor(\tau\ \sigma)\rfloor_V \subseteq \lfloor(\tau'\ \sigma)\rfloor_V$

2. $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor(\tau\ \sigma)\rfloor_E \subseteq \lfloor(\tau'\ \sigma)\rfloor_E$

Proof. Proof of Statement (1)
Proof by induction on $\tau <: \tau'$

1. CGsub-arrow:

   Given:

$$\frac{\mathcal{L} \vdash \tau_1' <: \tau_1 \qquad \mathcal{L} \vdash \tau_2 <: \tau_2'}{\mathcal{L} \vdash \tau_1 \to \tau_2 <: \tau_1' \to \tau_2'}$$

   To prove: $\lfloor((\tau_1 \to \tau_2)\ \sigma)\rfloor_V \subseteq \lfloor((\tau_1' \to \tau_2')\ \sigma)\rfloor_V$

   IH1: $\lfloor(\tau_1'\ \sigma)\rfloor_V \subseteq \lfloor(\tau_1\ \sigma)\rfloor_V$ (Statement (1))
   $\lfloor(\tau_2)\rfloor_E \subseteq \lfloor(\tau_2')\rfloor_E$ (Sub-A0, From Statement (2))
   It suffices to prove: $\forall(\theta, n, \lambda x.e_i) \in \lfloor((\tau_1 \to \tau_2)\ \sigma)\rfloor_V.\ (\theta, n, \lambda x.e_i) \in \lfloor((\tau_1' \to \tau_2')\ \sigma)\rfloor_V$

   This means that given some θ, n and $\lambda x.e_i$ s.t $(\theta, n, \lambda x.e_i) \in \lfloor((\tau_1 \to \tau_2)\ \sigma)\rfloor_V$
   Therefore from Definition 4.6 we are given:

$$\exists \theta_1.\theta \sqsubseteq \theta_1 \wedge \forall i < n.\forall v.(\theta_1, i, v) \in \lfloor\tau_1\ \sigma\rfloor_V \implies (\theta_1, i, e_i[v/x]) \in \lfloor\tau_2\ \sigma\rfloor_E \tag{95}$$

   And it suffices to prove: $(\theta, n, \lambda x.e_i) \in \lfloor((\tau_1' \to \tau_2')\ \sigma)\rfloor_V$

   Again from Definition 4.6, it suffices to prove:
   $\exists \theta_2.\theta \sqsubseteq \theta_2 \wedge \forall j < n.\forall v.(\theta_2, j, v) \in \lfloor\tau_1'\ \sigma\rfloor_V \implies (\theta_2, j, e_i[v/x]) \in \lfloor\tau_2'\ \sigma\rfloor_E$

   This means that given some $\theta_2, j < n, v$ s.t $\theta \sqsubseteq \theta_2$ and $(\theta_2, j, v) \in \lfloor\tau_1'\ \sigma\rfloor_V$
   And we are required to prove: $(\theta_2, j, e_i[v/x]) \in \lfloor\tau_2'\ \sigma\rfloor_E$

   Since $(\theta_2, j, v) \in \lfloor\tau_1'\ \sigma\rfloor_V$ therefore from IH1 we know that $(\theta_2, j, v) \in \lfloor\tau_1\ \sigma\rfloor_V$
   As a result from Equation 95 we know that
   $(\theta_2, j, e_i[v/x]) \in \lfloor\tau_2\ \sigma\rfloor_E$
   From (Sub-A0), we know that
   $(\theta_2, j, e_i[v/x]) \in \lfloor\tau_2'\ \sigma\rfloor_E$

2. CGsub-prod:

   Given:
$$\frac{\mathcal{L} \vdash \tau_1 <: \tau_1' \qquad \mathcal{L} \vdash \tau_2 <: \tau_2'}{\mathcal{L} \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}$$

   To prove: $\lfloor ((\tau_1 \times \tau_2)\ \sigma) \rfloor_V \subseteq \lfloor ((\tau_1' \times \tau_2')\ \sigma) \rfloor_V$

   IH1: $\lfloor (\tau_1\ \sigma) \rfloor_V \subseteq \lfloor (\tau_1'\ \sigma) \rfloor_V$ (Statement (1))

   IH2: $\lfloor (\tau_2\ \sigma) \rfloor_V \subseteq \lfloor (\tau_2'\ \sigma) \rfloor_V$ (Statement (1))

   It suffices to prove: $\forall (\theta, n, (v_1, v_2)) \in \lfloor ((\tau_1 \times \tau_2)\ \sigma) \rfloor_V.\ (\theta, n, (v_1, v_2)) \in \lfloor ((\tau_1' \times \tau_2')\ \sigma) \rfloor_V$

   This means that given some θ, n and $(v_1, v_2\ (\theta, (v_1, v_2)) \in \lfloor ((\tau_1 \times \tau_2)\ \sigma) \rfloor_V$

   Therefore from Definition 4.6 we are given:
$$(\theta, n, v_1) \in \lfloor \tau_1\ \sigma \rfloor_V \wedge (\theta, n, v_2) \in \lfloor \tau_2\ \sigma \rfloor_V \tag{96}$$

   And it suffices to prove: $(\theta, (v_1, v_2)) \in \lfloor ((\tau_1' \times \tau_2')\ \sigma) \rfloor_V$

   Again from Definition 4.6, it suffices to prove:
   $(\theta, n, v_1) \in \lfloor \tau_1'\ \sigma \rfloor_V \wedge (\theta, n, v_2) \in \lfloor \tau_2'\ \sigma \rfloor_V$

   Since from Equation 96 we know that $(\theta, n, v_1) \in \lfloor \tau_1\ \sigma \rfloor_V$ therefore from IH1 we have $(\theta, n, v_1) \in \lfloor \tau_1'\ \sigma \rfloor_V$

   Similarly since $(\theta, n, v_2) \in \lfloor \tau_2\ \sigma \rfloor_V$ from Equation 96 therefore from IH2 we have $(\theta, n, v_2) \in \lfloor \tau_2'\ \sigma \rfloor_V$

3. CGsub-sum:

   Given:
$$\frac{\mathcal{L} \vdash \tau_1 <: \tau_1' \qquad \mathcal{L} \vdash \tau_2 <: \tau_2'}{\mathcal{L} \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'}$$

   To prove: $\lfloor ((\tau_1 + \tau_2)\ \sigma) \rfloor_V \subseteq \lfloor ((\tau_1' + \tau_2')\ \sigma) \rfloor_V$

   IH1: $\lfloor (\tau_1\ \sigma) \rfloor_V \subseteq \lfloor (\tau_1'\ \sigma) \rfloor_V$ (Statement (1))

   IH2: $\lfloor (\tau_2\ \sigma) \rfloor_V \subseteq \lfloor (\tau_2'\ \sigma) \rfloor_V$ (Statement (1))

   It suffices to prove: $\forall (\theta, n, v_s) \in \lfloor ((\tau_1 + \tau_2)\ \sigma) \rfloor_V.\ (\theta, v_s) \in \lfloor ((\tau_1' + \tau_2')\ \sigma) \rfloor_V$

   This means that given: $(\theta, n, v_s) \in \lfloor ((\tau_1 + \tau_2)\ \sigma) \rfloor_V$

   And it suffices to prove: $(\theta, n, v_s) \in \lfloor ((\tau_1' + \tau_2')\ \sigma) \rfloor_V$

   2 cases arise

(a) $v_s = \mathsf{inl}\ v_i$:
From Definition 4.6 we are given:

$$(\theta, n, v_i) \in \lfloor \tau_1\ \sigma \rfloor_V \tag{97}$$

And we are required to prove that:
$(\theta, n, v_i) \in \lfloor \tau_1'\ \sigma \rfloor_V$
From Equation 97 and IH1 we know that
$(\theta, n, v_i) \in \lfloor \tau_1'\ \sigma \rfloor_V$

(b) $v_s = \mathsf{inr}\ v_i$:
From Definition 4.6 we are given:

$$(\theta, n, v_i) \in \lfloor \tau_2\ \sigma \rfloor_V \tag{98}$$

And we are required to prove that:
$(\theta, n, v_i) \in \lfloor \tau_2'\ \sigma \rfloor_V$
From Equation 98 and IH2 we know that
$(\theta, n, v_i) \in \lfloor \tau_2'\ \sigma \rfloor_V$

4. CGsub-forall:

Given:

$$\frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash \forall \alpha.\tau_1 <: \forall \alpha.\tau_2}$$

To prove: $\lfloor ((\forall \alpha.\tau_1)\ \sigma) \rfloor_V \subseteq \lfloor (\forall \alpha.\tau_2)\ \sigma \rfloor_V$

It suffices to prove: $\forall (\theta, n, \Lambda e_i) \in \lfloor ((\forall \alpha.\tau_1)\ \sigma) \rfloor_V .\ (\theta, n, \Lambda e_i) \in \lfloor ((\forall \alpha.\tau_2)\ \sigma) \rfloor_V$

This means that given: $(\theta, n, \Lambda e_i) \in \lfloor ((\forall \alpha.\tau_1)\ \sigma) \rfloor_V$
Therefore from Definition 4.6 we are given:

$$\exists \theta_1.\theta \sqsubseteq \theta_1 \wedge \forall i < n. \forall \ell' \in \mathcal{L} \implies (\theta_1, i, e_i) \in \lfloor \tau_1\ (\sigma \cup [\alpha \mapsto \ell']) \rfloor_E \tag{99}$$

And it suffices to prove: $(\theta, n, \Lambda e_i) \in \lfloor ((\forall \alpha.\tau_2)\ \sigma) \rfloor_V$

Again from Definition 4.6, it suffices to prove:
$\exists \theta_2.\theta \sqsubseteq \theta_2 \wedge \forall j < n. \forall \ell' \in \mathcal{L} \implies (\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma \cup [\alpha \mapsto \ell']) \rfloor_E$

This means that given some $\theta_2, j < n, \ell' \in \mathcal{L}$ s.t $\theta \sqsubseteq \theta_2$
And we are required to prove: $(\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma \cup [\alpha \mapsto \ell']) \rfloor_E$

Since we are given $\theta \sqsubseteq \theta_2 \wedge j < n \wedge \ell' \in \mathcal{L}$ therefore from Equation 99 we have
$(\theta_2, j, e_i) \in \lfloor \tau_1\ (\sigma \cup [\alpha \mapsto \ell']) \rfloor_E$

$\lfloor (\tau_1\ (\sigma \cup [\alpha \mapsto \ell'])) \rfloor_E \subseteq \lfloor (\tau_2\ (\sigma \cup [\alpha \mapsto \ell'])) \rfloor_E$ (Sub-F0, Statement (2))

From (Sub-F0), we know that
$(\theta_2, j, e_i) \in \lfloor \tau_2\ (\sigma \cup [\alpha \mapsto \ell']) \rfloor_E$

5. CGsub-constraint:

   Given:

$$\frac{\Sigma;\Psi \vdash c_2 \implies c_1 \qquad \Sigma;\Psi \vdash \tau_1 <: \tau_2}{\Sigma;\Psi \vdash c_1 \Rightarrow \tau_1 <: c_2 \Rightarrow \tau_2}$$

   To prove: $\lfloor((c_1 \Rightarrow \tau_1)\ \sigma)\rfloor_V \subseteq \lfloor((c_2 \Rightarrow \tau_2))\ \sigma\rfloor_V$

   It suffices to prove: $\forall(\theta, n, \nu e_i) \in \lfloor((c_1 \Rightarrow \tau_1)\ \sigma)\rfloor_V.\ (\theta, n, \nu e_i) \in \lfloor((c_2 \Rightarrow \tau_2)\ \sigma)\rfloor_V$

   This means that given: $(\theta, n, \nu e_i) \in \lfloor((c_1 \Rightarrow \tau_1)\ \sigma)\rfloor_V$
   Therefore from Definition 4.6 we are given:

$$\exists\theta_1.\theta \sqsubseteq \theta_1 \wedge \forall i < n.\mathcal{L} \models c_1\ \sigma \implies (\theta_1, i, e_i) \in \lfloor\tau_1\ (\sigma)\rfloor_E \tag{100}$$

   And it suffices to prove: $(\theta, n, \nu e_i) \in \lfloor((c_2 \Rightarrow \tau_2)\ \sigma)\rfloor_V$

   Again from Definition 4.6, it suffices to prove:
   $\exists\theta_2.\theta \sqsubseteq \theta_2 \wedge \forall j < n.\mathcal{L} \models c_2\ \sigma \implies (\theta_2, j, e_i) \in \lfloor\tau_2\ (\sigma)\rfloor_E$

   This means that given some θ_2, j s.t $\theta \sqsubseteq \theta_2 \wedge j < n \wedge \mathcal{L} \models c_2\ \sigma$
   And we are required to prove: $(\theta_2, j, e_i) \in \lfloor\tau_2\ (\sigma)\rfloor_E$

   Since we are given $\theta \sqsubseteq \theta_2 \wedge j < n \wedge \mathcal{L} \models c_2\ \sigma$ and $\mathcal{L} \models c_2\ \sigma \implies c_1\ \sigma$ therefore from Equation 100 we have
   $(\theta_2, j, e_i) \in \lfloor\tau_1\ (\sigma)\rfloor_E$

   $\lfloor(\tau_1\ \sigma)\rfloor_E \subseteq \lfloor(\tau_2\ \sigma)\rfloor_E$ (Sub-C0, Statement (2))

   From (Sub-C0), we know that
   $(\theta_2, j, e_i) \in \lfloor\tau_2\ (\sigma)\rfloor_E$

6. CGsub-label:

$$\frac{\mathcal{L} \vdash \tau <: \tau' \qquad \mathcal{L} \vdash \ell \sqsubseteq \ell'}{\mathcal{L} \vdash \mathsf{Labeled}\ \ell\ \tau <: \mathsf{Labeled}\ \ell'\ \tau'}$$

   To prove: $\lfloor((\mathsf{Labeled}\ \ell\ \tau))\rfloor_V \subseteq \lfloor((\mathsf{Labeled}\ \ell\ '\tau')\ \sigma)\rfloor_V$

   IH: $\lfloor(\tau\ \sigma)\rfloor_V \subseteq \lfloor(\tau'\ \sigma)\rfloor_V$ (Statement (1))

   It suffices to prove:
   $\forall(\theta, n, \mathsf{Lb}(v_i)) \in \lfloor((\mathsf{Labeled}\ \ell\ \tau)\ \sigma)\rfloor_V.\ (\theta, n, \mathsf{Lb}(v_i)) \in \lfloor((\mathsf{Labeled}\ \ell'\ \tau')\ \sigma)\rfloor_V$

   This means that given some θ, n and $\mathsf{Lb}(e_i)$ s.t $(\theta, n, \mathsf{Lb}(v_i)) \in \lfloor((\mathsf{Labeled}\ \ell\ \tau)\ \sigma)\rfloor_V$
   Therefore from Definition 4.6 we are given:
   $(\theta, n, v_i) \in \lfloor(\tau\ \sigma)\rfloor_V$ (SL)

And we are required to prove that

$(\theta, n, \mathsf{Lb}(v_i)) \in \lfloor((\mathsf{Labeled}\ \ell'\ \tau')\ \sigma)\rfloor_V$

From Definition 4.6 it suffices to prove

$(\theta, n, v_i) \in \lfloor(\tau'\ \sigma)\rfloor_V$

We get this directly from (SL) and IH

7. CGsub-CG:

$$\frac{\mathcal{L} \vdash \tau <: \tau' \qquad \mathcal{L} \vdash \ell'_i \sqsubseteq \ell_i \qquad \mathcal{L} \vdash \ell_o \sqsubseteq \ell'_o}{\mathcal{L} \vdash \mathbb{C}\ \ell_i\ \ell_o\ \tau <: \mathbb{C}\ \ell'_i\ \ell'_o\ \tau'}$$

To prove: $\lfloor((\mathbb{C}\ \ell_i\ \ell_o\ \tau))\rfloor_V \subseteq \lfloor((\mathbb{C}\ \ell'_i\ \ell'_o\ \tau')\ \sigma)\rfloor_V$

IH: $\lfloor(\tau\ \sigma)\rfloor_V \subseteq \lfloor(\tau'\ \sigma)\rfloor_V$ (Statement (1))

It suffices to prove:

$\forall(\theta, n, e) \in \lfloor((\mathbb{C}\ \ell_i\ \ell_o\ \tau)\ \sigma)\rfloor_V.\ (\theta, n, e) \in \lfloor((\mathbb{C}\ \ell'_i\ \ell'_o\ \tau')\ \sigma)\rfloor_V$

This means that given some θ, n and e s.t $(\theta, n, e) \in \lfloor((\mathbb{C}\ \ell_i\ \ell_o\ \tau)\ \sigma)\rfloor_V$

Therefore from Definition 4.6 we are given:

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, e) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i)$ (SC0)

And we are required to prove

$(\theta, n, e) \in \lfloor((\mathbb{C}\ \ell'_i\ \ell'_o\ \tau'))\rfloor_V$

So again from Definition 4.6 we need to prove

$\forall k \leq n, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, e) \Downarrow_j^f (H', v') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor \tau'\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell'_i \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell'_i)$

This means we are given some $k \leq n, \theta_e \sqsupseteq \theta, H, j < k$ s.t $(k, H) \triangleright \theta_e \wedge (H, e) \Downarrow_j^f (H', v')$ (SC1)

And we need to prove

$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor \tau'\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell'_i \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell'_i)$

We instantiate (SC0) with k, θ_e, H, j from (SC1) and we get

$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i)$

Since $\tau <: \tau'$ therefore from IH we get

$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v') \in \lfloor \tau' \; \sigma \rfloor_V$

And since $\ell_i' \sqsubseteq \ell_i$ therefore we also have
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i' \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i')$

8. CGsub-base:

   Trivial

Proof of Statement(2)
It suffice to prove that
$\forall (\theta, n, e) \in \lfloor (\tau \; \sigma) \rfloor_E.\ (\theta, n, e) \in \lfloor (\tau' \; \sigma) \rfloor_E$

This means that we are given $(\theta, n, e) \in \lfloor (\tau \; \sigma) \rfloor_E$
From Definition 4.7 it means we have
$\forall i < n.e \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor \tau \; \sigma \rfloor_V$ (Sub-E0)
And we need to prove
$(\theta, n, e) \in \lfloor (\tau' \; \sigma) \rfloor_E$

From Definition 4.7 we need to prove
$\forall i < n.e \Downarrow_i v \implies (\theta, n-i, v) \in \lfloor \tau' \; \sigma \rfloor_V$

This further means that given some $i < n$ s.t $e \Downarrow_i v$, it suffices to prove that
$(\theta, n-i, v) \in \lfloor \tau' \; \sigma \rfloor_V$

Instantiating (Sub-E0) with the given i we get $(\theta, n-i, v) \in \lfloor \tau \; \sigma \rfloor_V$

Finally from Statement(1) we get $(\theta, n-i, v) \in \lfloor \tau' \; \sigma \rfloor_V$

□

Lemma 4.23 (Binary interpretation of Γ implies Unary interpretation of Γ)**.** $\forall W, \gamma, \Gamma, n.$
$(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}} \implies \forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, \gamma \downarrow_i) \in \lfloor \Gamma \rfloor_V$

Proof. Given: $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$
To prove: $\forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, \gamma \downarrow_i) \in \lfloor \Gamma \rfloor_V$

From Definition 4.13 we know that we are given:
$dom(\Gamma) \subseteq dom(\gamma) \wedge \forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$
And we are required to prove:
$\forall i \in \{1, 2\}.\ \forall m.$
$dom(\Gamma) \subseteq dom(\gamma \downarrow_i) \wedge \forall x \in dom(\Gamma).(W.\theta_i, m, \gamma \downarrow_i (x)) \in \lfloor \Gamma(x) \rfloor_V$

Case $i = 1$
Given some m we need to show:

- $dom(\Gamma) \subseteq dom(\gamma \downarrow_i)$:

  $dom(\gamma) = dom(\gamma \downarrow_i)$

  Therefore, $dom(\Gamma) \subseteq (dom(\gamma) = dom(\gamma \downarrow_i))$ (Given)

- $\forall x \in dom(\Gamma).(W.\theta_i, m, \gamma \downarrow_i (x)) \in \lfloor \Gamma(x) \rfloor_V$:
  We are given: $\forall x \in dom(\Gamma).(W, n, \pi_1(\gamma(x)), \pi_2(\gamma(x))) \in \lceil \Gamma(x) \rceil_V^{\mathcal{A}}$
  Therefore from Lemma 4.14 we know that
  $\forall m'.(W.\theta_i, m', \gamma \downarrow_i (x)) \in \lfloor \Gamma(x) \rfloor_V$
  Instantiating m' with m we get
  $(W.\theta_i, m, \gamma \downarrow_i (x)) \in \lfloor \Gamma(x) \rfloor_V$

Case $i = 2$
Symmetric reasoning as in the $i = 1$ case above

□

Theorem 4.24 (Fundamental theorem binary)**.** $\forall \Sigma, \Psi, \Gamma, pc, W, \mathcal{A}, \mathcal{L}, e, \tau, \sigma, \gamma, n.$
$\Sigma; \Psi; \Gamma \vdash e : \tau \wedge \mathcal{L} \models \Psi\ \sigma\ \wedge$
$(W, n, \gamma) \in \lceil \Gamma\ \sigma \rceil_V^{\mathcal{A}} \implies$
$(W, n, e\ (\gamma \downarrow_1), e\ (\gamma \downarrow_2)) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$

Proof. Proof by induction on the typing derivation

1. CG-var:

$$\frac{}{\Gamma, x : \tau \vdash x : \tau}\ \text{CG-var}$$

   To prove: $(W, n, x\ (\gamma \downarrow_1), x\ (\gamma \downarrow_2)) \in \lceil \tau \rceil_E^{\mathcal{A}}$
   Say $e_1 = x\ (\gamma \downarrow_1)$ and $e_2 = x\ (\gamma \downarrow_2)$

   From Definition 4.5 it suffices to prove that
   $\forall i < n. e_1 \Downarrow_i v_1' \wedge e_2 \Downarrow v_2' \implies (W, n - i, v_1', v_2') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

   This means given some $i < n$ s.t $e_1 \Downarrow_i v_1' \wedge e_2 \Downarrow v_2'$
   We are required to prove: $(W, n - i, v_1', v_2') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

   From cg-val we know that $x\ (\gamma \downarrow_1) \Downarrow x\ (\gamma \downarrow_1)$ and $x\ (\gamma \downarrow_2) \Downarrow x\ (\gamma \downarrow_2)$
   This means $v_1' = x\ (\gamma \downarrow_1)$ and $v_2' = x\ (\gamma \downarrow_2)$
   Since $(W, n, \gamma) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$. Therefore from Definition 4.13 we know that
   $(W, n, v_1', v_2') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$
   From Lemma 4.16 we get
   $(W, n - i, v_1', v_2') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

2. CG-lam:

$$\frac{\Gamma, x : \tau_1 \vdash e_i : \tau_2}{\Gamma \vdash \lambda x.e_i : (\tau_1 \to \tau_2)}$$

   To prove: $(W, n, \lambda x.e\ (\gamma \downarrow_1), \lambda x.e\ (\gamma \downarrow_2)) \in \lceil (\tau_1 \to \tau_2)\ \sigma \rceil_E^{\mathcal{A}}$

Say $e_1 = \lambda x.e\ (\gamma\downarrow_1)$ and $e_2 = \lambda x.e\ (\gamma\downarrow_2)$

From Definition of $\lceil(\tau_1 \to \tau_2)\ \sigma\rceil_E^{\mathcal{A}}$ it suffices to prove that

$\forall i < n.e_1 \Downarrow_i v_1' \wedge e_2 \Downarrow v_2' \implies (W, n-i, v_1', v_2') \in \lceil(\tau_1 \to \tau_2)\ \sigma\rceil_V^{\mathcal{A}}$

This means given some $i < n$ s.t $e_1 \Downarrow_i v_1' \wedge e_2 \Downarrow v_2'$

From cg-val we know that $v_1' = (\lambda x.e_i)\gamma\downarrow_1$ and $v_2' = (\lambda x.e_i)\gamma\downarrow_2$

We are required to prove:

$(W, n-i, (\lambda x.e_i)\gamma\downarrow_1, (\lambda x.e_i)\gamma\downarrow_2) \in \lceil(\tau_1 \to \tau_2)\ \sigma\rceil_V^{\mathcal{A}}$

From Definition 4.4 it suffices to prove

$\forall W' \sqsupseteq W, j < n, v_1, v_2.$
$((W', j, v_1, v_2) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}} \implies (W', j, e_1[v_1/x]\ \gamma\downarrow_1, e_2[v_2/x]\ \gamma\downarrow_1) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}}) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, v_c, j.$
$((\theta_l, j, v_c) \in \lfloor\tau_1\ \sigma\rfloor_V \implies (\theta_l, j, e_1[v_c/x]\ \gamma\downarrow_1) \in \lfloor\tau_2\ \sigma\rfloor_E) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, v_c, j.$
$((\theta_l, j, v_c) \in \lfloor\tau_1\ \sigma\rfloor_V \implies (\theta_l, j, e_2[v_c/x]\ \gamma\downarrow_2) \in \lfloor\tau_2\ \sigma\rfloor_E)$ (FB-L0)

IH:

$\forall W, n.\ (W, n, e_i\ (\gamma\downarrow_1 \cup \{x \mapsto v_1\}), e_i\ (\gamma\downarrow_2 \cup \{x \mapsto v_2\})) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}}$

s.t

$(W, n, (\gamma \cup \{x \mapsto (v_1, v_2)\})) \in \lceil\Gamma\rceil_V^{\mathcal{A}}$

In order to prove (FB-L0) we need to prove the following:

(a) $\forall W' \sqsupseteq W, j < n, v_1, v_2.$
$((W', j, v_1, v_2) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}} \implies (W', j, e_1[v_1/x]\ \gamma\downarrow_1, e_2[v_2/x]\ \gamma\downarrow_2) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}})$:

This means given some $W' \sqsupseteq W, j < n, v_1, v_2$ s.t. $(W', j, v_1, v_2) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}}$
We need to prove $(W', j, e_1[v_1/x]\ \gamma\downarrow_1, e_2[v_2/x]\ \gamma\downarrow_2) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}}$

We get this by instantiating IH with W' and j

(b) $\forall \theta_l \sqsupseteq W.\theta_1, v_c, j.$
$((\theta_l, j, v_c) \in \lfloor\tau_1\ \sigma\rfloor_V \implies (\theta_l, j, e_1[v_c/x]\ \gamma\downarrow_1) \in \lfloor\tau_2\ \sigma\rfloor_E)$:
This means given some $\theta_l \sqsupseteq W.\theta_1, v_c, j$ s.t $(\theta_l, j, v_c) \in \lfloor\tau_1\ \sigma\rfloor_V$
We need to prove: $(\theta_l, j, e_1[v_c/x]\ \gamma\downarrow_1) \in \lfloor\tau_2\ \sigma\rfloor_E$

It is given to us that
$(W, n, \gamma) \in \lceil\Gamma\rceil_V^{\mathcal{A}}$

Therefore from Lemma 4.23 we know that
$\forall m.\ (W.\theta_1, m, \gamma\downarrow_1) \in \lfloor\Gamma\rfloor_V$
Intantiating m with j we get
$(W.\theta_1, j, \gamma\downarrow_1) \in \lfloor\Gamma\rfloor_V$

From Lemma 4.18 we know that

$(\theta_l, j, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$

Since we know that $(\theta_l, j, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V$
Therefore we also have
$(\theta_l, j, \gamma \downarrow_1 \cup \{x \mapsto v_c\}) \in \lfloor \Gamma \cup \{x \mapsto \tau_1\ \sigma\} \rfloor_V$

Therefore, we can apply Theorem 4.21 to obtain
$(\theta_l, j, e[v_c/x]\ \gamma \downarrow_1) \in \lfloor \tau_2\ \sigma \rfloor_V$

(c) $\forall \theta_l \sqsupseteq W.\theta_2, v_c, j.$
$((\theta_l, j, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta_l, j, e_2[v_c/x]\gamma \downarrow_2) \in \lfloor \tau_2\ \sigma \rfloor_E)$:
Similar reasoning as in the previous case

3. CG-app:

$$\frac{\Gamma \vdash e_1 : (\tau_1 \to \tau_2) \qquad \Gamma \vdash e_2 : \tau_1}{\Gamma \vdash e_1\ e_2 : \tau_2}$$

To prove: $(W, n, (e_1\ e_2)\ (\gamma \downarrow_1), (e_1\ e_2)\ (\gamma \downarrow_2)) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:
$\forall i < n.(e_1\ e_2)\ \gamma \Downarrow_i v_{f1} \wedge e_2 \Downarrow v_{f2} \implies (W, n-i, v_{f1}, v_{f2}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$

This further means that given some $i < n$ s.t $(e_1\ e_2)\ \gamma \Downarrow_i v_{f1} \wedge e_2 \Downarrow v_{f2}$
<u>It sufficies to prove</u>:
$(W, n-i, v_{f1}, v_{f2}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$

<u>IH1</u>: $(W, n, (e_1)\ (\gamma \downarrow_1), (e_1)\ (\gamma \downarrow_2)) \in \lceil (\tau_1 \to \tau_2)\ \sigma \rceil_E^{\mathcal{A}}$
This means from Definition 4.5 we know that
$\forall j < n.e_1\ \gamma \downarrow_1 \Downarrow_j v_{h1} \wedge e_1\ \gamma \downarrow_2 \Downarrow v_{h2} \implies (W, n-j, v_{h1}, v_{h2}) \in \lceil (\tau_1 \to \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e_1\ e_2)\ \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists j < i < n$ s.t $e_1\ \gamma \downarrow_1 \Downarrow_j v_{h1}$. Similarly since $(e_1\ e_2)\ \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e_1\ \gamma \downarrow_2 \Downarrow v_{h2}$
This means we have $(W, n-j, v_{h1}, v_{h2}) \in \lceil (\tau_1 \to \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$
From cg-app we know that $val_{h1} = \lambda x.e_{h1}$ and $val_{h2} = \lambda x.e_{h2}$
From Definition 4.4 this further means
$\forall W' \sqsupseteq W, J < (n-j), v_1, v_2.$
$((W', J, v_1, v_2) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}} \implies (W', J, e_{h1}[v_1/x], e_{h2}[v_2/x]) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, v_c, j.$
$((\theta_l, j, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta_l, j, e_1[v_c/x]) \in \lfloor \tau_2\ \sigma \rfloor_E) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, v_c, j.$
$((\theta_l, j, v_c) \in \lfloor \tau_1\ \sigma \rfloor_V \implies (\theta_l, j, e_2[v_c/x]) \in \lfloor \tau_2\ \sigma \rfloor_E)$ (FB-A1)

<u>IH2</u>: $(W, n-j, (e_2)\ (\gamma \downarrow_1), (e_2)\ (\gamma \downarrow_2)) \in \lceil \tau_1\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we know that

$\forall k < n-j.e_2\ \gamma \downarrow_1 \Downarrow_j v_{h1'} \wedge e_2\ \gamma \downarrow_2 \Downarrow v_{h2'} \implies (W, n-j-k, v_{h1'}, v_{h2'}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e_1\ e_2)\ \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists k < i-j < n-j$ s.t $e_2\ \gamma \downarrow_1 \Downarrow_k v_{h1'}$. Similarly since $(e_1\ e_2)\ \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e_2\ \gamma \downarrow_2 \Downarrow v_{h2'}$

This means we have $(W, n-j-k, v_{h1'}, v_{h2'}) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$ (FB-A2)

Instantiating the first conjunct of (FB-A1) as follows W' with W, J with $n-j-k$, v_1 and v_2 with v'_{h1} and v'_{h2} respectively, we obtain

$(W, n-j-k, e_{h1}[v'_{h1}/x], e_{h2}[v'_{h2}/x]) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$

From Definition 4.5

$\forall l < n-j-k.(e_{h1}[v'_{h1}/x])\ \gamma \Downarrow_l v_{f1} \wedge e_{h2}[v'_{h2}/x] \Downarrow v_{f2} \implies (W, n-j-k-l, v_{f1}, v_{f2}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e_1\ e_2)\ \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists l < i-j-k < n-j-k$ s.t $e_{h1}[v'_{h1}/x] \Downarrow_l v_{f1}$. Similarly since $(e_1\ e_2)\ \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e_{h2}[v'_{h2}/x] \Downarrow v_{f2}$

Therefore we have $(W, n-j-k-l, v_{f1}, v_{f2}) \in \lceil \tau_2\ \sigma \rceil_V^{\mathcal{A}}$

Since $i = j+k+l$ threfore we are done

4. CG-prod:

$$\frac{\Gamma \vdash e_1 : \tau_1 \qquad \Gamma \vdash e_2 : \tau_2}{\Gamma \vdash (e_1, e_2) : (\tau_1 \times \tau_2)}$$

To prove: $(W, n, (e_1, e_2)\ (\gamma \downarrow_1), (e_1, e_2)\ (\gamma \downarrow_2)) \in \lceil (\tau_1 \times \tau_2)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:

$\forall i < n.(e_1, e_2)\ \gamma \downarrow_1 \Downarrow_i (v_{f1}, v_{f2}) \wedge (e_1, e_2)\ \gamma \downarrow_2 \Downarrow (v'_{f1}, v'_{f2}) \implies$
$(W, n-i, (v_{f1}, v_{f1}), (v'_{f1}, v'_{f2})) \in \lceil (\tau_1 \times \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $(e_1, e_2)\ \gamma \downarrow_1 \Downarrow_i (v_{f1}, v_{f2}) \wedge (e_1, e_2) \gamma \downarrow_2 \Downarrow (v'_{f1}, v'_{f2})$

We are required to prove

$(W, n-i, (v_{f1}, v_{f1}), (v'_{f1}, v'_{f2})) \in \lceil (\tau_1 \times \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$ (FB-P0)

IH1: $(W, n, e_1\ (\gamma \downarrow_1), e_1\ (\gamma \downarrow_2)) \in \lceil \tau_1\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we know that

$\forall j < n.e_1\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge e_1\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies (W, n-j, (v_{f1}, v'_{f1})) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e_1, e_2)\ \gamma \downarrow_1 \Downarrow_i (v_{f1}, v_{f2})$. Therefore $\exists j < i < n$ s.t $e_1\ \gamma \downarrow_1 \Downarrow_j v_{f1}$. Similarly since $(e_1\ e_2)\ \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e_1\ \gamma \downarrow_2 \Downarrow v'_{f1}$

This means we have

$(W, n-j, (v_{f1}, v'_{f1})) \in \lceil \tau_1\ \sigma \rceil_V^{\mathcal{A}}$ (FB-P1)

IH2: $(W, n-j, e_2\ (\gamma \downarrow_1), e_2\ (\gamma \downarrow_2)) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we know that

$\forall k < n-j.e_2 \ \gamma \downarrow_1 \Downarrow_i v_{f2} \wedge e_2 \ \gamma \downarrow_2 \Downarrow v'_{f2} \implies (W, n-j-k, (v_{f2}, v'_{f2})) \in \lceil \tau_2 \ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e_1, e_2) \ \gamma \downarrow_1 \Downarrow_i (v_{f1}, v_{f2})$. Therefore $\exists k < i-j < n-j$ s.t $e_2 \ \gamma \downarrow_1 \Downarrow_j v_{f2}$. Similarly since $(e_1 \ e_2) \ \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e_2 \ \gamma \downarrow_2 \Downarrow v'_{f2}$

This means we have

$(W, n-j-k, (v_{f2}, v'_{f2})) \in \lceil \tau_2 \ \sigma \rceil_V^{\mathcal{A}}$ (FB-P2)

In order to prove (FB-P0) from Definition 4.4 it suffices to prove that

$(W, n-i, (v_{f1}, v'_{f1})) \in \lceil \tau_1 \ \sigma \rceil_V^{\mathcal{A}}$ and $(W, n-i, (v_{f2}, v'_{f2})) \in \lceil \tau_2 \ \sigma \rceil_V^{\mathcal{A}}$

Since $i = j + k + 1$ therefore from (FB-P1) and (FB-P2) and from Lemma 4.16 we get

$(W, n-i, (v_{f1}, v_{f1}), (v'_{f1}, v'_{f2})) \in \lceil (\tau_1 \times \tau_2) \ \sigma \rceil_V^{\mathcal{A}}$

5. CG-fst:

$$\frac{\Gamma \vdash e' : (\tau_1 \times \tau_2)}{\Gamma \vdash \mathsf{fst}(e') : \tau_1}$$

To prove: $(W, n, \mathsf{fst}(e') \ (\gamma \downarrow_1), \mathsf{fst}(e') \ (\gamma \downarrow_2)) \in \lceil \tau_1 \ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:

$\forall i < n.\mathsf{fst}(e') \ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{fst}(e') \ \gamma \downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n-i, v_{f1}, v'_{f1}) \in \lceil \tau_1 \ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{fst}(e') \ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{fst}(e') \ \gamma \downarrow_2 \Downarrow v'_{f1}$

We are required to prove

$(W, n-i, v_{f1}, v_{f1}) \in \lceil \tau_1 \ \sigma \rceil_V^{\mathcal{A}}$ (FB-F0)

<u>IH</u>:

$(W, n, e' \ (\gamma \downarrow_1), e' \ (\gamma \downarrow_2)) \in \lceil (\tau_1 \times \tau_2) \ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we have:

$\forall j < n.e' \ \gamma \downarrow_1 \Downarrow_i (v_{f1}, v_{f2}) \wedge e' \ \gamma \downarrow_2 \Downarrow (v'_{f1}, v'_{f2}) \implies$
$(W, n-j, (v_{f1}, v_{f2}), (v'_{f1}, v'_{f2})) \in \lceil (\tau_1 \times \tau_2) \ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $\mathsf{fst}(e') \ \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists j < i < n$ s.t $e' \ \gamma \downarrow_1 \Downarrow_j (v_{f1}, -)$. Similarly since $\mathsf{fst}(e') \ \gamma \downarrow_2 \Downarrow v'_{f1}$ therefore $e' \ \gamma \downarrow_2 \Downarrow (v'_{f1}, -)$

This means we have

$(W, n-j, (v_{f1}, v_{f2}), (v'_{f1}, v'_{f2})) \in \lceil (\tau_1 \times \tau_2) \ \sigma \rceil_V^{\mathcal{A}}$

From Definition 4.4 we know that

$(W, n-j, v_{f1}, v'_{f1}) \in \lceil \tau_1 \ \sigma \rceil_V^{\mathcal{A}}$

Since from cg-fst $i = j + 1$ therefore from Lemma 4.16 we get

$(W, n-i, v_{f1}, v'_{f1}) \in \lceil \tau_1 \ \sigma \rceil_V^{\mathcal{A}}$

6. CG-snd:

   Symmetric reasoning as in the CG-fst case above

7. CG-inl:

$$\frac{\Gamma \vdash e' : \tau_1}{\Gamma \vdash \mathsf{inl}(e') : (\tau_1 + \tau_2)}$$

To prove: $(W, n, \mathsf{inl}(e')\ (\gamma \downarrow_1), \mathsf{inl}(e')\ (\gamma \downarrow_2)) \in \lceil(\tau_1 + \tau_2)\ \sigma\rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:
$\forall i < n.\mathsf{inl}(e')\ \gamma \downarrow_1 \Downarrow_i \mathsf{inl}(v_{f1}) \wedge \mathsf{inl}(e')\gamma \downarrow_2 \Downarrow \mathsf{inl}(v'_{f1}) \implies$
$(W, n-i, \mathsf{inl}(v_{f1}), \mathsf{inl}(v'_{f1})) \in \lceil(\tau_1 + \tau_2)\ \sigma\rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{inl}(e')\ \gamma \downarrow_1 \Downarrow_i \mathsf{inl}(v_{f1}) \wedge \mathsf{fst}(e')\ \gamma \downarrow_2 \Downarrow \mathsf{inl}(v'_{f1})$
We are required to prove
$(W, n-i, \mathsf{inl}(v_{f1}), \mathsf{inl}(v_{f1})) \in \lceil(\tau_1 + \tau_2)\ \sigma\rceil_V^{\mathcal{A}}$ (FB-IL0)

<u>IH</u>:
$(W, n, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil(\tau_1 \times \tau_2)\ \sigma\rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we have:
$\forall j < n.e'\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge e'\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n-j, v_{f1}, v'_{f1}) \in \lceil \tau_1\ \sigma\rceil_V^{\mathcal{A}}$
Since we know that $\mathsf{inl}(e')\ \gamma \downarrow_1 \Downarrow_i \mathsf{inl}(v_{f1})$. Therefore $\exists j < i < n$ s.t $e'\ \gamma \downarrow_1 \Downarrow_j v_{f1}$. Similarly since $\mathsf{fst}(e')\ \gamma \downarrow_2 \Downarrow \mathsf{inl}(v'_{f1})$ therefore $e'\ \gamma \downarrow_2 \Downarrow v'_{f1}$
This means we have
$(W, n-j, v_{f1}, v'_{f1}) \in \lceil \tau_1\ \sigma\rceil_V^{\mathcal{A}}$ (FB-IL1)

In order to prove (FB-IL0) from Definition 4.4 it suffices to prove
$(W, n-i, v_{f1}, v'_{f1}) \in \lceil \tau_1\ \sigma\rceil_V^{\mathcal{A}}$
From cg-inl since $i = j + 1$ therefore from (FB-IL1) and Lemma 4.16 we get (FB-IL0)

8. CG-inr:

   Symmetric reasoning as in the CG-inl case above

9. CG-case:

$$\frac{\Gamma \vdash e_c : (\tau_1 + \tau_2) \qquad \Gamma, x : \tau_1 \vdash e_1 : \tau \qquad \Gamma, y : \tau_2 \vdash e_2 : \tau}{\Gamma \vdash \mathsf{case}(e_c, x.e_1, y.e_2) : \tau}$$

To prove: $(W, n, \mathsf{case}(e_c, x.e_1, y.e_2)\ (\gamma \downarrow_1), \mathsf{inl}(e')\ (\gamma \downarrow_2)) \in \lceil \tau\ \sigma\rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:

$\forall i < n.\mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_2 \Downarrow v_{f2} \implies$
$(W, n-i, v_{f1}, v_{f2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_2 \Downarrow v_{f2}$

We are required to prove

$(W, n-i, v_{f1}, v_{f2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$ (FB-C0)

<u>IH1</u>:

$(W, n, e_c\ (\gamma \downarrow_1), e_c\ (\gamma \downarrow_2)) \in \lceil (\tau_1 + \tau_2)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we have:

$\forall j < n.e_c\ \gamma \downarrow_1 \Downarrow_i v_{h1} \wedge e_c\ \gamma \downarrow_2 \Downarrow v'_{h1} \implies$
$(W, n-j, v_{h1}, v'_{h1}) \in \lceil (\tau_1 + \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $\mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists j < i < n$ s.t $e_c\ \gamma \downarrow_1 \Downarrow_j v_{h1}$. Similarly since $\mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_2 \Downarrow v'_{h1}$ therefore $e_c\ \gamma \downarrow_2 \Downarrow v'_{h1}$

This means we have

$(W, n-j, v_{h1}, v'_{h1}) \in \lceil (\tau_1 + \tau_2)\ \sigma \rceil_V^{\mathcal{A}}$ (FB-C1)

2 cases arise

(a) $v_{h1} = \mathsf{inl}(v_1)$ and $v'_{h1} = \mathsf{inl}(v'_1)$:
<u>IH2</u>:
$(W, n, e_c\ (\gamma \downarrow_1), e_c\ (\gamma \downarrow_2)) \in \lceil (\tau_1 + \tau_2)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we have:
$\forall k < n-j.e_1\ \gamma \downarrow_1 \cup \{x \mapsto v_1\} \Downarrow_i v_{h2} \wedge e_1\ \gamma \downarrow_2 \cup \{x \mapsto v'_1\} \Downarrow v'_{h2} \implies$
$(W, n-j-k, v_{h2}, v'_{h2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$
Since we know that $\mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists k < i-j < n-j$ s.t $e_1\ \gamma \downarrow_1 \cup \{x \mapsto v_1\} \Downarrow_j v_{h2}$. Similarly since $\mathsf{case}(e_c, x.e_1, y.e_2)\ \gamma \downarrow_2 \cup \{x \mapsto v'_1\} \Downarrow v'_{h2}$ therefore $e_1\ \gamma \downarrow_2 \Downarrow v'_{h2}$
This means we have
$(W, n-j-k, v_{h2}, v'_{h2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

From cg-case1 we know that $i = j+k+1$ therefore from Lemma 4.16 we get (FB-C0)

(b) $v_{h1} = \mathsf{inr}(v_1)$ and $v'_{h1} = \mathsf{inr}(v'_1)$:
Symmetric case

10. CG-FI:

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash e' : \tau}{\Sigma; \Gamma \vdash \Lambda e' : \forall \alpha.\tau}$$

To prove: $(W, n, \Lambda e'\ (\gamma \downarrow_1), \Lambda e'\ (\gamma \downarrow_2)) \in \lceil (\forall \alpha.\tau)\ \sigma \rceil_E^{\mathcal{A}}$

From Definition 4.5 it suffices to prove that

$\forall i < n.(\Lambda e')\gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (\Lambda e')\gamma \downarrow_2 \Downarrow v_{f2} \implies (W, n-i, v_{f1}, v_{f2}) \in \lceil (\forall \alpha.\tau)\ \sigma \rceil_V^{\mathcal{A}}$

This means given some $i < n$ s.t $(\Lambda e')\gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (\Lambda e')\gamma \downarrow_2 \Downarrow v_{f2}$
From CG-Sem-val we know that $v_{f1} = (\Lambda e')\gamma \downarrow_1$ and $v_{f2} = (\Lambda e')\gamma \downarrow_2$
We are required to prove:
$(W, n-i, (\Lambda e')\gamma \downarrow_1, (\Lambda e')\gamma \downarrow_2) \in \lceil (\forall \alpha.\tau)\ \sigma \rceil_V^{\mathcal{A}}$

Let $e_1 = (\Lambda e')\gamma \downarrow_1$ and $e_2 = (\Lambda e')\gamma \downarrow_2$
From Definition 4.4 it suffices to prove
$\forall W' \sqsupseteq W, j < (n-i), \ell' \in \mathcal{L}.((W', j, e_1, e_2) \in \lceil \tau[\ell'/\alpha]\ \sigma \rceil_E^{\mathcal{A}}) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, \ell'' \in \mathcal{L}, j.(\theta_l, j, e_1) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, \ell'' \in \mathcal{L}, j.(\theta_l, j, e_2) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E$ (FB-FI0)

IH: $\forall W, n.\ (W, n, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil \tau\ \sigma \cup \{\alpha \mapsto \ell'\} \rceil_E^{\mathcal{A}}$
In order to prove (FB-FI0) we need to prove the following

(a) $\forall W' \sqsupseteq W, j < (n-i), \ell' \in \mathcal{L}.((W', j, e_1, e_2) \in \lceil \tau[\ell'/\alpha]\ \sigma \rceil_E^{\mathcal{A}})$:
This means given $W' \sqsupseteq W, j < (n-i), \ell' \in \mathcal{L}$ and we are required to prove
$(W', j, e_1, e_2) \in \lceil \tau[\ell'/\alpha]\ \sigma \rceil_E^{\mathcal{A}}$
Instantiating IH with W' and j we get the desired
(b) $\forall \theta_l \sqsupseteq W.\theta_1, \ell'' \in \mathcal{L}, j.(\theta_l, j, e_1) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E$:
This means given $\theta_l \sqsupseteq W.\theta_1, \ell'' \in \mathcal{L}, j$ and we are required to prove
$(\theta_l, j, e_1) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E$
Since from Lemma 4.23
$(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}} \implies \forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, \gamma \downarrow_i) \in \lfloor \Gamma \rfloor_V$
Therefore we get
$(W.\theta_1, j, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$
And from Lemma 4.16 we also get
$(\theta_l, j, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$
Therefore we can apply Theorem 4.21 to get
$(\theta_l, j, e_1) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E$
(c) $\forall \theta_l \sqsupseteq W.\theta_2, \ell'' \in \mathcal{L}, j.(\theta_l, j, e_2) \in \lfloor \tau[\ell''/\alpha] \rfloor_E$:
Symmetric reasoning as before

11. CG-FE:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : \forall \alpha.\tau \qquad \mathrm{FV}(\ell) \in \Sigma}{\Sigma; \Psi; \Gamma \vdash e'\ [] : \tau[\ell/\alpha]}$$

To prove: $(W, n, e'[]\ (\gamma \downarrow_1), e'[]\ (\gamma \downarrow_2)) \in \lceil (\forall \alpha.\tau)\ \sigma \rceil_E^{\mathcal{A}}$
From Definition 4.5 it suffices to prove that
$\forall i < n.(e'[])\gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (e'[])\gamma \downarrow_2 \Downarrow v_{f2} \implies (W, n-i, v_{f1}, v_{f2}) \in \lceil (\tau[\ell/\alpha])\ \sigma \rceil_V^{\mathcal{A}}$

This means given some $i < n$ s.t $(e'[])\gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (e'[])\gamma \downarrow_2 \Downarrow v_{f2}$

We are required to prove:

$(W, n-i, v_{f1}, v_{f2}) \in \lceil (\tau[\ell/\alpha])\ \sigma \rceil_V^{\mathcal{A}}$ (FB-FE0)

IH: $(W, n, e'\ (\gamma\downarrow_1), e'\ (\gamma\downarrow_2)) \in \lceil (\forall\alpha.\tau)\ \sigma \rceil_E^{\mathcal{A}}$

From Definition 4.5 it suffices to prove that

$\forall i < n.(e')\gamma\downarrow_1\Downarrow_i v_{h1} \wedge (e')\gamma\downarrow_2\Downarrow v_{h2} \implies (W, n-i, v_{h1}, v_{h2}) \in \lceil (\forall\alpha.\tau)\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e'[])\ \gamma\downarrow_1\Downarrow_i v_{f1}$. Therefore $\exists j < i < n$ s.t $e'\ \gamma\downarrow_1\Downarrow_j v_{h1}$. Similarly since $(e'[])\ \gamma\downarrow_2\Downarrow v_{f2}$ therefore $e'\ \gamma\downarrow_2\Downarrow v_{h2}$

This means we have $(W, n-j, v_{h1}, v_{h2}) \in \lceil (\forall\alpha.\tau)\ \sigma \rceil_V^{\mathcal{A}}$

From CG-Sem-FE we know that $v_{h1} = \Lambda e_{h1}$ and $v_{h2} = \Lambda e_{h2}$

From Definition 4.4 this further means

$\forall W' \sqsupseteq W, k < (n-j), \ell' \in \mathcal{L}.((W', k, e_{h1}, e_{h2}) \in \lceil \tau[\ell'/\alpha]\ \sigma \rceil_E^{\mathcal{A}}) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, \ell'' \in \mathcal{L}, k.(\theta_l, k, e_{h1}) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, \ell'' \in \mathcal{L}, k.(\theta_l, k, e_{h2}) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E$ (FB-FE1)

Instantiating the first conjunct of (FB-FE1) with W, $n-j-1$ and ℓ we get

$(W, n-j-1, e_{h1}, e_{h2}) \in \lceil \tau[\ell/\alpha]\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we know that

$\forall l < n-j-1.(e_{h1}) \Downarrow_l v_{f1} \wedge e_{h2} \Downarrow v_{f2} \implies (W, n-j-1-l, v_{f1}, v_{f2}) \in \lceil (\tau[\ell/\alpha])\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e'[])\ \gamma\downarrow_1\Downarrow_i v_{f1}$ therefore from CG-Sem-FE we know that $(i = j+l+1)$ and since we know that $i < n$ therefore we have $l < n-j-1$ s.t $e_{h1}\ \gamma\downarrow_1\Downarrow_j v_{f1}$. Similarly since $(e'[])\ \gamma\downarrow_2\Downarrow v_{f2}$ therefore $e_{h2}\ \gamma\downarrow_2\Downarrow v_{f2}$

Therefore we get

$(W, n-j-1-l, v_{f1}, v_{f2}) \in \lceil (\tau[\ell/\alpha])\ \sigma \rceil_V^{\mathcal{A}}$ (FB-FE2)

Since we know that $i = j+l+1$ therefore from (FB-FE2) we get (FB-FE0)

12. CG-CI:

$$\frac{\Sigma; \Psi, c; \Gamma \vdash e' : \tau}{\Sigma; \Gamma \vdash \nu\ e' : c \Rightarrow \tau}$$

To prove: $(W, n, \nu e'\ (\gamma\downarrow_1), \nu e'\ (\gamma\downarrow_2)) \in \lceil (c \Rightarrow \tau)\ \sigma \rceil_E^{\mathcal{A}}$

From Definition 4.5 it suffices to prove that

$\forall i < n.(\nu e')\gamma\downarrow_1\Downarrow_i v_{f1} \wedge (\nu e')\gamma\downarrow_2\Downarrow v_{f2} \implies (W, n-i, v_{f1}, v_{f2}) \in \lceil (c \Rightarrow \tau)\ \sigma \rceil_V^{\mathcal{A}}$

This means given some $i < n$ s.t $(\nu e')\gamma\downarrow_1\Downarrow_i v_{f1} \wedge (\nu e')\gamma\downarrow_2\Downarrow v_{f2}$

From CG-Sem-val we know that $v_{f1} = (\nu e')\gamma\downarrow_1$ and $v_{f2} = (\nu e')\gamma\downarrow_2$

We are required to prove:

$(W, n-i, (\nu e')\gamma\downarrow_1, (\nu e')\gamma\downarrow_2) \in \lceil (c \Rightarrow \tau)\ \sigma \rceil_V^{\mathcal{A}}$

Let $e_1 = (\nu e')\gamma\downarrow_1$ and $e_2 = (\nu e')\gamma\downarrow_2$

From Definition 4.4 it suffices to prove

$\forall W' \sqsupseteq W, j < n.\mathcal{L} \models c \implies (W', j, e_1, e_2) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}} \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c \implies (\theta_l, j, e_1) \in \lfloor \tau\ \sigma \rfloor_E \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c \implies (\theta_l, j, e_2) \in \lfloor \tau\ \sigma \rfloor_E$ (FB-CI0)

<u>IH</u>: $\forall W, n.\ (W, n, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$

In order to prove (FB-CI0) we need to prove the following

(a) $\forall W' \sqsupseteq W, j < n.\mathcal{L} \models c\ \sigma \implies (W', j, e_1, e_2) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$:
This means given $W' \sqsupseteq W, j < n, \mathcal{L} \models c\ \sigma$ and we are required to prove
$(W', j, e_1, e_2) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$
Instantiating IH with W' and j we get the desired

(b) $\forall \theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c\ \sigma \implies (\theta_l, j, e_1) \in \lfloor \tau\ \sigma \rfloor_E$:
This means given $\theta_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c\ \sigma$ and we are required to prove
$(\theta_l, j, e_1) \in \lfloor \tau\ \sigma \rfloor_E$
Since from Lemma 4.23 $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}} \implies \forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, \gamma \downarrow_i) \in \lfloor \Gamma \rfloor_V$
Therefore we get
$(W.\theta_1, j, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$
And from Lemma 4.16 we also get
$(\theta_l, j, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$
Therefore we can apply Theorem 4.21 to get
$(\theta_l, j, e_1) \in \lfloor \tau\ \sigma \rfloor_E$

(c) $\forall \theta_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c \implies (\theta_l, j, e_2) \in \lfloor \tau\ \sigma \rfloor_E$:
Symmetric reasoning as before

13. CG-CE:

$$\frac{\Sigma; \Psi; \Gamma \vdash e' : c \Rightarrow \tau \qquad \Sigma; \Psi \vdash c}{\Sigma; \Psi; \Gamma \vdash e'\ \bullet : \tau}$$

To prove: $(W, n, e' \bullet\ (\gamma \downarrow_1), e' \bullet\ (\gamma \downarrow_2)) \in \lceil \tau)\ \sigma \rceil_E^{\mathcal{A}}$

From Definition 4.5 it suffices to prove that

$\forall i < n.(e'\bullet)\gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (e'\bullet)\gamma \downarrow_2 \Downarrow v_{f2} \implies (W, n - i, v_{f1}, v_{f2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

This means given some $i < n$ s.t $(e'\bullet)\gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (e'\bullet)\gamma \downarrow_2 \Downarrow v_{f2}$

<u>We are required to prove:</u>

$(W, n - i, v_{f1}, v_{f2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$ (FB-CE0)

<u>IH</u>: $(W, n, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil (c \Rightarrow \tau)\ \sigma \rceil_E^{\mathcal{A}}$

From Definition 4.5 it suffices to prove that

$\forall i < n.e'\gamma \downarrow_1 \Downarrow_i v_{h1} \wedge e'\gamma \downarrow_2 \Downarrow v_{h2} \implies (W, n - i, v_{h1}, v_{h2}) \in \lceil (c \Rightarrow \tau)\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e'\bullet)\ \gamma \downarrow_1 \Downarrow_i v_{f1}$. Therefore $\exists j < i < n$ s.t $e'\ \gamma \downarrow_1 \Downarrow_j v_{h1}$. Similarly since $(e'\bullet)\ \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e'\ \gamma \downarrow_2 \Downarrow v_{h2}$

This means we have $(W, n-j, v_{h1}, v_{h2}) \in \lceil (c \Rightarrow \tau)\ \sigma \rceil_V^{\mathcal{A}}$

From CG-Sem-CE we know that $v_{h1} = \nu e_{h1}$ and $v_{h2} = \nu e_{h2}$

From Definition 4.4 this further means

$\forall W' \sqsupseteq W, k < n-j.\mathcal{L} \models c\ \sigma \implies (W', k, e_1, e_2) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}} \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, k.\mathcal{L} \models c\ \sigma \implies (\theta_l, k, e_1) \in \lfloor \tau\ \sigma \rfloor_E \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, k.\mathcal{L} \models c\ \sigma \implies (\theta_l, k, e_2) \in \lfloor \tau\ \sigma \rfloor_E$ (FB-CE1)

Instantiating the first conjunct of (FB-CE1) with W, $n-j-1$ and since we know that $\mathcal{L} \models c\ \sigma$ therefore we get

$(W, n-j-1, e_{h1}, e_{h2}) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we know that

$\forall l < n-j-1.(e_{h1}) \Downarrow_l v_{f1} \wedge e_{h2} \Downarrow v_{f2} \implies (W, n-j-1-l, v_{f1}, v_{f2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(e' \bullet)\ \gamma \downarrow_1 \Downarrow_i v_{f1}$ therefore from CG-Sem-CE we know that $(i = j+l+1)$ and since we know that $i < n$ therefore we have $l < n-j-1$ s.t $e_{h1}\ \gamma \downarrow_1 \Downarrow_l v_{f1}$. Similarly since $(e' \bullet)\ \gamma \downarrow_2 \Downarrow v_{f2}$ therefore $e_{h2}\ \gamma \downarrow_2 \Downarrow v_{f2}$

Therefore we get

$(W, n-j-1-l, v_{f1}, v_{f2}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$ (FB-CE2)

Since we know that $i = j+l+1$ therefore from (FB-CE2) we get (FB-CE0)

14. CG-label:

$$\frac{\Gamma \vdash e' : \tau}{\Gamma \vdash \mathsf{Lb}(e') : \mathsf{Labeled}\ \ell\ \tau}$$

To prove: $(W, n, \mathsf{Lb}(e')\ (\gamma \downarrow_1), \mathsf{Lb}(e')\ (\gamma \downarrow_2)) \in \lceil (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:

$\forall i < n.\mathsf{Lb}(e')\ \gamma \downarrow_1 \Downarrow_i \mathsf{Lb}(v_{f1}) \wedge \mathsf{Lb}(e')\ \gamma \downarrow_2 \Downarrow \mathsf{Lb}(v'_{f1}) \implies$
$(W, n-i, \mathsf{Lb}(v_{f1}), \mathsf{Lb}(v'_{f1})) \in \lceil (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{Lb}(e')\ \gamma \downarrow_1 \Downarrow_i \mathsf{Lb}(v_{f1}) \wedge \mathsf{Lb}(e')\ \gamma \downarrow_2 \Downarrow \mathsf{Lb}(v'_{f1})$

We are required to prove

$(W, n-i, v_{f1}, v'_{f1}) \in \lceil (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rceil_V^{\mathcal{A}}$ (FB-LB0)

<u>IH</u>:

$(W, n, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we have:

$\forall j < n.e'\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge e'\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies (W, n-j, v_{f1}, v'_{f1}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $\mathsf{Lb}(e')\ \gamma \downarrow_1 \Downarrow_i \mathsf{Lb}(v_{f1})$. Therefore $\exists j < i < n$ s.t $e'\ \gamma \downarrow_1 \Downarrow_j v_{f1}$. Similarly since $\mathsf{Lb}(e')\ \gamma \downarrow_2 \Downarrow \mathsf{Lb}(v'_{f1})$ therefore $e'\ \gamma \downarrow_2 \Downarrow v'_{f1}$

This means we have

$(W, n-j, v_{f1}, v'_{f1}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$ (FB-LB1)

In order to prove (FB-LB0) from Definition 4.4 it suffices to prove that
$(W, n-i, v_{f1}, v'_{f1}) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

From cg-label we know that $i = j+1$. Therefore we get the desired from (FB-LB1) and Lemma 4.16

15. CG-unlabel:

$$\frac{\Gamma \vdash e' : \mathsf{Labeled}\ \ell\ \tau}{\Gamma \vdash \mathsf{unlabel}(e') : \mathbb{C}\ \top\ \ell\ \tau}$$

To prove: $(W, n, \mathsf{unlabel}(e')\ (\gamma \downarrow_1), \mathsf{unlabel}(e')\ (\gamma \downarrow_2)) \in \lceil (\mathbb{C}\ \top\ \ell\ \tau)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:
$\forall i < n.\mathsf{unlabel}(e')\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{unlabel}(e')\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n-i, v_{f1}, v'_{f1}) \in \lceil (\mathbb{C}\ \top\ \ell\ \tau)\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{unlabel}(e')\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{unlabel}(e') \gamma \downarrow_2 \Downarrow v'_{f1}$

From cg-val we know that $v_{f1} = \mathsf{unlabel}(e')\ \gamma \downarrow_1$ and $v'_{f1} = \mathsf{unlabel}(e')\ \gamma \downarrow_2$. Also $i = 0$

We are required to prove
$(W, n, \mathsf{unlabel}(e')\ \gamma \downarrow_1, \mathsf{unlabel}(e')\ \gamma \downarrow_2) \in \lceil (\mathbb{C}\ \top\ \ell\ \tau)\ \sigma \rceil_V^{\mathcal{A}}$

This means from Definition 4.4 we need to prove
Let $e_1 = \mathsf{unlabel}(e')\ \gamma \downarrow_1$ and $e_2 = \mathsf{unlabel}(e')\ \gamma \downarrow_2$
$\Big(\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, e_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, e_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell, v'_1, v'_2, \tau\ \sigma)\Big) \wedge$
$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, e_l) \Downarrow_j^f (H', v'_l) \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v'_l) \in \lfloor \tau' \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \top \sqsubseteq \ell') \wedge$
$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \top)\Big)$

We need to show

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, e_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, e_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell, v'_1, v'_2, \tau\ \sigma)$:

Also given is some $k \leq n$, $W_e \sqsupseteq W, H_1, H_2, v'_1, v'_2, j$ s.t $(k, H_1, H_2) \triangleright W_e$ and $(H_1, e_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, e_2) \Downarrow^f (H'_2, v'_2) \wedge j < k$

And we are required to prove
$\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell, v'_1, v'_2, \tau\ \sigma)$ (FB-U0)

IH: $(W_e, k, e'\ (\gamma\downarrow_1), e'\ (\gamma\downarrow_2)) \in \lceil(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we are given
$\forall I < k.e'\ \gamma\downarrow_1\Downarrow_I \mathsf{Lb}(v_{h1}) \wedge e'\ \gamma\downarrow_2\Downarrow \mathsf{Lb}(v'_{h1}) \implies$
$(W_e, k - I, \mathsf{Lb}(v_{h1}), \mathsf{Lb}(v'_{h1})) \in \lceil(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rceil_V^{\mathcal{A}}$

Since we know that
$(H_1, \mathsf{unlabel}(e')\ \gamma\downarrow_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, \mathsf{unlabel}(e')\ \gamma\downarrow_2) \Downarrow^f (H'_2, v'_2) \wedge j < k$ therefore
$\exists I < j < k$ s.t $e'\ \gamma\downarrow_1\Downarrow_I \mathsf{Lb}(v_{h1}) \wedge e'\ \gamma\downarrow_2\Downarrow \mathsf{Lb}(v'_{h1})$

Therefore we have
$(W_e, k - I, \mathsf{Lb}(v_{h1}), \mathsf{Lb}(v'_{h1})) \in \lceil(\mathsf{Labeled}\ \ell\ \tau)\ \sigma\rceil_V^{\mathcal{A}}$

This means from Definition 4.4 we have
$ValEq(\mathcal{A}, W_e, k - I, \ell, v_{h1}, v'_{h1}, \tau\ \sigma)$ (FB-U1)

In order to prove (FB-U0) we choose W' as W_e and from cg-unlabel we know that $H'_1 = H_1$ and $H'_2 = H_2$. And we already know that $(k, H_1, H_2) \triangleright W_e$. Therefore from Lemma 4.20 we get $(k - j, H_1, H_2) \triangleright W_e$

From cg-unlabel we know that v'_1, v'_2 in (FB-U0) is v_{h1}, v'_{h1} respectively. And since from (FB-U1) we know that $ValEq(\mathcal{A}, W_e, k - I, \ell, v_{h1}, v'_{h1}, \tau\ \sigma)$. Therefore from Lemma 4.25 we get
$ValEq(\mathcal{A}, W_e, k - j, \ell\ , v_{h1}, v'_{h1}, \tau\ \sigma)$

(b) $\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, e_l) \Downarrow_j^f (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor\tau\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \top \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \top)\Big)$:

Case $l = 1$
Given some $k, \theta_e \sqsupseteq W.\theta_l, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, e_l) \Downarrow_j^f (H', v'_l) \wedge j < k$

We need to prove
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor\tau\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \top \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \top)$

Since $(W, n, \gamma) \in \lceil\Gamma\rceil_V^{\mathcal{A}}$ therefore from Lemma 4.23 we know that
$\forall m.\ (W.\theta_1, m, \gamma\downarrow_1) \in \lfloor\Gamma\rfloor_V$ and $(W.\theta_2, m, \gamma\downarrow_2) \in \lfloor\Gamma\rfloor_V$

Instantiating m with k we get $(W.\theta_1, k, \gamma\downarrow_1) \in \lfloor\Gamma\rfloor_V$

Now we can apply Theorem 4.21 to get
$(W.\theta_1, k, (\mathsf{unlabel}\ e')\gamma\downarrow_1) \in \lfloor(\mathbb{C}\ \top\ \ell\ \tau)\ \sigma\rfloor_E$

This means from Definition 4.7 we get
$\forall c < k.(\mathsf{unlabel}\ e')\gamma\downarrow_1\Downarrow_c v \implies (W.\theta_1, k - c, v) \in \lfloor(\mathbb{C}\ \top\ \ell\ \tau)\ \sigma\rfloor_V$

This further means that given some $c < k$ s.t $(\mathsf{unlabel}\ e')\gamma\downarrow_1\Downarrow_c v$. From cg-val we know that $c = 0$ and $v = (\mathsf{unlabel}\ e')\gamma\downarrow_1$

And we have $(W.\theta_1, k, (\textsf{unlabel } e')\gamma \downarrow_1) \in \lfloor(\mathbb{C} \top \ell \tau) \ \sigma\rfloor_V$

From Definition 4.6 we have
$\forall K \leq k, \theta'_e \sqsupseteq W.\theta_1, H_1, J.(K, H_1) \rhd \theta'_e \wedge (H_1, (\textsf{unlabel } e')\gamma \downarrow_1) \Downarrow^f_J (H', v') \wedge J < K \implies$
$\exists \theta' \sqsupseteq \theta'_e.(K - J, H') \rhd \theta' \wedge (\theta', K - J, v') \in \lfloor \tau \ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H'(a) \implies \exists \ell'.\theta'_e(a) = \textsf{Labeled } \ell' \ \tau' \wedge \top \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta'_e).\theta'(a) \searrow \top)$

Instantiating K with k, θ'_e with θ_e, H_1 with H and J with j we get the desired

Case $l = 2$
Symmetric reasoning as in the $l = 1$ case above

16. CG-tolabeled:

$$\frac{\Gamma \vdash e' : \mathbb{C} \ \ell_1 \ \ell_2 \ \tau}{\Gamma \vdash \textsf{toLabeled}(e') : \mathbb{C} \ \ell_1 \perp (\textsf{Labeled } \ell_2 \ \tau)}$$

To prove: $(W, n, \textsf{toLabeled}(e') \ (\gamma \downarrow_1), \textsf{toLabeled}(e') \ (\gamma \downarrow_2)) \in \lceil (\mathbb{C} \ \ell_1 \perp (\textsf{Labeled } \ell_2 \ \tau)) \ \sigma \rceil^{\mathcal{A}}_E$

This means from Definition 4.5 we need to prove:
$\forall i < n.\textsf{toLabeled}(e') \ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \textsf{toLabeled}(e') \ \gamma \downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n - i, v_{f1}, v'_{f1}) \in \lceil (\mathbb{C} \ \ell_1 \perp (\textsf{Labeled } \ell_2 \ \tau)) \ \sigma \rceil^{\mathcal{A}}_V$

This means that given some $i < n$ s.t $\textsf{toLabeled}(e') \ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \textsf{toLabeled}(e') \ \gamma \downarrow_2 \Downarrow v'_{f1}$
From cg-val we know that $v_{f1} = \textsf{toLabeled}(e') \ \gamma \downarrow_1$, $v_{f2} = \textsf{toLabeled}(e') \ \gamma \downarrow_2$ and $i = 0$
We are required to prove
$(W, n, \textsf{toLabeled}(e') \ \gamma \downarrow_1, \textsf{toLabeled}(e') \ \gamma \downarrow_2) \in \lceil (\mathbb{C} \ \ell_1 \perp (\textsf{Labeled } \ell_2 \ \tau)) \ \sigma \rceil^{\mathcal{A}}_V$

Let $v_1 = \textsf{toLabeled}(e') \ \gamma \downarrow_1$ and $v_2 = \textsf{toLabeled}(e') \ \gamma \downarrow_2$
This means from Definition 4.4 we are required to prove
$\Big(\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \rhd W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow^f_j (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \rhd W' \wedge ValEq(\mathcal{A}, W', k - j, \perp, v'_1, v'_2, (\textsf{Labeled } \ell_2 \ \tau) \ \sigma)\Big) \wedge$
$\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \rhd \theta_e \wedge (H, v_l) \Downarrow^f_j (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \rhd \theta' \wedge (\theta', k - j, v'_l) \in \lfloor (\textsf{Labeled } \ell_o \ \tau) \ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \textsf{Labeled } \ell' \ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_1)\Big)$

We need to prove:

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \rhd W_e \wedge \forall v'_1, v'_2, j.$
$(H_1, v_1) \Downarrow^f_j (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \rhd W' \wedge ValEq(\mathcal{A}, W', k - j, \perp, v'_1, v'_2, (\textsf{Labeled } \ell_2 \ \tau) \ \sigma)$:

This means that we are given some $k \leq n$, $W_e \sqsupseteq W, H_1, H_2, v'_1, v'_2, j < k$ s.t

$(k, H_1, H_2) \triangleright W_e$ and $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2')$

And we need to prove
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \bot, v_1', v_2', (\mathsf{Labeled}\ \ell_2\ \tau)\ \sigma)$
From Definition 4.3 it suffices to prove that
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge (W', k-j, v_1', v_2') \in \lceil (\mathsf{Labeled}\ \ell_2\ \tau)\ \sigma \rceil_V^{\mathcal{A}}$

Further from Definition 4.4 it suffices to prove
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_2, v_1'', v_2'', \tau\ \sigma)$ (FB-TL0)
where $v_1' = \mathsf{Lb}\, v_1''$ and $v_2' = \mathsf{Lb}\, v_2''$

IH:
$(W_e, k, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil \mathbb{C}\ \ell_1\ \ell_2\ \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:
$\forall J < k.e'\ \gamma \downarrow_1 \Downarrow_J v_{h1} \wedge e'\ \gamma \downarrow_2 \Downarrow v_{h1}' \implies (W_e, n-J, v_{h1}, v_{h1}') \in \lceil \mathbb{C}\ \ell_1\ \ell_2\ \tau\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(H_1, \mathsf{toLabeled}(e')\gamma \downarrow_1) \Downarrow_j (H_1', v_1')$ and $(H_2, \mathsf{toLabeled}(e')\gamma \downarrow_1) \Downarrow_j (H_2', v_2')$. Therefore from cg-val we know that $\exists J < j < k \leq n$ s.t $e'\ \gamma \downarrow_1 \Downarrow_J v_{h1}$ and similarly we also know that $e'\ \gamma \downarrow_2 \Downarrow v_{h1}'$

This means we have
$(W_e, k-J, v_{h1}, v_{h1}') \in \lceil \mathbb{C}\ \ell_1\ \ell_2\ \tau\ \sigma \rceil_V^{\mathcal{A}}$

From Definition 4.4 we know that
$\Big(\forall k_1 \leq (k-J), W_e'' \sqsupseteq W_e.\forall H_1'', H_2''.(k_1, H_1'', H_2'') \triangleright W_e'' \wedge \forall v_1'', v_2'', m.$
$(H_1'', v_{h1}) \Downarrow_m^f (H_1', v_1'') \wedge (H_2'', v_{h1}') \Downarrow^f (H_2', v_2'') \wedge m < k_1 \implies$
$\exists W' \sqsupseteq W_e''.(k_1 - m, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k_1 - m, \ell_2, v_1'', v_2'', \tau\ \sigma)\Big) \wedge$
$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \ell_1)\Big)$ (FB-TL1)

We instantiate W_e'' with W_e, H_1'' with H_1, H_2'' with H_2 and k_1 with k in (FB-TL1). Since we know that $(H_1, \mathsf{toLabeled}(e')\gamma \downarrow_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, \mathsf{toLabeled}(e')\gamma \downarrow_2) \Downarrow^f (H_2', v_2')$, therefore $\exists m < j < k \leq n$ s.t $(H_1, v_{h1}) \Downarrow_m^f (H_1', v_1') \wedge (H_2, v_{h1}') \Downarrow^f (H_2', v_2')$
This means we have
$\exists W' \sqsupseteq W_e.(k-m, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-m, \ell_2, v_1'', v_2'', \tau\ \sigma)$ (FB-TL2)

In order to prove (FB-TL0) we choose W' as W' from (FB-TL2). Since from cg-tolabeled we know that $v_1' = \mathsf{Lb}(v_1'')$, $v_2' = \mathsf{Lb}(v_2'')$ and $j = m+1$ (therefore from Lemma 4.20 we get $(k-j, H_1', H_2') \triangleright W'$) and from (FB-TL2) and Lemma 4.25 we get $\mathit{ValEq}(\mathcal{A}, W', k-j, \ell_2, v_1'', v_2'', \tau\ \sigma)$

(b) $\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor (\mathsf{Labeled}\ \ell_2\ \tau)\ \sigma \rfloor_V \wedge$

$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta_e).\theta'(a) \searrow \ell_1)\Big)$:

Case $l = 1$

Given some $k, \theta_e \sqsupseteq W.\theta_l, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k$

We need to prove

$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v_l') \in \lfloor (\mathsf{Labeled}\ \ell_2\ \tau)\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta_e).\theta'(a) \searrow \ell_1)$

Since $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$ therefore from Lemma 4.23 we know that
$\forall m.\ (W.\theta_1, m, \gamma\downarrow_1) \in \lfloor \Gamma \rfloor_V$ and $(W.\theta_2, m, \gamma\downarrow_2) \in \lfloor \Gamma \rfloor_V$

Instantiating m with k we get $(W.\theta_1, k, \gamma\downarrow_1) \in \lfloor \Gamma \rfloor_V$

Now we can apply Theorem 4.21 to get
$(W.\theta_1, k, (\mathsf{toLabeled}\ e')\gamma\downarrow_1) \in \lfloor (\mathbb{C}\ \ell_1\ \bot\ \mathsf{Labeled}\ \ell_2\ \tau) \rfloor_E$

This means from Definition 4.7 we get
$\forall c < k.(\mathsf{toLabeled}\ e')\gamma\downarrow_1 \Downarrow_c v \implies (W.\theta_1, k - c, v) \in \lfloor (\mathbb{C}\ \ell_1\ \bot\ \mathsf{Labeled}\ \ell_2\ \tau) \rfloor_V$

Instantiating c with 0 and from cg-val we know $v = (\mathsf{toLabeled}\ e')\gamma\downarrow_1$

And we have $(W.\theta_1, k, (\mathsf{toLabeled}\ e')\gamma\downarrow_1) \in \lfloor (\mathbb{C}\ \ell_1\ \bot\ \mathsf{Labeled}\ \ell_2\ \tau) \rfloor_V$

From Definition 4.6 we have
$\forall K \leq k, \theta_e' \sqsupseteq W.\theta_1, H_1, J.(K, H_1) \triangleright \theta_e' \wedge (H_1, (\mathsf{toLabeled}\ e')\gamma\downarrow_1) \Downarrow_J^f (H', v') \wedge J < K \implies$
$\exists \theta' \sqsupseteq \theta_e'.(K - J, H') \triangleright \theta' \wedge (\theta', K - J, v') \in \lfloor \mathsf{Labeled}\ \ell_2\ \tau) \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H'(a) \implies \exists \ell'.\theta_e'(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta_e').\theta'(a) \searrow \ell_1)$

Instantiating K with k, θ_e' with θ_e, H_1 with H and J with j we get the desired

Case $l = 2$

Symmetric reasoning as in the $l = 1$ case above

17. CG-ret:

$$\frac{\Gamma \vdash e' : \tau}{\Gamma \vdash \mathsf{ret}(e') : \mathbb{C}\ \ell_1\ \ell_2\ \tau}$$

To prove: $(W, n, \mathsf{ret}(e')\ (\gamma\downarrow_1), \mathsf{ret}(e')\ (\gamma\downarrow_2)) \in \lceil (\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:

$\forall i < n.\mathsf{ret}(e')\ \gamma\downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{ret}(e')\ \gamma\downarrow_2 \Downarrow v_{f1}' \implies$
$(W, n - i, v_{f1}, v_{f1}') \in \lceil (\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{ret}(e')\ \gamma\downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{ret}(e')\ \gamma\downarrow_2 \Downarrow v_{f1}'$

From cg-val we know that $v_{f1} = \mathsf{ret}(e')\gamma\downarrow_1$, $v_{f2} = \mathsf{ret}(e')\gamma\downarrow_2$ and $i = 0$

We are required to prove
$(W, n, \mathsf{ret}(e')\gamma\downarrow_1, \mathsf{ret}(e')\gamma\downarrow_2) \in \lceil(\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma\rceil_V^{\mathcal{A}}$

Let $v_1 = \mathsf{ret}(e')\gamma\downarrow_1$ and $v_2 = \mathsf{ret}(e')\gamma\downarrow_2$

From Definition 4.4 it suffices to prove

$\Big(\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \rhd W_e \wedge \forall v_1', v_2'.$
$(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \rhd W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_2, v_1', v_2', \tau\ \sigma)\Big) \wedge$
$\forall l \in \{1,2\}.\Big(\forall v, i.\ (e_l \Downarrow_i v_l) \implies$
$\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \rhd \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \rhd \theta' \wedge (\theta', k-j, v_l') \in \lfloor\tau\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_1)\Big)$

It suffices to prove:

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \rhd W_e \wedge \forall v_1', v_2'.$
$(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \rhd W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_2, v_1', v_2', \tau\ \sigma)$:

We are given is some $k \leq n$, $W_e \sqsupseteq W, H_1, H_2, v_1', v_2', j < k$ s.t $(k, H_1, H_2) \rhd W_e$ and $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2')$

From cg-ret we know that $H_1' = H_1$ and $H_2' = H_2$

<u>And we are required to prove:</u>
$\exists W' \sqsupseteq W_e.(k-j, H_1, H_2) \rhd W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_2, v_1', v_2', \tau\ \sigma)$ (FB-R0)

<u>IH</u>: $(W_e, n, e'\ (\gamma\downarrow_1), e'\ (\gamma\downarrow_2)) \in \lceil\tau\ \sigma\rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:
$\forall J < k.e'\ \gamma\downarrow_1\Downarrow_J v_{h1} \wedge e'\ \gamma\downarrow_2\Downarrow v_{h1}' \implies (W_e, k-J, v_{h1}, v_{h1}') \in \lceil\tau\ \sigma\rceil_V^{\mathcal{A}}$

Since we know that $(H_1, \mathsf{ret}(e')\gamma\downarrow_1) \Downarrow_j^f (H_1, v_1') \wedge (H_2, \mathsf{ret}(e')\gamma\downarrow_2) \Downarrow^f (H_2, v_2')$, therefore $\exists J < j < k$ s.t $e'\ \gamma\downarrow_1\Downarrow_J v_{h1}$ and similarly $e'\ \gamma\downarrow_2\Downarrow v_{h1}'$.
Therefore we have $(W_e, k-J, v_{h1}, v_{h1}') \in \lceil\tau\ \sigma\rceil_V^{\mathcal{A}}$ (FB-R1)

In order to prove (FB-R0) we choose W' as W_e and from cg-ret we know that $v_1' = v_{h1}$ and $v_2' = v_{h1}'$. We need to prove the following:

i. $(k-j, H_1, H_2) \rhd W_e$:
Since we have $(k, H_1, H_2) \rhd W_e$ therefore from Lemma 4.20 we get
$(k-j, H_1, H_2) \rhd W_e$

ii. $\mathit{ValEq}(\mathcal{A}, W_e, k-j, \ell_2, v_1', v_2', \tau\ \sigma)$:
2 cases arise:

A. $\ell_2 \sqsubseteq \mathcal{A}$:
In this case from Definition 4.3 it suffices to prove
$(W_e, k-j, v_1', v_2') \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

Since $j = J+1$ therefore we get this from (FB-R1) and Lemma 4.16

B. $\ell_2 \not\sqsubseteq \mathcal{A}$:
In this case from Definition 4.3 it suffices to prove that
$\forall m.(W_e, m, v_1') \in \lfloor \tau\ \sigma \rfloor_V$ and $\forall m.(W_e, m, v_2') \in \lfloor \tau\ \sigma \rfloor_V$

We get this From (FB-R1) and Lemma 4.14

(b) $\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k,H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \textsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_1)$:

Case $l = 1$
Given some $k, \theta_e \sqsupseteq W.\theta_l, H, j$ s.t $(k,H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k$

We need to prove
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \textsf{Labeled}\ \ell'\ \tau \wedge \ell_o \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_o)$

Since $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$ therefore from Lemma 4.23 we know that
$\forall m.\ (W.\theta_1, m, \gamma\downarrow_1) \in \lfloor \Gamma \rfloor_V$ and $(W.\theta_2, m, \gamma\downarrow_2) \in \lfloor \Gamma \rfloor_V$

Instantiating m with k we get $(W.\theta_1, k, \gamma\downarrow_1) \in \lfloor \Gamma \rfloor_V$

Now we can apply Theorem 4.21 to get
$(W.\theta_1, k, (\textsf{ret}\ e')\gamma\downarrow_1) \in \lfloor (\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma \rfloor_E$

This means from Definition 4.7 we get
$\forall c < k.(\textsf{ret}\ e')\gamma\downarrow_1 \Downarrow_c v \implies (W.\theta_1, k-c, v) \in \lfloor (\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma \rfloor_V$

Instantiating c with 0 and from cg-val we know that $v = (\textsf{ret}\ e')\gamma\downarrow_1$

And we have $(W.\theta_1, k, (\textsf{ret}\ e')\gamma\downarrow_1) \in \lfloor (\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma \rfloor_V$

From Definition 4.6 we have
$\forall K \leq k, \theta_e' \sqsupseteq W.\theta_1, H_1, J.(K, H_1) \triangleright \theta_e' \wedge (H_1, v) \Downarrow_J^f (H', v') \wedge J < K \implies$
$\exists \theta' \sqsupseteq \theta_e'.(K-J, H') \triangleright \theta' \wedge (\theta', K-J, v') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H'(a) \implies \exists \ell'.\theta_e'(a) = \textsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e').\theta'(a) \searrow \ell_1)$

Instantiating K with k, θ_e' with θ_e, H_1 with H and J with j we get the desired

Case $l = 2$
Symmetric reasoning as in the $l = 1$ case above

18. CG-bind:

$$\frac{\Gamma, x : \tau \vdash e_b : \mathbb{C}\ \ell_3\ \ell_4\ \tau' \qquad \begin{array}{c}\Gamma \vdash e_l : \mathbb{C}\ \ell_1\ \ell_2\ \tau \\ \ell \sqsubseteq \ell_1 \qquad \ell \sqsubseteq \ell_3 \qquad \ell_2 \sqsubseteq \ell_3 \qquad \ell_2 \sqsubseteq \ell_4 \qquad \ell_4 \sqsubseteq \ell'\end{array}}{\Gamma \vdash \textsf{bind}(e_l, x.e_b) : \mathbb{C}\ \ell\ \ell'\ \tau'}$$

To prove: $(W, n, \mathsf{bind}(e_l, x.e_b)\ (\gamma\downarrow_1), \mathsf{bind}(e_l, x.e_b)\ (\gamma\downarrow_2)) \in \lceil(\mathbb{C}\ \ell\ \ell'\ \tau')\ \sigma\rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:

$\forall i < n.\mathsf{bind}(e_l, x.e_b)\ \gamma\downarrow_1\Downarrow_i v_{f1} \wedge \mathsf{bind}(e_l, x.e_b)\ \gamma\downarrow_2\Downarrow v'_{f1} \implies$
$(W, n-i, v_{f1}, v'_{f1}) \in \lceil(\mathbb{C}\ \ell\ \ell'\ \tau')\ \sigma\rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{bind}(e_l, x.e_b)\ \gamma\downarrow_1\Downarrow_i v_{f1} \wedge \mathsf{bind}(e_l, x.e_b)\gamma\downarrow_2\Downarrow v'_{f1}$

From cg-val we know that $v_{f1} = \mathsf{bind}(e_l, x.e_b)\gamma\downarrow_1,\ v_{f2} = \mathsf{bind}(e_l, x.e_b)\gamma\downarrow_2$ and $i = 0$

We are required to prove

$(W, n, \mathsf{bind}(e_l, x.e_b)\gamma\downarrow_1, \mathsf{bind}(e_l, x.e_b)\gamma\downarrow_2) \in \lceil(\mathbb{C}\ \ell\ \ell'\ \tau')\ \sigma\rceil_V^{\mathcal{A}}$

Let $v_1 = \mathsf{bind}(e_l, x.e_b)\gamma\downarrow_1$ and $v_2 = \mathsf{bind}(e_1, x.e_b)\gamma\downarrow_2$

This means from Definition 4.4 we need to prove

$\Big(\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k-j, \ell', v'_1, v'_2, \tau\ \sigma)\Big) \wedge$
$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v'_l) \in \lfloor\tau\ \sigma\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta')\backslash dom(\theta_e).\theta'(a) \searrow \ell)\Big)$

This means we need to prove:

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2, j.$
$(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k-j, \ell', v'_1, v'_2, \tau\ \sigma)$:

This means we are given some $k \leq n, W_e \sqsupseteq W, H_1, H_2$ s.t $(k, H_1, H_2) \triangleright W_e$

Also given some $v'_1, v'_2, j < k$ s.t $(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2)$

And we are required to prove:

$\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k-j, \ell', v'_1, v'_2, \tau'\ \sigma)$ (FB-B0)

IH1:

$(W_e, k, e_l\ (\gamma\downarrow_1), e_l\ (\gamma\downarrow_2)) \in \lceil(\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma\rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:

$\forall f < k.e_l\ \gamma\downarrow_1\Downarrow_f v_{h1} \wedge e_l\ \gamma\downarrow_2\Downarrow v'_{h1} \implies$
$(W_e, k-f, v_{h1}, v'_{h1}) \in \lceil(\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma\rceil_V^{\mathcal{A}}$

Since we know that $(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2)$ therefore $\exists f < j < k$ s.t $e_l\ \gamma\downarrow_f\Downarrow_j v_{h1} \wedge e_l\ \gamma\downarrow_2\Downarrow v'_{h1}$

This means we have

$(W_e, k-f, v_{h1}, v'_{h1}) \in \lceil(\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma\rceil_V^{\mathcal{A}}$

This means from Definition 4.4 we have

$\Big(\forall K \leq (k-f), W'_e \sqsupseteq W_e.\forall H''_1, H''_2.(K, H''_1, H''_2) \triangleright W'_e \wedge \forall v''_1, v''_2, J.$
$(H''_1, v_{h1}) \Downarrow^f_J (H'_1, v''_1) \wedge (H''_2, v'_{h1}) \Downarrow^f (H'_2, v''_2) \wedge J < K \implies$
$\exists W'' \sqsupseteq W'_e.(K-J, H'_1, H'_2) \triangleright W'' \wedge ValEq(\mathcal{A}, W'', K-J, \ell_2, v''_1, v''_2, \tau\ \sigma)\Big) \wedge$
$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow^f_j (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v'_l) \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_1)\Big)$

Instantiating K with $(k-f)$, W'_e with W_e, H''_1 with H_1 and H''_2 with H_2 in the first conjunct of the above equation. Since we know that $(k, H_1, H_2) \triangleright W_e$ therefore from Lemma 4.20 we also have $(k-f, H_1, H_2) \triangleright W_e$

Since we know that $(H_1, v_1) \Downarrow^f_j (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2)$ therefore $\exists J < j - f < k - f$ s.t $(H_1, v_{h1}) \Downarrow^f_J (H'_1, v''_1) \wedge (H_2, v'_{h1}) \Downarrow^f (H'_2, v''_2)$

This means we have
$\exists W'' \sqsupseteq W'_e.(k-f-J, H'_1, H'_2) \triangleright W'' \wedge ValEq(\mathcal{A}, W'', k-f-J, \ell_2, v''_1, v''_2, \tau\ \sigma)$ (FB-B1)

From Definition 4.3 two cases arise:

i. $\ell_2 \sqsubseteq \mathcal{A}$:

In this case we know that $(W'', k-f-J, v''_1, v''_2) \in \lceil \tau\ \sigma \rceil^{\mathcal{A}}_V$

<u>IH2</u>:
$(W'', k-f-J, e_b\ (\gamma \downarrow_1 \cup \{x \mapsto v''_1\}), e_b\ (\gamma \downarrow_2 \cup \{x \mapsto v''_2\})) \in \lceil (\mathbb{C}\ \ell_3\ \ell_4\ \tau')\ \sigma \rceil^{\mathcal{A}}_E$

This means from Definition 4.5 we need to prove:
$\forall s < k-f-J.e_b\ (\gamma \downarrow_1 \cup \{x \mapsto v''_1\}) \Downarrow_s v_{h2} \wedge e_b\ (\gamma \downarrow_2 \cup \{x \mapsto v''_2\}) \Downarrow v'_{h2} \implies$
$(W'', k-f-J-s, v_{h2}, v'_{h2}) \in \lceil (\mathbb{C}\ \ell_3\ \ell_4\ \tau')\ \sigma \rceil^{\mathcal{A}}_V$

Since we know that $(H_1, \mathsf{bind}(e_l, x.e_b)\ \gamma \downarrow_1) \Downarrow^f_j (H'_1, v'_1) \wedge (H_2, \mathsf{bind}(e_l, x.e_b)\ \gamma \downarrow_2) \Downarrow^f (H'_2, v'_2)$ therefore $\exists s < j-f-J < k-f-J$ s.t $e_b\ (\gamma \downarrow_1 \cup \{x \mapsto v''_1\}) \Downarrow_s v_{h2} \wedge e_b\ (\gamma \downarrow_2 \cup \{x \mapsto v''_2\}) \Downarrow v'_{h2}$

This means we have
$(W'', k-f-J-s, v_{h2}, v'_{h2}) \in \lceil (\mathbb{C}\ \ell_3\ \ell_4\ \tau')\ \sigma \rceil^{\mathcal{A}}_V$

This means from Definition 4.4 we know that
$\Big(\forall K_s \leq (k-f-J-s), W_s \sqsupseteq W''.\forall H_1, H_2.(K_s, H_1, H_2) \triangleright W_s \wedge \forall v'_{s1}, v'_{s2}, J_s.$
$(H_1, v_{h2}) \Downarrow^f_{J_s} (H'_{s1}, v'_{s1}) \wedge (H_2, v'_{h2}) \Downarrow^f (H'_{s2}, v'_{s2}) \wedge J_s < K_s \implies$
$\exists W'_s \sqsupseteq W_s.(K_s - J_s, H'_{s1}, H'_{s2}) \triangleright W'_s \wedge ValEq(\mathcal{A}, W'_s, K_s - J_s, \ell_4, v'_1, v'_2, \tau'\ \sigma)\Big) \wedge$
$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow^f_j (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v'_l) \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_3 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_3)\Big)$

Instantiating K_s with $(k-f-J-s)$, W_s with W'', H_1 with H_1' and H_2' with H_2. Since we know that $(k-f-J, H_1', H_2') \triangleright W''$ therefore from Lemma 4.20 we also have $(k-f-J-s, H_1', H_2') \triangleright W''$

Since we know that $(H_1, \mathsf{bind}(e_l, x.e_b)\ \gamma \downarrow_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, \mathsf{bind}(e_l, x.e_b)\ \gamma \downarrow_2) \Downarrow^f (H_2', v_2')$ therefore $\exists J_s < j-f-J-s < k-f-J-s$ s.t $(H_1', v_1'') \Downarrow_{J_s}^f (H_{s1}', v_{s1}') \wedge (H_2', v_2'') \Downarrow^f (H_{s2}', v_{s2}')$

This means we have
$\exists W_s' \sqsupseteq W_s.(k-f-J-s-J_s, H_{s1}', H_{s2}') \triangleright W_s' \wedge \mathit{ValEq}(\mathcal{A}, W_s', k-f-J-s-J_S, \ell_4, v_{s1}', v_{s2}', \tau'\ \sigma)$ (FB-B2)

In order to prove (FB-B0) we choose W' as W_s'. From cg-bind we know that $H_1' = H_{s1}'$, $H_2' = H_{s2}'$, $v_1' = v_{s1}'$, $v_2' = v_{s2}'$ and $j = f+J+s+J_s+1$. And we need to prove:

A. $(k-j, H_{s1}', H_{s2}') \triangleright W_s'$:
Since from (FB-B2) we know that $(k-f-J-s-J_s, H_{s1}', H_{s2}') \triangleright W_s'$ therefore from Lemma 4.20 we get
$(k-j, H_{s1}', H_{s2}') \triangleright W_s'$

B. $\mathit{ValEq}(\mathcal{A}, W_s', k-j, \ell', v_{s1}', v_{s2}', \tau'\ \sigma)$:
Since from (FB-B2) we know that $\mathit{ValEq}(\mathcal{A}, W_s', k-f-J-s-J_S, \ell_4, v_{s1}', v_{s2}', \tau'\ \sigma)$ therefore from Lemma 4.25 we get
$\mathit{ValEq}(\mathcal{A}, W_s', k-j, \ell', v_{s1}', v_{s2}', \tau'\ \sigma)$

ii. $\ell_2 \not\sqsubseteq \mathcal{A}$:

From (FB-B0) we know that we need to prove
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_o, v_1', v_2', \tau'\ \sigma)$
Since $\ell_2 \sqsubseteq \ell_4 \sqsubseteq \ell'$ and $\ell \not\sqsubseteq \mathcal{A}$ therefore we have $\ell_4 \not\sqsubseteq \mathcal{A}$ and $\ell' \not\sqsubseteq \mathcal{A}$

This means that from Definition 4.3 it suffices to prove
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \forall m_{u1}.(W'.\theta_1, m_{u1}, v_1') \in \lfloor \tau'\ \sigma \rfloor_V \wedge \forall m_{u2}.(W'.\theta_2, m_{u2}, v_2') \in \lfloor \tau'\ \sigma \rfloor_V$

This means given some m_{u1}, m_{u2} and we need to prove
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge (W'.\theta_1, m_{u1}, v_1') \in \lfloor \tau'\ \sigma \rfloor_V \wedge (W'.\theta_2, m_{u2}, v_2') \in \lfloor \tau'\ \sigma \rfloor_V$ (FB-B01)

In this case from (FB-B1) and Definition 4.3 we know that
$\forall m.\ (W''.\theta_1, m, v_1'') \in \lfloor \tau\ \sigma \rfloor_V$ and $\forall m.\ (W''.\theta_2, m, v_2'') \in \lfloor \tau\ \sigma \rfloor_V$ (FB-B3)

Since $\mathsf{bind}(e_l, x.e_b)\gamma \downarrow_1 \Downarrow_j v_1'$ therefore $\exists J_1 < j-f-J < k-f-J$ s.t $(e_b)\gamma \downarrow_1 \cup \{x \mapsto v_1''\} \Downarrow_{J_1} v_1'$. Similarly, $\exists J_1' < j-f-J-J_1 < k-f-J-J_1$ s.t $(H_1', v_1') \Downarrow_{J_1'}^f -$

Instantiating m with $m_{u1}+1+J_1+J_1'$ in the first conjunct of (FB-B3)
$(W''.\theta_1, m_{u1}+1+J_1+J_1', v_1'') \in \lfloor \tau\ \sigma \rfloor_V$

Since $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$ therefore from Lemma 4.23 we know that
$\forall m.\ (W.\theta_1, m, \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$

Instantiating m with $m_{u1}+1+J_1+J_1'$ we get $(W.\theta_1, m_{u1}+1+J_1+J_1', \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$

From Lemma 4.17 we know that
$(W''.\theta_1, m_{u1} + 1 + J_1 + J_1', \gamma \downarrow_1) \in \lfloor \Gamma \rfloor_V$ (FB-B4)

Now we can apply Theorem 4.21 to get
$(W''.\theta_1, m_{u1} + 1 + J_1 + J_1', (e_b)\gamma \downarrow_1 \cup \{x \mapsto v_1''\}) \in \lfloor (\mathbb{C}\ \ell_3\ \ell_4\ \tau')\ \sigma \rfloor_E$

This means from Definition 4.7 we get
$\forall c_1 < m_{u1} + 1 + J_1 + J_1'.(e_b)\gamma \downarrow_1 \cup \{x \mapsto v_1''\} \Downarrow_{c_1} v_{o1} \implies (W''.\theta_1, m_{u1} + 1 + J_1 + J_1' - c_1, v_{o1}) \in \lfloor (\mathbb{C}\ \ell_3\ \ell_4\ \tau')\ \sigma \rfloor_V$ (FB-B5)

Instantiating c_1 with J_1 in (FB-B5)
Therefore we have $(W''.\theta_1, m_{u1} + 1 + J_1', v_{o1}) \in \lfloor (\mathbb{C}\ \ell_3\ \ell_4\ \tau')\ \sigma \rfloor_V$

From Definition 4.6 we have
$\forall K \leq (m_{u1}+1+J_1'), \theta_e' \sqsupseteq W''.\theta_1, H_1, J_2.(K, H_1) \rhd \theta_e' \wedge (H_1, v_{o1}) \Downarrow^f_{J_2} (H_1'', v_1') \wedge J_2 < K \implies$
$\exists \theta_1' \sqsupseteq \theta_e'.(K - J_2, H_1'') \rhd \theta_1' \wedge (\theta_1', K - J_2, v_1') \in \lfloor \tau'\ \sigma \rfloor_V \wedge$
$(\forall a. H_1(a) \neq H_1''(a) \implies \exists \ell'.\theta_e'(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_3 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta_e').\theta_1'(a) \searrow \ell_3)$

Instantiating K with $m_{u1} + 1 + J_1'$, θ_e' with $W''.\theta_1$, H_1 with H_1' (from FB-B1) and J_2 with J_1' we get

$\exists \theta_1' \sqsupseteq W''.\theta_1.(m_{u1} + 1, H_1'') \rhd \theta_1' \wedge (\theta_1', m_{u1} + 1, v_1') \in \lfloor \tau'\ \sigma \rfloor_V \wedge$
$(\forall a. H_1(a) \neq H_1''(a) \implies \exists \ell'. W''.\theta_1(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_3 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta_e').\theta_1'(a) \searrow \ell_3)$ (FB-B6)

Since we know that $\mathsf{bind}(e_l, x.e_b)\gamma \downarrow_2 \Downarrow v_2'$. Say this reduction happens in t steps. Therefore $\exists t_1 < t < k \leq n$ s.t $(e_l)\gamma \downarrow_2 \cup \{x \mapsto v_2''\} \Downarrow_{t_1} v_{l2}$ and simialrly $\exists t_2 < t - t_1 < k - t_1$ s.t $(H, v_{l2})\gamma \downarrow_2 \Downarrow^f_{t_2} (H_2'', v_2'')$

Again since $\mathsf{bind}(e_l, x.e_b)\gamma \downarrow_2 \Downarrow_t v_2'$ therefore $\exists J_2 < t - t_1 - t_2 < k - t_1 - t_2$ s.t $(e_b)\gamma \downarrow_2 \cup \{x \mapsto v_2''\} \Downarrow_{J_2} v_2'$. Similarly $\exists J_2' < t - t_1 - t_2 - J_2 < k - t_1 - t_2 - J_2$ s.t $(H_2', v_2') \Downarrow^f_{J_2'} -$

Instantiating the second conjunct of (FB-B3) with $m_{u2} + 1 + J_2 + J_2'$ we get
$(W''.\theta_2, m_{u2} + 1 + J_2 + J_2', v_2'') \in \lfloor \tau\ \sigma \rfloor_V$

Again since $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$ therefore from Lemma 4.23 we know that
$\forall m.\ (W.\theta_2, m, \gamma \downarrow_2) \in \lfloor \Gamma \rfloor_V$

Instantiating m with $m_{u2}+1+J_2+J_2'$ we get $(W.\theta_2, m_{u2}+1+J_2+J_2', \gamma \downarrow_2) \in \lfloor \Gamma \rfloor_V$

From Lemma 4.17 we know that
$(W''.\theta_2, m_{u2} + 1 + J_2 + J_2', \gamma \downarrow_2) \in \lfloor \Gamma \rfloor_V$ (FB-B7)

Now we can apply Theorem 4.21 to get
$(W''.\theta_2, m_{u2} + 1 + J_2 + J_2', (e_b)\gamma \downarrow_2 \cup \{x \mapsto v_2''\}) \in \lfloor (\mathbb{C}\ \ell_3\ \ell_4\ \tau')\ \sigma \rfloor_E$

This means from Definition 4.7 we get
$\forall c_2 < (m_{u2} + 1 + J_2 + J_2').(e_b)\gamma \downarrow_2 \cup \{x \mapsto v_2''\} \Downarrow_{c_2} v_{o2} \implies (W''.\theta_2, m_{u2} + 1 + J_2 - c_2, v_{o2}) \in \lfloor (\mathbb{C}\ \ell_3\ \ell_4\ \tau')\ \sigma \rfloor_V$ (FB-B8)

Instantiating c_2 with J_2 in (FB-B8) we get

$(W''.\theta_2, m_{u2} + 1 + J_2', v_{o2}) \in \lfloor(\mathbb{C}\ \ell_3\ \ell_4\ \tau')\ \sigma\rfloor_V$

From Definition 4.6 we have
$\forall K \leq (m_{u2}+1+J_2'), \theta_e' \sqsupseteq W''.\theta_2, H_2, J_3.(K, H_2) \triangleright \theta_e' \wedge (H_2, v_{o2}) \Downarrow_{J_3}^{f} (H_2'', v_2') \wedge J_3 < K \implies$
$\exists \theta_2' \sqsupseteq \theta_e'.(K - J_3, H_2'') \triangleright \theta_2' \wedge (\theta_2', K - J_3, v_2') \in \lfloor\tau'\ \sigma\rfloor_V \wedge$
$(\forall a.H_2(a) \neq H_2''(a) \implies \exists \ell'.\theta_e'(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_3 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2') \backslash dom(\theta_e').\theta_2'(a) \searrow \ell_3)$

Instantiating K with $m_{u2} + 1 + J_2'$, θ_e' with $W''.\theta_2$, H_2 with H_2' (from FB-B1) and J_3 with J_2', we get

$\exists \theta_2' \sqsupseteq W''.\theta_2.(m_{u2} + 1, H_2'') \triangleright \theta_2' \wedge (\theta_2', m_{u2} + 1, v_2') \in \lfloor\tau'\ \sigma\rfloor_V \wedge$
$(\forall a.H_2(a) \neq H_2''(a) \implies \exists \ell'. W''.\theta_2(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_3 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_2') \backslash dom(\theta_e').\theta_2'(a) \searrow \ell_3)$ (FB-B9)

In order to prove (FB-B01) we chose W' as W_n where W_n is defined as follows:
$W_n.\theta_1 = \theta_1'$ (From (FB-B6))
$W_n.\theta_2 = \theta_2'$ (From (FB-B9))
$W_n.\hat{\beta} = W''.\hat{\beta}$ (From (FB-B1))

It suffices to prove

- $(k - j, H_1'', H_2'') \triangleright W_n$:
  From Definition 4.9 we need to prove the following
  - $dom(W_n.\theta_1) \subseteq dom(H_1'') \wedge dom(W_n.\theta_2) \subseteq dom(H_2'')$:

    From (FB-B6) we know that $(m_{u1}+1, H_1'') \triangleright \theta_1'$ therefore from Definition 4.8 we know that $dom(W_n.\theta_1) \subseteq dom(H_1'')$
    Similarly from (FB-B9) we know that $(m_{u2} + 1, H_2'') \triangleright \theta_2'$ therefore from Definition 4.8 we know that $dom(W_n.\theta_2) \subseteq dom(H_2'')$
  - $(W_n.\hat{\beta}) \subseteq (dom(W_n.\theta_1) \times dom(W_n.\theta_2))$:

    Since from (FB-B1) we know that $(k - f - J, H_1', H_2') \triangleright W''$ therefore from Definition 4.9 we know that $(W''.\hat{\beta}) \subseteq (dom(W''.\theta_1) \times dom(W''.\theta_2))$

    Since from (FB-B6) and (FB-B9) we know that $W''.\theta_1 \sqsubseteq W_n.\theta_1$ and $W''.\theta_2 \sqsubseteq W_n.\theta_2$

    Therefore we get
    $(W_n.\hat{\beta}) \subseteq (dom(W_n.\theta_1) \times dom(W_n.\theta_2))$
  - $\forall (a_1, a_2) \in (W_n.\hat{\beta}).(W_n.\theta_1(a_1) = W_n.\theta_2(a_2) \wedge (W_n, k-j-1, H_1''(a_1), H_2''(a_2)) \in \lceil W_n.\theta_1(a_1)\rceil_V^{\mathcal{A}})$:

    4 cases arise for each $(a_1, a_2) \in W_n.\hat{\beta}$

    A. $H_1'(a_1) = H_1''(a_1) \wedge H_2'(a_2) = H_2''(a_2)$:

       To prove:
       $W_n.\theta_1(a_1) = W_n.\theta_2(a_2)$:
       We know from that $(k - f - J, H_1', H_2') \triangleright W''$

       Therefore from Definition 4.9 we have
       $\forall (a_1', a_2') \in (W''.\hat{\beta}). W''.\theta_1(a_1') = W''.\theta_2(a_2')$

Since $W_n.\hat{\beta} = W''.\hat{\beta}$ by construction therefore
$\forall (a_1', a_2') \in (W_n.\hat{\beta}). W''.\theta_1(a_1') = W''.\theta_2(a_2')$

From (FB-B6) and (FB-B9) we know that $W''.\theta_1 \sqsubseteq \theta_1'$ and $W''.\theta_2 \sqsubseteq \theta_2'$ respectively.

Therefore from Definition 4.1
$\forall (a_1', a_2') \in (W_n.\hat{\beta}).\theta_1'(a_1) = \theta_2'(a_2)$

To prove:
$(W_n, k - j - 1, H_1''(a_1), H_2''(a_2)) \in \lceil W_n.\theta_1(a_1)\rceil_V^{\mathcal{A}}$:
From (FB-B1) we know that $(k - f - J, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W''$

This means from Definition 4.9 we know that
$\forall (a_{i1}, a_{i2}) \in (W''.\hat{\beta}). W''.\theta_1(a_{i1}) = W''.\theta_2(a_{i2}) \wedge$
$(W'', k - f - J - 1, H_1'(a_{i1}), H_2'(a_{i2})) \in \lceil W''.\theta_1(a_{i1})\rceil_V^{\mathcal{A}}$

Instantiating with a_1 and a_2 and since $W'' \sqsubseteq W_n$ and $k - j - 1 < k - f - J - 1$ (since $j = f + J + J_1 + 1$ therefore from Lemma 4.16 we get
$(W_n, k - j - 1, H_1'(a_1), H_2'(a_2)) \in \lceil W_n.\theta_1(a_1)\rceil_V^{\mathcal{A}}$

B. $H_1'(a_1) \neq H_1''(a_1) \wedge H_2'(a_2) \neq H_2''(a_2)$:

To prove:
$W_n.\theta_1(a_1) = W_n.\theta_2(a_2)$
Same reasoning as in the previous case

To prove:
$(W_n, k - j - 1, H_1''(a_1), H_2''(a_2)) \in \lceil W_n.\theta_1(a_1)\rceil_V^{\mathcal{A}}$

From (FB-B6) and (FB-B9) we know that
$(\forall a.H_1'(a) \neq H_1''(a) \implies \exists \ell'. W''.\theta_1(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge (\ell_3) \sqsubseteq \ell')$
$(\forall a.H_2'(a) \neq H_2''(a) \implies \exists \ell'. W''.\theta_2(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge (\ell_3) \sqsubseteq \ell')$
This means we have
$\exists \ell'. W''.\theta_1(a_1) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge (\ell_3) \sqsubseteq \ell'$ and
$\exists \ell'. W''.\theta_2(a_2) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge (\ell_3) \sqsubseteq \ell'$

Since $\ell_2 \not\sqsubseteq \mathcal{A}$. Therefore, $\ell_3 \not\sqsubseteq \mathcal{A}$.

Also from (FB-B6) and (FB-B9), $(m_{u1}+1, H_1'') \triangleright \theta_1'$ and $(m_{u2}+1, H_2'') \triangleright \theta_2'$.
Therefore from Definition 4.8 we have
$(\theta_1', m_{u1}, H_1''(a_1)) \in \lfloor \theta_1'(a_1)\rfloor_V$ and
$(\theta_2', m_{u2}, H_2''(a_1)) \in \lfloor \theta_2'(a_2)\rfloor_V$

Since m_{u1} and m_{u2} are arbitrary indices therefore from Definition 4.4 we get
$(W_n, k - j - 1, H_1''(a_1), H_2''(a_2)) \in \lceil \theta_1'(a_1)\rceil_V^{\mathcal{A}}$

C. $H_1'(a_1) = H_1''(a_1) \wedge H_2'(a_2) \neq H_2''(a_2)$:

To prove:
$W_n.\theta_1(a_1) = W_n.\theta_2(a_2)$

Same reasoning as in the previous case

To prove:
$(W_n, k-j-1, H_1''(a_1), H_2''(a_2)) \in \lceil W_n.\theta_1(a_1)\rceil_V^{\mathcal{A}}$

From (FB-B9) we know that
$(\forall a. H_2'(a) \neq H_2''(a) \implies \exists \ell'. W''.\theta_2(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge (\ell_3) \sqsubseteq \ell')$

This means we have
$\exists \ell'. W''.\theta_2(a_2) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge (\ell_3) \sqsubseteq \ell'$
Since $\ell_2 \not\sqsubseteq \mathcal{A}$. Therefore, $\ell_3 \not\sqsubseteq \mathcal{A}$.

Since from (FB-B1) we know that $(k-f-J, H_1', H_2') \overset{\mathcal{A}}{\triangleright} W''$ that means from Definition 4.9 that $(W'', k-f-J-1, H_1'(a_1), H_2'(a_2)) \in \lceil W''.\theta_1(a_1)\rceil_V^{\mathcal{A}}$. Since $W''.\theta_1(a_1) = W''.\theta_2(a_2) = \mathsf{Labeled}\ \ell'\ \tau''$ and since $\ell' \not\sqsubseteq \mathcal{A}$ therefore from Definition 4.4 and Definition 4.3 we know that

Therefore
$\forall m.\ (W''.\theta_1, m, H_1'(a_1)) \in W''.\theta_1(a_1) \quad$ (F)

Instantiating the (F) with m_{u1} and using Lemma 4.15 we get
$(\theta_1', m_{u1}, H_1'(a_1)) \in \theta_1'(a_1)$

Since from (FB-B9) we know that $(m_{u2}+1, H_2'') \triangleright \theta_2'$ therefore from Definition 4.8 we know that $(\theta_2', m_{u2}, H_2''(a_2)) \in \theta_2'(a_2)$
Therefore from Definition 4.4 we get
$(W', k-j-1, H_1''(a_1), H_2''(a_2)) \in \lceil \theta_1'(a_1)\rceil_V^{\mathcal{A}}$

D. $H_1'(a_1) \neq H_1''(a_1) \wedge H_2'(a_2) = H_2''(a_2)$:
Symmetric reasoning as in the previous case

– $\forall i \in \{1,2\}.\forall m.\forall a_i \in dom(W_n.\theta_i).(W_n.\theta_i, m, H_i''(a_i)) \in \lfloor W_n.\theta_i(a_i)\rfloor_V$:

Case $i = 1$
Given some m we need to prove
$\forall a_i \in dom(W_n.\theta_i).(W_n.\theta_i, m, H_i''(a_i)) \in \lfloor W_n.\theta_i(a_i)\rfloor_V$

This further means that given some $a_1 \in dom(W_n.\theta_i)$ we need to show
$(W_n.\theta_1, m, H_1''(a_1)) \in \lfloor W_n.\theta_1(a_1)\rfloor_V$

Since $W_n.\theta_1 = \theta_1'$, it suffices to prove
$(\theta_1', m, H_1''(a_1)) \in \lfloor \theta_1'(a_1)\rfloor_V$

Like before we apply Theorem 4.21 on $e_b\ \gamma \downarrow_1 \cup \{x \mapsto v_1''\}$ but this time at $m + 1 + J_1 + J_1'$ to get
$\exists \theta_1' \sqsupseteq W''.\theta_1.(m+1, H_1'') \triangleright \theta_1' \wedge (\theta_1', m_{u1}+1, v_1') \in \lfloor \tau' \rfloor_V \wedge$
$(\forall a. H_1(a) \neq H_1''(a) \implies \exists \ell'. W''.\theta_1(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_3 \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta_1') \backslash dom(\theta_e').\theta_1'(a) \searrow \ell_3)$

Since we have $\ell \sqsubseteq \ell_3$ and $(m+1, H_1'') \triangleright \theta_1'$ therefore from Definition 4.8 we get the desired.
Case $i = 2$
Similar reasoning as in the $i = 1$ case

- $(W'.\theta_1, m_{u1}, v_1') \in \lfloor \tau' \rfloor_V \wedge (W'.\theta_2, m_{u2}, v_2') \in \lfloor \tau'\ \sigma \rfloor_V$:
We get this from (FB-B6), (FB-B9) and Lemma 4.15 we get the desired

19. CG-ref:

$$\frac{\Gamma \vdash e' : \mathsf{Labeled}\ \ell'\ \tau \qquad \mathcal{L} \vdash \ell \sqsubseteq \ell'}{\Gamma \vdash \mathsf{new}\ (e') : \mathbb{C}\ \ell\ \bot\ (\mathsf{ref}\ \ell'\ \tau)}$$

To prove: $(W, n, \mathsf{new}\ (e')\ (\gamma \downarrow_1), \mathsf{new}\ (e')\ (\gamma \downarrow_2)) \in \lceil (\mathbb{C}\ \ell\ \bot\ (\mathsf{ref}\ \ell'\ \tau))\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:
$\forall i < n.\mathsf{new}\ (e')\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{new}\ (e')\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n - i, v_{f1}, v'_{f1}) \in \lceil (\mathbb{C}\ \ell\ \bot\ (\mathsf{ref} \ell'\ \tau))\ \sigma \rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $\mathsf{new}\ (e')\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge \mathsf{new}\ (e')\ \gamma \downarrow_2 \Downarrow v'_{f1}$
From cg-val we know that $v_{f1} = \mathsf{new}\ (e')\gamma \downarrow_1$, $v_{f2} = \mathsf{new}\ (e')\gamma \downarrow_2$ and $i = 0$
We are required to prove
$(W, n, \mathsf{new}\ (e')\gamma \downarrow_1, \mathsf{new}\ (e')\gamma \downarrow_2) \in \lceil (\mathbb{C}\ \ell\ \bot\ (\mathsf{ref}\ \ell'\ \tau))\ \sigma \rceil_V^{\mathcal{A}}$

Let $v_1 = \mathsf{new}\ (e')\gamma \downarrow_1$ and $v_2 = \mathsf{new}\ (e')\gamma \downarrow_2$
From Definition 4.4 we are required to prove
$\Big(\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k - j, \bot, v'_1, v'_2, (\mathsf{ref}\ \ell'\ \tau))\Big) \wedge$
$\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor (\mathsf{ref}\ \ell'\ \tau) \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)\Big)$

This means we need to prove the following:

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k - j, \bot, v'_1, v'_2, (\mathsf{ref}\ \ell'\ \tau)\ \sigma)$:

This means we are given some $k \leq n, W_e \sqsupseteq W, H_1, H_2$ s.t $(k, H_1, H_2) \triangleright W_e$

Also we are given some $v'_1, v'_2, j < k$ s.t $(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2)$

And we are required to prove:
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \triangleright W' \wedge ValEq(\mathcal{A}, W', k - j, \bot, v'_1, v'_2, (\mathsf{ref}\ \ell'\ \tau)\ \sigma)$
Further from Definition 4.3 it suffices to prove
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \triangleright W' \wedge (W', k - j, v'_1, v'_2) \in \lceil (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rceil_V^{\mathcal{A}}$ (FB-R0)

IH:
$(W_e, k, e'\ (\gamma \downarrow_1), e'\ (\gamma \downarrow_2)) \in \lceil \mathsf{Labeled}\ \ell'\ \tau\ \sigma \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:
$\forall f < k.e'\ \gamma \downarrow_1 \Downarrow_f v_{h1} \wedge e'\ \gamma \downarrow_2 \Downarrow v'_{h1} \implies (W_e, k - f, v_{h1}, v'_{h1}) \in \lceil \mathsf{Labeled}\ \ell'\ \tau\ \sigma \rceil_V^{\mathcal{A}}$

Since we know that $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2')$ therefore $\exists f < j < k$ s.t $e' \; \gamma \downarrow_f \Downarrow_j v_{h1} \wedge e' \; \gamma \downarrow_2 \Downarrow v_{h1}'$

This means we have
$(W_e, k-f, v_{h1}, v_{h1}') \in \lceil \mathsf{Labeled}\; \ell' \; \tau \; \sigma \rceil_V^{\mathcal{A}}$ (FB-R1)

In order to prove (FB-R0) we choose W' as W_n where
$W_n.\theta_1 = W_e.\theta_1 \cup \{a_1 \mapsto (\mathsf{Labeled}\; \ell' \; \tau)\}$
$W_n.\theta_2 = W_e.\theta_2 \cup \{a_2 \mapsto (\mathsf{Labeled}\; \ell' \; \tau)\}$
$W_n.\hat{\beta} = W_e.\hat{\beta} \cup \{a_1, a_2\}$
Now we need to prove:

i. $(k-j, H_1', H_2') \triangleright W_n$:

   From Definition 4.9 it suffices to prove:
   $dom(W_n.\theta_1) \subseteq dom(H_1') \wedge dom(W_n.\theta_2) \subseteq dom(H_2') \wedge$
   $(W_n.\hat{\beta}) \subseteq (dom(W_n.\theta_1) \times dom(W_n.\theta_2)) \wedge$
   $\forall (a_1, a_2) \in (W_n.\hat{\beta}).(W_n.\theta_1(a_1) = W_n.\theta_2(a_2) \wedge$
   $(W_n, (k-j)-1, H_1'(a_1), H_2'(a_2)) \in \lceil W_n.\theta_1(a_1) \rceil_V^{\mathcal{A}}) \wedge$
   $\forall i \in \{1,2\}.\forall m.\forall a_i \in dom(W_n.\theta_i).(W_n.\theta_i, m, H_i(a_i)) \in \lfloor W_n.\theta_i(a_i) \rfloor_V$
   This means we need to prove

   - $dom(W_n.\theta_1) \subseteq dom(H_1') \wedge dom(W_n.\theta_2) \subseteq dom(H_2') \wedge (W_n.\hat{\beta}) \subseteq (dom(W_n.\theta_1) \times dom(W_n.\theta_2))$:

     We know that $dom(W_n.\theta_1) = dom(W_e.\theta_1) \cup \{a_1\}$ and $dom(W_n.\theta_2) = dom(W_e.\theta_2) \cup \{a_2\}$
     Also $dom(H_1') = dom(H_1) \cup \{a_1\}$ and $dom(H_2') = dom(H_2) \cup \{a_2\}$
     Therefore from $(k, H_1, H_2) \triangleright W_e$ and from construction of W_n we get the desired.

   - $\forall (a_1', a_2') \in (W_n.\hat{\beta}).(W_n.\theta_1(a_1') = W_n.\theta_2(a_2') \wedge$
     $(W_n, k-j-1, H_1'(a_1'), H_2'(a_2')) \in \lceil W_n.\theta_1(a_1') \rceil_V^{\mathcal{A}})$:

     $\forall (a_1', a_2') \in (W_n.\hat{\beta})$.

     A. When $a_1' = a_1$ and $a_2' = a_2$:
        From construction
        $(W_n.\theta_1(a_1) = W_n.\theta_2(a_2) = (\mathsf{Labeled}\; \ell' \; \tau)$
        Since from (FB-R1) we know that $(W_e, k-f, v_{h1}, v_{h1}') \in \lceil \mathsf{Labeled}\; \ell' \; \tau \rceil_V^{\mathcal{A}}$
        And since from cg-ref we know that $H_1'(a_1) = v_{h1}$, $H_2'(a_2) = v_{h1}'$ and $j = f + 1$ threfore from Lemma 4.16 we get
        $(W_n, k-j-1, H_1'(a_1), H_2'(a_2)) \in \lceil W_n.\theta_1(a_1) \rceil_V^{\mathcal{A}}$
     B. When $a_1' = a_1$ and $a_2' \neq a_2$: This case cannot arise
     C. When $a_1' \neq a_1$ and $a_2' = a_2$: This case cannot arise
     D. When $a_1' \neq a_1$ and $a_2' \neq a_2$:
        Since $(k, H_1, H_2) \triangleright W_e$ therefore the desired is obtained directly from Definition 4.9

   - $\forall i \in \{1,2\}.\forall m.\forall a_i' \in dom(W_n.\theta_i).(W_n.\theta_i, m, H_i(a_i')) \in \lfloor W_n.\theta_i(a_i') \rfloor_V$:
     <u>When $i = 1$</u>
     Given some m
     $\forall a_1' \in dom(W_n.\theta_1)$.

– when $a'_1 = a_1$:
From construction
$(W_n.\theta_1(a_1) = W_n.\theta_2(a_2) = (\mathsf{Labeled}\ \ell'\ \tau)$

And from (FB-R1) we know that $(W_e, k - f, v_{h1}, v'_{h1}) \in \lceil \mathsf{Labeled}\ \ell'\ \tau \rceil_V^{\mathcal{A}}$
Therefore from Lemma 4.14 get the desired

– Otherwise:
Since $(k, H_1, H_2) \triangleright W_e$ therefore the desired is obtained directly from Definition 4.9

When $i = 2$
Similar reasoning as with $i = 1$

ii. $(W', k - j, v'_1, v'_2) \in \lceil (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rceil_V^{\mathcal{A}}$:
From cg-ref we know that $v'_1 = a_1$ and $v'_2 = a_2$
From Definition 4.4 it suffices to prove
$(a_1, a_2) \in W_n.\hat{\beta} \wedge W_n.\theta_1(a_1) = W_n.\theta_2(a_2) = (\mathsf{Labeled}\ \ell'\ \tau)$
This holds from construciton of W_n

(b) $\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$:

Case $l = 1$
Given some $k, \theta_e \sqsupseteq W.\theta_l, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k$

We need to prove
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor (\mathsf{ref}\ \ell'\ \tau) \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$

Since $(W, n, \gamma) \in \lceil \Gamma \rceil_V^{\mathcal{A}}$ therefore from Lemma 4.23 we know that
$\forall m.\ (W.\theta_1, m, \gamma\downarrow_1) \in \lfloor \Gamma \rfloor_V$ and $(W.\theta_2, m, \gamma\downarrow_2) \in \lfloor \Gamma \rfloor_V$

Instantiating m with k we get $(W.\theta_1, k, \gamma\downarrow_1) \in \lfloor \Gamma \rfloor_V$

Now we can apply Theorem 4.21 to get
$(W.\theta_1, k, (\mathsf{ref}\ (e')\gamma\downarrow_1) \in \lfloor (\mathbb{C}\ \ell \perp (\mathsf{ref}\ \ell'\ \tau)) \rfloor_E$

This means from Definition 4.7 we get
$\forall c < k.\mathsf{ref}\ (e')\gamma\downarrow_1 \Downarrow_c v \implies (W.\theta_1, k - c, v) \in \lfloor (\mathbb{C}\ \ell \perp (\mathsf{ref}\ \ell'\ \tau)) \rfloor_V$

This further means that given some $c < k$ s.t $\mathsf{ref}\ (e')\gamma\downarrow_1 \Downarrow_c v$. From cg-val we know that $c = 0$ and $v = \mathsf{ref}\ (e')\gamma\downarrow_1$

And we have $(W.\theta_1, k, \mathsf{ref}\ (e')\gamma\downarrow_1) \in \lfloor (\mathbb{C}\ \ell \perp (\mathsf{ref}\ \ell'\ \tau)) \rfloor_V$

From Definition 4.6 we have
$\forall K \leq k, \theta'_e \sqsupseteq W.\theta_1, H_1, J.(K, H_1) \triangleright \theta'_e \wedge (H_1, \mathsf{ref}\ (e')\gamma\downarrow_1) \Downarrow_J^f (H', v') \wedge J < K \implies$
$\exists \theta' \sqsupseteq \theta'_e.(K - J, H') \triangleright \theta' \wedge (\theta', K - J, v') \in \lfloor (\mathsf{ref}\ \ell'\ \tau) \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H'(a) \implies \exists \ell'.\theta'_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta'_e).\theta'(a) \searrow \ell)$

Instantiating K with k, θ'_e with θ_e, H_1 with H and J with j we get the desired

Case $l = 2$

Symmetric reasoning as in the $l = 1$ case above

20. CG-deref:

$$\frac{\Gamma \vdash e' : \mathsf{ref}\ \ell\ \tau}{\Gamma \vdash !e' : \mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau)}$$

To prove: $(W, n, !e'\ (\gamma\downarrow_1), !e'\ (\gamma\downarrow_2)) \in \lceil(\mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau))\ \sigma\rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:

$\forall i < n. !e'\ \gamma\downarrow_1 \Downarrow_i v_{f1} \wedge !e'\ \gamma\downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n-i, v_{f1}, v'_{f1}) \in \lceil(\mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau))\ \sigma\rceil_V^{\mathcal{A}}$

This means that given some $i < n$ s.t $!e'\ \gamma\downarrow_1 \Downarrow_i v_{f1} \wedge !e'\ \gamma\downarrow_2 \Downarrow v'_{f1}$

From cg-val we know that $v_{f1} = !e'\gamma\downarrow_1$, $v_{f2} = !e'\gamma\downarrow_2$ and $i = 0$

We are required to prove

$(W, n, !e'\gamma\downarrow_1, !e'\gamma\downarrow_2) \in \lceil(\mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau))\ \sigma\rceil_V^{\mathcal{A}}$

Let $v_1 = !e'\gamma\downarrow_1$ and $v_2 = !e'\gamma\downarrow_2$

From Definition 4.4 it suffices to prove

$\Big(\forall k \leq n, W_e \sqsupseteq W. \forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \bot, v'_1, v'_2, (\mathsf{Labeled}\ \ell\ \tau))\Big) \wedge$
$\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v'_l) \in \lfloor(\mathsf{Labeled}\ \ell\ \tau)\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau' \wedge \top \sqsubseteq \ell'') \wedge$
$(\forall a \in \mathit{dom}(\theta') \backslash \mathit{dom}(\theta_e).\theta'(a) \searrow \top)\Big)$

This means we need to prove:

(a) $\forall k \leq n, W_e \sqsupseteq W. \forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \bot, v'_1, v'_2, (\mathsf{Labeled}\ \ell\ \tau))$:

This means we are given is some $k \leq n$, $W_e \sqsupseteq W, H_1, H_2$ s.t $(k, H_1, H_2) \triangleright W_e$

Also given some $v'_1, v'_2, j < k$ s.t $(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2)$

And we are required to prove:
$\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \bot, v'_1, v'_2, (\mathsf{Labeled}\ \ \ell\ \tau))$

This means from Definition 4.3 it suffices to prove $\exists W' \sqsupseteq W_e.(k-j, H'_1, H'_2) \triangleright W' \wedge$
$(W', k-j, v'_1, v'_2) \in \lceil(\mathsf{Labeled}\ \ \ell\ \tau)\rceil_V^{\mathcal{A}}$ (FB-D0)

IH:
$(W_e, k, e'\ (\gamma\downarrow_1), e'\ (\gamma\downarrow_2)) \in \lceil(\mathsf{ref}\ \ell\ \tau)\rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:
$\forall f < k.e_l\ \gamma \downarrow_1 \Downarrow_f v_{h1} \wedge e_l\ \gamma \downarrow_2 \Downarrow v'_{h1} \implies$
$(W_e, k - f, v_{h1}, v'_{h1}) \in \lceil(\mathsf{ref}\ \ell\ \tau)\rceil_V^{\mathcal{A}}$

Since we know that $(H_1, v_1) \Downarrow_j^f (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2)$ therefore $\exists f < j < k$ s.t $e_l\ \gamma \downarrow_f \Downarrow_j v_{h1} \wedge e_l\ \gamma \downarrow_2 \Downarrow v'_{h1}$

This means we have
$(W_e, k - f, v_{h1}, v'_{h1}) \in \lceil(\mathsf{ref}\ \ell\ \tau)\rceil_V^{\mathcal{A}}$ (FB-D1)

In order to prove (FB-D0) we choose W' as W_e. Also from cg-deref we know that $H'_1 = H_1$ and $H'_2 = H_2$. Also we know that $v_{h1} = a_1$ and $v'_{h1} = a_2$.

- $(k - j, H_1, H_2) \triangleright W_e$:
  Since we know that $(k, H_1, H_2) \triangleright W_e$ therefore from Lemma 4.20 we get
  $(k - j, H_1, H_2) \triangleright W_e$
- $(W', k - j, v'_1, v'_2) \in \lceil(\mathsf{Labeled}\ \ \ell\ \tau)\rceil_V^{\mathcal{A}}$:
  Since from (FB-D1) we know that $(W_e, k - f, a_1, a_2) \in \lceil \mathsf{ref}\ \ell\ \tau\rceil_V^{\mathcal{A}}$
  Therefore from Definition 4.4 we know that $(a_1, a_2) \in W_e.\hat{\beta} \wedge W_e.\theta_1(a_1) = W_e.\theta_2(a_2) = \mathsf{Labeled}\ \ell\ \tau$

  And since we know that $(k, H_1, H_2) \triangleright W_e$ therefore from Definition we know that $(W_e, k, H_1(a_1), H_2(a_2)) \in \lceil \mathsf{Labeled}\ \ \ell\ \tau\rceil_V^{\mathcal{A}}$
  Also from cg-ref we know that $v'_1 = H_1(a_1)$ and $v'_2 = H_2(a_2)$
  From Lemma 4.16 we get $(W', k - j, H_1(a_1), H_2(a_2)) \in \lceil(\mathsf{Labeled}\ \ \ell\ \tau)\rceil_V^{\mathcal{A}}$

(b) $\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor(\mathsf{Labeled}\ \ \ell\ \tau)\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau' \wedge \top \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \top)$:

<u>Case $l = 1$</u>
Given some $k, \theta_e \sqsupseteq W.\theta_l, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v'_l) \wedge j < k$

<u>We need to prove</u>
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor(\mathsf{Labeled}\ \ \ell\ \tau)\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau'' \wedge \ell' \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell')$

Since $(W, n, \gamma) \in \lceil\Gamma\rceil_V^{\mathcal{A}}$ therefore from Lemma 4.23 we know that
$\forall m.\ (W.\theta_1, m, \gamma \downarrow_1) \in \lfloor\Gamma\rfloor_V$ and $(W.\theta_2, m, \gamma \downarrow_2) \in \lfloor\Gamma\rfloor_V$

Instantiating m with k we get $(W.\theta_1, k, \gamma \downarrow_1) \in \lfloor\Gamma\rfloor_V$

Now we can apply Theorem 4.21 to get
$(W.\theta_1, k, (!e'\gamma \downarrow_1) \in \lfloor(\mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ \ell\ \tau))\rfloor_E$

This means from Definition 4.7 we get
$\forall c < k.!e'\gamma \downarrow_1 \Downarrow_c v \implies (W.\theta_1, k - c, v) \in \lfloor(\mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ \ell\ \tau))\rfloor_V$

Instantianting c with 0 and from cg-val we know that $v = !e'\gamma \downarrow_1$

And we have $(W.\theta_1, k, !e'\gamma \downarrow_1) \in \lfloor(\mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ \ell\ \tau))\rfloor_V$

From Definition 4.6 we have
$\forall K \leq k, \theta'_e \sqsupseteq W.\theta_1, H_1, J.(K, H_1) \triangleright \theta'_e \wedge (H_1, v) \Downarrow^f_J (H', v') \wedge J < K \implies$
$\exists \theta' \sqsupseteq \theta'_e.(K - J, H') \triangleright \theta' \wedge (\theta', K - J, v') \in \lfloor (\mathsf{Labeled}\ \ \ell\ \tau) \rfloor_V \wedge$
$(\forall a.H_1(a) \neq H'(a) \implies \exists \ell'.\theta'_e(a) = \mathsf{Labeled}\ \ell''\ \tau'' \wedge \top \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta'_e).\theta'(a) \searrow \top)$

Instantiating K with k, θ'_e with θ_e, H_1 with H and J with j we get the desired

Case $l = 2$
Symmetric reasoning as in the $l = 1$ case above

21. CG-assign:

$$\frac{\Gamma \vdash e_l : \mathsf{ref}\ \ell'\ \tau \qquad \Gamma \vdash e_r : \mathsf{Labeled}\ \ell'\ \tau \qquad \mathcal{L} \vdash \ell \sqsubseteq \ell'}{\Gamma \vdash e_l := e_r : \mathbb{C}\ \ell\ \bot\ \mathsf{unit}}$$

To prove: $(W, n, (e_l := e_r)\ (\gamma \downarrow_1), (e_l := e_r)\ (\gamma \downarrow_2)) \in \lceil \mathbb{C}\ \ell\ \bot\ \mathsf{unit}\ \sigma \rceil^{\mathcal{A}}_E$

This means from Definition 4.5 we need to prove:
$\forall i < n.(e_l := e_r)\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (e_l := e_r)\ \gamma \downarrow_2 \Downarrow v'_{f1} \implies$
$(W, n - i, v_{f1}, v'_{f1}) \in \lceil \mathbb{C}\ \ell\ \bot\ \mathsf{unit} \rceil^{\mathcal{A}}_V$

This means that given some $i < n$ s.t $(e_l := e_r)\ \gamma \downarrow_1 \Downarrow_i v_{f1} \wedge (e_l := e_r)\ \gamma \downarrow_2 \Downarrow v'_{f1}$
From cg-val we know that $v_{f1} = (e_l := e_r)\gamma \downarrow_1$, $v_{f2} = (e_l := e_r)\gamma \downarrow_2$ and $i = 0$
We are required to prove
$(W, n, (e_l := e_r)\gamma \downarrow_1, (e_l := e_r)\gamma \downarrow_2) \in \lceil \mathbb{C}\ \ell\ \ell\ \mathsf{unit} \rceil^{\mathcal{A}}_V$

Let $e_1 = (e_l : -e_r)\ \gamma \downarrow_1$ and $e_2 = (e_l : -e_r)\ \gamma \downarrow_2$
From Definition 4.4 it suffices to prove
$\Big(\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow^f_j (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k - j, \bot, v'_1, v'_2, \mathsf{unit})\Big) \wedge$
$\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow^f_j (H', v'_l) \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v'_l) \in \lfloor \mathsf{unit} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)\Big)$
This means we need to prove:

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v'_1, v'_2.$
$(H_1, v_1) \Downarrow^f_j (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2) \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H'_1, H'_2) \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k - j, \bot, v'_1, v'_2, \mathsf{unit})$:

This means we are given some $k \leq n$, $W_e \sqsupseteq W, H_1, H_2$ s.t $(k, H_1, H_2) \triangleright W_e$

And finally given some $v'_1, v'_2, j < k$ s.t $(H_1, v_1) \Downarrow^f_j (H'_1, v'_1) \wedge (H_2, v_2) \Downarrow^f (H'_2, v'_2)$

And we are required to prove:

$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge ValEq(\mathcal{A}, W', k-j, \bot, v_1', v_2', \mathsf{unit})$
(FB-A0)

<u>IH1</u>:
$(W_e, k, e_l\ (\gamma\downarrow_1), e_l\ (\gamma\downarrow_2)) \in \lceil \mathsf{ref}\ \ell'\ \tau \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:
$\forall f < k.e_l\ \gamma\downarrow_1 \Downarrow_f v_{h1} \wedge e_l\ \gamma\downarrow_2 \Downarrow v_{h1}' \implies$
$(W_e, k-f, v_{h1}, v_{h1}') \in \lceil \mathsf{ref}\ \ell'\ \tau \rceil_V^{\mathcal{A}}$

Since we know that $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2')$ therefore $\exists f < j < k$ s.t $e_l\ \gamma\downarrow_f \Downarrow_j v_{h1} \wedge e_l\ \gamma\downarrow_2 \Downarrow v_{h1}'$

This means we have
$(W_e, k-f, v_{h1}, v_{h1}') \in \lceil \mathsf{ref}\ \ell'\ \tau \rceil_V^{\mathcal{A}}$ (FB-A1)

<u>IH2</u>:
$(W_e, k-f, e_r\ (\gamma\downarrow_1), e_r\ (\gamma\downarrow_2)) \in \lceil \mathsf{Labeled}\ \ell'\ \tau \rceil_E^{\mathcal{A}}$

This means from Definition 4.5 we need to prove:
$\forall s < k-f.e'\ \gamma\downarrow_1 \Downarrow_s v_{h2} \wedge e'\ \gamma\downarrow_2 \Downarrow v_{h2}' \implies$
$(W_e, k-f-s, v_{h2}, v_{h2}') \in \lceil \mathsf{Labeled}\ \ell'\ \tau \rceil_V^{\mathcal{A}}$

Since we know that $(H_1, v_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, v_2) \Downarrow^f (H_2', v_2')$ therefore $\exists s < j-f < k-f$ s.t $e_r\ \gamma\downarrow_1 \Downarrow_s v_{h2} \wedge e_r\ \gamma\downarrow_2 \Downarrow v_{h2}'$

This means we have
$(W_e, k-f-s, v_{h2}, v_{h2}') \in \lceil \mathsf{Labeled}\ \ell'\ \tau \rceil_V^{\mathcal{A}}$ (FB-A2)

In order to prove (FB-A0) we choose W' as W_e. Also from cg-assign we know that $H_1' = H_1[v_{h1} \mapsto v_{h2}]$ and $H_2' = H_2[v_{h1}' \mapsto v_{h2}']$, and $j = f + s + 1$
We need to prove the following:

i. $(k-j, H_1', H_2') \triangleright W_e$:

Say $v_{h1} = a_1$ and $v_{h1}' = a_2$

From Definition 4.9 it suffices to prove:
$dom(W_e.\theta_1) \subseteq dom(H_1') \wedge dom(W_e.\theta_2) \subseteq dom(H_2') \wedge$
$(W_e.\hat{\beta}) \subseteq (dom(W_e.\theta_1) \times dom(W_e.\theta_2)) \wedge$
$\forall (a_1, a_2) \in (W_e.\hat{\beta}).(W_e.\theta_1(a_1) = W_e.\theta_2(a_2) \wedge$
$(W_e, (k-j)-1, H_1'(a_1), H_2'(a_2)) \in \lceil W_e.\theta_1(a_1) \rceil_V^{\mathcal{A}}) \wedge$
$\forall i \in \{1,2\}.\forall m.\forall a_i \in dom(W_e.\theta_i).(W_e.\theta_i, m, H_i(a_i)) \in \lfloor W_e.\theta_i(a_i) \rfloor_V$
This means we need to prove

- $dom(W_e.\theta_1) \subseteq dom(H_1') \wedge dom(W_e.\theta_2) \subseteq dom(H_2') \wedge (W_e.\hat{\beta}) \subseteq (dom(W_e.\theta_1) \times dom(W_e.\theta_2))$:
  Since $dom(H_1) = dom(H_1')$ and $dom(H_2) = dom(H_2')$, and also we know that $(k, H_1, H_2) \triangleright W_e$. Therefore we obtain the desired direclty from Definition 4.9

- $\forall(a_1', a_2') \in (W_e.\hat{\beta}).(W_e.\theta_1(a_1') = W_e.\theta_2(a_2') \wedge (W_e, k-j-1, H_1'(a_1'), H_2'(a_2')) \in \lceil W_e.\theta_1(a_1')\rceil_V^{\mathcal{A}})$:

  $\forall(a_1', a_2') \in (W_e.\hat{\beta})$.

  A. When $a_1' = a_1$ and $a_2' = a_2$:
  From (FB-A1) and from Definition 4.4 we get
  $(W_e.\theta_1(a_1) = W_e.\theta_2(a_2) = (\mathsf{Labeled}\ \ell'\ \tau)$

  Since from (FB-A2) we know that $(W_e, k-f-s, v_{h2}, v_{h2}') \in \lceil\mathsf{Labeled}\ \ell'\ \tau\rceil_V^{\mathcal{A}}$
  And since from cg-assign we know that $H_1'(a_1) = v_{h2}$, $H_2'(a_2) = v_{h2}'$ and $j = f + s + 1$ threfore from Lemma 4.16 we get
  $(W_e, k-j-1, H_1'(a_1), H_2'(a_2)) \in \lceil W_e.\theta_1(a_1)\rceil_V^{\mathcal{A}}$

  B. When $a_1' = a_1$ and $a_2' \neq a_2$: This case cannot arise

  C. When $a_1' \neq a_1$ and $a_2' = a_2$: This case cannot arise

  D. When $a_1' \neq a_1$ and $a_2' \neq a_2$:
  Since $(k, H_1, H_2) \triangleright W_e$ therefore the desired is obtained directly from Definition 4.9

- $\forall i \in \{1,2\}.\forall m.\forall a_i' \in dom(W_e.\theta_i).(W_e.\theta_i, m, H_i(a_i')) \in \lfloor W_e.\theta_i(a_i')\rfloor_V$:
  <u>When $i = 1$</u>
  Given some m
  $\forall a_1' \in dom(W_e.\theta_1)$.

  – when $a_1' = a_1$:
  From (FB-A1) and from Definition 4.4 we get
  $(W_e.\theta_1(a_1) = W_e.\theta_2(a_2) = (\mathsf{Labeled}\ \ell'\ \tau)$

  Since from (FB-A2) we know that $(W_e, k-f-s, v_{h2}, v_{h2}') \in \lceil\mathsf{Labeled}\ \ell'\ \tau\rceil_V^{\mathcal{A}}$
  Therefore from Lemma 4.14 get the desired

  – Otherwise:
  Since $(k, H_1, H_2) \triangleright W_e$ therefore the desired is obtained directly from Definition 4.9

  <u>When $i = 2$</u>
  Similar reasoning as with $i = 1$

ii. $ValEq(\mathcal{A}, W_e, k-j, \bot, (), (), \mathsf{unit})$:
Holds directly from Definition 4.3 and Definition 4.4

(b) $\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor\mathsf{unit}\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$:

<u>Case $l = 1$</u>
Given some $k, \theta_e \sqsupseteq W.\theta_l, H, j$ s.t $(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k$

<u>We need to prove</u>
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor(\mathsf{unit})\rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell''\ \tau'' \wedge \ell \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell)$

Since $(W, n, \gamma) \in \lceil\Gamma\rceil_V^{\mathcal{A}}$ therefore from Lemma 4.23 we know that
$\forall m.\ (W.\theta_1, m, \gamma\downarrow_1) \in \lfloor\Gamma\rfloor_V$ and $(W.\theta_2, m, \gamma\downarrow_2) \in \lfloor\Gamma\rfloor_V$

Instantiating m with k we get $(W.\theta_1, k, \gamma\downarrow_1) \in \lfloor \Gamma \rfloor_V$

Now we can apply Theorem 4.21 to get
$(W.\theta_1, k, ((e_l := e_r)\gamma\downarrow_1) \in \lfloor(\mathbb{C}\ \ell\ \perp\ (\mathsf{unit}))\rfloor_E$

This means from Definition 4.7 we get
$\forall c < k.(e_l := e_r)\gamma\downarrow_1\Downarrow_c v \implies (W.\theta_1, k-c, v) \in \lfloor(\mathbb{C}\ \ell\ \perp\ (\mathsf{unit}))\rfloor_V$

Instantiating c with 0 and from cg-val we know that $v = (e_l := e_r)\gamma\downarrow_1$

And we have $(W.\theta_1, k, (e_l := e_r)\gamma\downarrow_1) \in \lfloor(\mathbb{C}\ \ell\ \ell\ (\mathsf{unit}))\rfloor_V$

From Definition 4.6 we have
$\forall K \leq k, \theta'_e \sqsupseteq W.\theta_1, H_1, J.(K, H_1) \triangleright \theta'_e \wedge (H_1, v) \Downarrow^f_J (H', v') \wedge J < K \implies$
$\exists \theta' \sqsupseteq \theta'_e.(K-J, H') \triangleright \theta' \wedge (\theta', K-J, v') \in \lfloor(\mathsf{Labeled}\quad \ell\ \tau)\rfloor_V \wedge$
$(\forall a.H_1(a) \neq H'(a) \implies \exists \ell'.\theta'_e(a) = \mathsf{Labeled}\ \ell''\ \tau'' \wedge \ell' \sqsubseteq \ell'') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta'_e).\theta'(a) \searrow \ell')$

Instantiating K with k, θ'_e with θ_e, H_1 with H and J with j we get the desired

<u>Case $l = 2$</u>
Symmetric reasoning as in the $l = 1$ case above

□

Lemma 4.25. $\forall \mathcal{A}, W, W, \ell, \ell', v_1, v_2, \tau, i, j.$
$\mathit{ValEq}(\mathcal{A}, W, \ell, i, v_1, v_2, \tau) \wedge j < i \wedge \ell \sqsubseteq \ell' \wedge W \sqsubseteq W' \implies$
$\mathit{ValEq}(\mathcal{A}, W', \ell', j, v_1, v_2, \tau)$

Proof. Given that $\mathit{ValEq}(\mathcal{A}, W, \ell, i, v_1, v_2, \tau)$. From Definition 4.3 two cases arise

1. $\ell \sqsubseteq \mathcal{A}$:

   In this case we know that $(W, i, v_1, v_2) \in \lceil \tau \rceil^{\mathcal{A}}_V$

   2 cases arise

   (a) $\ell' \sqsubseteq \mathcal{A}$:
   Since $(W, i, v_1, v_2) \in \lceil \tau \rceil^{\mathcal{A}}_V$ therefore from Lemma 4.16 we know that $(W', j, v_1, v_2) \in \lceil \tau \rceil^{\mathcal{A}}_V$
   And thus from Definition 4.3 we know that $\mathit{ValEq}(\mathcal{A}, W', \ell', j, v_1, v_2, \tau)$

   (b) $\ell' \not\sqsubseteq \mathcal{A}$:
   Since $(W, i, v_1, v_2) \in \lceil \tau \rceil^{\mathcal{A}}_V$ therefore from Lemma 4.14 we know that $\forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, v_i) \in \lfloor \tau \rfloor_V$
   And from Lemma 4.15 we know that $\forall i \in \{1, 2\}.\ \forall m.\ (W'.\theta_i, m, v_i) \in \lfloor \tau \rfloor_V$
   Hence from Definition 4.3 we know that $\mathit{ValEq}(\mathcal{A}, W', \ell', j, v_1, v_2, \tau)$

2. $\ell \not\sqsubseteq \mathcal{A}$:

   Given is $\ell \sqsubseteq \ell' \not\sqsubseteq \mathcal{A}$

   In this case we know that $\forall i \in \{1, 2\}.\ \forall m.\ (W.\theta_i, m, v_i) \in \lfloor \tau \rfloor_V$

   And from Lemma 4.15 we know that $\forall i \in \{1, 2\}.\ \forall m.\ (W'.\theta_i, m, v_i) \in \lfloor \tau \rfloor_V$

   Hence from Definition 4.3 we know that $\mathit{ValEq}(\mathcal{A}, W', \ell', j, v_1, v_2, \tau)$

□

Lemma 4.26 (Subtyping binary)**.** *The following holds:*
$\forall \Sigma, \Psi, \sigma, \tau, \tau'$.

1. $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lceil(\tau\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau'\ \sigma)\rceil_V^{\mathcal{A}}$
2. $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lceil(\tau\ \sigma)\rceil_E^{\mathcal{A}} \subseteq \lceil(\tau'\ \sigma)\rceil_E^{\mathcal{A}}$

Proof. Proof of statement (1)
Proof by induction on the $\tau <: \tau'$

1. CGsub-arrow:

   Given:

   $$\frac{\mathcal{L} \vdash \tau_1' <: \tau_1 \qquad \mathcal{L} \vdash \tau_2 <: \tau_2'}{\mathcal{L} \vdash \tau_1 \to \tau_2 <: \tau_1' \to \tau_2'}$$

   To prove: $\lceil((\tau_1 \to \tau_2)\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil((\tau_1' \to \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   IH1: $\lceil(\tau_1'\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau_1\ \sigma)\rceil_V^{\mathcal{A}}$ (Statement 1)
   $\lceil(\tau_2\ \sigma)\rceil_E^{\mathcal{A}} \subseteq \lceil(\tau_2'\ \sigma)\rceil_E^{\mathcal{A}}$ (Sub-A0 From Statement 2)

   It suffices to prove:
   $\forall (W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil((\tau_1 \to \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}.\ (W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil((\tau_1' \to \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   This means that given: $(W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil((\tau_1 \to \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}$
   And it suffices to prove: $(W, n, \lambda x.e_1, \lambda x.e_2) \in \lceil((\tau_1' \to \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   From Definition 4.4 we are given:
   $\forall W' \sqsupseteq W, j < n, v_1, v_2.((W', j, v_1, v_2) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}} \implies$
   $(W', j, e_1[v_1/x], e_2[v_2/x]) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}}) \wedge$
   $\forall \theta_l \sqsupseteq W.\theta_1, j, v_c.((\theta_l, j, v_c) \in \lfloor\tau_1\ \sigma\rfloor_V \implies (\theta_l, j, e_1[v_1/x]) \in \lfloor\tau_2\ \sigma\rfloor_E) \wedge$
   $\forall \theta_l \sqsupseteq W.\theta_2, j, v_c.((\theta_l, j, v_c) \in \lfloor\tau_1\ \sigma\rfloor_V \implies (\theta_l, j, e_2[v_c/x]) \in \lfloor\tau_2\ \sigma\rfloor_E)$ (Sub-A1)

   Again from Definition 4.4 we are required to prove:
   $\forall W'' \sqsupseteq W, k < n, v_1', v_2'.((W'', k, v_1', v_2') \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}} \implies (W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2'\ \sigma\rceil_E^{\mathcal{A}}) \wedge$
   $\forall \theta_l' \sqsupseteq W.\theta_1, k, v_c'.((\theta_l', k, v_c') \in \lfloor\tau_1'\ \sigma\rfloor_V \implies (\theta_l', k, e_1[v_c'/x]) \in \lfloor\tau_2'\ \sigma\rfloor_E) \wedge$
   $\forall \theta_l' \sqsupseteq W.\theta_2, k, v_c'.((\theta_l', k, v_c') \in \lfloor\tau_1'\ \sigma\rfloor_V \implies (\theta_l', k, e_2[v_c'/x]) \in \lfloor\tau_2'\ \sigma\rfloor_E)$

   This means need to prove:

   (a) $\forall W'' \sqsupseteq W, k < n, v_1', v_2'.((W'', k, v_1', v_2') \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}} \implies (W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2'\ \sigma\rceil_E^{\mathcal{A}})$:
   Given: $W'' \sqsupseteq W$, $k < n$ and v_1', v_2'. We are also given $(W'', k, v_1', v_2') \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}}$
   To prove: $(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2'\ \sigma\rceil_E^{\mathcal{A}}$

   Instantiating the first conjunct of Sub-A1 with W'', k, v_1' and v_2' we get

   $$((W'', k, v_1', v_2') \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}} \implies (W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil\tau_2\ \sigma\rceil_E^{\mathcal{A}}) \tag{101}$$

Since $(W'', k, v_1', v_2') \in \lceil \tau_1' \ \sigma \rceil_V^{\mathcal{A}}$ therefore from IH1 we know that $(W'', k, v_1', v_2') \in \lceil \tau_1 \ \sigma \rceil_V^{\mathcal{A}}$

Thus from Equation 101 we get $(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil \tau_2 \ \sigma \rceil_E^{\mathcal{A}}$

Finally using (Sub-A0) we get $(W'', k, e_1[v_1'/x], e_2[v_2'/x]) \in \lceil \tau_2' \ \sigma \rceil_E^{\mathcal{A}}$

(b) $\forall \theta_l' \sqsupseteq W.\theta_1, k, v_c'.((\theta_l', k, v_c') \in \lfloor \tau_1' \ \sigma \rfloor_V \implies (\theta_l', k, e_1[v_c'/x]) \in \lfloor \tau_2' \ \sigma \rfloor_E)$:
Given: $\theta_l' \sqsupseteq W.\theta_1, k, v_c'$. We are also given $(\theta_l', k, v_c') \in \lfloor \tau_1' \ \sigma \rfloor_V$
To prove: $(\theta_l', k, e_1[v_c'/x]) \in \lfloor \tau_2' \ \sigma \rfloor_E$

Since we are given $(\theta_l', k, v_c') \in \lfloor \tau_1' \ \sigma \rfloor_V$ and since $\tau_1' <: \tau_1$ therefore from Lemma 4.22 we get

$$(\theta_l', k, v_c') \in \lfloor \tau_1 \ \sigma \rfloor_V \tag{102}$$

Instantiating the second conjunct of Sub-A1 with θ_l', k, v_1' and v_2' we get

$$((\theta_l', k, v_c') \in \lfloor \tau_1 \ \sigma \rfloor_V \implies (\theta_l', e_1[v_c'/x]) \in \lfloor \tau_2 \ \sigma \rfloor_E) \tag{103}$$

Therefore from Equation 102 and 103 we get $(\theta_l', k, e_1[v_c'/x]) \in \lfloor \tau_2 \ \sigma \rfloor_E$

Since $\tau_2 <: \tau_2'$ therefore from Lemma 4.22 we get
$(\theta_l', k, e_1[v_c'/x]) \in \lfloor \tau_2' \ \sigma \rfloor_E$

(c) $\forall \theta_l' \sqsupseteq W.\theta_2, k, v_c'.((\theta_l', k, v_c') \in \lfloor \tau_1' \ \sigma \rfloor_V \implies (\theta_l', k, e_2[v_c'/x]) \in \lfloor \tau_2' \ \sigma \rfloor_E)$:
Similar reasoning as in the previous case

2. CGsub-prod:
Given:

$$\frac{\mathcal{L} \vdash \tau_1 <: \tau_1' \qquad \mathcal{L} \vdash \tau_2 <: \tau_2'}{\mathcal{L} \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}$$

To prove: $\lceil ((\tau_1 \times \tau_2) \ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil ((\tau_1' \times \tau_2') \ \sigma) \rceil_V^{\mathcal{A}}$

IH1: $\lceil (\tau_1 \ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil (\tau_1' \ \sigma) \rceil_V^{\mathcal{A}}$ (Statement (1))
IH2: $\lceil (\tau_2 \ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil (\tau_2' \ \sigma) \rceil_V^{\mathcal{A}}$ (Statement (1))
It suffices to prove: $\forall (W, n, (v_1, v_2), (v_1', v_2')) \in \lceil ((\tau_1 \times \tau_2) \ \sigma) \rceil_V^{\mathcal{A}}.\ (W, n, (v_1, v_2), (v_1', v_2')) \in \lceil ((\tau_1' \times \tau_2') \ \sigma) \rceil_V^{\mathcal{A}}$

This means that given: $(W, n, (v_1, v_2), (v_1', v_2')) \in \lceil ((\tau_1 \times \tau_2) \ \sigma) \rceil_V^{\mathcal{A}}$
Therefore from Definition 4.4 we are given:

$$(W, n, v_1, v_1') \in \lceil \tau_1 \ \sigma \rceil_V^{\mathcal{A}} \land (W, n, v_2, v_2') \in \lceil \tau_2 \ \sigma \rceil_V^{\mathcal{A}} \tag{104}$$

And it suffices to prove: $(W, n, (v_1, v_2), (v_1', v_2')) \in \lceil ((\tau_1' \times \tau_2') \ \sigma) \rceil_V^{\mathcal{A}}$

Again from Definition 4.4, it suffices to prove:
$(W, n, v_1, v_1') \in \lceil \tau_1' \ \sigma \rceil_V^{\mathcal{A}} \land (W, n, v_2, v_2') \in \lceil \tau_2' \ \sigma \rceil_V^{\mathcal{A}}$

Since from Equation 104 we know that $(W, n, v_1, v_1') \in \lceil \tau_1 \ \sigma \rceil_V^{\mathcal{A}}$ therefore from IH1 we have $(W, n, v_1, v_1') \in \lceil \tau_1' \ \sigma \rceil_V^{\mathcal{A}}$
Similarly since $(W, n, v_2, v_2') \in \lceil \tau_2 \ \sigma \rceil_V^{\mathcal{A}}$ from Equation 104 therefore from IH2 we have $(W, n, v_2, v_2') \in \lceil \tau_2' \ \sigma \rceil_V^{\mathcal{A}}$

3. CGsub-sum:

   Given:

$$\frac{\mathcal{L} \vdash \tau_1 <: \tau_1' \qquad \mathcal{L} \vdash \tau_2 <: \tau_2'}{\mathcal{L} \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'}$$

   To prove: $\lceil((\tau_1 + \tau_2)\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil((\tau_1' + \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   IH1: $\lceil(\tau_1\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau_1'\ \sigma)\rceil_V^{\mathcal{A}}$ (Statement (1))
   IH2: $\lceil(\tau_2\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau_2'\ \sigma)\rceil_V^{\mathcal{A}}$ (Statement (1))
   It suffices to prove: $\forall(W, n, v_{s1}, v_{s2}) \in \lceil((\tau_1 + \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}.\ (W, n, v_{s1}, v_{s2}) \in \lceil((\tau_1' + \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   This means that given: $(W, n, v_{s1}, v_{s2}) \in \lceil((\tau_1 + \tau_2)\ \sigma)\rceil_V^{\mathcal{A}}$
   And it suffices to prove: $(W, n, v_{s1}, v_{s2}) \in \lceil((\tau_1' + \tau_2')\ \sigma)\rceil_V^{\mathcal{A}}$

   2 cases arise

   (a) $v_{s1} = \mathsf{inl}\ v_{i1}$ and $v_{s1} = \mathsf{inl}\ v_{i2}$:
       From Definition 4.4 we are given:

$$(W, n, v_{i1}, v_{i2}) \in \lceil\tau_1\ \sigma\rceil_V^{\mathcal{A}} \tag{105}$$

       And we are required to prove that:
       $(W, n, v_{i1}, v_{i2}) \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}}$
       From Equation 105 and IH1 we know that
       $(W, n, v_{i1}, v_{i2}) \in \lceil\tau_1'\ \sigma\rceil_V^{\mathcal{A}}$

   (b) $v_s = \mathsf{inr}\ v_{i1}$ and $v_{s2} = \mathsf{inr}\ v_{i2}$:
       From Definition 4.4 we are given:

$$(W, n, v_{i1}, v_{i2}) \in \lceil\tau_2\ \sigma\rceil_V^{\mathcal{A}} \tag{106}$$

       And we are required to prove that:
       $(W, n, v_{i1}, v_{i2}) \in \lceil\tau_2'\ \sigma\rceil_V^{\mathcal{A}}$
       From Equation 106 and IH2 we know that
       $(W, n, v_{i1}, v_{i2}) \in \lceil\tau_2'\ \sigma\rceil_V^{\mathcal{A}}$

4. CGsub-forall:

   Given:

$$\frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash \forall\alpha.\tau_1 <: \forall\alpha.\tau_2}$$

   To prove: $\lceil((\forall\alpha.\tau_1)\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\forall\alpha.\tau_2)\ \sigma\rceil_V^{\mathcal{A}}$

   $\forall\sigma.\ \lceil(\tau_1\ \sigma)\rceil_E^{\mathcal{A}} \subseteq \lceil(\tau_2\ \sigma)\rceil_E^{\mathcal{A}}$ (Sub-F2, From Statement (2))
   It suffices to prove: $\forall(W, n, \Lambda e_1, \Lambda e_2) \in \lceil((\forall\alpha.\tau_1)\ \sigma)\rceil_V^{\mathcal{A}}$.
   $(W, n, \Lambda e_1, \Lambda e_2) \in \lceil((\forall\alpha.\tau_2)\ \sigma)\rceil_V^{\mathcal{A}}$

   This means that given: $(W, n, \Lambda e_1, \Lambda e_2) \in \lceil((\forall\alpha.(\tau_1))\ \sigma)\rceil_V^{\mathcal{A}}$
   Therefore from Definition 4.4 we are given:

$\forall W' \sqsupseteq W, n' < n, \ell' \in \mathcal{L}.((W', n', e_1, e_2) \in \lceil \tau_1[\ell'/\alpha]\ \sigma \rceil_E^{\mathcal{A}}) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, j, \ell' \in \mathcal{L}.((\theta_l, j, e_1) \in \lfloor \tau_1[\ell'/\alpha] \rfloor_E) \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, j, \ell' \in \mathcal{L}.((\theta_l, j, e_2) \in \lfloor \tau_1[\ell''/\alpha] \rfloor_E)$ (Sub-F1)

And it suffices to prove: $(W, n, \Lambda e_1, \Lambda e_2) \in \lceil ((\forall \alpha.\tau_2)\ \sigma) \rceil_V^{\mathcal{A}}$

Again from Definition 4.4, it suffices to prove:

$\forall W'' \sqsupseteq W, n'' < n, \ell'' \in \mathcal{L}.((W'', n'', e_1, e_2) \in \lceil \tau_2[\ell''/\alpha]\ \sigma \rceil_E^{\mathcal{A}}) \wedge$
$\forall \theta'_l \sqsupseteq W.\theta_1, k, \ell'' \in \mathcal{L}.((\theta'_l, k, e_1) \in \lfloor \tau_2[\ell''/\alpha] \rfloor_E) \wedge$
$\forall \theta'_l \sqsupseteq W.\theta_2, k, \ell'' \in \mathcal{L}.((\theta'_l, k, e_2) \in \lfloor \tau_2[\ell''/\alpha] \rfloor_E)$

This means we are required to show:

(a) $\forall W'' \sqsupseteq W, n'' < n, \ell' \in \mathcal{L}.((W'', n', e_1, e_2) \in \lceil \tau_2[\ell'/\alpha]\ \sigma \rceil_E^{\mathcal{A}})$:
By instantiating the first conjunct of Sub-F1 with W'', n'' and ℓ'' we know that the following holds
$((W'', n'', e_1, e_2) \in \lceil \tau_1[\ell''/\alpha]\ \sigma \rceil_E^{\mathcal{A}})$

Therefore from Sub-F2 instantiated at $\sigma \cup \{\alpha \mapsto \ell''\}$
$((W'', n'', e_1, e_2) \in \lceil \tau_2[\ell''/\alpha]\ \sigma \rceil_E^{\mathcal{A}})$

(b) $\forall \theta'_l \sqsupseteq W.\theta_1, k, \ell'' \in \mathcal{L}.((\theta'_l, k, e_1) \in \lfloor \tau_2[\ell''/\alpha] \rfloor_E)$:
By instantiating the second conjunct of Sub-F1 with θ'_l and ℓ'' we know that the following holds
$((\theta'_l, k, e_1) \in \lfloor \tau_1[\ell''/\alpha]\ \sigma \rfloor_E)$

Since $\tau_1\ \sigma \cup \{\alpha \mapsto \ell''\} <: \tau_2\ \sigma \cup \{\alpha \mapsto \ell''\}$ therefore from Lemma 4.22 we know that
$((\theta'_l, k, e1) \in \lfloor \tau_2[\ell''/\alpha]\ \sigma \rfloor_E)$

(c) $\forall \theta'_l \sqsupseteq W.\theta_2, k, \ell'' \in \mathcal{L}.((\theta'_l, k, e_2) \in \lfloor \tau_2[\ell''/\alpha] \rfloor_E)$:
Similar reasoning as in the previous case

5. CGsub-constraint:

Given:

$$\frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash c_1 \Rightarrow \tau_1 <: c_2 \Rightarrow \tau_2}$$

To prove: $\lceil ((c_1 \Rightarrow \tau_1)\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil ((c_2 \Rightarrow \tau_2))\ \sigma \rceil_V^{\mathcal{A}}$

$\lceil (\tau_1\ \sigma) \rceil_E^{\mathcal{A}} \subseteq \lceil (\tau_2\ \sigma) \rceil_E^{\mathcal{A}}$ (Sub-C0, From Statement (2))

It suffices to prove: $\forall (W, n, \nu e_1, \nu e_2) \in \lceil ((c_1 \Rightarrow \tau_1)\ \sigma) \rceil_V^{\mathcal{A}}.\ (W, n, \nu e_1, \nu e_2) \in \lceil ((c_2 \Rightarrow \tau_2)\ \sigma) \rceil_V^{\mathcal{A}}$

This means that given: $(W, n, \nu e_1, \nu e_2) \in \lceil ((c_1 \Rightarrow \tau_1)\ \sigma) \rceil_V^{\mathcal{A}}$

Therefore from Definition 4.4 we are given:

$\forall W' \sqsupseteq W, n' < n.\mathcal{L} \models c_1\ \sigma \implies (W', n', e_1, e_2) \in \lceil \tau_1\ \sigma \rceil_E^{\mathcal{A}} \wedge$
$\forall \theta_l \sqsupseteq W.\theta_1, k.\mathcal{L} \models c_1 \implies (\theta_l, k, e_1) \in \lfloor \tau_1\ \sigma \rfloor_E \wedge$
$\forall \theta_l \sqsupseteq W.\theta_2, k.\mathcal{L} \models c_1 \implies (\theta_l, k, e_2) \in \lfloor \tau_1\ \sigma \rfloor_E$ (Sub-C1)

And it suffices to prove: $(W, n, \nu e_1, \nu e_2) \in \lceil ((c_2 \Rightarrow \tau_2)\ \sigma) \rceil_V^{\mathcal{A}}$

Again from Definition 4.4, it suffices to prove:

$\forall W'' \sqsupseteq W, n'' < n.\mathcal{L} \models c_2\ \sigma \implies (W'', n'', e_1, e_2) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}} \wedge$
$\forall \theta'_l \sqsupseteq W.\theta_1, j.\mathcal{L} \models c_2 \implies (\theta'_l, j, e_1) \in \lfloor \tau_2\ \sigma \rfloor_E \wedge$
$\forall \theta'_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c_2 \implies (\theta'_l, j, e_2) \in \lfloor \tau_2\ \sigma \rfloor_E$

This means that we are required to show the following:

(a) $\forall W'' \sqsupseteq W, n'' < n.\mathcal{L} \models c_2\ \sigma \implies (W'', n'', e_1, e_2) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$:
We are given $W'' \sqsupseteq W, n'' < n$ also we know that $\mathcal{L} \models c_2\ \sigma$ and $c_2\ \sigma \implies c_1\ \sigma$ therefore we also know that $\mathcal{L} \models c_1\ \sigma$
Hence by instantiating the first conjunct of Sub-C1 with W'' and n'' we know that the following holds
$(W'', n'', e_1, e_2) \in \lceil \tau_1\ \sigma \rceil_E^{\mathcal{A}}$
Therefore from (Sub-C0) we get $(W'', n'', e_1, e_2) \in \lceil \tau_2\ \sigma \rceil_E^{\mathcal{A}}$

(b) $\forall \theta'_l \sqsupseteq W.\theta_1, k.\mathcal{L} \models c_2 \implies (\theta'_l, k, e_1) \in \lfloor \tau_2\ \sigma \rfloor_E$:
We are given some $\theta'_l \sqsupseteq W.\theta_1, k$, also we know that $\mathcal{L} \models c_2\ \sigma$ and $c_2\ \sigma \implies c_1\ \sigma$ therefore we also know that $\mathcal{L} \models c_1\ \sigma$
Hence by instantiating the second conjunct of Sub-C1 with θ'_l we know that the following holds
$(\theta'_l, k, e_1) \in \lfloor \tau_1\ \sigma \rfloor_E$
Since $\tau_1\ \sigma <: \tau_2\ \sigma$ therefore from Lemma 4.22 we get
$(\theta'_l, k, e_1) \in \lfloor \tau_2\ \sigma \rfloor_E$

(c) $\forall \theta'_l \sqsupseteq W.\theta_2, j.\mathcal{L} \models c_2 \implies (\theta'_l, j, e_2) \in \lfloor \tau_2\ \sigma \rfloor_E$:
Similar reasoning as in the previous case

6. CGsub-label:

$$\frac{\mathcal{L} \vdash \tau <: \tau' \qquad \mathcal{L} \vdash \ell \sqsubseteq \ell'}{\mathcal{L} \vdash \mathsf{Labeled}\ \ell\ \tau <: \mathsf{Labeled}\ \ell'\ \tau'}$$

To prove: $\lceil ((\mathsf{Labeled}\ \ell\ \tau)\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil ((\mathsf{Labeled}\ \ell'\tau')\ \sigma) \rceil_V^{\mathcal{A}}$

IH: $\lceil (\tau\ \sigma) \rceil_V^{\mathcal{A}} \subseteq \lceil (\tau'\ \sigma) \rceil_V^{\mathcal{A}}$

It suffices to prove: $\forall (W, n, \mathsf{Lb}(v_1), \mathsf{Lb}(v_2)) \in \lceil ((\mathsf{Labeled}\ \ell\ \tau)\ \sigma) \rceil_V^{\mathcal{A}}.\ (W, n, \mathsf{Lb}(v_1), \mathsf{Lb}(v_2)) \in \lceil ((\mathsf{Labeled}\ \ell'\tau')\ \sigma) \rceil_V^{\mathcal{A}}$

This means we are given $(W, n, \mathsf{Lb}(v_1), \mathsf{Lb}(v_2)) \in \lceil ((\mathsf{Labeled}\ \ell\ \tau)\ \sigma) \rceil_V^{\mathcal{A}}$
From Definition 4.4 it means we have $\mathit{ValEq}(\mathcal{A}, W, \ell, n, v_1, v_2, \tau\ \sigma)$ (Sub-L0)
and it suffices to prove $(W, n, \mathsf{Lb}(v_1), \mathsf{Lb}(v_2)) \in \lceil ((\mathsf{Labeled}\ \ell'\tau')\ \sigma) \rceil_V^{\mathcal{A}}$
Again from Definition 4.4 it means w need to prove that
$\mathit{ValEq}(\mathcal{A}, W, \ell', n, \mathsf{Lb}(v_1), \mathsf{Lb}_\ell(v_2), \tau'\ \sigma)$

Since we have (Sub-L0) and $\ell \sqsubseteq \ell'$ therefore from Lemma 4.25 we have
$\mathit{ValEq}(\mathcal{A}, W, \ell', n, \mathsf{Lb}(v_1), \mathsf{Lb}_\ell(v_2), \tau\ \sigma)$

2 cases arise:

(a) $\ell' \sqsubseteq \mathcal{A}$:
In this case from Definition 4.3 we know that $(W, n, v_1, v_2) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$
From IH we also know that $(W, n, v_1, v_2) \in \lceil \tau'\ \sigma \rceil_V^{\mathcal{A}}$
And from Definition 4.4 we get $ValEq(\mathcal{A}, W, \ell', n, \mathsf{Lb}(v_1), \mathsf{Lb}_\ell(v_2), \tau'\ \sigma)$

(b) $\ell' \not\sqsubseteq \mathcal{A}$:
In this case from Definition 4.3 we know that $\forall j.\ (W.\theta_1, j, v_1) \in \lfloor \tau\ \sigma \rfloor_V$ and $(W.\theta_2, j, v_2) \in \lfloor \tau\ \sigma \rfloor_V$
Since $\tau <: \tau'$ therefore from Lemma 4.22 we get $(W.\theta_1, j, v_1) \in \lfloor \tau'\ \sigma \rfloor_V$ and $(W.\theta_2, j, v_2) \in \lfloor \tau'\ \sigma \rfloor_V$

And from Definition 4.4 we get $ValEq(\mathcal{A}, W, \ell', n, \mathsf{Lb}(v_1), \mathsf{Lb}_\ell(v_2), \tau'\ \sigma)$

7. CGsub-CG:

$$\frac{\mathcal{L} \vdash \tau <: \tau' \qquad \mathcal{L} \vdash \ell_i' \sqsubseteq \ell_i \qquad \mathcal{L} \vdash \ell_o \sqsubseteq \ell_o'}{\mathcal{L} \vdash \mathbb{C}\ \ell_i\ \ell_o\ \tau <: \mathbb{C}\ \ell_i'\ \ell_o'\ \tau'}$$

To prove: $\lceil((\mathbb{C}\ \ell_i\ \ell_o\ \tau)\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil((\mathbb{C}\ \ell_i'\ \ell_o'\ \tau')\ \sigma)\rceil_V^{\mathcal{A}}$

IH: $\lceil(\tau\ \sigma)\rceil_V^{\mathcal{A}} \subseteq \lceil(\tau'\ \sigma)\rceil_V^{\mathcal{A}}$

It suffices to prove: $\forall (W, n, e_1, e_2) \in \lceil((\mathbb{C}\ \ell_i\ \ell_o\ \tau)\ \sigma)\rceil_V^{\mathcal{A}}.\ (W, n, e_1, e_2) \in \lceil((\mathbb{C}\ \ell_i'\ \ell_o'\ \tau')\ \sigma)\rceil_V^{\mathcal{A}}$

This means we are given $(W, n, e_1, e_2) \in \lceil((\mathbb{C}\ \ell_i\ \ell_o\ \tau)\ \sigma)\rceil_V^{\mathcal{A}}$
From Definition 4.4 it means we have
$\Big(\forall k \leq n, W_e \sqsupseteq W, H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v_1', v_2', j.$
$(H_1, e_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, e_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H_1', H_2') \triangleright W' \wedge ValEq(\mathcal{A}, W', k - j, \ell_o, v_1', v_2', \tau\ \sigma)\Big) \wedge$
$\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, e_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v_l') \in \lfloor \tau\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_i \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i)\Big)$ (Sub-CG0)

And we need to prove
$(W, n, e_1, e_2) \in \lceil((\mathbb{C}\ \ell_i'\ \ell_o'\ \tau')\ \sigma)\rceil_V^{\mathcal{A}}$
Again from Definition 4.4 it means we need to prove
$\Big(\forall k \leq n, W_e \sqsupseteq W, H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v_1', v_2', j.$
$(H_1, e_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, e_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k - j, H_1', H_2') \triangleright W' \wedge ValEq(\mathcal{A}, W', k - j, \ell_o', v_1', v_2', \tau'\ \sigma)\Big) \wedge$
$\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \triangleright \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k - j, H') \triangleright \theta' \wedge (\theta', k - j, v_l') \in \lfloor \tau'\ \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i' \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i')\Big)$

It means we need to prove:

(a) $\forall k \leq n, W_e \sqsupseteq W.\forall H_1, H_2.(k, H_1, H_2) \triangleright W_e \wedge \forall v_1', v_2', j.$
$(H_1, e_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, e_2) \Downarrow^f (H_2', v_2') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_o, v_1', v_2', \tau' \sigma)$:

This means we are given $k \leq n$, $W_e \sqsupseteq W, H_1, H_2, v_1', v_2', j < k$ s.t
$(k, H_1, H_2) \triangleright W_e$, $(H_1, e_1) \Downarrow_j^f (H_1', v_1') \wedge (H_2, e_2) \Downarrow^f (H_2', v_2')$

And we need to prove
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_o', v_1', v_2', \tau' \sigma)$

Instantiating the first conjuct of (Sub-CG0) to get
$$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \triangleright W' \wedge \mathit{ValEq}(\mathcal{A}, W', k-j, \ell_o, v_1', v_2', \tau\ \sigma) \quad \text{(Sub-CG1)}$$

Since from (Sub-CG1) $\mathit{ValEq}(\mathcal{A}, W', k-j, \ell_o, v_1', v_2', \tau\ \sigma)$
Therefore from Lemma 4.25 we get $\mathit{ValEq}(\mathcal{A}, W', k-j, \ell_o', v_1', v_2', \tau\ \sigma)$

(b) $\forall l \in \{1,2\}.\Big(\forall k, \theta_e \sqsupseteq \theta, H, j.(k, H) \triangleright \theta_e \wedge (H, e_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau' \sigma \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i)$:

Case $l = 1$

Here we are given $k, \theta_e \sqsupseteq \theta, H, j < k$ s.t $(k, H) \triangleright \theta_e \wedge (H, e_l) \Downarrow_j^f (H', v_l')$

And we need to prove

i. $\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau' \sigma \rfloor_V$:
Instantiating the second conjunct of (Sub-CG0) with the given k, θ_e, H, j to get
$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \tau\ \sigma \rfloor_V$

Since $\tau <: \tau'$ therefore from Lemma 4.22 we get $(\theta', k-j, v_l') \in \lfloor \tau' \sigma \rfloor_V$

ii. $(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i' \sqsubseteq \ell')$:
Instantiating the second conjunct of (Sub-CG0) with the given v, i, k, θ_e, H, j to get
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i \sqsubseteq \ell')$
Since $\ell_i' \sqsubseteq \ell_i$ therefore we also get
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau'' \wedge \ell_i' \sqsubseteq \ell')$

iii. $(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i')$:
Instantiating the second conjunct of (Sub-CG0) with the given v, i, k, θ_e, H, j to get
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i)$
Since $\ell_i' \sqsubseteq \ell_i$ therefore we also get
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \ell_i')$

Case $l = 2$

Symmetric reasoning as in the previous $l = 1$ case

8. CGsub-base:

Trivial

Proof of Statement (2)

It suffice to prove that
$\forall (W, n, e_1, e_2) \in \lceil (\tau\ \sigma) \rceil_E^{\mathcal{A}}.\ (W, n, e_1, e_2) \in \lceil (\tau'\ \sigma) \rceil_E^{\mathcal{A}}$

This means given $(W, n, e_1, e_2) \in \lceil (\tau\ \sigma) \rceil_E^{\mathcal{A}}$
From Definition 4.5 it means we have
$\forall i < n. e_1 \Downarrow_i v_1 \wedge e_2 \Downarrow v_2 \implies (W, n-i, v_1, v_2) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$ (Sub-E0)

And it suffices to prove $(W, n, e_1, e_2) \in \lceil (\tau'\ \sigma) \rceil_E^{\mathcal{A}}$
Again from Definition 4.5 it means we need to prove
$\forall i < n. e_1 \Downarrow_i v_1 \wedge e_2 \Downarrow v_2 \implies (W, n-i, v_1, v_2) \in \lceil \tau'\ \sigma \rceil_V^{\mathcal{A}}$

This means that given $i < n$ s.t $e_1 \Downarrow_i v_1 \wedge e_2 \Downarrow v_2$ we need to prove $(W, n-i, v_1, v_2) \in \lceil \tau'\ \sigma \rceil_V^{\mathcal{A}}$

Instantiating (Sub-E0) with the given i we get $(W, n-i, v_1, v_2) \in \lceil \tau\ \sigma \rceil_V^{\mathcal{A}}$

From Statement (1) we get $(W, n-i, v_1, v_2) \in \lceil \tau'\ \sigma \rceil_V^{\mathcal{A}}$ □

Theorem 4.27 (NI for CG)**.** *Say* $\mathsf{bool} = (\mathsf{unit} + \mathsf{unit})$
$\forall v_1, v_2, e, n'.$
$\emptyset \vdash v_1 : \mathsf{Labeled}\ \top\ \mathsf{bool} \wedge \emptyset \vdash v_2 : \mathsf{Labeled}\ \top\ \mathsf{bool} \wedge$
$x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e : \mathbb{C}\ \bot\ \bot\ \mathsf{bool} \wedge$
$(\emptyset, e[v_1/x]) \Downarrow_{n'}^f (-, v_1') \wedge (\emptyset, e[v_2/x]) \Downarrow_{-}^f (-, v_2') \implies$
$v_1' = v_2'$

Proof. Given some
$\emptyset \vdash v_1 : \mathsf{Labeled}\ \top\ \mathsf{bool} \wedge \emptyset \vdash v_2 : \mathsf{Labeled}\ \top\ \mathsf{bool} \wedge$
$x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e : \mathbb{C}\ \bot\ \bot\ \mathsf{bool} \wedge$
$(\emptyset, e[v_1/x]) \Downarrow_{n'}^f (-, v_1') \wedge (\emptyset, e[v_2/x]) \Downarrow_{-}^f (-, v_2')$

And we need to prove
$v_1' = v_2'$

From Theorem 4.24 we know that
$\forall n. (\emptyset, n, v_1, v_2) \in \lceil \mathsf{Labeled}\ \top\ \mathsf{bool} \rceil_E^{\bot}$
Similarly from Theorem 4.24 and Definition 4.13 we also get
$\forall n. (\emptyset, n, e[v_1/x], e[v_2/x]) \in \lceil \mathbb{C}\ \bot\ \bot\ \mathsf{bool} \rceil_E^{\bot}$

From Definition 4.5 we get
$\forall n. \forall i < n. e[v_1/x] \Downarrow_i v_{11} \wedge e[v_2/x] \Downarrow v_{22} \implies (\emptyset, n-i, v_{11}, v_{22}) \in \lceil \mathbb{C}\ \bot\ \bot\ \mathsf{bool} \rceil_V^{\bot}$

Instantiating it with $n'+1$ and then with 0, from CG-val we have $v_{11} = e[v_1/x]$ and $v_{22} = e[v_2/x]$
Therefore we have
$(\emptyset, n'+1, e[v_1/x], e[v_2/x]) \in \lceil \mathbb{C}\ \bot\ \bot\ \mathsf{bool} \rceil_V^{\bot}$

From Definition 4.6 we have
$\Big(\forall k \leq n'+1, W_e \sqsupseteq \emptyset, H_1, H_2.(k, H_1, H_2) \rhd W_e \wedge$
$\forall v_1'', v_2'', j.(H_1, e[v_1/x]) \Downarrow_j^f (H_1', v_1'') \wedge (H_2, e[v_2/x]) \Downarrow^f (H_2', v_2'') \wedge j < k \implies$
$\exists W' \sqsupseteq W_e.(k-j, H_1', H_2') \rhd W' \wedge \mathit{ValEq}(\bot, W', k-j, \bot, v_1', v_2', \mathsf{b})\Big) \wedge$
$\forall l \in \{1, 2\}.\Big(\forall k, \theta_e \sqsupseteq W.\theta_l, H, j.(k, H) \rhd \theta_e \wedge (H, v_l) \Downarrow_j^f (H', v_l') \wedge j < k \implies$

$\exists \theta' \sqsupseteq \theta_e.(k-j, H') \triangleright \theta' \wedge (\theta', k-j, v_l') \in \lfloor \mathsf{b} \rfloor_V \wedge$
$(\forall a.H(a) \neq H'(a) \implies \exists \ell'.\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \bot \sqsubseteq \ell') \wedge$
$(\forall a \in dom(\theta') \backslash dom(\theta_e).\theta'(a) \searrow \bot)\Big)$

Instantiating the first conjunct with $n'+1, \emptyset, \emptyset, \emptyset$. And then with v_1', v_2', n' we get $\exists W' \sqsupseteq \emptyset.(1, H_1', H_2') \triangleright W' \wedge ValEq(\bot, W', 1, \bot, v_1', v_2', \mathsf{bool})$

From Definition 4.3 and Definition 4.6 we get $v_1' = v_2'$

□

5 Translations between FG and CG

5.1 CG to FG translation

5.1.1 Type directed translation from CG to FG

CG types are translated into FG types by the following definition of $[\![\cdot]\!]$

$$
\begin{aligned}
[\![\mathsf{b}]\!] &= \mathsf{b}^{\perp} \\
[\![\tau_1 \rightarrow \tau_2]\!] &= ([\![\tau_1]\!] \xrightarrow{\top} [\![\tau_2]\!])^{\perp} \\
[\![\tau_1 \times \tau_2]\!] &= ([\![\tau_1]\!] \times [\![\tau_2]\!])^{\perp} \\
[\![\tau_1 + \tau_2]\!] &= ([\![\tau_1]\!] + [\![\tau_2]\!])^{\perp} \\
[\![\mathsf{Labeled}\ \ell\ \tau]\!] &= ([\![\tau]\!] + \mathsf{unit})^{\ell}
\end{aligned}
\qquad
\begin{aligned}
[\![\mathsf{ref}\ \ell\ \tau]\!] &= (\mathsf{ref}\ ([\![\tau]\!] + \mathsf{unit})^{\ell})^{\perp} \\
[\![\mathbb{C}\ \ell_1\ \ell_2\ \tau]\!] &= (\mathsf{unit} \xrightarrow{\ell_1} ([\![\tau]\!] + \mathsf{unit})^{\ell_2})^{\perp} \\
[\![c \Rightarrow \tau]\!] &= (c \overset{\top}{\Rightarrow} [\![\tau]\!])^{\perp} \\
[\![\forall \alpha.\tau]\!] &= (\forall \alpha.(\top, [\![\tau]\!]))^{\perp}
\end{aligned}
$$

The translation judgment for expressions is of the form $\boxed{\Sigma; \Psi; \Gamma \vdash_{pc} e_C : \tau_C \leadsto e_F}$.

$$\frac{\Sigma;\Psi;\Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma;\Psi;\Gamma \vdash \lambda x.e : \tau_1 \to \tau_2 \rightsquigarrow \lambda x.e_F}\ \text{lambda}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash e_1 : \tau \rightsquigarrow e_{F1} \qquad \Sigma;\Psi;\Gamma \vdash e_2 : \tau \rightsquigarrow e_{F2}}{\Sigma;\Psi;\Gamma \vdash e_1\ e_2 : \tau \rightsquigarrow e_{F1}\ e_{F2}}\ \text{app}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash e_1 : \tau \rightsquigarrow e_{F1} \qquad \Sigma;\Psi;\Gamma \vdash e_2 : \tau \rightsquigarrow e_{F2}}{\Sigma;\Psi;\Gamma \vdash (e_1, e_2) : \tau_1 \times \tau_2 \rightsquigarrow (e_{F1}, e_{F2})}\ \text{prod}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma;\Psi;\Gamma \vdash \mathsf{fst}(e) : \tau_1 \rightsquigarrow \mathsf{fst}(e_F)}\ \text{fst} \qquad \frac{\Sigma;\Psi;\Gamma \vdash e : \tau \rightsquigarrow e_F}{\Gamma \vdash \mathsf{snd}(e) : \tau_2 \rightsquigarrow \mathsf{snd}(e_F)}\ \text{snd}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash e : \tau_1 \rightsquigarrow e_F}{\Sigma;\Psi;\Gamma \vdash \mathsf{inl}(e) : \tau_1 + \tau_2 \rightsquigarrow \mathsf{inl}(e_F)}\ \text{inl} \qquad \frac{\Sigma;\Psi;\Gamma \vdash e : \tau_2 \rightsquigarrow e_F}{\Sigma;\Psi;\Gamma \vdash \mathsf{inr}(e) : \tau_1 + \tau_2 \rightsquigarrow \mathsf{inr}(e_F)}\ \text{inr}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash e : (\tau_1 + \tau_2) \rightsquigarrow e_F \qquad \Sigma;\Psi;\Gamma, x : \tau_1 \vdash e_1 : \tau \rightsquigarrow e_{F1} \qquad \Sigma;\Psi;\Gamma, y : \tau_2 \vdash e_2 : \tau \rightsquigarrow e_{F2}}{\Sigma;\Psi;\Gamma \vdash \mathsf{case}(e, x.e_1, y.e_2) : \tau \rightsquigarrow \mathsf{case}(e_F, x.e_{F1}, y.e_{F2})}\ \text{case}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma;\Psi;\Gamma \vdash \mathsf{Lb}_\ell(e) : (\mathsf{Labeled}\ \ell\ \tau) \rightsquigarrow \mathsf{inl}(e_F)}\ \text{label}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash e : \mathsf{Labeled}\ \ell\ \tau \rightsquigarrow e_F}{\Sigma;\Psi;\Gamma \vdash \mathsf{unlabel}(e) : \mathbb{C}\ \top\ \ell\ \tau \rightsquigarrow \lambda\_.e_F}\ \text{unlabel}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash e : \mathbb{C}\ \ell_1\ \ell_2\ \tau \rightsquigarrow e_F}{\Sigma;\Psi;\Gamma \vdash \mathsf{toLabeled}(e) : \mathbb{C}\ \ell_1\ \bot\ (\mathsf{Labeled}\ \ell_2\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(e_F\ ())}\ \text{toLabeled}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma;\Psi;\Gamma \vdash \mathsf{ret}(e) : \mathbb{C}\ \ell_1\ \ell_2\ \tau \rightsquigarrow \lambda\_.\mathsf{inl}(e_F)}\ \text{ret}$$

$$\frac{\begin{array}{c}\Sigma;\Psi;\Gamma \vdash e_1 : \mathbb{C}\ \ell_1\ \ell_2\ \tau \rightsquigarrow e_{F1} \qquad \Sigma;\Psi;\Gamma, x : \tau \vdash e_2 : \mathbb{C}\ \ell_3\ \ell_4\ \tau' \rightsquigarrow e_{F2} \\ \Sigma;\Psi \vdash \ell \sqsubseteq \ell_1 \qquad \Sigma;\Psi \vdash \ell \sqsubseteq \ell_3 \qquad \Sigma;\Psi \vdash \ell_2 \sqsubseteq \ell_3 \qquad \Sigma;\Psi \vdash \ell_2 \sqsubseteq \ell_4 \qquad \Sigma;\Psi \vdash \ell_4 \sqsubseteq \ell'\end{array}}{\Sigma;\Psi;\Gamma \vdash \mathsf{bind}(e_1, x.e_2) : \mathbb{C}\ \ell\ \ell'\ \tau' \rightsquigarrow \lambda\_.\mathsf{case}(e_{F1}(), x.e_{F2}(), y.\mathsf{inr}())}\ \text{bind}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash e : \mathsf{Labeled}\ \ell'\ \tau \rightsquigarrow e_F \qquad \Sigma;\Psi \vdash \ell \sqsubseteq \ell'}{\Sigma;\Psi;\Gamma \vdash \mathsf{new}\ e : \mathbb{C}\ \ell\ \bot\ (\mathsf{ref}\ \ell'\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_F))}\ \text{ref}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash e : \mathsf{ref}\ \ell\ \tau \rightsquigarrow e_F}{\Sigma;\Psi;\Gamma \vdash !e : \mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(e_F)}\ \text{deref}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash e_1 : \mathsf{ref}\ \ell'\ \tau \rightsquigarrow e_{F1} \qquad \Sigma;\Psi;\Gamma \vdash e_2 : \mathsf{Labeled}\ \ell'\ \tau \rightsquigarrow e_{F2} \qquad \mathcal{L} \vdash \ell \sqsubseteq \ell'}{\Sigma;\Psi;\Gamma \vdash e_1 := e_2 : \mathbb{C}\ \ell\ \bot\ \mathsf{unit} \rightsquigarrow \lambda\_.\mathsf{inl}(e_{F1} := e_{F2})}\ \text{assign}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau' \rightsquigarrow e_F \qquad \Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi; \Gamma \vdash e : \tau \rightsquigarrow e_F} \text{ sub} \qquad \frac{\Sigma, \alpha; \Psi; \Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \Lambda e : \forall \alpha.\tau \rightsquigarrow \Lambda e_F} \text{ FI}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \forall \alpha.\tau \rightsquigarrow e_F \qquad FV(\ell) \in \Sigma}{\Sigma; \Psi; \Gamma \vdash e\ [] : \tau[\ell/\alpha] \rightsquigarrow e_F[]} \text{ FE} \qquad \frac{\Sigma; \Psi, c; \Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \nu\ e : c \Rightarrow \tau \rightsquigarrow \nu\ e_F} \text{ CI}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : c \Rightarrow \tau \rightsquigarrow e_F \qquad \Sigma; \Psi \vdash c}{\Sigma; \Psi; \Gamma \vdash e \bullet : \tau \rightsquigarrow e_F \bullet} \text{ CE}$$

5.1.2 Type preservation for CG to FG translation

Theorem 5.1 (Type preservation, CG $\rightsquigarrow$ FG)**.** $\forall \Sigma; \Psi; \Gamma, e_C, \tau.$
$\Gamma \vdash e_C : \tau$ *is a valid typing derivation in CG* $\implies$
$\exists e_F.$
$\Gamma \vdash e_C : \tau \rightsquigarrow e_F \wedge$
$[\![\Gamma]\!] \vdash_\top e_F : [\![\tau]\!]$ *is a valid typing derivation in FG*

Proof. Proof by induction on the translation judgment. We show selected cases below.

1. label:

$$\frac{\Gamma \vdash e : \tau \rightsquigarrow e_F}{\Gamma \vdash \mathsf{Lb}_\ell(e) : (\mathsf{Labeled}\ \ell\ \tau) \rightsquigarrow \mathsf{inl}(e_F)} \text{ label}$$

$$\cfrac{\cfrac{\cfrac{}{[\![\Gamma]\!] \vdash_\top e_F : [\![\tau]\!]} \text{ IH}}{[\![\Gamma]\!] \vdash_\top \mathsf{inl}(e_F) : ([\![\tau]\!] + \mathsf{unit})^\perp} \text{ FG-inl}}{[\![\Gamma]\!] \vdash_\top \mathsf{inl}(e_F) : ([\![\tau]\!] + \mathsf{unit})^\ell} \text{ FG-sub}$$

2. unlabel:

$$\frac{\Gamma \vdash e : \mathsf{Labeled}\ \ell\ \tau \rightsquigarrow e_F}{\Gamma \vdash \mathsf{unlabel}(e) : \mathbb{C}\ \top\ \ell\ \tau \rightsquigarrow \lambda\_.e_F} \text{ unlabel}$$

Main derivation:

$$\cfrac{\cfrac{}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_\top e_F : ([\![\tau]\!] + \mathsf{unit})^\ell} \text{ IH}}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_\top \lambda\_.e_F : (\mathsf{unit} \xrightarrow{\top} ([\![\tau]\!] + \mathsf{unit})^\ell)^\perp} \text{ FG-lam}$$

3. toLabeled:

$$\frac{\Gamma \vdash e : \mathbb{C}\ \ell_1\ \ell_2\ \tau \rightsquigarrow e_F}{\Gamma \vdash \mathsf{toLabeled}(e) : \mathbb{C}\ \ell_1\ \perp\ (\mathsf{Labeled}\ \ell_2\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(e_F\ ())} \text{ toLabeled}$$

P2:

$$\cfrac{\cfrac{}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_\top e_F : (\mathsf{unit} \xrightarrow{\ell_1} ([\![\tau]\!] + \mathsf{unit})^{\ell_2})^\perp} \text{ IH, Weakening} \qquad \mathcal{L} \vdash \ell_1 \sqsubseteq \top}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_1} e_F : (\mathsf{unit} \xrightarrow{\ell_1} ([\![\tau]\!] + \mathsf{unit})^{\ell_2})^\perp} \text{ FG-sub}$$

P1:

$$\dfrac{P2 \qquad \dfrac{}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_1} () : \mathsf{unit}} \qquad \mathcal{L} \vdash \ell_1 \sqcup \bot \sqsubseteq \ell_1 \qquad \mathcal{L} \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell_2} \searrow \bot}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_1} e_F() : ([\![\tau]\!] + \mathsf{unit})^{\ell_2}} \text{ FG-app}$$

Main derivation:

$$\dfrac{\dfrac{P1}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_1} \mathsf{inl}(e_F()) : (([\![\tau]\!] + \mathsf{unit})^{\ell_2} + \mathsf{unit})^{\bot}} \text{ FG-inl}}{[\![\Gamma]\!] \vdash_{\top} \lambda\_.\mathsf{inl}(e_F()) : (\mathsf{unit} \xrightarrow{\ell_1} (([\![\tau]\!] + \mathsf{unit})^{\ell_2} + \mathsf{unit})^{\bot})^{\bot}} \text{ FG-lam}$$

4. ret:

$$\dfrac{\Gamma \vdash e : \tau \rightsquigarrow e_F}{\Gamma \vdash \mathsf{ret}(e) : \mathbb{C}\ \ell_1\ \ell_2\ \tau \rightsquigarrow \lambda\_.\mathsf{inl}(e_F)} \text{ ret}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\top} e_F : [\![\tau]\!]} \text{ IH, Weakening} \qquad \mathcal{L} \vdash \ell_1 \sqsubseteq \top}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_1} e_F : [\![\tau]\!]} \text{ FG-sub} \qquad \mathcal{L} \vdash \bot \sqsubseteq \ell_2}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_1} \mathsf{inl}(e_F) : ([\![\tau]\!] + \mathsf{unit})^{\ell_2}} \text{ FG-sub, FG-inl}}{[\![\Gamma]\!] \vdash_{\top} \lambda\_.\mathsf{inl}(e_F) : (\mathsf{unit} \xrightarrow{\ell_1} ([\![\tau]\!] + \mathsf{unit})^{\ell_2})^{\bot}} \text{ FG-lam}$$

5. bind:

$$\dfrac{\begin{array}{c}\Gamma \vdash e_1 : \mathbb{C}\ \ell_1\ \ell_2\ \tau \rightsquigarrow e_{F1} \\ \Gamma, x : \tau \vdash e_2 : \mathbb{C}\ \ell_3\ \ell_4\ \tau' \rightsquigarrow e_{F2} \qquad \ell \sqsubseteq \ell_1 \qquad \ell \sqsubseteq \ell_3 \qquad \ell_2 \sqsubseteq \ell_3 \qquad \ell_2 \sqsubseteq \ell_4 \qquad \ell_4 \sqsubseteq \ell'\end{array}}{\Gamma \vdash \mathsf{bind}(e_1, x.e_2) : \mathbb{C}\ \ell\ \ell'\ \tau' \rightsquigarrow \lambda\_.\mathsf{case}(e_{F1}(), x.e_{F2}(), y.\mathsf{inr}())} \text{ bind}$$

P1.1:

$$\dfrac{\dfrac{}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\top} e_{F1} : (\mathsf{unit} \xrightarrow{\ell_1} ([\![\tau]\!] + \mathsf{unit})^{\ell_2})^{\bot}} \text{ IH1, Weakening} \qquad \mathcal{L} \vdash \ell \sqsubseteq \top}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell} e_{F1} : (\mathsf{unit} \xrightarrow{\ell_1} ([\![\tau]\!] + \mathsf{unit})^{\ell_2})^{\bot}} \text{ FG-sub}$$

P1:

$$\dfrac{P1.1 \qquad \dfrac{}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell} () : \mathsf{unit}} \text{ FG-var} \qquad \mathcal{L} \vdash (\ell \sqcup \bot) \sqsubseteq \ell_1 \qquad \dfrac{\mathcal{L} \vdash \bot \sqsubseteq \ell_2}{\mathcal{L} \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell_2} \searrow \bot}}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_1} e_{F1}() : ([\![\tau]\!] + \mathsf{unit})^{\ell_2}} \text{ FG-app}$$

P2.1:

$$\dfrac{\dfrac{}{[\![\Gamma]\!], \_ : \mathsf{unit}, x : [\![\tau]\!] \vdash_{\top} e_{F2} : (\mathsf{unit} \xrightarrow{\ell_3} ([\![\tau']\!] + \mathsf{unit})^{\ell_4})^{\bot}} \text{ IH2, Weakening} \qquad \mathcal{L} \vdash \ell \sqcup \ell_2 \sqsubseteq \top}{[\![\Gamma]\!], \_ : \mathsf{unit}, x : [\![\tau]\!] \vdash_{\ell \sqcup \ell_2} e_{F2} : (\mathsf{unit} \xrightarrow{\ell_3} ([\![\tau']\!] + \mathsf{unit})^{\ell_4})^{\bot}} \text{ FG-sub}$$

P2:

$$\dfrac{P2.1 \qquad \dfrac{}{[\![\Gamma]\!], \_ : \mathsf{unit}, x : [\![\tau]\!] \vdash_{\ell \sqcup \ell_2} () : \mathsf{unit}}\text{ FG-var} \qquad \mathcal{L} \vdash (\ell \sqcup \ell_2 \sqcup \bot) \sqsubseteq \ell_3 \qquad \dfrac{\mathcal{L} \vdash \bot \sqsubseteq \ell_4}{\mathcal{L} \vdash ([\![\tau']\!] + \mathsf{unit})^{\ell_4} \searrow \bot}}{[\![\Gamma]\!], \_ : \mathsf{unit}, x : [\![\tau]\!] \vdash_{\ell \sqcup \ell_2} e_{F2}() : ([\![\tau']\!] + \mathsf{unit})^{\ell_4}}\text{ FG-app}$$

P3:

$$\dfrac{\dfrac{}{[\![\Gamma]\!], \_ : \mathsf{unit}, y : \mathsf{unit} \vdash_{\ell \sqcup \ell_2} () : \mathsf{unit}}\text{ FG-var} \qquad \mathcal{L} \vdash \bot \sqsubseteq \ell_4}{[\![\Gamma]\!], \_ : \mathsf{unit}, y : \mathsf{unit} \vdash_{\ell \sqcup \ell_2} \mathsf{inr}() : ([\![\tau']\!] + \mathsf{unit})^{\ell_4}}\text{ FG-sub, FG-inr}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad P2 \qquad P3 \qquad \dfrac{\dfrac{}{\mathcal{L} \vdash \ell_2 \sqsubseteq \ell_4}\text{ Given}}{\mathcal{L} \vdash ([\![\tau']\!] + \mathsf{unit})^{\ell_4} \searrow \ell_2} \qquad \dfrac{}{\ell_4 \sqsubseteq \ell'}\text{ Given}}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell} \mathsf{case}(e_{F1}(), x.e_{F2}(), y.\mathsf{inr}()) : ([\![\tau']\!] + \mathsf{unit})^{\ell'}}\text{ FG-case, FG-sub}}{[\![\Gamma]\!] \vdash_{\top} \lambda\_.\mathsf{case}(e_{F1}(), x.e_{F2}(), y.\mathsf{inr}()) : (\mathsf{unit} \xrightarrow{\ell} ([\![\tau']\!] + \mathsf{unit})^{\ell'})^{\bot}}\text{ FG-lam}$$

6. ref:

$$\dfrac{\Gamma \vdash e : \mathsf{Labeled}\ \ell'\ \tau \rightsquigarrow e_F \qquad \mathcal{L} \vdash \ell \sqsubseteq \ell'}{\Gamma \vdash \mathsf{new}\ e : \mathbb{C}\ \ell\ \bot\ (\mathsf{ref}\ \ell'\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_F))}\text{ ref}$$

P1:

$$\dfrac{\dfrac{\dfrac{}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\top} e_F : ([\![\tau]\!] + \mathsf{unit})^{\ell'}}\text{ IH, Weakening} \qquad \mathcal{L} \vdash \ell \sqsubseteq \top}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell} e_F : ([\![\tau]\!] + \mathsf{unit})^{\ell'}}\text{ FG-sub} \qquad \dfrac{\mathcal{L} \vdash \ell \sqsubseteq \ell'}{\mathcal{L} \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell'} \searrow \ell}}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell} \mathsf{new}\ e_F : (\mathsf{ref}([\![\tau]\!] + \mathsf{unit})^{\ell'})^{\bot}}\text{ FG-ref}$$

Main derivation:

$$\dfrac{\dfrac{P1}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell} \mathsf{inl}(\mathsf{new}\ e_F) : ((\mathsf{ref}([\![\tau]\!] + \mathsf{unit})^{\ell'})^{\bot} + \mathsf{unit})^{\bot}}\text{ FG-inl}}{[\![\Gamma]\!] \vdash_{\top} \lambda\_.\mathsf{inl}(\mathsf{new}\ e_F) : (\mathsf{unit} \xrightarrow{\ell} ((\mathsf{ref}([\![\tau]\!] + \mathsf{unit})^{\ell'})^{\bot} + \mathsf{unit})^{\bot})^{\bot}}\text{ FG-lam}$$

7. deref:

$$\dfrac{\Gamma \vdash e : \mathsf{ref}\ \ell\ \tau \rightsquigarrow e_F}{\Gamma \vdash !e : \mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(e_F)}\text{ deref}$$

P2:

$$\dfrac{}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\top} e_F : (\mathsf{ref}\ ([\![\tau]\!] + \mathsf{unit})^{\ell})^{\bot}}\text{ IH}$$

P1:

$$\dfrac{P2 \qquad \dfrac{}{\mathcal{L} \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell} <: ([\![\tau]\!] + \mathsf{unit})^{\ell}}\ \text{Lemma 1.1} \qquad \dfrac{}{\mathcal{L} \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell} \searrow \bot}}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\top} !e_F : ([\![\tau]\!] + \mathsf{unit})^{\ell}}\ \text{FG-deref}$$

Main derivation:

$$\dfrac{\dfrac{P1}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\top} \mathsf{inl}(!e_F) : ((([\![\tau]\!] + \mathsf{unit})^{\ell} + \mathsf{unit})^{\bot}}\ \text{FG-inl}}{[\![\Gamma]\!] \vdash_{\top} \lambda\_.\mathsf{inl}(!e_F) : (\mathsf{unit} \xrightarrow{\top} ((([\![\tau]\!] + \mathsf{unit})^{\ell} + \mathsf{unit})^{\bot})^{\bot}}\ \text{FG-lam}$$

8. assign:

$$\dfrac{\Gamma \vdash e_1 : \mathsf{ref}\ \ell'\ \tau \rightsquigarrow e_{F1} \qquad \Gamma \vdash e_2 : \mathsf{Labeled}\ \ell'\ \tau \rightsquigarrow e_{F2} \qquad \mathcal{L} \vdash \ell \sqsubseteq \ell'}{\Gamma \vdash e_1 := e_2 : \mathbb{C}\ \ell\ \bot\ \mathsf{unit} \rightsquigarrow \lambda\_.\mathsf{inl}(e_{F1} := e_{F2})}\ \text{assign}$$

P3:

$$\dfrac{\dfrac{}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\top} e_{F2} : ([\![\tau]\!] + \mathsf{unit})^{\ell'}}\ \text{IH2, Weakening} \qquad \mathcal{L} \vdash \ell \sqsubseteq \top}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell} e_{F2} : ([\![\tau]\!] + \mathsf{unit})^{\ell'}}\ \text{FG-sub}$$

P2:

$$\dfrac{\dfrac{}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\top} e_{F1} : (\mathsf{ref}([\![\tau]\!] + \mathsf{unit})^{\ell'})^{\bot}}\ \text{IH1, Weakening} \qquad \mathcal{L} \vdash \ell \sqsubseteq \top}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell} e_{F1} : (\mathsf{ref}([\![\tau]\!] + \mathsf{unit})^{\ell'})^{\bot}}\ \text{FG-sub}$$

P1:

$$\dfrac{P2 \qquad P3 \qquad \dfrac{\dfrac{}{\mathcal{L} \vdash \ell \sqsubseteq \ell'}\ \text{Given}}{\mathcal{L} \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell'} \searrow (\ell \sqcup \bot)}}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell} e_{F1} := e_{F2} : \mathsf{unit}}\ \text{FG-assign}$$

Main derivation:

$$\dfrac{\dfrac{P1}{[\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell} \mathsf{inl}(e_{F1} := e_{F2}) : (\mathsf{unit} + \mathsf{unit})^{\bot}}\ \text{FG-inl}}{[\![\Gamma]\!] \vdash_{\top} \lambda\_.\mathsf{inl}(e_{F1} := e_{F2}) : (\mathsf{unit} \xrightarrow{\ell} (\mathsf{unit} + \mathsf{unit})^{\bot})^{\bot}}\ \text{FG-lam}$$

9. sub:

$$\dfrac{\dfrac{}{[\![\Gamma]\!] \vdash_{\top} e_F : [\![\tau']\!]}\ \text{IH} \qquad \mathcal{L} \vdash \top \sqsubseteq \top \qquad \dfrac{\mathcal{L} \vdash \tau' <: \tau}{\mathcal{L} \vdash [\![\tau']\!] <: [\![\tau]\!]}\ \text{Lemma 5.2}}{[\![\Gamma]\!] \vdash_{\top} e_F : [\![\tau]\!]}\ \text{FG-sub}$$

10. FI:

$$\dfrac{\dfrac{}{\Sigma, \alpha; \Psi; [\![\Gamma]\!] \vdash_{\top} e_F : [\![\tau]\!]}\ \text{IH}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_{\top} \Lambda e_F : (\forall \alpha.(\top, [\![\tau]\!]))^{\bot}}\ \text{FG-FI}$$

11. FE:

$$\dfrac{\mathrm{FV}(\ell) \in \Sigma \qquad \dfrac{}{\Sigma;\Psi;[\![\Gamma]\!] \vdash_\top e_F : (\forall\alpha.(\top,[\![\tau]\!]))^\perp}\text{IH} \qquad \Sigma;\Psi \vdash \top \sqcup \bot \sqsubseteq \top \qquad \Sigma;\Psi \vdash [\![\tau[\ell/\alpha]]\!] \searrow \bot}{\dfrac{\Sigma;\Psi;[\![\Gamma]\!] \vdash_\top e_F\ [] : [\![\tau]\!][\ell/\alpha]}{\Sigma;\Psi;[\![\Gamma]\!] \vdash_\top e_F\ [] : [\![\tau[\ell/\alpha]]\!]}\text{Lemma 5.5}}\text{FG-FE}$$

12. CI:

$$\dfrac{\dfrac{}{\Sigma;\Psi,c;[\![\Gamma]\!] \vdash_\top e_F : [\![\tau]\!]}\text{IH}}{\Sigma;\Psi;[\![\Gamma]\!] \vdash_\top \nu\ e_F : (c \overset{\top}{\Rightarrow} [\![\tau]\!])^\perp}\text{FG-CI}$$

13. CE:

$$\dfrac{\dfrac{}{\Sigma;\Psi;[\![\Gamma]\!] \vdash_\top e_F : (c \overset{\top}{\Rightarrow} [\![\tau]\!])^\perp}\text{IH} \qquad \Sigma;\Psi \vdash c \qquad \Sigma;\Psi \vdash \top \sqcup \bot \sqsubseteq \top \qquad \Sigma;\Psi \vdash [\![\tau]\!] \searrow \bot}{\Sigma;\Psi;[\![\Gamma]\!] \vdash_\top e_F \bullet : [\![\tau]\!]}\text{FG-CE}$$

□

Lemma 5.2 (Subtyping type preservation: CG to FG)**.** *For any CG types τ and τ', Σ, and Ψ, if $\mathcal{L} \vdash \tau <: \tau'$, then $\mathcal{L} \vdash [\![\tau]\!] <: [\![\tau']\!]$.*

Proof. Proof by induction on CG's subtyping relation

1. CGsub-base:

$$\dfrac{}{\mathcal{L} \vdash [\![\tau]\!] <: [\![\tau]\!]}\text{Lemma 1.1}$$

2. CGsub-arrow:

$$\dfrac{\dfrac{\dfrac{}{\mathcal{L} \vdash [\![\tau_1']\!] <: [\![\tau_1]\!]}\text{IH1} \qquad \dfrac{}{\mathcal{L} \vdash [\![\tau_2]\!] <: [\![\tau_2']\!]}\text{IH2} \qquad \mathcal{L} \vdash \top \sqsubseteq \top}{\mathcal{L} \vdash ([\![\tau_1]\!] \overset{\top}{\to} [\![\tau_2]\!])^\perp <: ([\![\tau_1']\!] \overset{\top}{\to} [\![\tau_2']\!])^\perp}\text{FGsub-arrow}}{\mathcal{L} \vdash [\![(\tau_1 \overset{\ell_e}{\to} \tau_2)]\!] <: [\![(\tau_1' \overset{\ell_e'}{\to} \tau_2')]\!]}\text{Definition of } [\![\cdot]\!]$$

3. CGsub-prod:

$$\dfrac{\dfrac{\dfrac{}{\mathcal{L} \vdash [\![\tau_1]\!] <: [\![\tau_1']\!]}\text{IH1} \qquad \dfrac{}{\mathcal{L} \vdash [\![\tau_2]\!] <: [\![\tau_2']\!]}\text{IH2}}{\mathcal{L} \vdash ([\![\tau_1]\!] \times [\![\tau_2]\!])^\perp <: ([\![\tau_1']\!] \times [\![\tau_2']\!])^\perp}\text{FGsub-arrow}}{\mathcal{L} \vdash [\![(\tau_1 \times \tau_2)]\!] <: [\![(\tau_1' \times \tau_2')]\!]}\text{Definition of } [\![\cdot]\!]$$

4. CGsub-sum:

$$\dfrac{\dfrac{\dfrac{}{\mathcal{L} \vdash [\![\tau_1]\!] <: [\![\tau_1']\!]}\text{IH1} \qquad \dfrac{}{\mathcal{L} \vdash [\![\tau_2]\!] <: [\![\tau_2']\!]}\text{IH2}}{\mathcal{L} \vdash ([\![\tau_1]\!] + [\![\tau_2]\!])^\perp <: ([\![\tau_1']\!] + [\![\tau_2']\!])^\perp}\text{FGsub-arrow}}{\mathcal{L} \vdash [\![(\tau_1 + \tau_2)]\!] <: [\![(\tau_1' + \tau_2')]\!]}\text{Definition of } [\![\cdot]\!]$$

5. CGsub-labeled:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\mathcal{L} \vdash [\![\tau_1]\!] <: [\![\tau_1']\!]}\,\text{IH1} \qquad \dfrac{}{\mathcal{L} \vdash \mathsf{unit} <: \mathsf{unit}}\,\text{FGsub-unit}}{\mathcal{L} \vdash ([\![\tau_1]\!] + \mathsf{unit}) <: ([\![\tau_1']\!] + \mathsf{unit})}\,\text{FGsub-sum} \qquad \dfrac{\dfrac{}{\mathsf{Labeled}\ \ell_1\ \tau_1 <: \mathsf{Labeled}\ \ell_1'\ \tau_1'}\,\text{Given}}{\ell_1 \sqsubseteq \ell_1'}\,\text{By inversion}}{\mathcal{L} \vdash ([\![\tau_1]\!] + \mathsf{unit})^{\ell_1} <: ([\![\tau_1']\!] + \mathsf{unit})^{\ell_1'}}\,\text{FGsub-arrow}}{\mathcal{L} \vdash [\![\mathsf{Labeled}\ \ell_1\ \tau_1]\!] <: [\![\mathsf{Labeled}\ \ell_1'\ \tau_1']\!]}\,\text{Definition of } [\![\cdot]\!]$$

6. CGsub-monad:

P3:

$$\dfrac{\dfrac{}{\mathcal{L} \vdash [\![\tau_1]\!] <: [\![\tau_1']\!]}\,\text{IH} \qquad \dfrac{}{\mathcal{L} \vdash \mathsf{unit} <: \mathsf{unit}}\,\text{FGsub-unit}}{\mathcal{L} \vdash ([\![\tau_1]\!] + \mathsf{unit}) <: ([\![\tau_1']\!] + \mathsf{unit})}\,\text{FGsub-sum}$$

P2:

$$\dfrac{P3 \qquad \dfrac{\dfrac{}{\mathcal{L} \vdash \mathbb{C}\ \ell_i\ \ell_o\ \tau_1 <: \mathbb{C}\ \ell_i'\ \ell_o'\ \tau_1'}\,\text{Given}}{\mathcal{L} \vdash \ell_o \sqsubseteq \ell_o'}\,\text{By inversion}}{\mathcal{L} \vdash ([\![\tau_1]\!] + \mathsf{unit})^{\ell_o} <: ([\![\tau_1']\!] + \mathsf{unit})^{\ell_o'}}\,\text{FGsub-label}$$

P1:

$$\dfrac{\dfrac{}{\mathcal{L} \vdash \mathsf{unit} <: \mathsf{unit}} \qquad P2 \qquad \dfrac{\dfrac{}{\mathcal{L} \vdash \mathbb{C}\ \ell_i\ \ell_o\ \tau_1 <: \mathbb{C}\ \ell_i'\ \ell_o'\ \tau_1'}\,\text{Given}}{\mathcal{L} \vdash \ell_i' \sqsubseteq \ell_i}}{\mathcal{L} \vdash (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau_1]\!] + \mathsf{unit})^{\ell_o}) <: (\mathsf{unit} \xrightarrow{\ell_i'} ([\![\tau_1']\!] + \mathsf{unit})^{\ell_o'})}\,\text{FGsub-arrow}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad \dfrac{}{\mathcal{L} \vdash \bot \sqsubseteq \bot}}{\mathcal{L} \vdash (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau_1]\!] + \mathsf{unit})^{\ell_o})^{\bot} <: (\mathsf{unit} \xrightarrow{\ell_i'} ([\![\tau_1']\!] + \mathsf{unit})^{\ell_o'})^{\bot}}\,\text{FGsub-label}}{\mathcal{L} \vdash [\![\mathbb{C}\ \ell_i\ \ell_o\ \tau_1]\!] <: [\![\mathbb{C}\ \ell_i'\ \ell_o'\ \tau_1']\!]}\,\text{Definition of } [\![\cdot]\!]$$

7. SLIO*sub-forall:

P1:

$$\dfrac{\dfrac{}{\Sigma, \alpha; \Psi \vdash [\![\tau]\!] <: [\![\tau']\!]}\,\text{IH, Weakening} \qquad \dfrac{}{\Sigma, \alpha; \Psi \vdash \top \sqsubseteq \top}}{\Sigma; \Psi \vdash (\forall \alpha.(\top, [\![\tau]\!])) <: (\forall \alpha.(\top, [\![\tau']\!]))}\,\text{FGsub-forall}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad \dfrac{}{\Sigma, \alpha; \Psi \vdash \bot \sqsubseteq \bot}}{\Sigma; \Psi \vdash (\forall \alpha.(\top, [\![\tau]\!]))^{\bot} <: (\forall \alpha.(\top, [\![\tau']\!]))^{\bot}}\,\text{FGsub-label}}{\Sigma; \Psi \vdash [\![\forall \alpha.\tau]\!] <: [\![\forall \alpha.\tau']\!]}$$

8. SLIO*sub-constraint:

P1:

$$\dfrac{\dfrac{}{\Sigma;\Psi\vdash \llbracket\tau\rrbracket <: \llbracket\tau'\rrbracket}\text{IH} \qquad \dfrac{}{\Sigma;\Psi\vdash \top \sqsubseteq \top} \qquad \dfrac{\dfrac{}{\Sigma;\Psi\vdash c\Rightarrow\tau <: c'\Rightarrow\tau'}\text{Given}}{\Sigma;\Psi\vdash c' \implies c}\text{By inversion}}{\Sigma;\Psi\vdash (c \overset{\top}{\Rightarrow} \llbracket\tau\rrbracket) <: (c' \overset{\top}{\Rightarrow} \llbracket\tau'\rrbracket)}\text{FGsub-constra}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad \dfrac{}{\Sigma,\alpha;\Psi\vdash \bot\sqsubseteq\bot}}{\Sigma;\Psi\vdash (c \overset{\top}{\Rightarrow} \llbracket\tau\rrbracket)^{\bot} <: (c' \overset{\top}{\Rightarrow} \llbracket\tau'\rrbracket)^{\bot}}\text{FGsub-label}}{\Sigma;\Psi\vdash \llbracket c\Rightarrow\tau\rrbracket <: \llbracket c'\Rightarrow\tau'\rrbracket}$$

□

Lemma 5.3 (CG $\rightsquigarrow$ FG: Preservation of well-formedness)**.** $\forall\Sigma,\Psi,\tau.$
$\Sigma;\Psi\vdash\tau\ WF \implies \Sigma;\Psi\vdash\llbracket\tau\rrbracket\ WF$

Proof. Proof by induction on the $\tau\ WF$ relation.

1. CG-wff-base:

$$\dfrac{\dfrac{}{\Sigma;\Psi\vdash \mathsf{b}\ WF}\text{FG-wff-base}}{\Sigma;\Psi\vdash \mathsf{b}^{\bot}\ WF}\text{FG-wff-label}$$

2. CG-wff-unit:

$$\dfrac{}{\Sigma;\Psi\vdash \mathsf{unit}\ WF}\text{FG-wff-unit}$$

3. CG-wff-arrow:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi\vdash \llbracket\tau_1\rrbracket\ WF}\text{IH1} \qquad \dfrac{}{\Sigma;\Psi\vdash \llbracket\tau_2\rrbracket\ WF}\text{IH2}}{\Sigma;\Psi\vdash (\llbracket\tau_1\rrbracket \overset{\top}{\to} \llbracket\tau_2\rrbracket)\ WF}\text{FG-wff-arrow}}{\Sigma;\Psi\vdash (\llbracket\tau_1\rrbracket \overset{\top}{\to} \llbracket\tau_2\rrbracket)^{\bot}\ WF}\text{FG-wff-label}$$

4. CG-wff-prod:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi\vdash \llbracket\tau_1\rrbracket\ WF}\text{IH1} \qquad \dfrac{}{\Sigma;\Psi\vdash \llbracket\tau_2\rrbracket\ WF}\text{IH2}}{\Sigma;\Psi\vdash \llbracket(\rrbracket\tau_1 \times \llbracket\tau_2\rrbracket)\ WF}\text{FG-wff-prod}}{\Sigma;\Psi\vdash \llbracket(\rrbracket\tau_1 \times \llbracket\tau_2\rrbracket)^{\bot}\ WF}\text{FG-wff-label}$$

5. CG-wff-sum:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi\vdash \llbracket\tau_1\rrbracket\ WF}\text{IH1} \qquad \dfrac{}{\Sigma;\Psi\vdash \llbracket\tau_2\rrbracket\ WF}\text{IH2}}{\Sigma;\Psi\vdash \llbracket\tau_1\rrbracket + \llbracket\tau_2\rrbracket\ WF}\text{FG-wff-prod}}{\Sigma;\Psi\vdash \llbracket(\rrbracket\tau_1 + \llbracket\tau_2\rrbracket)^{\bot}\ WF}\text{FG-wff-label}$$

6. CG-wff-ref:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi \vdash \mathsf{ref}\ \ell\ \tau\ WF}\text{Given}}{\mathrm{FV}(\tau)=\emptyset}\text{By inversion}}{\mathrm{FV}(\llbracket\tau\rrbracket)=\emptyset}\text{Lemma 5.4} \quad \dfrac{}{\mathrm{FV}(\mathsf{unit})=\emptyset} \quad \dfrac{\dfrac{}{\Sigma;\Psi \vdash \mathsf{ref}\ \ell\ \tau\ WF}\text{Given}}{\mathrm{FV}(\ell)=\emptyset}\text{By inversion}}{\dfrac{\Sigma;\Psi \vdash \mathrm{FV}((\llbracket\tau\rrbracket + \mathsf{unit})^{\ell})=\emptyset}{\dfrac{\Sigma;\Psi \vdash \mathsf{ref}\ (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell}\ WF}{\Sigma;\Psi \vdash (\mathsf{ref}\ (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell})^{\perp}\ WF}\text{FG-wff-label}}\text{FG-wff-ref}}$$

7. CG-wff-forall:

$$\dfrac{\dfrac{\dfrac{}{\Sigma,\alpha;\Psi \vdash \llbracket\tau\rrbracket\ WF}\text{IH}}{\Sigma;\Psi \vdash (\forall\alpha.(\top,\llbracket\tau\rrbracket))\ WF}\text{FG-wff-forall}}{\Sigma;\Psi \vdash (\forall\alpha.(\top,\llbracket\tau\rrbracket))^{\perp}\ WF}\text{CG-wff-label}$$

8. CG-wff-constraint:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi,c \vdash \llbracket\tau\rrbracket\ WF}\text{IH}}{\Sigma;\Psi \vdash (c \overset{\top}{\Rightarrow} \llbracket\tau\rrbracket)\ WF}\text{FG-wff-constraint}}{\Sigma;\Psi \vdash (c \overset{\top}{\Rightarrow} \llbracket\tau\rrbracket)^{\perp}\ WF}\text{CG-wff-label}$$

9. CG-wff-labeled:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi \vdash \llbracket\tau\rrbracket\ WF}\text{IH} \qquad \dfrac{}{\Sigma;\Psi \vdash \mathsf{unit}\ WF}\text{FG-wff-unit}}{\Sigma;\Psi \vdash (\llbracket\tau\rrbracket + \mathsf{unit})\ WF}\text{FG-wff-sum}}{\Sigma;\Psi \vdash (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell}\ WF}\text{CG-wff-label}$$

10. CG-wff-monad:

P1:

$$\dfrac{\dfrac{}{\Sigma;\Psi \vdash \llbracket\tau\rrbracket\ WF}\text{IH} \qquad \dfrac{}{\Sigma;\Psi \vdash \mathsf{unit}\ WF}\text{FG-wff-unit}}{\Sigma;\Psi \vdash (\llbracket\tau\rrbracket + \mathsf{unit})\ WF}\text{FG-wff-sum}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi \vdash \mathsf{unit}\ WF}\text{FG-wff-unit} \qquad \dfrac{P1}{\Sigma;\Psi \vdash (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell_2}\ WF}\text{FG-wff-label}}{\Sigma;\Psi \vdash (\mathsf{unit} \xrightarrow{\ell_1} (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell_2})\ WF}\text{FG-wff-sum}}{\Sigma;\Psi \vdash (\mathsf{unit} \xrightarrow{\ell_1} (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell_2})^{\perp}\ WF}\text{CG-wff-label}$$

□

Lemma 5.4 (CG ⇝ FG: Free variable lemma). $\forall \tau.\ FV(\llbracket \tau \rrbracket) \subseteq FV(\tau)$

Proof. Proof by inducitoon on the CG types, τ

1. $\tau = \mathsf{b}$:

$$\begin{array}{lll} & \mathrm{FV}(\llbracket \mathsf{b} \rrbracket) & \\ = & \mathrm{FV}(\mathsf{b}^{\perp}) & \text{Definition of } \llbracket \cdot \rrbracket \\ = & \emptyset & \\ = & \mathrm{FV}(\mathsf{b}) & \end{array}$$

2. $\tau = \mathsf{unit}$:

$$\begin{array}{lll} & \mathrm{FV}(\llbracket \mathsf{b} \rrbracket) & \\ = & \mathrm{FV}(\mathsf{unit}^{\perp}) & \text{Definition of } \llbracket \cdot \rrbracket \\ = & \emptyset & \\ = & \mathrm{FV}(\mathsf{unit}) & \end{array}$$

3. $\tau = \tau_1 \to \tau_2$:

$$\begin{array}{lll} & \mathrm{FV}(\llbracket \tau_1 \to \tau_2 \rrbracket) & \\ = & \mathrm{FV}(\llbracket \tau_1 \rrbracket \xrightarrow{\top} \llbracket \tau_2 \rrbracket)^{\perp} & \text{Definition of } \llbracket \cdot \rrbracket \\ = & \mathrm{FV}(\llbracket \tau_1 \rrbracket) \cup \mathrm{FV}(\llbracket \tau_2 \rrbracket) & \\ \subseteq & \mathrm{FV}(\tau_1) \cup \mathrm{FV}(\tau_2) & \text{IH on } \tau_1 \text{ and } \tau_2 \\ = & \mathrm{FV}(\tau_1 \to \tau_2) & \end{array}$$

4. $\tau = \tau_1 \times \tau_2$:

$$\begin{array}{lll} & \mathrm{FV}(\llbracket \tau_1 \times \tau_2 \rrbracket) & \\ = & \mathrm{FV}(\llbracket \tau_1 \rrbracket \times \llbracket \tau_2 \rrbracket)^{\perp} & \text{Definition of } \llbracket \cdot \rrbracket \\ = & \mathrm{FV}(\llbracket \tau_1 \rrbracket) \cup \mathrm{FV}(\llbracket \tau_2 \rrbracket) & \\ \subseteq & \mathrm{FV}(\tau_1) \cup \mathrm{FV}(\tau_2) & \text{IH on } \tau_1 \text{ and } \tau_2 \\ = & \mathrm{FV}(\tau_1 \times \tau_2) & \end{array}$$

5. $\tau = \tau_1 + \tau_2$:

$$\begin{array}{lll} & \mathrm{FV}(\llbracket \tau_1 + \tau_2 \rrbracket) & \\ = & \mathrm{FV}(\llbracket \tau_1 \rrbracket + \llbracket \tau_2 \rrbracket)^{\perp} & \text{Definition of } \llbracket \cdot \rrbracket \\ = & \mathrm{FV}(\llbracket \tau_1 \rrbracket) \cup \mathrm{FV}(\llbracket \tau_2 \rrbracket) & \\ \subseteq & \mathrm{FV}(\tau_1) \cup \mathrm{FV}(\tau_2) & \text{IH on } \tau_1 \text{ and } \tau_2 \\ = & \mathrm{FV}(\tau_1 + \tau_2) & \end{array}$$

6. $\tau = \mathsf{ref}\ \ell_i\ \tau_i$:

$$\begin{array}{lll} & \mathrm{FV}(\llbracket \mathsf{ref}\ \ell_i\ \tau_i \rrbracket) & \\ = & \mathrm{FV}(\mathsf{ref}\ (\llbracket \tau_i \rrbracket + \mathsf{unit})^{\ell_i})^{\perp} & \text{Definition of } \llbracket \cdot \rrbracket \\ = & \mathrm{FV}(\llbracket \tau_i \rrbracket) \cup \mathrm{FV}(\ell_i) & \\ \subseteq & \mathrm{FV}(\tau_i) \cup \mathrm{FV}(\ell_i) & \text{IH} \\ = & \mathrm{FV}(\mathsf{ref}\ \ell_i\ \tau_i) & \end{array}$$

7. $\tau = \forall \alpha.\tau_i$:

$$\begin{array}{lll} & \mathrm{FV}(\llbracket \forall \alpha.\tau_i \rrbracket) & \\ = & \mathrm{FV}(\forall \alpha.(\top, \llbracket \tau_i \rrbracket))^{\perp} & \text{Definition of } \llbracket \cdot \rrbracket \\ = & \mathrm{FV}(\llbracket \tau_i \rrbracket) - \{\alpha\}) & \\ \subseteq & \mathrm{FV}(\tau_i) - \{\alpha\}) & \text{IH} \\ = & \mathrm{FV}(\forall \alpha.\tau_i) & \end{array}$$

8. $\tau = c \Rightarrow \tau_i$:

$$\begin{array}{lll} & \mathrm{FV}([\![c \Rightarrow \tau_i]\!]) & \\ = & \mathrm{FV}(c \stackrel{\top}{\Rightarrow} [\![\tau_i]\!])^{\perp} & \text{Definition of } [\![\cdot]\!] \\ = & \mathrm{FV}([\![c]\!]) \cup \mathrm{FV}([\![\tau_i]\!]) & \\ \subseteq & \mathrm{FV}([\![c]\!]) \cup \mathrm{FV}(\tau_i) & \text{IH} \\ = & \mathrm{FV}(c \Rightarrow \tau_i) & \end{array}$$

9. $\tau = \mathsf{Labeled}\ \ell_i\ \tau_i$:

$$\begin{array}{lll} & \mathrm{FV}([\![\mathsf{Labeled}\ \ell_i\ \tau_i]\!]) & \\ = & \mathrm{FV}([\![\tau_i]\!] + \mathsf{unit})^{\ell_i} & \text{Definition of } [\![\cdot]\!] \\ = & \mathrm{FV}([\![\tau_i]\!]) \cup \mathrm{FV}(\ell_i) & \\ \subseteq & \mathrm{FV}(\tau_i) \cup \mathrm{FV}(\ell_i) & \text{IH} \\ = & \mathrm{FV}(\mathsf{Labeled}\ \ell_i\ \tau_i) & \end{array}$$

10. $\tau = \mathbb{SLIO}\ \ell_1\ \ell_2\ \tau_i$:

$$\begin{array}{lll} & \mathrm{FV}([\![\mathbb{SLIO}\ \ell_1\ \ell_2\ \tau_i]\!]) & \\ = & \mathrm{FV}(\mathsf{unit} \stackrel{\ell_1}{\to} ([\![\tau_i]\!] + \mathsf{unit})^{\ell_2})^{\perp} & \text{Definition of } [\![\cdot]\!] \\ = & \mathrm{FV}([\![\tau_i]\!]) \cup \mathrm{FV}(\ell_1) \cup \mathrm{FV}(\ell_2) & \\ \subseteq & \mathrm{FV}(\tau_i) \cup \mathrm{FV}(\ell_1) \cup \mathrm{FV}(\ell_2) & \text{IH} \\ = & \mathrm{FV}(\mathbb{SLIO}\ \ell_1\ \ell_2\ \tau_i) & \end{array}$$

□

Lemma 5.5 (CG ⇝ FG: Substitution lemma)**.** *$\forall \tau.\ s.t \vdash \tau\ WF$ the following holds:* $[\![\tau]\!][\ell/\alpha] = [\![\tau[\ell/\alpha]]\!]$

Proof. Proof by induciton on the CG types, τ

1. $\tau = \mathsf{b}$:

$$\begin{array}{lll} & ([\![\mathsf{b}]\!])[\ell/\alpha] & \\ = & (\mathsf{b}^{\perp})[\ell/\alpha] & \text{Definition of } [\![\cdot]\!] \\ = & (\mathsf{b}^{\perp}) & \\ = & [\![\mathsf{b}]\!] & \\ = & [\![(\mathsf{b}[\ell/\alpha])]\!] & \end{array}$$

2. $\tau = \mathsf{unit}$:

$$\begin{array}{lll} & ([\![\mathsf{unit}]\!])[\ell/\alpha] & \\ = & (\mathsf{unit}^{\perp})[\ell/\alpha] & \text{Definition of } [\![\cdot]\!] \\ = & (\mathsf{unit}^{\perp}) & \\ = & [\![\mathsf{unit}]\!] & \\ = & [\![(\mathsf{unit}[\ell/\alpha])]\!] & \end{array}$$

3. $\tau = \tau_1 \to \tau_2$:

$$\begin{array}{lll} & ([\![\tau_1 \to \tau_2]\!])[\ell/\alpha] & \\ = & ([\![\tau_1]\!] \stackrel{\top}{\to} [\![\tau_2]\!])^{\perp}[\ell/\alpha] & \text{Definition of } [\![\cdot]\!] \\ = & ([\![\tau_1]\!][\ell/\alpha] \stackrel{\top}{\to} [\![\tau_2]\!][\ell/\alpha])^{\perp} & \\ = & ([\![\tau_1[\ell/\alpha]]\!] \stackrel{\top}{\to} [\![\tau_2[\ell/\alpha]]\!])^{\perp} & \text{IH on } \tau_1 \text{ and } \tau_2 \\ = & [\![(\tau_1[\ell/\alpha] \to \tau_2[\ell/\alpha])]\!] & \\ = & [\![(\tau_1 \to \tau_2)[\ell/\alpha]]\!] & \end{array}$$

4. $\tau = \tau_1 \times \tau_2$:

$$\begin{array}{lll} & (\llbracket\tau_1 \times \tau_2\rrbracket)[\ell/\alpha] & \\ = & (\llbracket\tau_1\rrbracket \times \llbracket\tau_2\rrbracket)^{\perp}[\ell/\alpha] & \text{Definition of } \llbracket\cdot\rrbracket \\ = & (\llbracket\tau_1\rrbracket[\ell/\alpha] \times \llbracket\tau_2\rrbracket[\ell/\alpha])^{\perp} & \\ = & (\llbracket\tau_1[\ell/\alpha]\rrbracket \times \llbracket\tau_2[\ell/\alpha]\rrbracket)^{\perp} & \text{IH on } \tau_1 \text{ and } \tau_2 \\ = & \llbracket(\tau_1[\ell/\alpha] \times \tau_2[\ell/\alpha])\rrbracket & \\ = & \llbracket(\tau_1 \times \tau_2)[\ell/\alpha]\rrbracket & \end{array}$$

5. $\tau = \tau_1 + \tau_2$:

$$\begin{array}{lll} & (\llbracket\tau_1 + \tau_2\rrbracket)[\ell/\alpha] & \\ = & (\llbracket\tau_1\rrbracket + \llbracket\tau_2\rrbracket)^{\perp}[\ell/\alpha] & \text{Definition of } \llbracket\cdot\rrbracket \\ = & (\llbracket\tau_1\rrbracket[\ell/\alpha] + \llbracket\tau_2\rrbracket[\ell/\alpha])^{\perp} & \\ = & (\llbracket\tau_1[\ell/\alpha]\rrbracket + \llbracket\tau_2[\ell/\alpha]\rrbracket)^{\perp} & \text{IH on } \tau_1 \text{ and } \tau_2 \\ = & \llbracket(\tau_1[\ell/\alpha] + \tau_2[\ell/\alpha])\rrbracket & \\ = & \llbracket(\tau_1 + \tau_2)[\ell/\alpha]\rrbracket & \end{array}$$

6. $\tau = \mathsf{ref}\ \ell_i\ \tau_i$:

$$\begin{array}{lll} & (\llbracket\mathsf{ref}\ \ell_i\ \tau_i\rrbracket)[\ell/\alpha] & \\ = & (\mathsf{ref}\ (\llbracket\tau_i\rrbracket + \mathsf{unit})^{\ell_i})^{\perp}[\ell/\alpha] & \text{Definition of } \llbracket\cdot\rrbracket \\ = & (\mathsf{ref}\ (\llbracket\tau_i\rrbracket + \mathsf{unit})^{\ell_i})^{\perp} & \text{Lemma 5.3} \\ = & \llbracket(\mathsf{ref}\ \ell_i\ \tau_i)\rrbracket & \text{since} \vdash \tau\ WF \\ = & \llbracket(\mathsf{ref}\ \ell_i\ \tau_i)[\ell/\alpha]\rrbracket & \end{array}$$

7. $\tau = \forall\alpha.\tau_i$:

$$\begin{array}{lll} & (\llbracket\forall\alpha.\tau_i\rrbracket)[\ell/\alpha] & \\ = & (\forall\alpha.(\top, \llbracket\tau_i\rrbracket))^{\perp}[\ell/\alpha] & \text{Definition of } \llbracket\cdot\rrbracket \\ = & (\forall\alpha.(\top, \llbracket\tau_i\rrbracket[\ell/\alpha]))^{\perp} & \\ = & (\forall\alpha.(\top, \llbracket\tau_i[\ell/\alpha]\rrbracket))^{\perp} & \text{IH} \\ = & (\forall\alpha.\tau_i[\ell/\alpha]) & \\ = & (\forall\alpha.\tau_i)[\ell/\alpha] & \end{array}$$

8. $\tau = c \Rightarrow \tau_i$:

$$\begin{array}{lll} & (\llbracket c \Rightarrow \tau_i\rrbracket)[\ell/\alpha] & \\ = & (c \overset{\top}{\Rightarrow} \llbracket\tau_i\rrbracket)^{\perp}[\ell/\alpha] & \text{Definition of } \llbracket\cdot\rrbracket \\ = & (c[\ell/\alpha] \overset{\top}{\Rightarrow} \llbracket\tau_i\rrbracket[\ell/\alpha])^{\perp} & \\ = & (c[\ell/\alpha] \overset{\top}{\Rightarrow} \llbracket\tau_i[\ell/\alpha]\rrbracket)^{\perp} & \text{IH} \\ = & (c[\ell/\alpha] \Rightarrow \tau_i[\ell/\alpha]) & \\ = & (c \Rightarrow \tau_i)[\ell/\alpha] & \end{array}$$

9. $\tau = \mathsf{Labeled}\ \ell_i\ \tau_i$:

$$\begin{array}{lll} & (\llbracket\mathsf{Labeled}\ \ell_i\ \tau_i\rrbracket)[\ell/\alpha] & \\ = & (\llbracket\tau_i\rrbracket + \mathsf{unit})^{\ell_i}[\ell/\alpha] & \text{Definition of } \llbracket\cdot\rrbracket \\ = & (\llbracket\tau_i\rrbracket[\ell/\alpha] + \mathsf{unit})^{\ell_i[\ell/\alpha]} & \\ = & (\llbracket\tau_i[\ell/\alpha]\rrbracket + \mathsf{unit})^{\ell_i[\ell/\alpha]} & \text{IH} \\ = & \llbracket(\mathsf{Labeled}\ \ell_i[\ell/\alpha]\ \tau_i[\ell/\alpha])\rrbracket & \\ = & \llbracket(\mathsf{Labeled}\ \ell_i\ \tau_i)[\ell/\alpha]\rrbracket & \end{array}$$

10. $\tau = \mathbb{C}\ \ell_1\ \ell_2\ \tau_i$:

$$
\begin{array}{lll}
 & ([\![\mathbb{C}\ \ell_1\ \ell_2\ \tau_i]\!])[\ell/\alpha] & \\
= & (\mathsf{unit} \xrightarrow{\ell_1} ([\![\tau_i]\!] + \mathsf{unit})^{\ell_2})^{\perp}[\ell/\alpha] & \text{Definition of } [\![\cdot]\!] \\
= & (\mathsf{unit} \xrightarrow{\ell_1[\ell/\alpha]} ([\![\tau_i]\!][\ell/\alpha] + \mathsf{unit})^{\ell_2[\ell/\alpha]})^{\perp} & \\
= & (\mathsf{unit} \xrightarrow{\ell_1[\ell/\alpha]} ([\![\tau_i[\ell/\alpha]]\!] + \mathsf{unit})^{\ell_2[\ell/\alpha]})^{\perp} & \text{IH} \\
= & (\mathbb{C}\ \ell_1[\ell/\alpha]\ \ell_2[\ell/\alpha]\ \tau_i[\ell/\alpha]) & \\
= & (\mathbb{C}\ \ell_1\ \ell_2\ \tau_i)[\ell/\alpha] &
\end{array}
$$

□

5.1.3 Model for CG to FG translation

Definition 5.6 (${}^s\theta_2$ extends ${}^s\theta_1$)**.** ${}^s\theta_1 \sqsubseteq {}^s\theta_2 \triangleq$
$\forall a \in {}^s\theta_1.{}^s\theta_1(a) = \tau \implies {}^s\theta_2(a) = \tau$

Definition 5.7 ($\hat{\beta}_2$ extends $\hat{\beta}_1$)**.** $\hat{\beta}_1 \sqsubseteq \hat{\beta}_2 \triangleq$
$\forall (a_1, a_2) \in \hat{\beta}_1.(a_1, a_2) \in \hat{\beta}_2$

Definition 5.8 (Unary value relation)**.**

$$
\begin{array}{lll}
\lfloor \mathsf{b} \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, {}^s v, {}^t v) \mid {}^s v \in [\![\mathsf{b}]\!] \wedge {}^t v \in [\![\mathsf{b}]\!] \wedge {}^s v = {}^t v\} \\
\lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, {}^s v, {}^t v) \mid {}^s v \in [\![\mathsf{unit}]\!] \wedge {}^t v \in [\![\mathsf{unit}]\!]\} \\
\lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \mid \\
 & & ({}^s\theta, m, {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}} \wedge ({}^s\theta, m, {}^s v_2, {}^t v_2) \in \lfloor \tau_2 \rfloor_V^{\hat{\beta}}\} \\
\lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, \mathsf{inl}\ {}^s v, \mathsf{inl}\ {}^t v) \mid ({}^s\theta, m, {}^s v, {}^t v) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}}\} \cup \\
 & & \{({}^s\theta, m, \mathsf{inr}\ {}^s v, \mathsf{inr}\ {}^t v) \mid ({}^s\theta, m, {}^s v, {}^t v) \in \lfloor \tau_2 \rfloor_V^{\hat{\beta}}\} \\
\lfloor \tau_1 \to \tau_2 \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, \lambda x.e_s, \lambda x.e_t) \mid \forall {}^s\theta' \sqsupseteq {}^s\theta, {}^s v, {}^t v, j < m, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, {}^s v, {}^t v) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}'} \\
 & & \implies ({}^s\theta', j, e_s[{}^s v/x], e_t[{}^t v/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}'}\} \\
\lfloor \forall \alpha.\tau \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, \Lambda e_s, \Lambda e_t) \mid \forall {}^s\theta' \sqsupseteq {}^s\theta, j < m, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, e_s, e_t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}'}\} \\
\lfloor c \Rightarrow \tau \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, \nu e_s, \nu e_t) \mid \mathcal{L} \models c \implies \forall {}^s\theta' \sqsupseteq {}^s\theta, j < m, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, e_s, e_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}'}\} \\
\lfloor \mathsf{ref}\ \ell\ \tau \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, {}^s a, {}^t a) \mid {}^s\theta({}^s a) = \mathsf{Labeled}\ \ell\ \tau \wedge ({}^s a, {}^t a) \in \hat{\beta}\} \\
\lfloor \mathsf{Labeled}\ \ell\ \tau \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, {}^s v, {}^t v) \mid \\
 & & \exists {}^s v', {}^t v'.{}^s v = \mathsf{Lb}({}^s v') \wedge {}^t v = \mathsf{inl}\ {}^t v' \wedge ({}^s\theta, m, {}^s v', {}^t v') \in \lfloor \tau \rfloor_V^{\hat{\beta}}\} \\
\lfloor \mathbb{C}\ \ell_1\ \ell_2\ \tau \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, {}^s v, {}^t v) \mid \forall {}^s\theta_e \sqsupseteq {}^s\theta, H_s, H_t, i, {}^s v', k \leq m, \hat{\beta} \sqsubseteq \hat{\beta}'. \\
 & & (k, H_s, H_t) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_s, {}^s v) \Downarrow_i^f (H_s', {}^s v') \wedge i < k \implies \\
 & & \exists H_t', {}^t v'.(H_t, {}^t v()) \Downarrow (H_t', {}^t v') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H_s', H_t') \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge \\
 & & \exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k - i, {}^s v', {}^t v'') \in \lfloor \tau \rfloor_V^{\hat{\beta}''}\}
\end{array}
$$

Definition 5.9 (Unary expression relation)**.**

$$
\begin{array}{lll}
\lfloor \tau \rfloor_E^{\hat{\beta}} & \triangleq & \{({}^s\theta, n, e_s, e_t) \mid \\
 & & \forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.e_s \Downarrow_i {}^s v \implies \\
 & & \exists H_t', {}^t v.(H_t, e_t) \Downarrow (H_t', {}^t v) \wedge ({}^s\theta, n - i, {}^s v, {}^t v) \in \lfloor \tau \rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta\}
\end{array}
$$

Definition 5.10 (Unary heap well formedness).

$$(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \triangleq \begin{array}{l} dom({}^s\theta) \subseteq dom(H_S) \wedge \\ \hat{\beta} \subseteq (dom({}^s\theta) \times dom(H_t)) \wedge \\ \forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}} \end{array}$$

Definition 5.11 (Value substitution). $\delta^s : Var \mapsto Val$, $\delta^t : Var \mapsto Val$

Definition 5.12 (Unary interpretation of Γ).

$$\lfloor \Gamma \rfloor_V^{\hat{\beta}} \triangleq \begin{array}{l} \{({}^s\theta, n, \delta^s, \delta^t) \mid dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t) \wedge \\ \forall x \in dom(\Gamma).({}^s\theta, n, \delta^s(x), \delta^t(x)) \in \lfloor \Gamma(x) \rfloor_V^{\hat{\beta}} \} \end{array}$$

5.1.4 Soundness proof for CG to FG translation

Lemma 5.13 (Monotonicity). $\forall {}^s\theta, {}^s\theta', n, {}^sv, {}^tv, n', \beta, \beta'$.
$({}^s\theta, n, {}^sv, {}^tv) \in \lfloor \tau \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n \implies ({}^s\theta', n', {}^sv, {}^tv) \in \lfloor \tau \rfloor_V^{\hat{\beta}'}$

Proof. Proof by induction on τ

1. Case b:

   Given:

   $({}^s\theta, n, {}^sv, {}^tv) \in \lfloor \mathsf{b} \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^sv, {}^tv) \in \lfloor \mathsf{b} \rfloor_V^{\hat{\beta}'}$

   Since $({}^s\theta, n, {}^sv, {}^tv) \in \lfloor \mathsf{b} \rfloor_V^{\hat{\beta}}$ therefore from Definition 5.8 we know that ${}^sv \in [\![\mathsf{b}]\!] \wedge {}^tv \in [\![\mathsf{b}]\!]$

   Therefore from Definition 5.8 ${}^sv \in [\![\mathsf{b}]\!] \wedge {}^tv \in [\![\mathsf{b}]\!]$ we get the desired

2. Case unit:

   Given:

   $({}^s\theta, n, {}^sv, {}^tv) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^sv, {}^tv) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}'}$

   Since $({}^s\theta, n, {}^sv, {}^tv) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}}$ therefore from Definition 5.8 we know that ${}^sv \in [\![\mathsf{unit}]\!] \wedge {}^tv \in [\![\mathsf{unit}]\!]$

   Therefore from Definition 5.8 ${}^sv \in [\![\mathsf{unit}]\!] \wedge {}^tv \in [\![\mathsf{unit}]\!]$ we get the desired

3. Case $\tau_1 \times \tau_2$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}'}$

   From Definition 5.8 we know that ${}^s v = ({}^s v_1, {}^s v_2)$ and ${}^t v = ({}^t v_1, {}^t v_2)$.

   We also know that $({}^s\theta, n, {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}}$ and $({}^s\theta, n, {}^s v_2, {}^t v_2) \in \lfloor \tau_2 \rfloor_V^{\hat{\beta}}$

   IH1: $({}^s\theta', n', {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}'}$

   IH2: $({}^s\theta', n', {}^s v_2, {}^t v_2) \in \lfloor \tau_2 \rfloor_V^{\hat{\beta}'}$

   Therefore from Definition 5.8, IH1 and IH2 we get

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}'}$

4. Case $\tau_1 + \tau_2$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}'}$

   From Definition 5.8 two cases arise

   (a) ${}^s v = \mathsf{inl}({}^s v')$ and ${}^t v = \mathsf{inl}({}^t v')$:
   IH: $({}^s\theta', n', {}^s v', {}^t v') \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}'}$
   Therefore from Definition 5.8 and IH we get
   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}'}$

   (b) ${}^s v = \mathsf{inr}({}^s v')$ and ${}^t v = \mathsf{inr}({}^t v')$:
   Symmetric reasosning as in the previous case

5. Case $\tau_1 \to \tau_2$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau_1 \to \tau_2 \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 \to \tau_2 \rfloor_V^{\hat{\beta}'}$

   From Definition 5.8 we know that

   $\forall {}^s\theta'' \sqsupseteq {}^s\theta, {}^s v_1, {}^t v_1, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta'', j, {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}} \implies ({}^s\theta'', j, e_s[{}^s v_1/x], e_t[{}^t v_1/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}'}$ (A0)

Similarly from Definition 5.8 we are required to prove

$\forall^s\theta'_1 \sqsupseteq {}^s\theta', {}^s v_2, {}^t v_2, j < n', \hat{\beta}' \sqsubseteq \hat{\beta}''.({}^s\theta'_1, j, {}^s v_2, {}^t v_2) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}} \implies ({}^s\theta'_1, j, e_s[{}^s v_2/x], e_t[{}^t v_2/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}''}$

This means we are given some ${}^s\theta'_1 \sqsupseteq {}^s\theta', {}^s v_2, {}^t v_2, j < n', \hat{\beta}' \sqsubseteq \hat{\beta}''$ s.t $({}^s\theta'_1, j, {}^s v_2, {}^t v_2) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}}$ and we are required to prove

$({}^s\theta'_1, j, e_s[{}^s v_2/x], e_t[{}^t v_2/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}'}$

Instantiating (A0) with ${}^s\theta'_1, {}^s v_2, {}^t v_2, j, \hat{\beta}''$ since ${}^s\theta'_1 \sqsupseteq {}^s\theta' \sqsupseteq {}^s\theta$, $j < n' < n$ and $\hat{\beta} \sqsubseteq \hat{\beta}' \sqsubseteq \hat{\beta}''$ therefore we get

$({}^s\theta'_1, j, e_s[{}^s v_2/x], e_t[{}^t v_2/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}''}$

6. Case $\forall \alpha.\tau$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \forall \alpha.\tau \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \forall \alpha.\tau \rfloor_V^{\hat{\beta}'}$

   From Definition 5.8 we know that ${}^s v = \Lambda e'_s$ and ${}^t v = \Lambda e'_t$. And

   $\forall^s\theta'' \sqsupseteq {}^s\theta, j < n, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}''.({}^s\theta'', j, e'_s, e'_t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}''}$ (F0)

   Similarly from Definition 5.8 we are required to prove

   $\forall^s\theta''_1 \sqsupseteq {}^s\theta', j < n', \ell' \in \mathcal{L}, \hat{\beta}' \sqsubseteq \hat{\beta}''_1.({}^s\theta''_1, j, e'_s, e'_t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}''_1}$

   This means we are given some ${}^s\theta''_1 \sqsupseteq {}^s\theta', j < n', \ell'' \in \mathcal{L}, \hat{\beta}' \sqsubseteq \hat{\beta}''_1$

   and we are required to prove

   $({}^s\theta''_1, j, e'_s, e'_t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}''_1}$

   Instantiating (F0) with ${}^s\theta''_1, j, \hat{\beta}''_1$ since ${}^s\theta''_1 \sqsupseteq {}^s\theta' \sqsupseteq {}^s\theta$, $j < n' < n$ and $\hat{\beta} \sqsubseteq \hat{\beta}' \sqsubseteq \hat{\beta}''_1$ therefore we get

   $({}^s\theta''_1, j, e'_s, e'_t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}''_1}$

7. Case $c \Rightarrow \tau$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor c \Rightarrow \tau \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor c \Rightarrow \tau \rfloor_V^{\hat{\beta}'}$

   From Definition 5.8 we know that ${}^s v = \nu\ (e'_s)$ and ${}^t v = \nu\ (e'_t)$. And

   $\mathcal{L} \models c \implies \forall^s\theta'' \sqsupseteq {}^s\theta, j < n, \hat{\beta}' \sqsubseteq \hat{\beta}''_1.({}^s\theta'', j, e'_s, e'_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}'}$ (C0)

Similarly from Definition 5.8 we are required to prove

$\mathcal{L} \models c \implies \forall^s\theta_1'' \sqsupseteq {}^s\theta', j < n', \hat{\beta}' \sqsubseteq \hat{\beta}_1''.({}^s\theta_1'', j, e_s', e_t') \in \lfloor\tau\rfloor_E^{\hat{\beta}_1''}$

This means we are given some $\mathcal{L} \models c, {}^s\theta_1'' \sqsupseteq {}^s\theta', j < n', \hat{\beta}' \sqsubseteq \hat{\beta}_1''$

and we are required to prove

$({}^s\theta_1'', j, e_s', e_t') \in \lfloor\tau\rfloor_E^{\hat{\beta}_1''}$

Since $\mathcal{L} \models c$ and instantiating (C0) with ${}^s\theta_1'', j, \hat{\beta}_1''$ since ${}^s\theta_1'' \sqsupseteq {}^s\theta' \sqsupseteq {}^s\theta$, $j < n' < n$ and $\hat{\beta} \sqsubseteq \hat{\beta}' \sqsubseteq \hat{\beta}_1''$ therefore we get

$({}^s\theta_1'', j, e_s', e_t') \in \lfloor\tau\rfloor_E^{\hat{\beta}_1''}$

8. Case $\mathsf{ref}\ \ell\ \tau$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{ref}\ \ell\ \tau\rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{ref}\ \ell\ \tau\rfloor_V^{\hat{\beta}'}$

   From Definition 5.8 we know that ${}^s v =^s a$ and ${}^t v =^t a$. We also know that ${}^s\theta({}^s a) = \mathsf{Labeled}\ \ell\ \tau \wedge ({}^s a, {}^t a) \in \hat{\beta}$

   From Definition 5.8, Definition 5.6 and Definition 5.7 we get

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{ref}\ \ell\ \tau\rfloor_V^{\hat{\beta}'}$

9. Case $\mathsf{Labeled}\ \ell\ \ \tau$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{Labeled}\ \ell\ \ \tau\rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{Labeled}\ \ell\ \ \tau\rfloor_V^{\hat{\beta}'}$

   From Definition 5.8 it means
   $\exists^s v', {}^t v'.{}^s v = \mathsf{Lb}_\ell({}^s v') \wedge {}^t v = \mathsf{inl}\ {}^t v' \wedge ({}^s\theta, n, {}^s v', {}^t v') \in \lfloor\tau\rfloor_V^{\hat{\beta}}$

   IH: $({}^s\theta', n', {}^s v', {}^t v') \in \lfloor\tau\rfloor_V^{\hat{\beta}}$

   Similarly from Definition 5.8 we need to prove that
   $\exists^s v'', {}^t v''.{}^s v = \mathsf{Lb}_\ell({}^s v'') \wedge {}^t v = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', n', {}^s v'', {}^t v'') \in \lfloor\tau\rfloor_V^{\hat{\beta}}$

   We choose ${}^s v''$ as ${}^s v'$ and ${}^t v''$ as ${}^t v'$ and since from IH we know that $({}^s\theta', n', {}^s v', {}^t v') \in \lfloor\tau\rfloor_V^{\hat{\beta}}$
   Therefore from Definition 5.8 we get
   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{Labeled}\ \ell\ \ \tau\rfloor_V^{\hat{\beta}'}$

10. Case $\mathbb{C}\ \ell_1\ \ell_2\ \tau$:

Given:

$({}^s\theta, n, {}^sv, {}^tv) \in \lfloor \mathbb{C}\ \ell_1\ \ell_2\ \tau \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

To prove:

$({}^s\theta', n', {}^sv, {}^tv) \in \lfloor \mathbb{C}\ \ell_1\ \ell_2\ \tau \rfloor_V^{\hat{\beta}'}$

This means from Definition 5.8 we know that

$\forall {}^s\theta_e \sqsupseteq {}^s\theta, H_s, H_t, i, {}^sv', {}^tv', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}_1.$
$(k, H_s, H_t) \overset{\hat{\beta}_1}{\triangleright} ({}^s\theta_e) \wedge (H_s, {}^sv) \Downarrow_i^f (H_s', {}^sv') \wedge i < k \implies$
$\exists {}^tv'.(H_t, {}^tv()) \Downarrow (H_t', {}^tv') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}_1 \sqsubseteq \hat{\beta}_2.(k-i, H_s', H_t') \overset{\hat{\beta}_2}{\triangleright} {}^s\theta' \wedge$
$\exists {}^tv''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', {}^t\theta', k-i, {}^sv', {}^tv'') \in \lfloor \tau \rfloor_V^{\hat{\beta}_2} \wedge$
$(\forall a.H_s(a) \neq H_s'(a) \implies \exists \ell'.{}^s\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom({}^s\theta')/dom({}^s\theta_e).{}^s\theta'(a) \searrow \ell_1)$ (CG0)

Similarly from Definition 5.8 we need to prove

$\forall {}^s\theta_e' \sqsupseteq {}^s\theta', H_s', H_t', i', {}^sv'', {}^tv'', k' \leq n', \hat{\beta}' \sqsubseteq \hat{\beta}_1'.$
$(k', H_s', H_t') \overset{\hat{\beta}_1'}{\triangleright} ({}^s\theta_e') \wedge (H_s', {}^sv) \Downarrow_i^f (H_s'', {}^sv'') \wedge (H_t', {}^tv()) \Downarrow (H_t'', {}^tv'') \wedge i' < k' \implies$
$\exists {}^tv''.(H_t', {}^tv()) \Downarrow (H_t'', {}^tv'') \wedge \exists {}^s\theta'' \sqsupseteq {}^s\theta_e', \hat{\beta}_1' \sqsubseteq \hat{\beta}_2'.(k'-i', H_s'', H_t'') \overset{\hat{\beta}_2'}{\triangleright} {}^s\theta'' \wedge$
$\exists {}^tv''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', k'-i, {}^sv', {}^tv'') \in \lfloor \tau \rfloor_V^{\hat{\beta}_2'} \wedge$
$(\forall a.H_s(a) \neq H_s'(a) \implies \exists \ell'.{}^s\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom({}^s\theta')/dom({}^s\theta_e).{}^s\theta'(a) \searrow \ell_1)$

This means we are given some ${}^s\theta_e' \sqsupseteq {}^s\theta', H_s', H_t', i', {}^sv'', k' \leq n', \hat{\beta}' \sqsubseteq \hat{\beta}_1'$ s.t $(k', H_s', H_t') \triangleright ({}^s\theta_e') \wedge (H_s', {}^sv) \Downarrow_i^f (H_s'', {}^sv'') \wedge i' < k'$

And we need to prove

$\exists {}^tv''.(H_t', {}^tv()) \Downarrow (H_t'', {}^tv'') \wedge \exists {}^s\theta'' \sqsupseteq {}^s\theta_e', \hat{\beta}_1' \sqsubseteq \hat{\beta}_2'.(k'-i', H_s'', H_t'') \overset{\hat{\beta}_2'}{\triangleright} {}^s\theta'' \wedge$
$\exists {}^tv''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta'', k'-i, {}^sv', {}^tv'') \in \lfloor \tau \rfloor_V^{\hat{\beta}_2'} \wedge$
$(\forall a.H_s(a) \neq H_s'(a) \implies \exists \ell'.{}^s\theta_e(a) = \mathsf{Labeled}\ \ell'\ \tau' \wedge \ell_1 \sqsubseteq \ell') \wedge$
$(\forall a \in dom({}^s\theta')/dom({}^s\theta_e).{}^s\theta'(a) \searrow \ell_1)$

Instantiating (CG0) with ${}^s\theta_e' \sqsupseteq {}^s\theta', H_s', H_t', i', {}^sv'', {}^tv'', k' \leq n', \hat{\beta}' \sqsubseteq \hat{\beta}_1'$ we get the desired

□

Lemma 5.14 (Unary monotonicity for Γ)**.** $\forall \theta, \theta', \delta, \Gamma, n, n', \hat{\beta}, \hat{\beta}'.$
$(\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}} \wedge n' < n \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \implies (\theta', n', \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}'}$

Proof. Given: $(\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}} \wedge n' < n \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}'$
To prove: $(\theta', n', \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}'}$

From Definition 5.12 it is given that
$dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t) \wedge \forall x \in dom(\Gamma).({}^s\theta, n, \delta^s(x), \delta^t(x)) \in \lfloor \Gamma(x) \rfloor_V^{\hat{\beta}}$

And again from Definition 5.12 we are required to prove that
$dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t) \wedge \forall x \in dom(\Gamma).({}^s\theta', n', \delta^s(x), \delta^t(x)) \in \lfloor \Gamma(x) \rfloor_V^{\hat{\beta}'}$

- $dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t)$:

  Given

- $\forall x \in dom(\Gamma).({}^s\theta', n', \delta^s(x), \delta^t(x)) \in \lfloor \Gamma(x) \rfloor_V^{\hat{\beta}'}$:

  Since we know that $\forall x \in dom(\Gamma).({}^s\theta, n, \delta^s(x), \delta^t(x)) \in \lfloor \Gamma(x) \rfloor_V^{\hat{\beta}}$ (given)

  Therefore from Lemma 5.13 we get

  $\forall x \in dom(\Gamma).({}^s\theta', n', \delta^s(x), \delta^t(x)) \in \lfloor \Gamma(x) \rfloor_V^{\hat{\beta}'}$

□

Lemma 5.15 (Unary monotonicity for H)**.** $\forall {}^s\theta, H_s, H_t, n, n', \hat{\beta}, \hat{\beta}'$.
$(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge n' < n \implies (n', H_s, H_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta$

Proof. Given: $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge n' < n$
To prove: $(n', H_s, H_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta$

From Definition 5.10 it is given that
$dom({}^s\theta) \subseteq dom(H_S) \wedge \hat{\beta} \subseteq (dom({}^s\theta) \times dom(H_t)) \wedge \forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$

And again from Definition 5.10 we are required to prove that
$dom({}^s\theta) \subseteq dom(H_S) \wedge \hat{\beta} \subseteq (dom({}^s\theta) \times dom(H_t)) \wedge \forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n'-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$

- $dom({}^s\theta) \subseteq dom(H_S)$:

  Given

- $\hat{\beta} \subseteq (dom({}^s\theta) \times dom(H_t))$:

  Given

- $\forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n'-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$:

  Since we know that $\forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$ (given)

  Therefore from Lemma 5.13 we get

  $\forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n'-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$

□

Theorem 5.16 (Fundamental theorem)**.** $\forall \Gamma, \tau, e, \delta^s, \delta^t, \sigma, {}^s\theta, n$.
$\Sigma; \Psi; \Gamma \vdash e_s : \tau \rightsquigarrow e_t \wedge$
$\mathcal{L} \models \Psi\ \sigma \wedge$
$({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$
$\implies$
$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

Proof. Proof by induction on the $\rightsquigarrow$ relation

1. CF-var:

$$\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash x : \tau \rightsquigarrow x} \text{CF-var}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \cup \{x \mapsto \tau\} \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, x\ \delta^s, x\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 5.9 it suffices to prove that

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta \wedge \forall i < n, {}^s v.x\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H_t', {}^t v.(H_t, x\ \delta^t) \Downarrow (H_t', {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H_t') \overset{\hat{\beta}}{\rhd} {}^s\theta$

This means given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta$. Also given some $i < n, {}^s v$ s.t $x\ \delta^s \Downarrow_i {}^s v$
From cg-val we know that $i = 0$, ${}^s v = x\ \delta^s$.

And we are required to prove

$\exists H_t', {}^t v.(H_t, x\ \delta^t) \Downarrow (H_t', {}^t v) \wedge ({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta$ (F-V0)
From fg-val we know that ${}^t v = x\ \delta^t$ and $H_t' = H_t$. So we are left with proving

$({}^s\theta, n, x\ \delta^s, x\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta$

Since we are given $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \cup \{x \mapsto \tau\ \sigma\} \rfloor_V^{\hat{\beta}}$, therefore from Definition 5.12 we get

$({}^s\theta, n, x\ \delta^s, x\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}}$. And we have $(n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta$ in the context. So we are done.

2. CF-lam:

$$\frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash e_s : \tau_2 \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \lambda x.e_s : \tau_1 \to \tau_2 \rightsquigarrow \lambda x.e_t} \text{lam}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, (\lambda x.e_s)\ \delta^s, (\lambda x.e_t)\ \delta^t) \in \lfloor (\tau_1 \to \tau_2)\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 5.9 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta \wedge \forall i < n, {}^s v.(\lambda x.e_s)\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H_t', {}^t v.(H_t, (\lambda x.e_t)\ \delta^t) \Downarrow (H_t', {}^t v)({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (\tau_1 \to \tau_2)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H_t') \overset{\hat{\beta}}{\rhd} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta$ and given some $i < n, {}^s v$ s.t $(\lambda x.e_s)\ \delta^s \Downarrow_i {}^s v$

From cg-val and fg-val we know that ${}^s v = (\lambda x.e_s)\ \delta^s$, ${}^t v = (\lambda x.e_t)\ \delta^t$, $H_t' = H_t$ and $i = 0$

It suffices to prove that

$({}^s\theta, n, (\lambda x.e_s)\ \delta^s, (\lambda x.e_t)\ \delta^t) \in \lfloor(\tau_1 \to \tau_2)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

We know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context. So, we are only left to prove $({}^s\theta, n, (\lambda x.e_s)\ \delta^s, (\lambda x.e_t)\ \delta^t) \in \lfloor(\tau_1 \to \tau_2)\ \sigma\rfloor_V^{\hat{\beta}}$

From Definition 5.8 it suffices to prove

$\forall {}^s\theta' \sqsupseteq {}^s\theta, {}^sv, {}^tv, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, {}^sv, {}^tv) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}'}$
$\implies ({}^s\theta', j, e_s[{}^sv/x], e_t[{}^tv/x]) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}'}$

This means that we are given ${}^s\theta' \sqsupseteq {}^s\theta, {}^sv, {}^tv, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t $({}^s\theta', j, {}^sv, {}^tv) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}'}$
And we need to prove

$({}^s\theta', j, e_s[{}^sv/x]\ \delta^s, e_t[{}^tv/x]\ \delta^t) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}'}$ (F-L0)

Since $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor\Gamma\ \rfloor_V^{\hat{\beta}}$ therefore from Lemma 5.14 we also have $({}^s\theta', j, \delta^s, \delta^t) \in \lfloor\Gamma\ \rfloor_V^{\hat{\beta}'}$

<u>IH:</u>

$({}^s\theta', j, e_s\ \delta^s \cup \{x \mapsto {}^sv_1\}, e_t \cup \{x \mapsto {}^tv_1\}) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}'}$ s.t

$({}^s\theta', j, {}^sv_1, {}^tv_1) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}'}$

We get (F-L0) directly from IH

3. CF-app:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_{s1} : (\tau_1 \to \tau_2) \rightsquigarrow e_{t1} \qquad \Sigma; \Psi; \Gamma \vdash e_{s2} : \tau_1 \rightsquigarrow e_{t2}}{\Sigma; \Psi; \Gamma \vdash e_{s1}\ e_{s2} : \tau_2 \rightsquigarrow e_{t1}\ e_{t2}}\ \text{app}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor\Gamma\rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, (e_{s1}\ e_{s2})\ \delta^s, (e_{t1}\ e_{t2})\ \delta^t) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}}$

This means from Definition 5.9 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv.(e_{s1}\ e_{s2})\ \delta^s \Downarrow_i {}^sv \implies$
$\exists H_t', {}^tv.(H_t, (e_{t1}\ e_{t2})\ \delta^t) \Downarrow (H_t', {}^tv) \wedge ({}^s\theta, n-i, {}^sv, {}^tv) \in \lfloor\tau_2\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This further means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^sv$ s.t $(e_{s1}\ e_{s2})\ \delta^s \Downarrow_i {}^sv$
And we need to prove

$\exists H_t', {}^tv.(H_t, (e_{t1}\ e_{t2})\ \delta^t) \Downarrow (H_t', {}^tv) \wedge ({}^s\theta, n-i, {}^sv, {}^tv) \in \lfloor\tau_2\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta$
(F-A0)

<u>IH1:</u>

$({}^s\theta, n, e_{s1}\ \delta^s, e_{t1}\ \delta^t) \in \lfloor(\tau_1 \to \tau_2)\ \sigma\rfloor_E^{\hat{\beta}}$

This means from Definition 5.9 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_{s1}\ \delta^s \Downarrow_j {}^s v_1 \implies$
$\exists H'_{t1}, {}^t v_1.(H_t, e_{t1}\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor(\tau_1 \to \tau_2)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and since we know that $(e_{s1}\ e_{s2})\ \delta^s \Downarrow_i {}^s v$ therefore $\exists j < i < n$ s.t $e_{s1}\ \delta^s \Downarrow_j {}^s v_1$.

And we have

$\exists H'_{t1}, {}^t v_1.(H_t, e_{t1}\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor(\tau_1 \to \tau_2)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-A1)

<u>IH2:</u>

$({}^s\theta, n-j, e_{s2}\ \delta^s, e_{t2}\ \delta^t) \in \lfloor\tau_1\ \sigma\rfloor_E^{\hat{\beta}}$

This means from Definition 5.9 it suffices to prove

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall k < n-j, {}^s v_2.e_{s2} \Downarrow_i {}^s v_2 \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t2}) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-j-k, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta'_2$

Instantiating with H_s, H'_{t1} and since we know that $(e_{s1}\ e_{s2})\ \delta^s \Downarrow_i {}^s v$ therefore $\exists k < i-j < n-j$ s.t $e_{s2}\ \delta^s \Downarrow_k {}^s v_2$.

And we have

$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t2}) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-j-k, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-A2)

Since from (F-A1) we know that $({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor(\tau_1 \to \tau_2)\ \sigma\rfloor_V^{\hat{\beta}}$ where ${}^s v_1 = \lambda x.e'_s$ and ${}^t v_1 = \lambda x.e'_t$

From Definition 5.8 we have
$\forall {}^s\theta'_3 \sqsupseteq {}^s\theta, {}^s v, {}^t v, l < n-j, \hat{\beta}_3 \sqsupseteq \hat{\beta}.({}^s\theta'_3, l, {}^s v, {}^t v) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}_3}$
$\implies ({}^s\theta'_3, l, e'_s[{}^s v/x], e'_t[{}^t v/x]) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}_3}$

Instantiating with ${}^s\theta, {}^s v_2, {}^t v_2, n-j-k, \hat{\beta}$ we get

$({}^s\theta, n-j-k, e'_s[{}^s v_2/x], e'_t[{}^t v_2/x]) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}}$

From Definition 5.9 we have

$\forall H_{s4}, H_{t4}.(n-j-k, H_{s4}, H_{t4}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall k' < n-j-k, {}^s v_4.e'_s[{}^s v_2/x] \Downarrow_{k'} {}^s v_4 \implies$
$\exists H'_{t4}, {}^t v_4.(H_{t4}, e'_t[{}^t v_2/x]) \Downarrow (H'_{t4}, {}^t v_4) \wedge ({}^s\theta, n-j-k-k', {}^s v_4, {}^t v_4) \in \lfloor\tau_2\ \sigma\rfloor_V^{\hat{\beta}} \wedge$
$(n-j-k-k', H_{s4}, H'_{t4}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H'_{t2}, from (F-A2) we know that $(n-j-k, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$. Instantiating ${}^s v_4$ wiht ${}^s v$ and since we know that $(e_{s1}\ e_{s2})\ \delta^s \Downarrow_i {}^s v$ therefore $\exists k' < i-j-k < n-j-k$ s.t $e'_s[{}^s v_2/x]\ \delta^s \Downarrow_{k'} {}^s v$. therefore we have

$\exists H'_{t4}, {}^t v_4.(H_{t4}, e'_t[{}^t v_2/x]) \Downarrow (H'_{t4}, {}^t v_4) \wedge ({}^s\theta, n-j-k-k', {}^s v, {}^t v_4) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j-k-k', H_{s4}, H'_{t4}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-A3)

Since from cg-app we know that $i = j + k + k'$ and $H'_t = H'_{t4}$, ${}^t v = {}^t v_4$ therefore we get (F-A0) from (F-A3) and Lemma 5.13 and Lemma 5.15

4. CF-prod:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_{s1} : \tau_1 \rightsquigarrow e_{t1} \qquad \Sigma; \Psi; \Gamma \vdash e_{s2} : \tau_2 \rightsquigarrow e_{t2}}{\Sigma; \Psi; \Gamma \vdash (e_{s1}, e_{s2}) : (\tau_1 \times \tau_2) \rightsquigarrow (e_{t1}, e_{t2})} \text{ prod}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, (e_{s1}, e_{s2})\ \delta^s, (e_{t1}, e_{t2})\ \delta^t) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 5.9 it suffices to prove

$\forall H_s, H_t, \hat{\beta}.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(e_{s1}, e_{s2})\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, (e_{t1}, e_{t2})\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that we are given some $H_s, H_t, \hat{\beta}$ s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $(e_{s1}, e_{s2})\ \delta^s \Downarrow_i {}^s v$

And we need to prove

$\exists H'_t, {}^t v.(H_t, (e_{t1}, e_{t2})\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta'$ (F-P0)

<u>IH1:</u>

$({}^s\theta, n, e_{s1}\ \delta^s, e_{t1}\ \delta^t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 5.9 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n.e_{s1}\ \delta^s \Downarrow_i {}^s v_1 \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and since we know that $(e_{s1}, e_{s2})\ \delta^s \Downarrow_i ({}^s v_1, {}^s v_2)$ therefore $\exists j < i < n$ s.t $e_{s1}\ \delta^s \Downarrow_j {}^s v_1$.

Therefore we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-P1)

<u>IH2:</u>

$({}^s\theta, n-j, e_{s2}\ \delta^s, e_{t2}\ \delta^t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat\beta}$

From Definition 5.9 we have

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat\beta}{\triangleright} {}^s\theta \wedge \forall k < n-j.e_{s2}\ \delta^s \Downarrow_k {}^s v_2 \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t2}\ \delta^t) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat\beta} \wedge (n-j-k, H_{s2}, H'_{t2}) \overset{\hat\beta}{\triangleright} {}^s\theta$

Instantiating with $H_s, H'_{t1}, \hat\beta'_1$ and since we know that $(e_{s1}, e_{s2})\ \delta^s \Downarrow_i ({}^s v_1, {}^s v_2)$ therefore $\exists k < i-j < n-j$ s.t $e_{s2}\ \delta^s \Downarrow_k {}^s v_2$.

Therefore we have

$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t2}\ \delta^t) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat\beta} \wedge (n-j-k, H_s, H'_{t2}) \overset{\hat\beta}{\triangleright} {}^s\theta$
(F-P2)

From cg-prod we know that $i = j + k + 1$, $H'_t = H'_{t2}$ and ${}^t v = ({}^t v_1, {}^t v_2)$ therefore from Definition 5.8 and Lemma 5.13 we get $({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V^{\hat\beta}$

And since we have $(n-j-k, H_s, H'_{t2}) \overset{\hat\beta}{\triangleright} {}^s\theta$ therefore from Lemma 5.15 we also get

$(n-i, H_s, H'_{t2}) \overset{\hat\beta}{\triangleright} {}^s\theta$

5. CF-fst:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \tau_1 \times \tau_2 \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \mathsf{fst}(e_s) : \tau_1 \rightsquigarrow \mathsf{fst}(e_t)}\ \text{fst}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat\beta}$

To prove: $({}^s\theta, n, \mathsf{fst}(e_s)\ \delta^s, \mathsf{fst}(e_t)\ \delta^t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat\beta}$ (F-F0)

This means from Definition 5.9 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat\beta}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{fst}(e_s)\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{fst}(e_t)\ \delta^s) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat\beta} \wedge (n-i, H_s, H'_t) \overset{\hat\beta}{\triangleright} {}^s\theta$

This means that we are given some $H_s, H_t, \hat\beta$ s.t $(n, H_s, H_t) \overset{\hat\beta}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $\mathsf{fst}(e_s)\ \delta^s \Downarrow_i {}^s v$

And we need to prove

$\exists H'_t, {}^t v.(H_t, \mathsf{fst}(e_t)\ \delta^s) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat\beta} \wedge (n-i, H_s, H'_t) \overset{\hat\beta}{\triangleright} {}^s\theta$ (F-F0)

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_E^{\hat\beta}$

From Definition 5.9 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_s\ \delta^s \Downarrow_j ({}^s v_1, -) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, (e_{t1}, e_{t2})\ \delta^t) \Downarrow (H'_{t1}, ({}^t v_1, -)) \wedge ({}^s\theta, n-j, ({}^s v_1, -), ({}^t v_1, -)) \in \lfloor(\tau_1 \times \tau_2)\ \sigma\rfloor_V^{\hat{\beta}} \wedge$
$(n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and ${}^s v_1$ with ${}^s v$ since we know that $\mathsf{fst}(e_s)\ \delta^s \Downarrow_i {}^s v$ therefore $\exists j < i < n$ s.t $e_s\ \delta^s \Downarrow_j ({}^s v, -)$.

Therefore we have
$\exists H'_{t1}, {}^t v_1.(H_{t1}, (e_{t1}, e_{t2})\ \delta^t) \Downarrow (H'_{t1}, ({}^t v_1, -)) \wedge ({}^s\theta, n-j, ({}^s v, -), ({}^t v_1, -)) \in \lfloor(\tau_1 \times \tau_2)\ \sigma\rfloor_V^{\hat{\beta}} \wedge$
$(n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-F1)

From cg-fst we know that $i = j+1$, $H'_t = H'_{t1}$ and ${}^t v = {}^t v_1$. Since we know $({}^s\theta, n - j, ({}^s v, -), ({}^t v_1, -)) \in \lfloor(\tau_1 \times \tau_2)\ \sigma\rfloor_V^{\hat{\beta}}$ therefore from Definition 5.8 and Lemma 5.13 we get $({}^s\theta, n-i, {}^s v, {}^t v_1) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}}$

And since from (F-F1) we have $(n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ therefore from Lemma 5.15 we get

$(n-i, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

6. CF-snd:
   Symmetric reasoning as in the CF-fst case

7. CF-inl:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \tau_1 \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \mathsf{inl}(e_s) : (\tau_1 + \tau_2) \rightsquigarrow \mathsf{inl}(e_t)} \text{CF-inl}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor\Gamma\ \sigma\rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{inl}(e_s)\ \delta^s, \mathsf{inl}(e_t)\ \delta^t) \in \lfloor(\tau_1 + \tau_2)\ \sigma\rfloor_E^{\hat{\beta}}$

From Definition 5.9 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{inl}(e_s)\ \delta^s \Downarrow_i \mathsf{inl}({}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{inl}(e_t)\ \delta^t) \Downarrow (H'_t, \mathsf{inl}({}^t v)) \wedge ({}^s\theta, n-i, \mathsf{inl}({}^s v), \mathsf{inl}({}^t v)) \in \lfloor(\tau_1 + \tau_2)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that we are given some $H_s, H_t, \hat{\beta}$ s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $\mathsf{inl}(e_s)\ \delta^s \Downarrow_i \mathsf{inl}({}^s v)$

And we need to prove
$\exists H'_t, {}^t v.(H_t, \mathsf{inl}(e_t)\ \delta^t) \Downarrow (H'_t, \mathsf{inl}({}^t v)) \wedge ({}^s\theta, n-i, \mathsf{inl}({}^s v), \mathsf{inl}({}^t v)) \in \lfloor(\tau_1 + \tau_2)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-IL0)

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 5.9 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_s\ \delta^s \Downarrow_j {}^s v_1 \implies \exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and since we know that $\mathsf{inl}(e_s)\ \delta^s \Downarrow_i {}^s v$ therefore $\exists j < i < n$ s.t $e_s\ \delta^s \Downarrow_j {}^s v$.

Therefore we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-IL1)

From cg-inl we know that $i = j + 1$ and $H'_t = H'_{t1}$, ${}^t v = {}^t v_1$. Since we know $({}^s\theta, n-j, {}^s v, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}}$ therefore from Definition 5.8 and Lemma 5.13 we get

$({}^s\theta, n-i, \mathsf{inl}({}^s v), \mathsf{inl}({}^t v_1)) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V^{\hat{\beta}}$

And since from (F-IL1) we have $(n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ therefore from Lemma 5.15 we get

$(n-i, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

8. CF-inr:

   Symmetric reasoning as in the CF-inl case

9. CF-case:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \tau_1 + \tau_2 \rightsquigarrow e_t \qquad \Sigma; \Psi; \Gamma, x : \tau_1 \vdash e_{s1} : \tau \rightsquigarrow e_{t1} \qquad \Sigma; \Psi; \Gamma, y : \tau_2 \vdash e_{s2} : \tau \rightsquigarrow e_{t2}}{\Sigma; \Psi; \Gamma \vdash \mathsf{case}(e_s, x.e_{s1}, y.e_{s2}) : \tau \rightsquigarrow \mathsf{case}(e_t, x.e_{t1}, y.e_{t2})} \text{ CF-case}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s, \mathsf{case}(e_t, x.e_{t1}, y.e_{t2})\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.9 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{case}(e_t, x.e_{t1}, y.e_{t2})\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that we are given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $\mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s \Downarrow_i {}^s v$

And we need to prove

$\exists H'_t, {}^t v.(H_t, \mathsf{case}(e_t, x.e_{t1}, y.e_{t2})\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-C0)

<u>IH1:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor(\tau_1 + \tau_2)\ \sigma\rfloor_E^{\hat{\beta}}$

From Definition 5.9 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_s\ \delta^s \Downarrow_j {}^s v_1 \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor(\tau_1+\tau_2)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and since we know that $\mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s \Downarrow_i {}^s v$ therefore $\exists j < i < n$ s.t $e_s\ \delta^s \Downarrow_j {}^s v_1$.

Therefore we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor(\tau_1+\tau_2)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$
(F-C1)

Two cases arise:

(a) ${}^s v_1 = \mathsf{inl}({}^s v'_1)$ and ${}^t v_1 = \mathsf{inl}({}^t v'_1)$:
<u>IH2:</u>
$({}^s\theta, n-j, e_{s1}\ \delta^s \cup \{x \mapsto {}^s v_1\}, e_{t1}\ \delta^t \cup \{x \mapsto {}^t v_1\}) \in \lfloor\tau\ \sigma\rfloor_E^{\hat{\beta}}$

From Definition 5.9 we have
$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall k < n-j, {}^s v_2.e_{s1}\ \delta^s \cup \{x \mapsto {}^s v_1\} \Downarrow_k {}^s v_2 \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t1}\ \delta^t \cup \{x \mapsto {}^t v_1\}) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n - j - k, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H'_{t1} and since we know that $\mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s \Downarrow_i {}^s v$ therefore $\exists k < i - j < n - j$ s.t $e_{s1}\ \delta^s \cup \{x \mapsto {}^s v_1\} \Downarrow_k {}^s v$.

Therefore we have
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t1}\ \delta^t \cup \{x \mapsto {}^t v_1\}) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-k, {}^s v, {}^t v_2) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n - j - k, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

From cg-case1 we know that $i = j + k + 1$ and $H'_t = H'_{t2}$, ${}^t v = {}^t v_2$. Since we know $({}^s\theta, n-j-k, {}^s v, {}^t v_2) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}}$ therefore from Definition 5.8 and Lemma 5.13 we get $({}^s\theta, n-i, {}^s v, {}^t v_2) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}}$

And since from (F-C2) we have $(n-j-k, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ therefore from Lemma 5.15 we get $(n-i, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

(b) ${}^s v_1 = \mathsf{inr}({}^s v'_1)$ and ${}^t v_1 = \mathsf{inr}({}^t v'_1)$:
Symmetric reasoning as in the previous case

10. CF-FI:

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash e_s : \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \Lambda e_s : \forall\alpha.\tau \rightsquigarrow \Lambda e_t}\ \text{FI}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \Lambda e_s\ \delta^s, \Lambda e_t\ \delta^t) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.9 we know that

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\Lambda e_s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, \Lambda e_t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $(\Lambda e_s)\ \delta^s \Downarrow_i {}^s v$

From CG-Sem-val and fg-val we know that ${}^s v = (\Lambda e_s)\ \delta^s$, ${}^t v = (\Lambda e_t)\ \delta^t$, $i = 0$ and $H'_t = H_t$

It suffices to prove that

$({}^s\theta, n, (\Lambda e_s)\ \delta^s, (\Lambda e_t)\ \delta^t) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

We know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context. So, we are only left to prove $({}^s\theta, n, (\Lambda e_s)\ \delta^s, (\Lambda e_t)\ \delta^t) \in \lfloor (\forall \alpha.\tau)\ \sigma \rfloor_V^{\hat{\beta}}$

From Definition 5.8 it suffices to prove
$\forall {}^s\theta' \sqsupseteq {}^s\theta, j < n, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}'}$

This means that we are given ${}^s\theta' \sqsupseteq {}^s\theta, j < n, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}'$
And we need to prove
$({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}'}$ (F-FI0)

Since $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$ therefore from Lemma 5.14 we also have $({}^s\theta', j, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}'}$
<u>IH:</u>
$({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \cup \{\alpha \mapsto \ell'\} \rfloor_E^{\hat{\beta}'}$

We get (F-FI0) directly from IH

11. CF-FE:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \forall \alpha.\tau \rightsquigarrow e_t \qquad \mathrm{FV}(\ell) \in \Sigma}{\Sigma; \Psi; \Gamma \vdash e_s\ []\ : \tau[\ell/\alpha] \rightsquigarrow e_t[]}\ \mathrm{FE}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, e_s\ []\ \delta^s, e_t\ []\ \delta^t) \in \lfloor \tau[\ell/\alpha]\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 5.9 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.e_s \; [] \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, e_t \; []) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau[\ell/\alpha] \; \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This further means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $e_s \; [] \; \delta^s \Downarrow_i {}^s v$
And we need to prove

$$\exists H'_t, {}^t v.(H_t, e_t \; []) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau[\ell/\alpha] \; \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \qquad \text{(F-FE0)}$$

<u>IH:</u>

$({}^s\theta, n, e_s \; \delta^s, e_t \; \delta^t) \in \lfloor (\forall \alpha.\tau) \; \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.9 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_s \; \delta^s \Downarrow_j {}^s v_1 \implies$
$\exists H'_{t1}, {}^t v_1.(H_t, e_t \; \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\forall \alpha.\tau) \; \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and since we know that $(e_s \; []) \; \delta^s \Downarrow_i {}^s v$ therefore $\exists j < i < n, {}^s v_1$ s.t $e_s \; \delta^s \Downarrow_j {}^s v_1$.

And we have

$\exists H'_{t1}, {}^t v_1.(H_t, e_t \; \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\forall \alpha.\tau) \; \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-FE1)

From CG-Sem-FE we know that ${}^s v_1 = \Lambda e'_s$ and ${}^t v_1 = \Lambda e'_t$
Therefore we have
$({}^s\theta, n-j, \Lambda e'_s, \Lambda e'_t) \in \lfloor (\forall \alpha.\tau) \; \sigma \rfloor_V^{\hat{\beta}}$

This means from Definition 5.8 we have
$\forall {}^s\theta' \sqsupseteq {}^s\theta, k < n-j, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}_2.({}^s\theta', k, e'_s, e'_t) \in \lfloor \tau[\ell'/\alpha] \; \sigma \rfloor_E^{\hat{\beta}_2}$

Instantiating ${}^s\theta'$ with ${}^s\theta$, k with $n-j-1$, ℓ' with $\ell \; \sigma$ and $\hat{\beta}_2$ with $\hat{\beta}$ and we get

$({}^s\theta, n-j-1, e'_s, e'_t) \in \lfloor \tau[\ell/\alpha] \; \sigma \rfloor_E^{\hat{\beta}}$

From Definition 5.9 we get

$\forall H_{s2}, H_{t2}.(n-j-1, H_{s2}, H_{t2}) \overset{\hat{\beta}_2}{\triangleright} {}^s\theta'_1 \wedge \forall k < n-j-1, {}^s v_2.e'_s \Downarrow_k {}^s v_2 \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e'_t) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-1-k, {}^s v_2, {}^t v_2) \in \lfloor \tau[\ell/\alpha] \; \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j-1-k, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H'_{t1}. Since from (F-FE1) we know that $(n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ therefore from Lemma 5.15 we get $(n-j-1, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we know that $e_s \; [] \; \delta^s \Downarrow_i {}^s v$ and from CG-Sem-FE we know that $i = j+k+1$ (for some k) and $i < n$ therefore we have $k < n-j-1$ s.t $e'_s \; \delta^s \Downarrow_k {}^s v_2$.

Therefore we have
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e'_t) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-1-k, {}^s v_2, {}^t v_2) \in \lfloor \tau[\ell/\alpha]\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j-1-k, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-FE2)

Since $H'_t = H_{t2'}$, ${}^s v = {}^s v_2$ and ${}^t v = {}^t v_2$ therefore we get (F-FE0) directly from (F-FE2)

12. CF-CI:

$$\frac{\Sigma; \Psi, c; \Gamma \vdash e_s : \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \nu\ e_s : c \Rightarrow \tau \rightsquigarrow \nu\ e_t} \text{CI}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \nu\ e_s\ \delta^s, \nu e_t\ \delta^t) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.9 we know that
$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n. \nu e_s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, \nu e_t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (c \Rightarrow \tau) \hat{\beta}\ \sigma \rfloor_V^{\wedge} (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some $H_s, H_t, \hat{\beta}$ s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $(\nu e_s)\ \delta^s \Downarrow_i {}^s v$

From CG-Sem-val and fg-val we know that ${}^s v = (\nu e_s)\ \delta^s$, ${}^t v = (\nu e_t)\ \delta^t$, $i = 0$ and $H'_t = H_t$

It suffices to prove that

$({}^s\theta, n, (\nu e_s)\ \delta^s, (\nu e_t)\ \delta^t) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

We know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context. So, we are only left to prove
$({}^s\theta, n, (\nu e_s)\ \delta^s, (\nu e_t)\ \delta^t) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_V^{\hat{\beta}}$

From Definition 5.8 it suffices to prove
$\mathcal{L} \models c\ \sigma \implies \forall {}^s\theta' \sqsupseteq {}^s\theta, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'}$

This means that we are given $\mathcal{L} \models c\ \sigma$ and ${}^s\theta' \sqsupseteq {}^s\theta, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'$
And we need to prove
$({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'}$ (F-CI0)

Since $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$ therefore from Lemma 5.14 we also have
$({}^s\theta', j, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}'}$
And since we know that $\mathcal{L} \models c\ \sigma$ therefore
IH: $({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'}$

We get (F-CI0) directly from IH

13. CF-CE:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : c \Rightarrow \tau \rightsquigarrow e_t \qquad \Sigma; \Psi \vdash c}{\Sigma; \Psi; \Gamma \vdash e_s \bullet : \tau \rightsquigarrow e_t \bullet} \text{ CE}$$

Also given is: $\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, e_s \bullet\ \delta^s, e_t \bullet\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 5.9 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.e_s \bullet \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, e_t \bullet) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This further means that given some $H_s, H_t, \hat{\beta}$ s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $e_s\ \bullet\ \delta^s \Downarrow_i {}^s v$
And we need to prove

$$\exists H'_t, {}^t v.(H_t, e_t \bullet) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \qquad \text{(F-CE0)}$$

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.9 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_s\ \delta^s \Downarrow_j {}^s v_1 \implies$
$\exists H'_{t1}, {}^t v_1.(H_t, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and since we know that $(e_s \bullet)\ \delta^s \Downarrow_i {}^s v$ therefore $\exists j < i < n$ s.t $e_s\ \delta^s \Downarrow_j {}^s v_1$.

And we have

$\exists H'_{t1}, {}^t v_1.(H_t, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-CE1)

From CG-Sem-CE we know that ${}^s v_1 = \nu e'_s$ and ${}^t v_1 = \nu e'_t$
Therefore we have
$({}^s\theta, n-j, \nu e'_s, \nu e'_t) \in \lfloor (c \Rightarrow \tau)\ \sigma \rfloor_V^{\hat{\beta}}$

This means from Definition 5.8 we have
$\forall {}^s\theta' \sqsupseteq {}^s\theta'_1, k < n-j, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}_2.({}^s\theta', k, e'_s, e'_t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}_2}$

Instantiating ${}^s\theta'$ with ${}^s\theta$, k with $n-j-1$, ℓ' with $\ell\ \sigma$ and $\hat{\beta}_2$ with $\hat{\beta}$ and we get
$({}^s\theta, n-j-1, e'_s, e'_t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 5.9 we get

$\forall H_{s2}, H_{t2}.(n-j-1, H_{s2}, H_{t2}) \overset{\hat{\beta}_2}{\triangleright} {}^s\theta'_1 \wedge \forall k < n-j-1.e'_s \Downarrow_k {}^s v_2 \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e'_t) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-1-k, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H'_{t1}. Since from (F-CE1) we know that $(n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ therefore from Lemma 5.15 we get $(n-j-1, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we know that $e_s \bullet \delta^s \Downarrow_i {}^s v$ and from CG-Sem-CE we know that $i = j+k+1$ (for some k) and $i < n$ therefore we have $k < n-j-1$ s.t $e'_s\ \delta^s \Downarrow_k {}^s v_2$.

Therefore we have

$\exists H'_{t2}, {}^t v_2.(H_{t2}, e'_t) \Downarrow (H'_{t2}, {}^t v_2) \wedge ({}^s\theta, n-j-1-k, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$
(F-CE2)

Since $H'_t = H_{t2'}$, ${}^s v = {}^s v_2$ and ${}^t v = {}^t v_2$ therefore we get (F-CE0) directly from (F-CE2)

14. CF-ret:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \mathsf{ret}(e_s) : \mathbb{C}\ \ell_1\ \ell_2\ \tau \rightsquigarrow \lambda\_.\mathsf{inl}(e_t)}\ \text{ret}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{ret}(e_s)\ \delta^s, \lambda\_.\mathsf{inl}(e_t)\ \delta^t) \in \lfloor (\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma \rfloor_E^{\hat{\beta}}$

It means from Definition 5.9 that we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{ret}(e_s) \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, \lambda\_.\mathsf{inl}(e_t)) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some $H_s, H_t, \hat{\beta}$ s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $\mathsf{ret}(e_s)\ \delta^s \Downarrow_i {}^s v$

And we need to prove

$\exists H'_t, {}^t v.(H_t, \lambda\_.\mathsf{inl}(e_t)) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

From CG-ret and FG-lam we know that $i = 0$, ${}^s v = \mathsf{ret}(e_s)\ \delta^s$, ${}^t v = \lambda\_.\mathsf{inl}(e_t)\ \delta^t$ and $H'_t = H_t$.

So we need to prove

$({}^s\theta, n, \mathsf{ret}(e_s)\ \delta^s, \lambda\_.\mathsf{inl}(e_t)\ \delta^t) \in \lfloor (\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we already know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context so we are left with proving
$({}^s\theta, n, \mathsf{ret}(e_s)\ \delta^s, \lambda\_.\mathsf{inl}(e_t)\ \delta^t) \in \lfloor (\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma \rfloor_V^{\hat{\beta}}$

From Definition 5.8 it means we need to prove

$\forall {}^s\theta_e \sqsupseteq {}^s\theta, H_s, H_t, i, {}^s v', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(k, H_s, H_t) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_s, \mathsf{ret}(e_s)\ \delta^s) \Downarrow_i^f (H_s', {}^s v') \wedge i < k \implies \exists H_t', {}^t v'.(H_t, (\lambda\_.\mathsf{inl}(e_t)\ ())\delta^t) \Downarrow (H_t', {}^t v') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H_s', H_t') \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k - i, {}^s v', {}^t v'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$

This means we are given some ${}^s\theta_e \sqsupseteq {}^s\theta, H_s, H_t, i, {}^s v', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t $(k, H_s, H_t) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_s, \mathsf{ret}(e_s)\ \delta^s) \Downarrow_i^f (H_s', {}^s v') \wedge i < k$. Also from cg-ret we know that $H_s' = H_s$

And we need to prove

$\exists H_t', {}^t v'.(H_t, (\lambda\_.\mathsf{inl}(e_t)\ ())\delta^t) \Downarrow (H_t', {}^t v') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H_s, H_t') \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k - i, {}^s v', {}^t v'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$ (F-R0)

<u>IH:</u>

$({}^s\theta_e, k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'}$

It means from Definition 5.9 that we need to prove

$\forall H_{s1}, H_{t1}.(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge \forall f < k.e_s\ \delta^s \Downarrow_f {}^s v \implies$
$\exists H_{t1}', {}^t v.(H_{t1}, e_t\ \delta^t) \Downarrow (H_{t1}', {}^t v) \wedge ({}^s\theta_e, k - f, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k - f, H_{s1}, H_{t1}') \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

Instantiating H_{s1} with H_s and H_{t1} with H_t. And since we know that $(H_s, \mathsf{ret}(e_s)\ \delta^s) \Downarrow_i^f (H_s', {}^s v')$ therefore $\exists f < i < k \leq n$ s.t $e_s\ \delta^s \Downarrow_f {}^s v_h$. Therefore we have

$\exists H_{t1}', {}^t v.(H_{t1}, e_t\ \delta^t) \Downarrow (H_{t1}', {}^t v) \wedge ({}^s\theta_e, k - f, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k - f, H_s, H_{t1}') \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$ (F-R1)

In order to prove (F-R0) we choose H_t' as H_{t1}', ${}^t v'$ as $\mathsf{inl}({}^t v)$, ${}^s\theta'$ as ${}^s\theta_e$, $\hat{\beta}''$ as $\hat{\beta}'$. Since from cg-ret we know that $i = f + 1$ therefore from (F-R1) and Lemma 5.15 we know that $(k - i, H_s, H_{t1}') \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

Next we choose ${}^t v''$ as ${}^t v$ (from F-R1) and from Lemma 5.13 we get $({}^s\theta_e, k - i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$ (we know from cg-ret that ${}^s v' = {}^s v$)

15. CF-bind:

$$\frac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash e_{s1} : \mathbb{C}\ \ell_1\ \ell_2\ \tau \rightsquigarrow e_{t1} \qquad \Sigma; \Psi; \Gamma, x : \tau \vdash e_{s2} : \mathbb{C}\ \ell_3\ \ell_4\ \tau' \rightsquigarrow e_{t2} \\ \Sigma; \Psi \vdash \ell_i \sqsubseteq \ell_1 \qquad \Sigma; \Psi \vdash \ell_i \sqsubseteq \ell_3 \qquad \Sigma; \Psi \vdash \ell_2 \sqsubseteq \ell_3 \qquad \Sigma; \Psi \vdash \ell_2 \sqsubseteq \ell_4 \qquad \Sigma; \Psi \vdash \ell_4 \sqsubseteq \ell_o\end{array}}{\Sigma; \Psi; \Gamma \vdash \mathsf{bind}(e_{s1}, x.e_{s2}) : \mathbb{C}\ \ell_i\ \ell_o\ \tau' \rightsquigarrow \lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}())}\ \text{bind}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s, \lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}())\ \delta^t) \in \lfloor (\mathbb{C}\ \ell_i\ \ell_o\ \tau')\ \sigma \rfloor_E^{\hat{\beta}}$

It means from Definition 5.9 that we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, \lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}())\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge$
$({}^s\theta, n - i, {}^s v, {}^t v) \in \lfloor(\mathbb{C}\ \ell_i\ \ell_o\ \tau')\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $\mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s \Downarrow_i {}^s v$

And we need to prove
$\exists H'_t, {}^t v.(H_t, \lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}())\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge$
$({}^s\theta, n - i, {}^s v, {}^t v) \in \lfloor(\mathbb{C}\ \ell_i\ \ell_o\ \tau')\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$
From cg-val and fg-val we know that $i = 0$, ${}^s v = \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s$,
${}^t v = \lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}())\ \delta^t$, $H'_t = H_t$

And we need to prove

$({}^s\theta, n, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s, \lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}())\ \delta^t) \in \lfloor(\mathbb{C}\ \ell_i\ \ell_o\ \tau')\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we already know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context so we are left with proving
$({}^s\theta, n, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s, \lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}())\ \delta^t) \in \lfloor(\mathbb{C}\ \ell_i\ \ell_o\ \tau')\ \sigma\rfloor_V^{\hat{\beta}}$

From Definition 5.8 it means we need to prove
$\forall {}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^s v', {}^t v', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s1}, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^s v') \wedge i < k \implies$
$\exists H'_{t1}, {}^t v'.(H_{t1}, (\lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}()))()\ \delta^t) \Downarrow (H'_{t1}, {}^t v') \wedge$
$\exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge \exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k - i, {}^s v', {}^t v'') \in \lfloor\tau'\ \sigma\rfloor_V^{\hat{\beta}''}$

This means we are given some ${}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^s v', {}^t v', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge (H_{s1}, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^s v') \wedge i < k.$

And we need to prove
$\exists H'_{t1}, {}^t v'.(H_{t1}, (\lambda\_.\mathsf{case}(e_{t1}(), x.e_{t2}(), y.\mathsf{inr}()))()\ \delta^t) \Downarrow (H'_{t1}, {}^t v') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge \exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k - i, {}^s v', {}^t v'') \in \lfloor\tau'\ \sigma\rfloor_V^{\hat{\beta}''}$ (F-B0)

<u>IH1:</u>
$({}^s\theta, k, e_{s1}\ \delta^s, e_{t1}\ \delta^t) \in \lfloor(\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma\rfloor_E^{\hat{\beta}}$

It means from Definition 5.9 that we need to prove

$\forall H_{s2}, H_{t2}.(k, H_{s2}, H_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_{h1}.e_{s1}\ \delta^s \Downarrow_j {}^s v_{h1} \implies$
$\exists H'_{t2}, {}^t v_{h1}.(H_{t2}, e_{t1}\ \delta^t) \Downarrow (H'_{t2}, {}^t v_{h1}) \wedge ({}^s\theta, k - j, {}^s v_{h1}, {}^t v_{h1}) \in \lfloor(\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (k - j, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating H_{s2} with H_{s1} and H_{t2} with H_{t1}. And since we know that $(H_{s1}, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists j < i < k \leq n$ s.t $e_{s1}\ \delta^s \Downarrow_j {}^s v_{h1}$.

Therefore we have

$\exists H'_{t2}, {}^t v_{h1}.(H_{t2}, e_{t1}\ \ \delta^t) \Downarrow (H'_{t2}, {}^t v_{h1}) \wedge ({}^s\theta, k-j, {}^s v_{h1}, {}^t v_{h1}) \in \lfloor(\mathbb{C}\ \ \ell_1\ \ \ell_2\ \ \tau)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (k - j, H_{s1}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-B1.1)

From Definition 5.8 we know have

$\forall^s\theta_e \sqsupseteq {}^s\theta, H_{s3}, H_{t3}, b, {}^s v'_{h1}, {}^t v'_{h1}, m \leq k-j, \hat{\beta} \sqsubseteq \hat{\beta}'.$

$(m, H_{s3}, H_{t3}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s3}, {}^s v_{h1}) \Downarrow_b^f (H'_{s3}, {}^s v'_{h1}) \wedge b < m \implies$

$\exists H'_{t3}, {}^t v'_{h1}.(H_{t3}, {}^t v_{h1}()) \Downarrow (H'_{t3}, {}^t v'_{h1}) \wedge \exists^s\theta'' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(m-b, H'_{s3}, H'_{t3}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta'' \wedge$

$\exists^t v''_{h1}.{}^t v'_{h1} = \mathsf{inl}\ {}^t v''_{h1} \wedge ({}^s\theta'', m-b, {}^s v'_{h1}, {}^t v''_{h1}) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}''}$

Instantiating ${}^s\theta_e$ with ${}^s\theta$, H_{s3} with H_{s1}, H_{t3} with H'_{t2}, m with $k-j$ and $\hat{\beta}'$ with $\hat{\beta}$. Since we know that $(H_{s1}, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists b < i-j < k-j$ s.t $(H_{s1}, {}^s v_{h1})\ \delta^s \Downarrow_b (H'_{s3}, {}^s v'_{h1})$.

Therefore we have

$\exists H'_{t3}, {}^t v'_{h1}.(H_{t3}, {}^t v_{h1}()) \Downarrow (H'_{t3}, {}^t v'_{h1}) \wedge \exists^s\theta'' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-j-b, H'_{s3}, H'_{t3}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta'' \wedge$
$\exists^t v''.{}^t v'_{h1} = \mathsf{inl}\ {}^t v''_{h1} \wedge ({}^s\theta'', k-j-b, {}^s v'_{h1}, {}^t v''_{h1}) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}''}$ (F-B1)

<u>IH2:</u>

$({}^s\theta'', k-j-b, e_{s2}\ \delta^s \cup \{x \mapsto {}^s v'_{h1}\}, e_{t2}\ \delta^t \cup \{x \mapsto {}^t v''_{h1}\}) \in \lfloor(\mathbb{C}\ \ell_3\ \ell_4\ \tau')\ \sigma\rfloor_E^{\hat{\beta}''}$

It means from Definition 5.9 that we need to prove

$\forall H_{s4}, H_{t4}.(k, H_{s4}, H_{t4}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta \wedge \forall c < (k-j-b), {}^s v_{h2}.e_{s2}\ \delta^s \Downarrow_j {}^s v_{h2} \implies$
$\exists H'_{t4}, {}^t v_{h2}.(H_{t4}, e_{t2}\ \delta^t) \Downarrow (H'_{t4}, {}^t v_{h2}) \wedge ({}^s\theta'', k-j-b-c, {}^s v_{h2}, {}^t v_{h2}) \in \lfloor(\mathbb{C}\ \ell_3\ \ell_4\ \tau')\ \sigma\rfloor_V^{\hat{\beta}''} \wedge$
$(k-j-b-c, H_{s4}, H'_{t4}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta''$

Instantiating H_{s4} with H'_{s3} and H_{t4} with H'_{t3}. And since we know that $(H_{s1}, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists c < i-j-b < k-j-b$ s.t $e_{s2}\ \delta^s \Downarrow_c {}^s v_{h2}$.

Therefore we have

$\exists H'_{t4}, {}^t v_{h2}.(H_{t4}, e_{t2}\ \delta^t) \Downarrow (H'_{t4}, {}^t v_{h2}) \wedge ({}^s\theta'', k-j-b-c, {}^s v_{h2}, {}^t v_{h2}) \in \lfloor(\mathbb{C}\ \ell_3\ \ell_4\ \tau')\ \sigma\rfloor_V^{\hat{\beta}''} \wedge$
$(k-j-b-c, H_{s4}, H'_{t4}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta''$ (F-B2.1)

From Definition 5.8 we know have

$\forall^s\theta_e \sqsupseteq {}^s\theta'', H_{s5}, H_{t5}, d, {}^s v'_{h2}, {}^t v'_{h2}, m \leq k-j-b-c, \hat{\beta}'' \sqsubseteq \hat{\beta}''_1.$

$(m, H_{s5}, H_{t5}) \overset{\hat{\beta}''_1}{\triangleright} ({}^s\theta_e) \wedge (H_{s5}, {}^s v_{h2}) \Downarrow_d^f (H'_{s5}, {}^s v'_{h2}) \wedge d < m \implies$

$\exists H'_{t5}, {}^t v'_{h2}.(H_{t5}, {}^t v_{h2}()) \Downarrow (H'_{t5}, {}^t v'_{h2}) \wedge \exists^s\theta''' \sqsupseteq {}^s\theta_e, \hat{\beta}''_1 \sqsubseteq \hat{\beta}''_2.(m-d, H'_{s5}, H'_{t5}) \overset{\hat{\beta}''_2}{\triangleright} {}^s\theta''' \wedge$
$\exists^t v''_{h2}.{}^t v'_{h2} = \mathsf{inl}\ {}^t v''_{h2} \wedge ({}^s\theta''', m-d, {}^s v'_{h2}, {}^t v''_{h2}) \in \lfloor\tau'\ \sigma\rfloor_V^{\hat{\beta}''_2}$

Instantiating ${}^s\theta_e$ with ${}^s\theta''$, H_{s5} with H'_{s3}, H_{t5} with H'_{t3}, m with $k-j-b-c$ and $\hat{\beta}''_1$ with $\hat{\beta}''$. Since we know that $(H_{s1}, \mathsf{bind}(e_{s1}, x.e_{s2})\ \delta^s) \Downarrow^f_i (H'_s, {}^s v')$ therefore $\exists d < i-j-b-c < k-j-b-c$ s.t $(H'_{s3}, {}^s v_{h2})\ \delta^s \Downarrow_d (H'_{s5}, {}^s v'_{h2})$.

Therefore we have

$\exists H'_{t5}, {}^t v'_{h2}.(H_{t5}, {}^t v_{h2}()) \Downarrow (H'_{t5}, {}^t v'_{h2}) \wedge \exists^s\theta''' \sqsupseteq {}^s\theta_e, \hat{\beta}''_1 \sqsubseteq \hat{\beta}''_2.(k-j-b-c-d, H'_{s5}, H'_{t5}) \overset{\hat{\beta}''_2}{\triangleright} {}^s\theta''' \wedge$
$\exists^t v''.{}^t v'_{h2} = \mathsf{inl}\ {}^t v''_{h2} \wedge ({}^s\theta''', k-j-b-c-d, {}^s v'_{h2}, {}^t v''_{h2}) \in \lfloor \tau'\ \sigma \rfloor^{\hat{\beta}''_2}_V$ (F-B2)

In order to prove (F-B0) we choose H'_{t1} as H'_{t5} and ${}^t v'$ as ${}^t v'_{h2}$. Next we choose ${}^s\theta'$ as ${}^s\theta'''$ and $\hat{\beta}''$ as $\hat{\beta}''_2$ (both chosen from (F-B2)). Also from cg-bind we know that in (F-B0) H'_{s1} will be H'_{s5}.

Since $(k-j-b-c-d, H'_{s5}, H'_{t5}) \overset{\hat{\beta}''_2}{\triangleright} {}^s\theta'''$ therefore Lemma 5.13 we get $(k-i, H'_{s5}, H'_{t5}) \overset{\hat{\beta}''_2}{\triangleright} {}^s\theta'''$
Also since from (F-B2) we have $\exists^t v''.{}^t v'_{h2} = \mathsf{inl}\ {}^t v''_{h2} \wedge ({}^s\theta''', k-j-b-c-d, {}^s v'_{h2}, {}^t v''_{h2}) \in \lfloor \tau'\ \sigma \rfloor^{\hat{\beta}''_2}_V$
Sicne $i = j+b+c+d+1$ therefore from Lemma 5.13 we get
$\exists^t v''.{}^t v'_{h2} = \mathsf{inl}\ {}^t v''_{h2} \wedge ({}^s\theta''', k-i, {}^s v'_{h2}, {}^t v''_{h2}) \in \lfloor \tau'\ \sigma \rfloor^{\hat{\beta}''_2}_V$

16. CF-label:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \mathsf{Lb}_\ell(e_s) : (\mathsf{Labeled}\ \ell\ \tau) \rightsquigarrow \mathsf{inl}(e_t)}\ \text{label}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor^{\hat{\beta}}_V$

To prove: $({}^s\theta, n, \mathsf{Lb}_\ell(e_s)\ \delta^s, \mathsf{inl}(e_t)\ \delta^t) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor^{\hat{\beta}}_E$

From Definition 5.9 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{Lb}_\ell(e_s)\ \delta^s \Downarrow_i \mathsf{Lb}_\ell({}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{inl}(e_t)\ \delta^t) \Downarrow (H'_t, \mathsf{inl}({}^t v)) \wedge ({}^s\theta, n-i, \mathsf{Lb}_\ell({}^s v), \mathsf{inl}({}^t v)) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor^{\hat{\beta}}_V \wedge$
$(n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that we are given some $H_s, H_t, \hat{\beta}$ s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $\mathsf{Lb}_\ell(e_s)\ \delta^s \Downarrow_i \mathsf{Lb}_\ell({}^s v)$.

And we need to prove
$\exists H'_t, {}^t v.(H_t, \mathsf{inl}(e_t)\ \delta^t) \Downarrow (H'_t, \mathsf{inl}({}^t v)) \wedge ({}^s\theta, n-i, \mathsf{Lb}_\ell({}^s v), \mathsf{inl}({}^t v)) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor^{\hat{\beta}}_V \wedge$
$(n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-LB0)

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor^{\hat{\beta}}_E$

From Definition 5.9 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_s\ \delta^s \Downarrow_j {}^s v_1 \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating with H_s, H_t and since we know that $\mathsf{Lb}_\ell(e_s)\ \delta^s \Downarrow_i \mathsf{Lb}_\ell({}^s v)$ therefore $\exists j < i < n$ s.t $e_s\ \delta^s \Downarrow_j {}^s v$.

Therefore we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v, {}^t v) \in \lfloor (\tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-j, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (F-LB1)

Since from (F-LB0) we are required to prove $({}^s\theta, n-i, \mathsf{Lb}_\ell({}^s v), \mathsf{inl}({}^t v)) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}}$. Since from cg-label we know that $i = j+1$, ${}^s v = {}^s v_1$ and ${}^t v = {}^t v_1$. Therefore we get this from Definition 5.8, (F-LB1) and Lemma 5.13.

From Lemma 5.13 we get $(n-i, H_s, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

17. CF-toLabeled:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \mathbb{C}\ \ell_1\ \ell_2\ \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \mathsf{toLabeled}(e_s) : \mathbb{C}\ \ell_1\ \bot\ (\mathsf{Labeled}\ \ell_2\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(e_t\ ())}\ \text{toLabeled}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{toLabeled}(e_s)\ \delta^s, (\lambda\_.\mathsf{inl}\ e_t())\ \delta^t) \in \lfloor (\mathbb{C}\ \ell_1\ \bot\ (\mathsf{Labeled}\ \ell_2\ \tau))\ \sigma \rfloor_E^{\hat{\beta}}$

It means from Definition 5.9 that we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{toLabeled}(e_s)\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, (\lambda\_.\mathsf{inl}\ e_t())\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (\mathbb{C}\ \ell_1\ \bot\ (\mathsf{Labeled}\ \ell_2\ \tau))\ \sigma \rfloor_V^{\hat{\beta}} \wedge$
$(n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t
$\mathsf{toLabeled}(e_s)\ \delta^s \Downarrow_i {}^s v$

And we need to prove
$\exists H'_t, {}^t v.(H_t, (\lambda\_.\mathsf{inl}\ e_t())\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (\mathbb{C}\ \ell_1\ \bot\ (\mathsf{Labeled}\ \ell_2\ \tau))\ \sigma \rfloor_V^{\hat{\beta}} \wedge$
$(n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$
From cg-val and fg-val we know that $i = 0$, ${}^s v = \mathsf{toLabeled}(e_s)\ \delta^s$,
${}^t v = (\lambda\_.\mathsf{inl}\ e_t())\ \delta^t$, $H'_t = H_t$

And we need to prove

$({}^s\theta, n, \mathsf{toLabeled}(e_s)\ \delta^s, (\lambda\_.\mathsf{inl}\ e_t())\ \delta^t) \in \lfloor (\mathbb{C}\ \ell_1\ \bot\ (\mathsf{Labeled}\ \ell_2\ \tau))\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we already know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context so we are left with proving

$({}^s\theta, n, \mathsf{toLabeled}(e_s)\ \delta^s, (\lambda\_.\mathsf{inl}\ e_t())\ \delta^t) \in \lfloor(\mathbb{C}\ \ell_1 \perp (\mathsf{Labeled}\ \ell_2\ \tau))\ \sigma\rfloor_V^{\hat{\beta}}$

From Definition 5.8 it means we need to prove
$\forall^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^sv', {}^tv', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s1}, \mathsf{toLabeled}(e_s)\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^sv') \wedge i < k \implies$
$\exists H'_{t1}, {}^tv'.(H_{t1}, (\lambda\_.\mathsf{inl}\ e_t())()\ \delta^t) \Downarrow (H'_{t1}, {}^tv') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists^t v''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', k-i, {}^sv', {}^tv'') \in \lfloor(\mathsf{Labeled}\ \ell_2\ \tau)\ \sigma\rfloor_V^{\hat{\beta}''}$

This means we are given some ${}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^sv', {}^tv', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge (H_{s1}, \mathsf{toLabeled}(e_s)\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^sv') \wedge i < k.$

And we need to prove

$\exists H'_{t1}, {}^tv'.(H_{t1}, (\lambda\_.\mathsf{inl}\ e_t())()\ \delta^t) \Downarrow (H'_{t1}, {}^tv') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists^t v''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', k-i, {}^sv', {}^tv'') \in \lfloor(\mathsf{Labeled}\ \ell_2\ \tau)\ \sigma\rfloor_V^{\hat{\beta}''}$ (F-TL0)

<u>IH:</u>

$({}^s\theta, k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor(\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma\rfloor_E^{\hat{\beta}}$

It means from Definition 5.9 that we need to prove

$\forall H_{s2}, H_{t2}.(k, H_{s2}, H_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^sv_{h1}.e_s\ \delta^s \Downarrow_j {}^sv_{h1} \implies$
$\exists H'_{t2}, {}^tv_{h1}.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^tv_{h1}) \wedge ({}^s\theta, k-j, {}^sv_{h1}, {}^tv_{h1}) \in \lfloor(\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (k-j, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright}$
${}^s\theta$

Instantiating H_{s2} with H_{s1} and H_{t2} with H_{t1}. And since we know that $(H_{s1}, \mathsf{toLabeled}(e_s)\ \delta^s) \Downarrow_i^f$ $(H'_s, {}^sv')$ therefore $\exists j < i < k \leq n$ s.t $e_s\ \delta^s \Downarrow_j {}^sv_{h1}$.
Therefore we have

$\exists H'_{t2}, {}^tv_{h1}.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^tv_{h1}) \wedge ({}^s\theta, k-j, {}^sv_{h1}, {}^tv_{h1}) \in \lfloor(\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma\rfloor_V^{\hat{\beta}} \wedge (k-j, H_{s1}, H'_{t2}) \overset{\hat{\beta}}{\triangleright}$
${}^s\theta$ (F-TL1.1)

From Definition 5.8 we know have
$\forall^s\theta_e \sqsupseteq {}^s\theta, H_{s3}, H_{t3}, b, {}^sv'_{h1}, {}^tv'_{h1}, m \leq k-j, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(m, H_{s3}, H_{t3}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s3}, {}^sv_{h1}) \Downarrow_b^f (H'_{s3}, {}^sv'_{h1}) \wedge b < m \implies$
$\exists H'_{t3}, {}^tv'_{h1}.(H_{t3}, {}^tv_{h1}\ ()) \Downarrow (H'_{t3}, {}^tv'_{h1}) \wedge \exists^s\theta'' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(m-b, H'_{s3}, H'_{t3}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta'' \wedge$
$\exists^t v''_{h1}.{}^tv'_{h1} = \mathsf{inl}\ {}^tv''_{h1} \wedge ({}^s\theta'', m-b, {}^sv'_{h1}, {}^tv''_{h1}) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}''}$

Instantiating ${}^s\theta_e$ with ${}^s\theta$, H_{s3} with H_{s1}, H_{t3} with H'_{t2}, m with $k-j$ and $\hat{\beta}'$ with $\hat{\beta}$. Since we know that $(H_{s1}, \mathsf{toLabeled}(e_s)\ \delta^s) \Downarrow_i^f (H'_s, {}^sv')$ therefore $\exists b < i-j < k-j$ s.t $(H_{s1}, {}^sv_{h1})\ \delta^s \Downarrow_b (H'_{s3}, {}^sv'_{h1})$.

Therefore we have

$\exists H'_{t3}, {}^t v'_{h1}.(H_{t3}, {}^t v_{h1}\ ()) \Downarrow (H'_{t3}, {}^t v'_{h1}) \wedge \exists^s\theta'' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-j-b, H'_{s3}, H'_{t3}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta'' \wedge$
$\exists^t v''.{}^t v'_{h1} = \mathsf{inl}\ {}^t v''_{h1} \wedge ({}^s\theta'', k-j-b, {}^s v'_{h1}, {}^t v''_{h1}) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$ (F-TL1)

In order to prove (F-TL0) we choose ${}^s\theta'$ as ${}^s\theta''$ and $\hat{\beta}'$ as $\hat{\beta}''$ (both chosen from (F-TL2))
Also from cg-toLabeled and fg-inl, fg-app we know that $H'_s = H'_{s3}$ and $H'_t = H'_{t3}$, and ${}^s v' = {}^s v'_{h1}$, ${}^t v' = {}^t v'_{h1}$
Therefore we get the desired from (F-TL1) and Lemma 5.13

18. CF-unlabel:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \mathsf{Labeled}\ \ell\ \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash \mathsf{unlabel}(e_s) : \mathbb{C}\ \top\ \ell\ \tau \rightsquigarrow \lambda\_.e_t}\ \text{unlabel}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{unlabel}(e_s)\ \delta^s, \lambda\_.e_t\ \delta^t \in \lfloor (\mathbb{C}\ \top\ (\ell)\ \tau)\ \sigma \rfloor_E^{\hat{\beta}}$

It means from Definition 5.9 that we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.\mathsf{unlabel}(e_s)\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, \lambda\_.e_t\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (\mathbb{C}\ \top\ (\ell)\ \tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $\mathsf{unlabel}(e_s)\ \delta^s \Downarrow_i {}^s v$

And we need to prove

$\exists H'_t, {}^t v.(H_t, \lambda\_.e_t\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor (\mathbb{C}\ \top\ (\ell)\ \tau)\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$
From cg-val and fg-val we know that $i = 0$, ${}^s v = \mathsf{unlabel}(e_s)\ \delta^s$, ${}^t v = \lambda\_.e_t\ \delta^t$, $H'_t = H_t$

And we need to prove

$({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathbb{C}\ \top\ (\ell)\ \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we already know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context so we are left with proving
$({}^s\theta, n, \mathsf{unlabel}(e_s)\ \delta^s, \lambda\_.e_t\ \delta^t) \in \lfloor (\mathbb{C}\ \top\ (\ell)\ \tau)\ \sigma \rfloor_V^{\hat{\beta}}$

From Definition 5.8 it means we need to prove
$\forall^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^s v', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s1}, \mathsf{unlabel}(e_s)\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^s v') \wedge i < k \implies$
$\exists H'_{t1}, {}^t v'.(H_{t1}, (\lambda\_.e_t)()\ \delta^t) \Downarrow (H'_{t1}, {}^t v') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k-i, {}^s v', {}^t v'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$

This means we are given some ${}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^s v', {}^t v', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge (H_{s1}, \mathsf{unlabel}(e_s)\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^s v') \wedge i < k.$

And we need to prove

$\exists H'_{t1}, {}^t v'.(H_{t1}, (\lambda\_.e_t)()\ \delta^t) \Downarrow (H'_{t1}, {}^t v') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k-i, {}^s v', {}^t v'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$ (F-U0)

<u>IH:</u>

$({}^s\theta_e, k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_E^{\hat{\beta}'}$

It means from Definition 5.9 that we need to prove

$\forall H_{s2}, H_{t2}.(k, H_{s2}, H_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge \forall f < k, {}^s v_h.e_s\ \delta^s \Downarrow_f {}^s v_h \implies$
$\exists H'_{t2}, {}^t v_h.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^t v_h) \wedge ({}^s\theta_e, k-f, {}^s v_h, {}^t v_h) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k-f, H_{s2}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

Instantiating H_{s2} with H_{s1} and H_{t2} with H_{t1}. And since we know that $(H_{s1}, \mathsf{unlabel}(e_s)\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists f < i < k \leq n$ s.t $e_s\ \delta^s \Downarrow_f {}^s v_h$.
Therefore we have
$\exists H'_{t2}, {}^t v_h.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^t v_h) \wedge ({}^s\theta_e, k-f, {}^s v_h, {}^t v_h) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k-f, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$ (F-U1)

In order to prove (F-U0) we choose H'_{t1} as H'_{t2}, ${}^t v'$ as ${}^t v_h$, ${}^s\theta'$ as ${}^s\theta_e$ and $\hat{\beta}''$ as $\hat{\beta}'$
From cg-unlabel and fg-app we also know that $H'_{s1} = H_{s1}$ and $H'_{t1} = H'_{t2}$
We need to prove

(a) $(k-i, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$:

Since from (F-U1) we know that $(k-f, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

Therefore from Lemma 5.15 we also get $(k-i, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

(b) $\exists^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta_e, k-i, {}^s v', {}^t v'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$:
Since from (F-U1) we have
$({}^s\theta_e, k-f, {}^s v_h, {}^t v_h) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'}$
This means from Definition 5.8 we know that
$\exists^s v_i, {}^t v_i.{}^s v_h = \mathsf{Lb}_\ell({}^s v_i) \wedge {}^t v_h = \mathsf{inl}\ {}^t v_i \wedge ({}^s\theta_e, k-f-1, {}^s v_i, {}^t v_i) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-U2)
Since we know that ${}^t v' = {}^t v_h$ and since from (F-U2) we have ${}^t v_h = \mathsf{inl}\ {}^t v_i$. Therefore from we choose ${}^t v''$ as ${}^t v_i$ to get the first conjunct
From cg-unlabel we know that ${}^s v = {}^s v_i$ and since we know that $({}^s\theta_e, k-f-1, {}^s v_i, {}^t v_i) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$
Therefore from Lemma 5.13 we also get $({}^s\theta_e, k-i, {}^s v_i, {}^t v_i) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$

19. CF-ref:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \mathsf{Labeled}\ \ell'\ \tau \rightsquigarrow e_t \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash \mathsf{new}\ e_s : \mathbb{C}\ \ell\ \bot\ (\mathsf{ref}\ \ell'\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_t))} \text{ref}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{new}\ e_s\ \delta^s, \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_t))\ \delta^t \in \lfloor \mathbb{C}\ \ell \perp (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_E^{\hat{\beta}}$

It means from Definition 5.9 that we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv.\mathsf{new}\ e_s\ \delta^s \Downarrow_i {}^sv \implies$
$\exists H'_t, {}^tv.(H_t, \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_t))\ \delta^t) \Downarrow (H'_t, {}^tv) \wedge ({}^s\theta, n-i, {}^sv, {}^tv) \in \lfloor (\mathbb{C}\ \ell \perp (\mathsf{ref}\ \ell'\ \tau))\ \sigma \rfloor_V^{\hat{\beta}} \wedge$
$(n-i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^sv$ s.t $\mathsf{new}\ e_s\ \delta^s \Downarrow_i {}^sv$

From cg-val and fg-val we know that $i = 0$, ${}^sv = \mathsf{new}\ e_s\ \delta^s$, ${}^tv = \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_t))\ \delta^t$, $H'_t = H_t$

And we need to prove

$({}^s\theta, n, \mathsf{new}\ e_s\ \delta^s, \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_t))\ \delta^t) \in \lfloor (\mathbb{C}\ \ell \perp (\mathsf{ref}\ \ell'\ \tau))\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we already know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context so we are left with proving
$({}^s\theta, n, \mathsf{new}\ e_s\ \delta^s, \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_t))\ \delta^t) \in \lfloor (\mathbb{C}\ \ell \perp (\mathsf{ref}\ \ell'\ \tau))\ \sigma \rfloor_V^{\hat{\beta}}$

From Definition 5.8 it means we need to prove
$\forall {}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^sv', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s1}, \mathsf{new}\ e_s\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^sv') \wedge i < k \implies$
$\exists H'_{t1}, {}^tv'.(H_{t1}, (\lambda\_.\mathsf{inl}(\mathsf{new}\ e_t))()\ \delta^t) \Downarrow (H'_{t1}, {}^tv') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists {}^tv''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', k-i, {}^sv', {}^tv'') \in \lfloor (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat{\beta}''}$

This means we are given some ${}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^sv', {}^tv', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge (H_{s1}, \mathsf{new}\ (e_s)\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^sv') \wedge i < k.$

And we need to prove

$\exists H'_{t1}, {}^tv'.(H_{t1}, (\lambda\_.\mathsf{inl}(\mathsf{new}\ e_t))()\ \delta^t) \Downarrow (H'_{t1}, {}^tv') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists {}^tv''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', k-i, {}^sv', {}^tv'') \in \lfloor (\mathsf{ref}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat{\beta}''}$ (F-N0)
From cg-ref we know that ${}^sv' = a_s$ and from fg-ref, fg-inl we know that ${}^tv' = \mathsf{inl}\ a_t$.

<u>IH:</u>

$({}^s\theta_e, k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_E^{\hat{\beta}'}$

It means from Definition 5.9 that we need to prove

$\forall H_{s2}, H_{t2}.(k, H_{s2}, H_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge \forall f < k, {}^sv_h.e_s\ \delta^s \Downarrow_f {}^sv_h \implies$
$\exists H'_{t2}, {}^tv_h.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^tv_h) \wedge ({}^s\theta_e, k-f, {}^sv_h, {}^tv_h) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k-f, H_{s2}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

Instantiating H_{s2} with H_{s1} and H_{t2} with H_{t1}. And since we know that $(H_{s1}, \mathsf{new}\ (e_s)\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists f < i < k \leq n$ s.t $e_s\ \delta^s \Downarrow_f {}^s v_h$.

Therefore we have

$\exists H'_{t2}, {}^t v_h.(H_{t2}, e_t\ \ \delta^t) \Downarrow (H'_{t2}, {}^t v_h) \wedge ({}^s\theta_e, k - f, {}^s v_h, {}^t v_h) \in \lfloor(\mathsf{Labeled}\ \ \ell'\ \ \tau)\ \ \sigma\rfloor_V^{\hat{\beta}'} \wedge (k - f, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\rhd} {}^s\theta_e$ (F-N1)

In order to prove (F-N0) we choose H'_{t1} as $H'_{t2} \cup \{a_t \mapsto {}^t v_h\}$, ${}^t v$ as a_t, ${}^s\theta'$ as ${}^s\theta_n$ where ${}^s\theta_n = {}^s\theta_e \cup \{a_s \mapsto (\mathsf{Labeled}\ \ell'\ \tau)\}$

And we choose $\hat{\beta}''$ as $\hat{\beta}_n$ where $\hat{\beta}_n = \hat{\beta}' \cup \{(a_s, a_t)\}$

From cg-ref and fg-ref we also know that $H'_{s1} = H_{s1} \cup \{a_s \mapsto {}^s v_h\}$

We need to prove

(a) $(k - i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}_n}{\rhd} {}^s\theta_n$:
From Definition 5.10 it suffices to prove that
- $dom({}^s\theta_n) \subseteq dom(H'_{s1})$:
  Since $dom({}^s\theta_e) \subseteq dom(H_{s1})$ (given that we have $(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\rhd} {}^s\theta_e$)
  And since we know that
  ${}^s\theta_n = {}^s\theta_e \cup \{a_s \mapsto (\mathsf{Labeled}\ \ell'\ \tau)\}$ and $H'_{s1} = H_{s1} \cup \{a_s \mapsto {}^s v_h\}$
  Therefore we get $dom({}^s\theta_n) \subseteq dom(H'_{s1})$
- $\hat{\beta}_n \subseteq (dom({}^s\theta_n) \times dom(H'_{t1}))$:
  Since $\hat{\beta}' \subseteq (dom({}^s\theta_e) \times dom(H_{t1}))$ (given that we have $(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\rhd} {}^s\theta_e$)
  And since we know that
  ${}^s\theta_n = {}^s\theta_e \cup \{a_s \mapsto (\mathsf{Labeled}\ \ell'\ \tau)\}$, $H'_{t1} = H_{t1} \cup \{a_t \mapsto {}^t v_h\}$ and $\hat{\beta}_n = \hat{\beta}' \cup \{(a_s, a_t)\}$
  Therefore we get $\hat{\beta}_n \subseteq (dom({}^s\theta_n) \times dom(H'_{t1}))$
- $\forall (a_1, a_2) \in \hat{\beta}_n.({}^s\theta_n, k - i - 1, H'_{s1}(a_1), H'_{t1}(a_2)) \in \lfloor {}^s\theta_n(a) \rfloor_V^{\hat{\beta}_n}$:
  $\forall (a_1, a_2) \in \hat{\beta}_n$
  - $(a_1, a_2) = (a_s, a_t)$:
    Since from (F-N1) we know that $({}^s\theta_e, k - f, {}^s v_h, {}^t v_h) \in \lfloor(\mathsf{Labeled}\ \ell'\ \tau)\rfloor_V^{\hat{\beta}'}$
    From Lemma 5.13 we get $({}^s\theta_n, k - i - 1, {}^s v_h, {}^t v_h) \in \lfloor(\mathsf{Labeled}\ \ell'\ \tau)\rfloor_V^{\hat{\beta}_n}$
  - $(a_1, a_2) \neq (a_s, a_t)$:
    Since we have $(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\rhd} {}^s\theta_e$ therefore
    from Definition 5.10 we get
    $({}^s\theta_e, k - 1, H_{s1}(a_1), H_{t1}(a_2)) \in \lfloor {}^s\theta_e(a_1) \rfloor_V^{\hat{\beta}'}$
    From Lemma 5.13 we get
    $({}^s\theta_n, k - i - 1, H_{s1}(a_1), H_{t1}(a_2)) \in \lfloor {}^s\theta_n(a_1) \rfloor_V^{\hat{\beta}'}$

(b) $\exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta_n, k - i, {}^s v', {}^t v'') \in \lfloor(\mathsf{ref}\ \ell'\ \tau)\ \sigma\rfloor_V^{\hat{\beta}_n}$:
We choose ${}^t v''$ as ${}^t v_h$ from (F-N1), fg-inl and fg-ref we know that ${}^t v' = \mathsf{inl}\ {}^t v_h$

In order to prove $({}^s\theta_n, k - i, {}^s v', {}^t v'') \in \lfloor(\mathsf{ref}\ \ell'\ \tau)\ \sigma\rfloor_V^{\hat{\beta}_n}$, from Definition 5.8 it suffices to prove that

${}^s\theta_n(a_s) = (\mathsf{Labeled}\ \ell'\ \tau) \wedge (a_s, a_t) \in \hat{\beta}_n$

We get this by construction of ${}^s\theta_n$ and $\hat{\beta}_n$

20. CF-deref:

$$\frac{\Sigma; \Psi; \Gamma \vdash e_s : \mathsf{ref}\ \ell\ \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash !e_s : \mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(e_t)}\ \text{deref}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, !e_s\ \delta^s, \lambda\_.\mathsf{inl}(e_t)\ \delta^t \in \lfloor (\mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau))\ \sigma \rfloor_E^{\hat{\beta}}$

It means from Definition 5.9 that we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv.!e_s\ \delta^s \Downarrow_i {}^sv \implies$
$\exists H'_t, {}^tv.(H_t, \lambda\_.\mathsf{inl}(e_t)\ \delta^t) \Downarrow (H'_t, {}^tv) \wedge ({}^s\theta, n-i, {}^sv, {}^tv) \in \lfloor (\mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau))\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n$ s.t $!e_s\ \delta^s \Downarrow_i {}^sv$

And we need to prove
$\exists H'_t, {}^tv.(H_t, \lambda\_.\mathsf{inl}(e_t)\ \delta^t) \Downarrow (H'_t, {}^tv) \wedge ({}^s\theta, n-i, {}^sv, {}^tv) \in \lfloor (\mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau))\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n - i, H_s, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$
From cg-val and fg-val we know that $i = 0$, ${}^sv = !e_s\ \delta^s$, ${}^tv = \lambda\_.\mathsf{inl}(e_t)\ \delta^t$, $H'_t = H_t$

And we need to prove

$({}^s\theta, n, {}^sv, {}^tv) \in \lfloor (\mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau))\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we already know $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ from the context so we are left with proving
$({}^s\theta, n, !e_s\ \delta^s, \lambda\_.\mathsf{inl}(e_t)\ \delta^t) \in \lfloor (\mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell\ \tau))\ \sigma \rfloor_V^{\hat{\beta}}$

From Definition 5.8 it means we need to prove
$\forall {}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^sv', {}^tv', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s1}, !e_s\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^sv') \wedge i < k \implies$
$\exists H'_{t1}, {}^tv'.(H_{t1}, (\lambda\_.\mathsf{inl}(e_t))()\ \delta^t) \Downarrow (H'_{t1}, {}^tv') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k - i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists {}^tv''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', k-i, {}^sv', {}^tv'') \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}''}$

This means we are given some ${}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^sv', {}^tv', k \leq n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t
$(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge (H_{s1}, !(e_s)\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^sv') \wedge i < k.$

And we need to prove

$\exists H'_{t1}, {}^t v'.(H_{t1}, (\lambda\_.\mathsf{inl}(e_t))()\ \delta^t) \Downarrow (H'_{t1}, {}^t v') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k-i, {}^s v', {}^t v'') \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}''}$ (F-D0)

<u>IH:</u>

$({}^s\theta_e, k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\mathsf{ref}\ \ell\ \tau)\ \sigma \rfloor_E^{\hat{\beta}'}$

It means from Definition 5.9 that we need to prove

$\forall H_{s2}, H_{t2}.(k, H_{s2}, H_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e \wedge \forall f < k, {}^s v_h.e_s\ \delta^s \Downarrow_f {}^s v_h \implies$
$\exists H'_{t2}, {}^t v_h.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^t v_h) \wedge ({}^s\theta_e, k-f, {}^s v_h, {}^t v_h) \in \lfloor (\mathsf{ref}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k-f, H_{s2}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

Instantiating H_{s2} with H_{s1} and H_{t2} with H_{t1}. And since we know that $(H_{s1}, !e_s\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists f < i < k \leq n$ s.t $e_s\ \delta^s \Downarrow_f {}^s v_h$.
Therefore we have

$\exists H'_{t2}, {}^t v_h.(H_{t2}, e_t\ \delta^t) \Downarrow (H'_{t2}, {}^t v_h) \wedge ({}^s\theta_e, k-f, {}^s v_h, {}^t v_h) \in \lfloor (\mathsf{ref}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'} \wedge (k-f, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$
(F-D1)

In order to prove (F-D0) we choose H'_{t1} as H'_{t2}, ${}^t v'_1$ as $H'_{t2}(a)$ (where ${}^t v_h = a_t$ from fg-deref), ${}^s\theta'$ as ${}^s\theta_e$ and we choose $\hat{\beta}''$ as $\hat{\beta}'$.
From cg-deref we also know that $H'_{s1} = H_{s1}$
We need to prove

(a) $(k-i, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$:
Since from (F-D1) we have $(k-f, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$ and since $f < i$ threfore from Lemma 5.15 we get $(k-i, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$

(b) $\exists^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta_e, k-i, {}^s v', {}^t v'') \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'}$:
Since from cg-deref and fg-deref we know that ${}^s v_h = a_s$ and ${}^t v_h = a_t$.
Therefore from (F-D1) and from Definition 5.8 we know that
${}^s\theta_e(a_s) = (\mathsf{Labeled}\ \ell\ \tau) \wedge (a_s, a_t) \in \hat{\beta}'$

Since from (F-D1) we know that $(k-f, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$ which means from Definition 5.10 we know that
$({}^s\theta, k-f-1, H_{s1}(a_s), H'_{t2}(a_t)) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-D2)
This means from Definition 5.8 we know that
$\exists^s v_i, {}^t v_i.H_{s1}(a_s) = \mathsf{Lb}_\ell({}^s v_i) \wedge H'_{t2}(a_t) = \mathsf{inl}\ {}^t v_i \wedge ({}^s\theta_e, k-f-1, {}^s v_i, {}^t v_i) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$
We choose ${}^t v''$ as ${}^t v_i$ and we know that ${}^t v' = H'_{t2}(a_t) = \mathsf{inl}\ {}^t v_i$. This proves the first conjunct.

Since from (F-D2) we have $({}^s\theta, k-f-1, H_{s1}(a_s), H'_{t2}(a_t)) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'}$ therefore from Lemma 5.13 we get
$({}^s\theta, k-i-1, H_{s1}(a_s), H'_{t2}(a_t)) \in \lfloor (\mathsf{Labeled}\ \ell\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'}$
This proves the second conjunct.

21. CF-assign:

$$\frac{\Sigma;\Psi;\Gamma \vdash e_{s1} : \mathsf{ref}\ \ell'\ \tau \leadsto e_{t1} \qquad \Sigma;\Psi;\Gamma \vdash e_{s2} : \mathsf{Labeled}\ \ell'\ \tau \leadsto e_{t2} \qquad \Sigma;\Psi \vdash \ell \sqsubseteq \ell'}{\Sigma;\Psi;\Gamma \vdash e_{s1} := e_{s2} : \mathbb{C}\ \ell\ \bot\ \mathsf{unit} \leadsto \lambda\_.\mathsf{inl}(e_{t1} := e_{t2})} \text{ assign}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat\beta}$

To prove: $({}^s\theta, n, (e_{s1} := e_{s2})\ \delta^s, \lambda\_.\mathsf{inl}(e_{t1} := e_{t2})\ \delta^t \in \lfloor \mathbb{C}\ \ell \perp \mathsf{unit}\ \rfloor_E^{\hat\beta}$

It means from Definition 5.9 that we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat\beta}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(e_{s1} := e_{s2})\ \delta^s \Downarrow_i {}^s v \implies$
$\exists H'_t, {}^t v.(H_t, \lambda\_.\mathsf{inl}(e_{t1} := e_{t2})\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \mathbb{C}\ \ell \perp \mathsf{unit}\ \rfloor_V^{\hat\beta} \wedge (n - i, H_s, H'_t) \overset{\hat\beta}{\triangleright} {}^s\theta$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat\beta}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $(e_{s1} := e_{s2})\ \delta^s \Downarrow_i {}^s v$

And we need to prove
$\exists H'_t, {}^t v.(H_t, \lambda\_.\mathsf{inl}(e_{t1} := e_{t2})\ \delta^t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-i, {}^s v, {}^t v) \in \lfloor \mathbb{C}\ \ell \perp \mathsf{unit}\ \rfloor_V^{\hat\beta} \wedge (n - i, H_s, H'_t) \overset{\hat\beta}{\triangleright} {}^s\theta$

From cg-val and fg-val we know that $i = 0$, ${}^s v = (e_{s1} := e_{s2})\ \delta^s$, ${}^t v = \lambda\_.\mathsf{inl}(e_{t1} := e_{t2})\ \delta^t$, $H'_t = H_t$

And we need to prove

$({}^s\theta, n, (e_{s1} := e_{s2})\ \delta^s, \lambda\_.\mathsf{inl}(e_{t1} := e_{t2})\ \delta^t) \in \lfloor \mathbb{C}\ \ell \perp \mathsf{unit}\ \rfloor_V^{\hat\beta} \wedge (n, H_s, H_t) \overset{\hat\beta}{\triangleright} {}^s\theta$

Since we already know $(n, H_s, H_t) \overset{\hat\beta}{\triangleright} {}^s\theta$ from the context so we are left with proving
$({}^s\theta, n, (e_{s1} := e_{s2})\ \delta^s, \lambda\_.\mathsf{inl}(e_{t1} := e_{t2})\ \delta^t) \in \lfloor \mathbb{C}\ \ell \perp \mathsf{unit}\ \rfloor_V^{\hat\beta}$

From Definition 5.8 it means we need to prove
$\forall {}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^s v', k \leq n, \hat\beta \sqsubseteq \hat\beta'.$
$(k, H_{s1}, H_{t1}) \overset{\hat\beta'}{\triangleright} ({}^s\theta_e) \wedge (H_{s1}, (e_{s1} := e_{s2})\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^s v') \wedge i < k \implies$
$\exists H'_{t1}, {}^t v'.(H_{t1}, (\lambda\_.\mathsf{inl}(e_{t1} := e_{t2})()\ \delta^t)) \Downarrow (H'_{t1}, {}^t v') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat\beta' \sqsubseteq \hat\beta''.(k - i, H'_{s1}, H'_{t1}) \overset{\hat\beta''}{\triangleright} {}^s\theta' \wedge \exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k - i, {}^s v', {}^t v'') \in \lfloor \mathsf{unit} \rfloor_V^{\hat\beta''}$

This means we are given some ${}^s\theta_e \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i, {}^s v', k \leq n, \hat\beta \sqsubseteq \hat\beta'$ s.t
$(k, H_{s1}, H_{t1}) \overset{\hat\beta'}{\triangleright} {}^s\theta_e \wedge (H_{s1}, (e_{s1} := e_{s2})\ \delta^s) \Downarrow_i^f (H'_{s1}, {}^s v') \wedge i < k.$

And we need to prove
$\exists H'_{t1}, {}^t v'.(H_{t1}, (\lambda\_.\mathsf{inl}(e_{t1} := e_{t2})()\ \delta^t)) \Downarrow (H'_{t1}, {}^t v') \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta_e, \hat\beta' \sqsubseteq \hat\beta''.$
$(k - i, H'_{s1}, H'_{t1}) \overset{\hat\beta''}{\triangleright} {}^s\theta' \wedge \exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta', k - i, {}^s v', {}^t v'') \in \lfloor \mathsf{unit} \rfloor_V^{\hat\beta''}$ (F-S0)

IH1:

$({}^s\theta_e, k, e_{s1}\ \delta^s, e_{t1}\ \delta^t) \in \lfloor(\mathsf{ref}\ \ell'\ \tau)\rfloor_E^{\hat{\beta}'}$

It means from Definition 5.9 that we need to prove

$\forall H_{s2}, H_{t2}.(k, H_{s2}, H_{t2}) \overset{\hat{\beta}'}{\rhd} {}^s\theta_e \wedge \forall f < k, {}^s v_{h1}.e_{s1}\ \delta^s \Downarrow_f {}^s v_{h1} \implies$
$\exists H'_{t2}, {}^t v_{h1}.(H_{t2}, e_{t1}\ \delta^t) \Downarrow (H'_{t2}, {}^t v_{h1}) \wedge ({}^s\theta_e, k-f, {}^s v_{h1}, {}^t v_{h1}) \in \lfloor(\mathsf{ref}\ \ell'\ \tau)\rfloor_V^{\hat{\beta}'} \wedge (k-f, H_{s2}, H'_{t2}) \overset{\hat{\beta}'}{\rhd} {}^s\theta_e$

Instantiating H_{s2} with H_{s1} and H_{t2} with H_{t1}. And since we know that $(H_{s1}, e_{s1} := e_{s2}\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists f < i < k \leq n$ s.t $e_s\ \delta^s \Downarrow_f {}^s v_{h1}$.

Therefore we have

$\exists H'_{t2}, {}^t v_{h1}.(H_{t2}, e_{t1}\ \delta^t) \Downarrow (H'_{t2}, {}^t v_{h1}) \wedge ({}^s\theta_e, k-f, {}^s v_{h1}, {}^t v_{h1}) \in \lfloor(\mathsf{ref}\ \ell'\ \tau)\rfloor_V^{\hat{\beta}'} \wedge (k-f, H_{s1}, H'_{t2}) \overset{\hat{\beta}'}{\rhd} {}^s\theta_e$ (F-S1)

IH2:

$({}^s\theta_e, k-f, e_{s2}\ \delta^s, e_{t2}\ \delta^t) \in \lfloor(\mathsf{Labeled}\ \ell'\ \tau)\rfloor_E^{\hat{\beta}'}$

It means from Definition 5.9 that we need to prove

$\forall H_{s3}, H_{t3}.(k, H_{s3}, H_{t3}) \overset{\hat{\beta}'}{\rhd} {}^s\theta_e \wedge \forall l < k-f, {}^s v_{h2}.e_{s2}\ \delta^s \Downarrow_l {}^s v_{h2} \implies$
$\exists H'_{t3}, {}^t v_{h2}.(H_{t3}, e_{t2}\ \delta^t) \Downarrow (H'_{t3}, {}^t v_{h2}) \wedge ({}^s\theta_e, k-f-l, {}^s v_{h2}, {}^t v_{h2}) \in \lfloor(\mathsf{Labeled}\ \ell'\ \tau)\rfloor_V^{\hat{\beta}'} \wedge (k-f-l, H_{s3}, H'_{t3}) \overset{\hat{\beta}'}{\rhd} {}^s\theta_e$

Instantiating H_{s3} with H_{s1} and H_{t3} with H'_{t2}. And since we know that $(H_{s1}, e_{s1} := e_{s2}\ \delta^s) \Downarrow_i^f (H'_s, {}^s v')$ therefore $\exists l < i-f < k-f$ s.t $e_{s2}\ \delta^s \Downarrow_l {}^s v_{h2}$.

Therefore we have

$\exists H'_{t3}, {}^t v_{h2}.(H_{t3}, e_{t2}\ \delta^t) \Downarrow (H'_{t3}, {}^t v_{h2}) \wedge ({}^s\theta_e, k-f-l, {}^s v_{h2}, {}^t v_{h2}) \in \lfloor(\mathsf{Labeled}\ \ell'\ \tau)\rfloor_V^{\hat{\beta}'} \wedge (k-f-l, H_{s1}, H'_{t3}) \overset{\hat{\beta}'}{\rhd} {}^s\theta_e$ (F-S2)

In order to prove (F-S0) we choose H'_{t1} as $H'_{t3}[a_t \mapsto {}^t v_{h3}]$, ${}^t v'$ as (), ${}^s\theta'$ as ${}^s\theta_e$ and $\hat{\beta}''$ as $\hat{\beta}'$
From cg-assign and fg-assign we also know that ${}^s v_{h2} = a_s$, ${}^t v_{h2} = a_t$, $H'_{s1} = H_{s1}[a_s \mapsto {}^s v_{h3}]$ and $H'_{t1} = H'_{t3}[a_t \mapsto {}^t v_{h3}]$

We need to prove

(a) $(k-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'}{\rhd} {}^s\theta_e$:
From Definition 5.10 it suffices to prove that

- $dom({}^s\theta_e) \subseteq dom(H'_{s1})$:

  Since $dom({}^s\theta_e) \subseteq dom(H_{s1})$ (given that we have $(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\rhd} {}^s\theta_e$)

  And since $dom(H_{s1}) = dom(H'_{s1})$ therefore we also get
  $dom({}^s\theta_e) \subseteq dom(H'_{s1})$

- $\hat{\beta}' \subseteq (dom({}^s\theta_e) \times dom(H'_{t1}))$:

  Since $\hat{\beta}' \subseteq (dom({}^s\theta_e) \times dom(H_{t1}))$ (given that we have $(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$)

  And since $dom(H_{t1}) \subseteq dom(H'_{t1})$ therefore we also have $\hat{\beta}' \subseteq (dom({}^s\theta_e) \times dom(H'_{t1}))$

- $\forall (a_1, a_2) \in \hat{\beta}'.({}^s\theta_e, k-i-1, H'_{s1}(a_1), H'_{t1}(a_2)) \in \lfloor {}^s\theta_e(a_1) \rfloor_V^{\hat{\beta}'}$:
  $\forall (a_1, a_2) \in \hat{\beta}_n$
  - $(a_1, a_2) = (a_s, a_t)$:
    Since from (F-S2) we know that $({}^s\theta_e, k-f-l, {}^s v_{h2}, {}^t v_{h2}) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau) \rfloor_V^{\hat{\beta}'}$
    From Lemma 5.13 we get $({}^s\theta_e, k-i-1, {}^s v_{h2}, {}^t v_{h2}) \in \lfloor (\mathsf{Labeled}\ \ell'\ \tau) \rfloor_V^{\hat{\beta}'}$
  - $(a_1, a_2) \neq (a_s, a_t)$:
    Since we have $(k, H_{s1}, H_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta_e$ therefore
    from Definition 5.10 we get
    $({}^s\theta_e, k-1, H_{s1}(a_1), H_{t1}(a_2)) \in \lfloor {}^s\theta_e(a_1) \rfloor_V^{\hat{\beta}'}$
    From Lemma 5.13 we get
    $({}^s\theta_n, k-i-1, H_{s1}(a_1), H_{t1}(a_2)) \in \lfloor {}^s\theta_e(a_1) \rfloor_V^{\hat{\beta}'}$

(b) $\exists {}^t v''.{}^t v' = \mathsf{inl}\ {}^t v'' \wedge ({}^s\theta_e, k-i, {}^s v', {}^t v'') \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}_n}$:
We choose ${}^t v''$ as () from (F-S1), fg-inl and fg-assign we know that ${}^t v' = \mathsf{inl}\ ()$

<u>To prove:</u> $({}^s\theta_n, k-i, (), ()) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}_n}$,
We get this directly from Definition 5.8

□

Lemma 5.17 (Subtyping). *The following holds:*
$\forall \Sigma, \Psi, \sigma, \tau, \tau'$.

1. $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor (\tau\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau'\ \sigma) \rfloor_V^{\hat{\beta}}$

2. $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor (\tau\ \sigma) \rfloor_E^{\hat{\beta}} \subseteq \lfloor (\tau'\ \sigma) \rfloor_E^{\hat{\beta}}$

Proof. <u>Proof of Statement (1)</u>
Proof by induction on $\tau <: \tau'$

1. CGsub-arrow:

   Given:

$$\frac{\Sigma; \Psi \vdash \tau'_1 <: \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau'_2}{\Sigma; \Psi \vdash \tau_1 \to \tau_2 <: \tau'_1 \to \tau'_2}$$

   To prove: $\lfloor ((\tau_1 \to \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor ((\tau'_1 \to \tau'_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

   It suffices to prove: $\forall ({}^s\theta, n, \lambda x.e_i) \in \lfloor ((\tau_1 \to \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, \lambda x.e_i) \in \lfloor ((\tau'_1 \to \tau'_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

   This means that given some ${}^s\theta, n$ and $\lambda x.e_i$ s.t $({}^s\theta, n, \lambda x.e_i) \in \lfloor ((\tau_1 \to \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$
   Therefore from Definition 5.8 we are given:

$\forall^s\theta' \sqsupseteq {}^s\theta, {}^sv, {}^tv, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$({}^s\theta', j, {}^sv, {}^tv) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'} \implies ({}^s\theta', j, e_s[{}^sv/x], e_t[{}^tv/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}'}$ (S-A0)

And it suffices to prove: $({}^s\theta, n, \lambda x.e_i) \in \lfloor ((\tau'_1 \to \tau'_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

Again from Definition 5.8 it suffices to prove:
$\forall^s\theta'_1 \sqsupseteq {}^s\theta, {}^sv_1, {}^tv_1, k < n, \hat{\beta} \sqsubseteq \hat{\beta}'_1.$
$({}^s\theta'_1, k, {}^sv_1, {}^tv_1) \in \lfloor \tau'_1\ \sigma \rfloor_V^{\hat{\beta}'_1} \implies ({}^s\theta'_1, k, e_s[{}^sv_1/x], e_t[{}^tv_1/x]) \in \lfloor \tau'_2\ \sigma \rfloor_E^{\hat{\beta}'_1}$

This means that given some ${}^s\theta'_1 \sqsubseteq {}^s\theta, {}^sv_1, {}^tv_1, k < n, \hat{\beta} \sqsubseteq \hat{\beta}'_1$ s.t $({}^s\theta'_1, k, {}^sv_1, {}^tv_1) \in \lfloor \tau'_1\ \sigma \rfloor_V^{\hat{\beta}'}$

And we are required to prove: $({}^s\theta'_1, k, e_s[{}^sv_1/x], e_t[{}^tv_1/x]) \in \lfloor \tau'_2\ \sigma \rfloor_E^{\hat{\beta}'_1}$

IH: $\lfloor (\tau'_1\ \sigma) \rfloor_V^{\hat{\beta}'_1} \subseteq \lfloor (\tau_1\ \sigma) \rfloor_V^{\hat{\beta}'_1}$ (Statement (1))

$\lfloor (\tau_2\ \sigma) \rfloor_E^{\hat{\beta}'_1} \subseteq \lfloor (\tau'_2\ \sigma) \rfloor_E^{\hat{\beta}'_1}$ (Sub-A0, From Statement (2))

Instantiating (S-A0) with ${}^s\theta'_1, {}^sv_1, {}^tv_1, k, \hat{\beta}'_1$

Since $({}^s\theta'_1, k, {}^sv_1, {}^tv_1) \in \lfloor \tau'_1\ \sigma \rfloor_V^{\hat{\beta}}$ therefore from IH1 we know that $({}^s\theta'_1, k, {}^sv_1, {}^tv_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}}$
As a result we get
$({}^s\theta'_1, k, e_s[{}^sv_1/x], e_t[{}^tv_1/x]) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}'_1}$
From (Sub-A0), we know that
$({}^s\theta'_1, k, e_s[{}^sv_1/x], e_t[{}^tv_1/x]) \in \lfloor \tau'_2\ \sigma \rfloor_E^{\hat{\beta}'_1}$

2. CGsub-prod:
Given:

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau'_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau'_2}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau'_1 \times \tau'_2}$$

To prove: $\lfloor ((\tau_1 \times \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor ((\tau'_1 \times \tau'_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

IH1: $\lfloor (\tau_1\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau'_1\ \sigma) \rfloor_V^{\hat{\beta}}$ (Statement (1))

IH2: $\lfloor (\tau_2\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau'_2\ \sigma) \rfloor_V^{\hat{\beta}}$ (Statement (1))
It suffices to prove:
$\forall ({}^s\theta, n, ({}^sv_1, {}^sv_2), ({}^tv_1, {}^tv_2)) \in \lfloor ((\tau_1 \times \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, ({}^sv_1, {}^sv_2), ({}^tv_1, {}^tv_2)) \in \lfloor ((\tau'_1 \times \tau'_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

This means that given $({}^s\theta, n, ({}^sv_1, {}^sv_2), ({}^tv_1, {}^tv_2)) \in \lfloor ((\tau_1 \times \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$
Therefore from Definition 5.8 we are given:
$({}^s\theta, n, {}^sv_1, {}^tv_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}} \wedge ({}^s\theta, n, {}^sv_2, {}^tv_2) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}}$ (S-P0)

And it suffices to prove: $({}^s\theta, ({}^sv_1, {}^sv_2), ({}^tv_1, {}^tv_2)) \in \lfloor ((\tau'_1 \times \tau'_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

Again from Definition 5.8, it suffices to prove:

$({}^s\theta, n, {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \ \sigma \rfloor_V^{\hat{\beta}} \wedge ({}^s\theta, n, {}^s v_2, {}^t v_2) \in \lfloor \tau_2 \ \sigma \rfloor_V^{\hat{\beta}}$

Since from (S-P0) we know that $({}^s\theta, n, {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \ \sigma \rfloor_V^{\hat{\beta}}$ therefore from IH1 we have $({}^s\theta, n, {}^s v_1, {}^t v_1) \in \lfloor \tau_1' \ \sigma \rfloor_V^{\hat{\beta}}$

Similarly since from (S-P0) we have $({}^s\theta, n, {}^s v_2, {}^t v_2) \in \lfloor \tau_2 \ \sigma \rfloor_V^{\hat{\beta}}$ therefore from IH2 we get $({}^s\theta, n, {}^s v_2, {}^t v_2) \in \lfloor \tau_2' \ \sigma \rfloor_V^{\hat{\beta}}$

3. CGsub-sum:

   Given:

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'}$$

   To prove: $\lfloor ((\tau_1 + \tau_2) \ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor ((\tau_1' + \tau_2') \ \sigma) \rfloor_V^{\hat{\beta}}$

   IH1: $\lfloor (\tau_1 \ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau_1' \ \sigma) \rfloor_V^{\hat{\beta}}$ (Statement (1))

   IH2: $\lfloor (\tau_2 \ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau_2' \ \sigma) \rfloor_V^{\hat{\beta}}$ (Statement (1))

   It suffices to prove: $\forall ({}^s\theta, n, {}^s v, {}^t v) \in \lfloor ((\tau_1 + \tau_2) \ \sigma) \rfloor_V^{\hat{\beta}}. \ ({}^s\theta, n, {}^s v, {}^t v) \in \lfloor ((\tau_1' + \tau_2') \ \sigma) \rfloor_V^{\hat{\beta}}$

   This means that given: $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor ((\tau_1 + \tau_2) \ \sigma) \rfloor_V^{\hat{\beta}}$

   And it suffices to prove: $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor ((\tau_1' + \tau_2') \ \sigma) \rfloor_V^{\hat{\beta}}$

   2 cases arise

   (a) ${}^s v = \mathsf{inl}\ {}^s v_i$ and ${}^t v = \mathsf{inl}\ {}^t v_i$:
   From Definition 5.8 we are given:
   $({}^s\theta, n, {}^s v_i, {}^t v_i) \in \lfloor \tau_1 \ \sigma \rfloor_V^{\hat{\beta}}$ (S-S0)
   And we are required to prove that:
   $({}^s\theta, n, {}^s v_i, {}^t v_i) \in \lfloor \tau_1' \ \sigma \rfloor_V^{\hat{\beta}}$
   From (S-S0) and IH1 we get
   $({}^s\theta, n, {}^s v_i, {}^t v_i) \in \lfloor \tau_1' \ \sigma \rfloor_V^{\hat{\beta}}$

   (b) ${}^s v = \mathsf{inr}\ {}^s v_i$ and ${}^t v = \mathsf{inr}\ {}^t v_i$:
   Symmetric reasoning

4. SLIO*sub-forall:

   Given:

$$\frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash \forall \alpha.\tau_1 <: \forall \alpha.\tau_2}$$

   To prove: $\lfloor ((\forall \alpha.\tau_1) \ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\forall \alpha.\tau_2) \ \sigma \rfloor_V^{\hat{\beta}}$

   It suffices to prove: $\forall ({}^s\theta, n, \Lambda e_s, \Lambda e_t) \in \lfloor ((\forall \alpha.\tau_1) \ \sigma) \rfloor_V^{\hat{\beta}}. \ ({}^s\theta, n, \Lambda e_s, \Lambda e_t) \in \lfloor ((\forall \alpha.\tau_2) \ \sigma) \rfloor_V^{\hat{\beta}}$

This means that given: $({}^s\theta, n, \Lambda e_s, \Lambda e_t) \in \lfloor((\forall\alpha.\tau_1)\ \sigma)\rfloor_V^{\hat{\beta}}$
Therefore from Definition 5.8 we are given:
$\forall^s\theta' \sqsupseteq {}^s\theta, j < n, \ell' \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, e_s, e_t) \in \lfloor\tau_1[\ell'/\alpha]\ \sigma\rfloor_E^{\hat{\beta}'}$ (S-F0)

And it suffices to prove: $({}^s\theta, n, \Lambda e_s, \Lambda e_t) \in \lfloor((\forall\alpha.\tau_2)\ \sigma)\rfloor_V^{\hat{\beta}}$

Again from Definition 5.8, it suffices to prove:
$\forall^s\theta'_1 \sqsupseteq {}^s\theta, k < n, \ell'_1 \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}'_1.({}^s\theta'_1, k, e_s, e_t) \in \lfloor\tau_2[\ell'_1/\alpha]\ \sigma\rfloor_E^{\hat{\beta}'_1}$

This means that given ${}^s\theta_1 \sqsupseteq {}^s\theta, k < n, \ell'_1 \in \mathcal{L}, \hat{\beta} \sqsubseteq \hat{\beta}'_1$

And we are required to prove: $({}^s\theta'_1, k, e_s, e_t) \in \lfloor\tau_2[\ell'_1/\alpha]\ \sigma\rfloor_E^{\hat{\beta}'_1}$

Instantiating (S-F0) with ${}^s\theta_1, k, \ell'_1, \hat{\beta}'_1$ we get
$({}^s\theta'_1, k, e_s, e_t) \in \lfloor\tau_1[\ell'_1/\alpha]\ \sigma\rfloor_E^{\hat{\beta}'_1}$

$\lfloor(\tau_1\ (\sigma \cup [\alpha \mapsto \ell']))\rfloor_E^{\hat{\beta}'_1} \subseteq \lfloor(\tau_2\ (\sigma \cup [\alpha \mapsto \ell']))\rfloor_E^{\hat{\beta}'_1}$ (Sub-F0, Statement (2))

From (Sub-F0), we know that
$({}^s\theta'_1, k, e_s, e_t) \in \lfloor\tau_2[\ell'_1/\alpha]\ \sigma\rfloor_E^{\hat{\beta}'_1}$

5. SLIO*sub-constraint:
   Given:

$$\frac{\Sigma;\Psi \vdash c_2 \implies c_1 \qquad \Sigma;\Psi \vdash \tau_1 <: \tau_2}{\Sigma;\Psi \vdash c_1 \Rightarrow \tau_1 <: c_2 \Rightarrow \tau_2}$$

To prove: $\lfloor((c_1 \Rightarrow \tau_1)\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor((c_2 \Rightarrow \tau_2))\ \sigma\rfloor_V^{\hat{\beta}}$

It suffices to prove: $\forall({}^s\theta, n, \nu e_s, \nu e_t) \in \lfloor((c_1 \Rightarrow \tau_1)\ \sigma)\rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, \nu e_s, \nu e_t) \in \lfloor((c_2 \Rightarrow \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}}$

This means that given: $({}^s\theta, n, \nu e_s, \nu e_t) \in \lfloor((c_1 \Rightarrow \tau_1)\ \sigma)\rfloor_V^{\hat{\beta}}$
Therefore from Definition 5.8 we are given:
$\mathcal{L} \models c_1\ \sigma \implies \forall^s\theta' \sqsupseteq {}^s\theta, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, e_s, e_t) \in \lfloor\tau_1\ \sigma\rfloor_E^{\hat{\beta}'}$ (S-C0)

And it suffices to prove: $({}^s\theta, n, \nu e_s, \nu e_t) \in \lfloor((c_2 \Rightarrow \tau_2)\ \sigma)\rfloor_V^{\hat{\beta}}$

Again from Definition 5.8, it suffices to prove:
$\mathcal{L} \models c_2\ \sigma \implies \forall^s\theta'_1 \sqsupseteq {}^s\theta, k < n, \hat{\beta} \sqsubseteq \hat{\beta}'_1.({}^s\theta'_1, k, e_s, e_t) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}'_1}$

This means that given $\mathcal{L} \models c_2, {}^s\theta'_1 \sqsupseteq {}^s\theta, k < n, \hat{\beta} \sqsubseteq \hat{\beta}'_1$

And we are required to prove:
$({}^s\theta'_1, k, e_s, e_t) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}'_1}$

since we know that $c_2 \implies c_1$ and since $\mathcal{L} \models c_2\ \sigma$ therefore $\mathcal{L} \models c_1\ \sigma$. Next we instantiate (S-C0) with ${}^s\theta'_1, k, \hat{\beta}'_1$ to get

$({}^s\theta'_1, k, e_s, e_t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}'_1}$

$\lfloor (\tau_1\ \sigma) \rfloor_E^{\hat{\beta}'_1} \subseteq \lfloor (\tau_2\ \sigma) \rfloor_E^{\hat{\beta}} \hat{\beta}'_1$ (Sub-C0, Statement (2))

Therefore from (Sub-C0), we get

$({}^s\theta'_1, k, e_s, e_t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}'_1}$

6. CGsub-label:

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi \vdash \mathsf{Labeled}\ \ell\ \tau <: \mathsf{Labeled}\ \ell'\ \tau'}$$

To prove: $\lfloor ((\mathsf{Labeled}\ \ell\ \tau)\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor ((\mathsf{Labeled}\ \ell\ '\tau')\ \sigma) \rfloor_V^{\hat{\beta}}$

IH: $\lfloor (\tau\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau'\ \sigma) \rfloor_V^{\hat{\beta}}$ (Statement (1))

It suffices to prove:

$\forall ({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathsf{Labeled}\ \ell\ \tau)\ \sigma) \rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathsf{Labeled}\ \ell'\ \tau')\ \sigma) \rfloor_V^{\hat{\beta}}$

This means that given some $({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathsf{Labeled}\ \ell\ \tau)\ \sigma) \rfloor_V^{\hat{\beta}}$
Therefore from Definition 5.8 we are given:

$\exists {}^sv', {}^tv'.{}^sv = \mathsf{Lb}_\ell({}^sv') \wedge {}^tv = \mathsf{inl}\ {}^tv' \wedge ({}^s\theta, m, {}^sv', {}^tv') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}}$ (S-L0)

And we are required to prove that

$({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathsf{Labeled}\ \ell'\ \tau')\ \sigma) \rfloor_V^{\hat{\beta}}$
From Definition 5.8 it suffices to prove

$\exists {}^sv', {}^tv'.{}^sv = \mathsf{Lb}_\ell({}^sv') \wedge {}^tv = \mathsf{inl}\ {}^tv' \wedge ({}^s\theta, m, {}^sv', {}^tv') \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}}$

We get this directly from (S-L0) and IH

7. CGsub-CG:

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell'_1 \sqsubseteq \ell_1 \qquad \Sigma; \Psi \vdash \ell_2 \sqsubseteq \ell'_2}{\Sigma; \Psi \vdash \mathbb{C}\ \ell_1\ \ell_2\ \tau <: \mathbb{C}\ \ell'_1\ \ell'_2\ \tau'}$$

To prove: $\lfloor ((\mathbb{C}\ \ell_i\ \ell_2\ \tau)\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor ((\mathbb{C}\ \ell'_1\ \ell'_2\ \tau')\ \sigma) \rfloor_V^{\hat{\beta}}$

It suffices to prove:

$\forall ({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma\ ) \rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathbb{C}\ \ell'_1\ \ell'_2\ \tau')\ \sigma) \rfloor_V^{\hat{\beta}}$

This means that given $({}^s\theta, n, {}^sv, {}^tv) \in \lfloor ((\mathbb{C}\ \ell_1\ \ell_2\ \tau)\ \sigma) \rfloor_V^{\hat{\beta}}$
Therefore from Definition 5.8 we are given:

$\forall^s\theta_e \sqsupseteq {}^s\theta, H_s, H_t, i, {}^sv', k \leq m, \hat{\beta} \sqsubseteq \hat{\beta}'.$
$(k, H_s, H_t) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_s, {}^sv) \Downarrow_i^f (H_s', {}^sv') \wedge i < k \implies$
$\exists H_t', {}^tv'.(H_t, {}^tv()) \Downarrow (H_t', {}^tv') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H_s', H_t') \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists^t v''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', k-i, {}^sv', {}^tv'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$ (S-M0)

And we are required to prove

$({}^s\theta, n, {}^sv, {}^tv) \in \lfloor((\mathbb{C}\ \ell_1'\ \ell_2'\ \tau')\ \sigma)\rfloor_V^{\hat{\beta}}$

So again from Definition 5.8 we need to prove
$\forall^s\theta_{e1} \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i_1, {}^sv_1', k_1 \leq n, \hat{\beta} \sqsubseteq \hat{\beta}_1'.$
$(k_1, H_{s1}, H_{t1}) \overset{\hat{\beta}_1'}{\triangleright} ({}^s\theta_{e1}) \wedge (H_{s1}, {}^sv) \Downarrow_{i_1}^f (H_{s1}', {}^sv_1') \wedge i_1 < k_1 \implies$
$\exists H_{t1}', {}^tv_1'.(H_{t1}, {}^tv()) \Downarrow (H_{t1}', {}^tv_1') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_{e1}, \hat{\beta}_1' \sqsubseteq \hat{\beta}_1''.(k_1 - i_1, H_{s1}', H_{t1}') \overset{\hat{\beta}_1''}{\triangleright} {}^s\theta' \wedge$
$\exists^t v_1''.{}^tv_1' = \mathsf{inl}\ {}^tv_1'' \wedge ({}^s\theta', k_1 - i_1, {}^sv_1', {}^tv_1'') \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}_1''}$

This means we are given some ${}^s\theta_{e1} \sqsupseteq {}^s\theta, H_{s1}, H_{t1}, i_1, {}^sv_1', k_1 \leq n, \hat{\beta} \sqsubseteq \hat{\beta}_1'$ s.t $(k_1, H_{s1}, H_{t1}) \overset{\hat{\beta}_1'}{\triangleright} ({}^s\theta_{e1}) \wedge (H_{s1}, {}^sv_1) \Downarrow_{i_1}^f (H_{s1}', {}^sv_1') \wedge i_1 < k_1$

<u>And we need to prove</u>

$\exists H_{t1}', {}^tv_1'.(H_{t1}, {}^tv_1()) \Downarrow (H_{t1}', {}^tv_1') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_{e1}, \hat{\beta}_1' \sqsubseteq \hat{\beta}_1''.(k_1 - i_1, H_{s1}', H_{t1}') \overset{\hat{\beta}_1''}{\triangleright} {}^s\theta' \wedge$
$\exists^t v_1''.{}^tv_1' = \mathsf{inl}\ {}^tv_1'' \wedge ({}^s\theta', k_1 - i_1, {}^sv_1', {}^tv_1'') \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}_1''}$

We instantiate (S-M0) with ${}^s\theta_{e1}, H_{s1}, H_{t1}, i_1, {}^sv_1', k_1, \hat{\beta}_1'$ we get

$\exists H_t', {}^tv'.(H_t, {}^tv()) \Downarrow (H_t', {}^tv') \wedge \exists^s\theta' \sqsupseteq {}^s\theta_{e1}, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H_s', H_t') \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge$
$\exists^t v''.{}^tv' = \mathsf{inl}\ {}^tv'' \wedge ({}^s\theta', k-i, {}^sv', {}^tv'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$

IH: $\lfloor(\tau\ \sigma)\rfloor_V^{\hat{\beta}''} \subseteq \lfloor(\tau'\ \sigma)\rfloor_V^{\hat{\beta}}\hat{\beta}''$ (Statement (1))

Since we have $({}^s\theta', k-i, {}^sv', {}^tv'') \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}''}$ therefore from IH we get $({}^s\theta', k-i, {}^sv', {}^tv'') \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}''}$

8. CGsub-base:

   Trivial

<u>Proof of Statement(2)</u>
<u>It suffice to prove that</u>
$\forall({}^s\theta, n, e_s, e_t) \in \lfloor(\tau\ \sigma)\rfloor_E^{\hat{\beta}}.\ ({}^s\theta, n, e_s, e_t) \in \lfloor(\tau'\ \sigma)\rfloor_E^{\hat{\beta}}$

This means that we are given $({}^s\theta, n, e_s, e_t) \in \lfloor(\tau\ \sigma)\rfloor_E^{\hat{\beta}}$
From Definition 5.9 it means we have
$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv.e_s \Downarrow_i {}^sv \implies$
$\exists H_t', {}^tv.(H_t, e_t) \Downarrow (H_t', {}^tv) \wedge ({}^s\theta, n-i, {}^sv, {}^tv) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}} \wedge (n-i, H_s, H_t') \overset{\hat{\beta}}{\triangleright} {}^s\theta$ (Sub-E0)

And we need to prove

$({}^s\theta, n, e_s, e_t) \in \lfloor(\tau'\ \sigma)\rfloor_E^{\hat{\beta}}$

From Definition 5.9 we need to prove

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.e_s \Downarrow_j {}^s v_1 \implies$

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor\tau'\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

This further means that given H_{s1}, H_{t1} s.t $(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $j < n, {}^s v_1$ s.t $e_s \Downarrow_j {}^s v_1$

And it suffices to prove that

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t) \Downarrow (H'_{t1}, {}^t v_1) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v_1) \in \lfloor\tau'\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Instantiating (Sub-E0) with the given H_{s1}, H_{t1} and $j < n, {}^s v_1$. We get

$\exists H'_t, {}^t v.(H_{t1}, e_t) \Downarrow (H'_t, {}^t v) \wedge ({}^s\theta, n-j, {}^s v_1, {}^t v) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}} \wedge (n-j, H_{s1}, H'_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Since we have $({}^s\theta, n-j, {}^s v_1, {}^t v) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}}$ therefore from Statement(1) we get $({}^s\theta, n-j, {}^s v_1, {}^t v) \in \lfloor\tau'\ \sigma\rfloor_V^{\hat{\beta}}$

□

Theorem 5.18 (Deriving CG NI via compilation)**.** $\forall e_s, {}^s v_1, {}^s v_2, {}^s v'_1, {}^s v'_2, n_1, n_2, H'_{s1}, H'_{s2}$.

let $\mathsf{bool} = (\mathsf{unit} + \mathsf{unit})$.

$x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e_s : \mathbb{C}\ \bot\ \bot\ \mathsf{bool}\ \wedge$

$\emptyset \vdash {}^s v_1 : \mathsf{Labeled}\ \top\ \mathsf{bool} \wedge \emptyset \vdash {}^s v_2 : \mathsf{Labeled}\ \top\ \mathsf{bool}\ \wedge$

$(\emptyset, e_s[{}^s v_1/x]) \Downarrow_{n_1}^f (H'_{s1}, {}^s v'_1)\ \wedge$

$(\emptyset, e_s[{}^s v_2/x]) \Downarrow_{n_2}^f (H'_{s2}, {}^s v'_2)$

$\implies$

${}^s v'_1 = {}^s v'_2$

Proof. From the CG to FG translation we know that $\exists e_t$ s.t

$x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e_s : \mathbb{C}\ \bot\ \bot\ \mathsf{bool} \rightsquigarrow e_t$

Similarly we also know that $\exists {}^t v_1, {}^t v_2$ s.t

$\emptyset \vdash {}^s v_1 : \mathsf{Labeled}\ \top\ \mathsf{bool} \rightsquigarrow {}^t v_1$ and $\emptyset \vdash {}^s v_2 : \mathsf{Labeled}\ \top\ \mathsf{bool} \rightsquigarrow {}^t v_2$ (NI-0)

From type preservation theorem we know that

$x : ((\mathsf{unit} + \mathsf{unit})^\bot + \mathsf{unit})^\top \vdash_\top e_t : (\mathsf{unit} \xrightarrow{\bot} ((\mathsf{unit} + \mathsf{unit})^\bot + \mathsf{unit})^\bot)^\bot$

$\emptyset \vdash_\top {}^t v_1 : ((\mathsf{unit} + \mathsf{unit})^\bot + \mathsf{unit})^\top$

$\emptyset \vdash_\top {}^t v_2 : ((\mathsf{unit} + \mathsf{unit})^\bot + \mathsf{unit})^\top$ (NI-1)

Since we have $\emptyset \vdash {}^s v_1 : \mathsf{Labeled}\ \top\ \mathsf{bool} \rightsquigarrow {}^t v_1$

And since ${}^s v_1$ and ${}^t v_1$ are closed terms (from given and NI-1)

Therefore from Theorem 5.16 we have (we choose n s.t $n > n_1$ and $n > n_2$)

$(\emptyset, n, {}^s v_1, {}^t v_1) \in \lfloor\mathsf{Labeled}\ \top\ \mathsf{bool}\rfloor_E^\emptyset$ (NI-2)

And therefore from Definition 5.12 and (NI-2) we have

$(\emptyset, n, (x \mapsto {}^s v_1), (x \mapsto {}^t v_1)) \in \lfloor x \mapsto \mathsf{Labeled}\ \top\ \mathsf{bool}\rfloor_V^\emptyset$

From (NI-0) we know that $x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e_s : \mathbb{C}\ \bot\ \bot\ \mathsf{bool} \rightsquigarrow e_t$

Therefore we can apply Theorem 5.16 to get

$(\emptyset, n, e_s[{}^s v_1/x], e_t[{}^t v_1/x]) \in \lfloor\mathbb{C}\ \bot\ \bot\ \mathsf{bool}\rfloor_E^\emptyset$ (NI-3.1)

Applying Definition 5.9 on (NI-3.1) we get

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}}{\triangleright} \emptyset \wedge \forall i < n.e_s[{}^s v_1/x] \Downarrow_i {}^s v \implies$

$\exists H'_{t2}, {}^t v.(H_{t2}, e_t[{}^t v_1/x]) \Downarrow (H'_{t2}, {}^t v) \wedge (\emptyset, n-i, {}^s v, {}^t v) \in \lfloor \mathbb{C} \perp \perp \mathsf{bool} \rfloor_V^{\hat{\beta}} \wedge (n-i, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} \emptyset$

Instantiating with $\emptyset, \emptyset$. From cg-val we know that $i = 0$ and ${}^s v = e_s[{}^s v_1/x]$.

Therefore we have

$\exists H'_{t2}, {}^t v.(H_{t2}, e_t[{}^t v_1/x]) \Downarrow (H'_{t2}, {}^t v) \wedge (\emptyset, n, {}^s v, {}^t v) \in \lfloor \mathbb{C} \perp \perp \mathsf{bool} \rfloor_V^{\hat{\beta}} \wedge (n, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} \emptyset$

From translation and from (NI-1) we know that ${}^t v = e_t[{}^t v_1/x] = \lambda\_.e_{b1}$ and therefore from fg-val we have $H'_{t2} = \emptyset$

Therefore we have
$(\emptyset, n, e_s[{}^s v_1/x], \lambda\_.e_{b1}) \in \lfloor \mathbb{C} \perp \perp \mathsf{bool} \rfloor_V^{\emptyset}$

Expanding $(\emptyset, n, e_s[{}^s v_1/x], \lambda\_.e_{b1}) \in \lfloor \mathbb{C} \perp \perp \mathsf{bool} \rfloor_V^{\emptyset}$ using Definition 5.8 we get

$\forall^s \theta_e \sqsupseteq \emptyset, H_{s3}, H_{t3}, i, {}^s v'', k \leq n, \emptyset \sqsubseteq \hat{\beta}'.$
$(k, H_{s3}, H_{t3}) \overset{\hat{\beta}'}{\triangleright} ({}^s \theta_e) \wedge (H_{s3}, e_s[{}^s v_1/x]) \Downarrow_i^f (H'_{s1}, {}^s v''_1) \wedge i < k \implies$
$\exists H''_{t1}, {}^t v'', (H_{t3}, (\lambda\_.e_{b1})()) \Downarrow (H''_{t1}, {}^t v''_1) \wedge \exists^s \theta' \sqsupseteq {}^s \theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H'_{s1}, H''_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s \theta' \wedge \exists^t v'''_1.{}^t v''_1 = \mathsf{inl}\ {}^t v'''_1 \wedge ({}^s \theta', k-i, {}^s v''_1, {}^t v'''_1) \in \lfloor \mathsf{bool} \rfloor_V^{\hat{\beta}''}$

Instantiating with $\emptyset, \emptyset, \emptyset, n_1, {}^s v'_1, n, \emptyset$ we get

$\exists H''_{t1}, {}^t v''.(\emptyset, (\lambda\_.e_{b1})()) \Downarrow (H''_{t1}, {}^t v''_1) \wedge \exists^s \theta' \sqsupseteq \emptyset, \emptyset \sqsubseteq \hat{\beta}''.(n-n_1, H'_{s1}, H''_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s \theta' \wedge \exists^t v'''_1.{}^t v''_1 = \mathsf{inl}\ {}^t v'''_1 \wedge ({}^s \theta', n-n_1, {}^s v'_1, {}^t v'''_1) \in \lfloor \mathsf{bool} \rfloor_V^{\hat{\beta}''}$ (NI-3.2)

Since we have $\exists^t v'''_1.{}^t v''_1 = \mathsf{inl}\ {}^t v'''_1 \wedge ({}^s \theta', n-n_1, {}^s v'_1, {}^t v'''_1) \in \lfloor (\mathsf{unit} + \mathsf{unit}) \rfloor_V^{\hat{\beta}''}$, therefore from Definition 5.8 we know that 2 cases arise

- ${}^s v'_1 = \mathsf{inl}^s v'_{i1}$ and ${}^t v'''_1 = \mathsf{inl}^t v'_{i1}$:
  And from Definition 5.8 we know that
  $({}^s \theta', n-n_1, {}^s v'_{i1}, {}^t v'_{i1}) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}''}$
  which means ${}^s v'_{i1} = {}^t v'_{i1} = ()$
- ${}^s v'_1 = \mathsf{inr}^s v'_{i1}$ and ${}^t v'''_1 = \mathsf{inr}^t v'_{i1}$:
  Same reasoning as in the previous case

Thus no matter which case occurs we have ${}^s v'_1 = {}^t v'''_1$ (NI-3.3)

Similarly we can apply Theorem 5.16 with the other substitution to get
$(\emptyset, n, e_s[{}^s v_2/x], e_t[{}^t v_2/x]) \in \lfloor \mathbb{C} \perp \perp \mathsf{bool} \rfloor_E^{\emptyset}$ (NI-4.1)

Applying Definition 5.9 on (NI-4.1) we get

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}}{\triangleright} \emptyset \wedge \forall i < n, {}^s v_s.e_s[{}^s v_2/x] \Downarrow_i {}^s v_s \implies \exists H'_{t2}, {}^t v_s.(H_{t2}, e_t[{}^t v_2/x]) \Downarrow (H'_{t2}, {}^t v_s) \wedge (\emptyset, n-i, {}^s v_s, {}^t v_s) \in \lfloor \mathbb{C} \perp \perp \mathsf{bool} \rfloor_V^{\hat{\beta}} \wedge (n-i, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} \emptyset$

Instantiating with $\emptyset, \emptyset$. From cg-val we know that $i = 0$ and ${}^s v_s = e_s[{}^s v_2/x]$.

Therefore we have

$\exists H'_{t2}, {}^t v_s.(H_{t2}, e_t[{}^t v_2/x]) \Downarrow (H'_{t2}, {}^t v_s) \wedge (\emptyset, n, {}^s v_s, {}^t v_s) \in \lfloor \mathbb{C} \perp \perp \mathsf{bool} \rfloor_V^{\hat{\beta}} \wedge (n, H_{s2}, H'_{t2}) \overset{\hat{\beta}}{\triangleright} \emptyset$

Also from (NI-1) and from translation we know that ${}^t v = e_t[{}^t v_2/x] = \lambda\_.e_{b2}$ and therefore from fg-val we know that $H'_{t2} = \emptyset$

Therefore we have
$(\emptyset, n, e_s[{}^s v_2/x], \lambda\_.e_{b2}) \in \lfloor \mathbb{C} \perp \perp \mathsf{bool} \rfloor_V^{\emptyset}$

Expanding $(\emptyset, n, e_s[{}^s v_2/x], \lambda x.e_{b2}) \in \lfloor \mathbb{C} \perp \perp \mathsf{bool} \rfloor_V^{\emptyset}$ using Definition 5.8 we get

$\forall^s \theta_e \sqsupseteq \emptyset, H_{s3}, H_{t3}, i, {}^s v'', k \leq n, \emptyset \sqsubseteq \hat{\beta}'.$
$(k, H_{s3}, H_{t3}) \overset{\hat{\beta}'}{\triangleright} ({}^s\theta_e) \wedge (H_{s3}, e_s[{}^s v_2/x]) \Downarrow_i^f (H'_{s2}, {}^s v''_2) \wedge i < k \implies$
$\exists H''_{t2}, {}^t v'', (H_{t3}, (\lambda\_.e_{b2})()) \Downarrow (H''_{t2}, {}^t v''_2) \wedge \exists^s \theta' \sqsupseteq {}^s\theta_e, \hat{\beta}' \sqsubseteq \hat{\beta}''.(k-i, H'_{s2}, H''_{t2}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge \exists^t v'''_2.{}^t v''_2 = \mathsf{inl}\ {}^t v'''_2 \wedge ({}^s\theta', k-i, {}^s v''_1, {}^t v'''_2) \in \lfloor \mathsf{bool} \rfloor_V^{\hat{\beta}''}$

Instantiating with $\emptyset, \emptyset, \emptyset, n_2, {}^s v'_2, n, \emptyset$ we get

$\exists H''_{t2}, {}^t v''.(\emptyset, (\lambda\_.e_{b2})()) \Downarrow (H''_{t2}, {}^t v''_2) \wedge \exists^s \theta' \sqsupseteq \emptyset, \emptyset \sqsubseteq \hat{\beta}''.(n-n_1, H'_{s2}, H''_{t2}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge \exists^t v'''_2.{}^t v''_2 = \mathsf{inl}\ {}^t v'''_2 \wedge ({}^s\theta', n-n_1, {}^s v'_1, {}^t v'''_2) \in \lfloor \mathsf{bool} \rfloor_V^{\hat{\beta}''}$ (NI-4.2)

Since we have $\exists^t v'''_2.{}^t v''_2 = \mathsf{inl}\ {}^t v'''_2 \wedge ({}^s\theta', n-n_1, {}^s v'_2, {}^t v'''_2) \in \lfloor \mathsf{bool} \rfloor_V^{\hat{\beta}''}$, therefore from Definition 5.8 2 cases arise

- ${}^s v'_2 = \mathsf{inl}^s v'_{i2}$ and ${}^t v'''_2 = \mathsf{inl}^t v'_{i2}$:
  And from Definition 5.8 we know that
  $({}^s\theta', n-n_1, {}^s v'_{i2}, {}^t v'_{i2}) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}''}$
  which means ${}^s v'_{i2} = {}^t v'_{i2} = ()$
- ${}^s v'_2 = \mathsf{inr}^s v'_{i2}$ and ${}^t v'''_2 = \mathsf{inr}^t v'_{i2}$:
  Same reasoning as in the previous case

Thus no matter which case occurs we have ${}^s v'_2 = {}^t v'''_2$ (NI-4.3)

From CG to FG translation we know that $\exists^t v_{i1}.{}^t v_1 = \mathsf{inl}\ {}^t v_{i1}$ and similarly $\exists^t v_{i2}.{}^t v_2 = \mathsf{inl}\ {}^t v_{i2}$

From (NI-1) since $\emptyset \vdash_\top {}^t v_1 : (\mathsf{bool}^\perp + \mathsf{unit})^\top$ therefore from CG-inl we know that $\emptyset \vdash_\top {}^t v_{i1} : \mathsf{bool}^\perp$

And from CGsub-sum we know that $\emptyset \vdash_\top {}^t v_{i1} : \mathsf{bool}^\top$
Therefore we also have $\emptyset \vdash_\perp {}^t v_{i1} : \mathsf{bool}^\top$ (NI-5.1)

Similarly we also have $\emptyset \vdash_\perp {}^t v_{i2} : \mathsf{bool}^\top$ (NI-5.2)

Next, let $e_T = (\lambda x : (\mathsf{bool}^\perp + \mathsf{unit})^\top.\mathsf{case}(e_t(), y.y, z.{}^t v_b))\ (\mathsf{case}(u, -.\mathsf{inl}\ true, -.\mathsf{inl}\ false)) : \mathsf{bool}^\perp$
where $true = \mathsf{inl}\ ()$ and $false = \mathsf{inr}\ ()$

We claim $u : \mathsf{bool}^\top \vdash_\perp e_T : \mathsf{bool}^\perp$

To show this we give its typing derivation
P2.3:

$$\dfrac{\dfrac{\dfrac{}{u : \mathsf{bool}^\top, - \vdash_\perp false : \mathsf{bool}^\perp}\ \text{FG-inl}}{u : \mathsf{bool}^\top, - \vdash_\perp \mathsf{inl}\ false : (\mathsf{bool}^\perp + \mathsf{unit})^\perp}\ \text{FG-inl}}{u : \mathsf{bool}^\top, - \vdash_\perp \mathsf{inl}\ false : (\mathsf{bool}^\perp + \mathsf{unit})^\top}\ \text{FGSub-base}$$

P2.2:

$$\dfrac{\dfrac{\overline{u : \mathsf{bool}^{\top}, - \vdash_{\bot} true : \mathsf{bool}^{\bot}}\ \text{FG-inl}}{u : \mathsf{bool}^{\top}, - \vdash_{\bot} \mathsf{inl}\ true : (\mathsf{bool}^{\bot} + \mathsf{unit})^{\bot}}\ \text{FG-inl}}{u : \mathsf{bool}^{\top}, - \vdash_{\bot} \mathsf{inl}\ true : (\mathsf{bool}^{\bot} + \mathsf{unit})^{\top}}\ \text{FGSub-base}$$

P2.1:

$$\overline{u : \mathsf{bool}^{\top} \vdash_{\bot} u : \mathsf{bool}^{\top}}$$

P2:

$$\dfrac{P2.1 \qquad P2.2 \qquad P2.3 \qquad \overline{\mathcal{L} \models (\mathsf{bool}^{\bot} + \mathsf{unit})^{\top} \searrow \bot}}{u : \mathsf{bool}^{\top} \vdash_{\bot} (\mathsf{case}(u, -.\mathsf{inl}\ true, -.\mathsf{inl}\ false)) : (\mathsf{bool}^{\bot} + \mathsf{unit})^{\top}}$$

P1.2:

$$\dfrac{\begin{array}{c}\overline{u : \mathsf{bool}^{\top}, x : (\mathsf{bool}^{\bot} + \mathsf{unit})^{\top} \vdash_{\bot} e_t : (\mathsf{unit} \xrightarrow{\bot} (\mathsf{bool}^{\bot} + \mathsf{unit})^{\bot})^{\bot}}\ \text{NI-1} \\ \overline{u : \mathsf{bool}^{\top}, x : (\mathsf{bool}^{\bot} + \mathsf{unit})^{\top} \vdash_{\bot} () : \mathsf{unit}}\ \text{FG-unit} \\ \overline{\mathcal{L} \models \bot \sqcup \bot \sqsubseteq \bot} \qquad \overline{\mathcal{L} \models (\mathsf{bool}^{\bot} + \mathsf{unit})^{\bot} \searrow \bot}\end{array}}{u : \mathsf{bool}^{\top}, x : (\mathsf{bool}^{\bot} + \mathsf{unit})^{\top} \vdash_{\bot} e_t() : (\mathsf{bool}^{\bot} + \mathsf{unit})^{\bot}}\ \text{FG-app}$$

P1.1:

$$\dfrac{\begin{array}{c}P1.2 \qquad \overline{u : \mathsf{bool}^{\top}, x : (\mathsf{bool}^{\bot} + \mathsf{unit})^{\top}, y : \mathsf{bool}^{\bot} \vdash_{\bot} y : \mathsf{bool}^{\bot}}\ \text{FG-var} \\ \overline{u : \mathsf{bool}^{\top}, x : (\mathsf{bool}^{\bot} + \mathsf{unit})^{\top}, z : \mathsf{unit} \vdash_{\bot} false : \mathsf{bool}^{\bot}}\ \text{FG-var} \qquad \overline{\mathcal{L} \models \mathsf{bool}^{\bot} \searrow \bot}\end{array}}{u : \mathsf{bool}^{\top}, x : (\mathsf{bool}^{\bot} + \mathsf{unit})^{\top} \vdash_{\bot} \mathsf{case}(e_t(), y.y, z.{}^{t}v_b) : \mathsf{bool}^{\bot}}\ \text{FG-case}$$

P1:

$$\dfrac{\dfrac{P1.1}{u : \mathsf{bool}^{\top}, x : (\mathsf{bool}^{\bot} + \mathsf{unit})^{\top} \vdash_{\bot} \mathsf{case}(e_t(), y.y, z.{}^{t}v_b) : \mathsf{bool}^{\bot}}}{u : \mathsf{bool}^{\top} \vdash_{\bot} (\lambda x : (\mathsf{bool}^{\bot} + \mathsf{unit})^{\top}.\mathsf{case}(e_t(), y.y, z.{}^{t}v_b)) : ((\mathsf{bool}^{\bot} + \mathsf{unit})^{\top} \xrightarrow{\bot} \mathsf{bool}^{\bot})^{\bot}}$$

Main derivation:

$$\dfrac{P1 \qquad P2 \qquad \overline{\mathcal{L} \models \bot \sqcup \bot \sqsubseteq \bot} \qquad \overline{\mathcal{L} \models \mathsf{bool}^{\bot} \searrow \bot}}{u : \mathsf{bool}^{\top} \vdash_{\bot} (\lambda x : (\mathsf{bool}^{\bot} + \mathsf{unit})^{\top}.\mathsf{case}(e_t(), y.y, z.{}^{t}v_b))\ (\mathsf{case}(u, -.\mathsf{inl}\ true, -.\mathsf{inl}\ false)) : \mathsf{bool}^{\bot}}\ \text{FG-app}$$

Assuming $e_{b1}()$ reduces in n_{t1} steps in (NI-3.2) and $e_{b2}()$ reduces in n_{t2} steps in (NI-4.2).

We instantiate Theorem 5.38 with $e_T, {}^{t}v_{i1}, {}^{t}v_{i2}$, $n_{t1}+2, n_{t2}+2$, H''_{t1}, H''_{t2} and $\bot$ and therefore from (NI-3.3) and (NI-4.3) we get ${}^{t}v'''_1 = {}^{t}v'''_2$ and thus ${}^{s}v'_1 = {}^{s}v'_2$

□

5.2 FG to CG translation

5.2.1 Type directed (direct) translation from FG to CG

Definition 5.19.

$$
\begin{array}{lcl}
(\!|\mathsf{b}|\!) & = & \mathsf{b} \\
(\!|\mathsf{unit}|\!) & = & \mathsf{unit} \\
(\!|\tau_1 \xrightarrow{\ell_e} \tau_2|\!) & = & (\!|\tau_1|\!) \to \mathbb{C}\ \ell_e\ \bot\ (\!|\tau_2|\!) \\
(\!|\forall\alpha.(\ell_e, \tau)|\!) & = & \forall\alpha.\mathbb{C}\ \ell_e\ \bot\ (\!|\tau|\!) \\
(\!|c \stackrel{\ell_e}{\Rightarrow} \tau)|\!) & = & c \Rightarrow \mathbb{C}\ \ell_e\ \bot\ (\!|\tau|\!) \\
(\!|\tau_1 \times \tau_2|\!) & = & (\!|\tau_1|\!) \times (\!|\tau_2|\!) \\
(\!|\tau_1 + \tau_2|\!) & = & (\!|\tau_1|\!) + (\!|\tau_2|\!) \\
(\!|\mathsf{ref}\ \mathsf{A}^\ell|\!) & = & \mathsf{ref}\ \ell\ (\!|\mathsf{A}|\!) \\
(\!|\mathsf{A}^\ell|\!) & = & \mathsf{Labeled}\ (\ell)\ (\!|\mathsf{A}|\!)
\end{array}
$$

For $\Gamma = x_1 : \tau_1, \ldots, x_n : \tau_n$, define $(\!|\Gamma|\!) = x_1 : (\!|\tau_1|\!), \ldots, x_n : (\!|\tau_n|\!)$.
We use a coersion function defined as follows:

$$
\begin{array}{l}
\texttt{coerce\_taint}\ :\ \mathbb{C}\ pc\ \ell_c\ \tau' \to \mathbb{C}\ pc\ \bot\ \tau' \quad \text{when } \tau' = \mathsf{Labeled}\ \ell_c'\ \tau \text{ and } \ell_c \sqsubseteq \ell_c' \\
\texttt{coerce\_taint} \triangleq \lambda x.\mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y)))
\end{array}
$$

$$
\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash_{pc} x : \tau \rightsquigarrow \mathsf{ret}\ x}\ \text{FC-var}
$$

$$
\frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{\ell_e} e : \tau_2 \rightsquigarrow e_{c1}}{\Sigma; \Psi; \Gamma \vdash_{pc} \lambda x.e : (\tau_1 \xrightarrow{\ell_e} \tau_2)^\bot \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\lambda x.e_{c1}))}\ \text{FC-lam}
$$

$$
\frac{\Sigma, \alpha; \Psi; \Gamma \vdash_{\ell_e} e : \tau \rightsquigarrow e_c}{\Sigma; \Psi; \Gamma \vdash_{pc} \Lambda e : (\forall\alpha.(\ell_e, \tau))^\bot \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\Lambda e_c))}\ \text{FC-FI}
$$

$$
\frac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e : (\forall\alpha.(\ell_e, \tau))^\ell \rightsquigarrow e_c \\ FV(\ell') \subseteq \Sigma \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e[\ell'/\alpha] \qquad \Sigma; \Psi \vdash \tau[\ell'/\alpha] \searrow \ell\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} e\ []: \tau[\ell'/\alpha] \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b[]))))}\ \text{FG-FE}
$$

$$
\frac{\Sigma; \Psi, c; \Gamma \vdash_{\ell_e} e : \tau \rightsquigarrow e_c}{\Sigma; \Psi; \Gamma \vdash_{pc} \nu\ e : (c \stackrel{\ell_e}{\Rightarrow} \tau)^\bot \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\nu e_c))}\ \text{FG-CI}
$$

$$
\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (c \stackrel{\ell_e}{\Rightarrow} \tau)^\ell \rightsquigarrow e_c \qquad \Sigma; \Psi \vdash c \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e \qquad \Sigma; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e \bullet : \tau \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b\bullet))))}\ \text{FG-CE}
$$

$$
\frac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\ell_e} \tau_2)^\ell \rightsquigarrow e_{c1} \\ \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_1 \rightsquigarrow e_{c2} \qquad \mathcal{L} \vdash \ell \sqcup pc \sqsubseteq \ell_e \qquad \mathcal{L} \vdash \tau_2 \searrow \ell\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1\ e_2 : \tau_2 \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b)))))}\ \text{FC-app}
$$

$$
\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : \tau_1 \rightsquigarrow e_{c1} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_2 \rightsquigarrow e_{c2}}{\Sigma; \Psi; \Gamma \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^\bot \rightsquigarrow \mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{ret}(\mathsf{Lb}(a, b))))}\ \text{FC-prod}
$$

$$
\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^\ell \rightsquigarrow e_c \qquad \mathcal{L} \vdash \tau_1 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{fst}(e) : \tau_1 \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))}\ \text{FC-fst}
$$

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^{\ell} \rightsquigarrow e_c \qquad \mathcal{L} \vdash \tau_2 \searrow \ell}{\Sigma;\Psi;\Gamma \vdash_{pc} \mathsf{snd}(e) : \tau_2 \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b))))))}\ \text{FC-snd}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e : \tau_1 \rightsquigarrow e_c}{\Sigma;\Psi;\Gamma \vdash_{pc} \mathsf{inl}(e) : (\tau_1 + \tau_2)^{\perp} \rightsquigarrow \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinl}(a)))}\ \text{FC-inl}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e : \tau_2 \rightsquigarrow e_c}{\Sigma;\Psi;\Gamma \vdash_{pc} \mathsf{inr}(e) : (\tau_1 + \tau_2)^{\perp} \rightsquigarrow \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinr}(a)))}\ \text{FC-inr}$$

$$\frac{\begin{array}{c}\Sigma;\Psi;\Gamma \vdash_{pc} e : (\tau_1 + \tau_2)^{\ell} \rightsquigarrow e_c \\ \Sigma;\Psi;\Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_1 : \tau \rightsquigarrow e_{c1} \qquad \Sigma;\Psi;\Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_2 : \tau \rightsquigarrow e_{c2} \qquad \mathcal{L} \vdash \tau \searrow \ell\end{array}}{\Sigma;\Psi;\Gamma \vdash_{pc} \mathsf{case}(e, x.e_1, y.e_2) : \tau \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2})))))}\ \text{FC-case}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e : \tau \rightsquigarrow e_c \qquad \mathcal{L} \vdash \tau \searrow pc}{\Sigma;\Psi;\Gamma \vdash_{pc} \mathsf{new}\ (e) : (\mathsf{ref}\ \tau)^{\perp} \rightsquigarrow \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb}b)))}\ \text{FC-ref}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e : (\mathsf{ref}\ \tau)^{\ell} \rightsquigarrow e_c \qquad \mathcal{L} \vdash \tau <: \tau' \qquad \mathcal{L} \vdash \tau' \searrow \ell}{\Sigma;\Psi;\Gamma \vdash_{pc} !e : \tau \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))}\ \text{FC-deref}$$

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e_1 : (\mathsf{ref}\ \tau)^{\ell} \rightsquigarrow e_{c1} \qquad \Sigma;\Psi;\Gamma \vdash_{pc} e_2 : \tau \rightsquigarrow e_{c2} \qquad \tau \searrow (pc \sqcup \ell)}{\Sigma;\Psi;\Gamma \vdash_{pc} e_1 := e_2 : \mathsf{unit} \rightsquigarrow \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())}\ \text{FC-assign}$$

5.2.2 Type preservation for FG to CG translation

Theorem 5.20 (Type preservation: FG to CG)**.** *If $\Gamma \vdash_{pc} e : \tau$ in FG then there exists e' such that $\Gamma \vdash_{pc} e : \tau \rightsquigarrow e'$ such that there is a derivation of $(\!|\Gamma|\!) \vdash e' : \mathbb{C}\ pc\ \perp\ (\!|\tau|\!)$ in CG.*

Proof. Proof by induction on the $\rightsquigarrow$ relation

1. FC-var:

$$\frac{}{\Gamma, x : \tau \vdash_{pc} x : \tau \rightsquigarrow \mathsf{ret}\ x}\ \text{FC-var}$$

$$\frac{\dfrac{}{(\!|\Gamma|\!), x : (\!|\tau|\!) \vdash x : (\!|\tau|\!)}\ \text{CG-var}}{(\!|\Gamma|\!), x : (\!|\tau|\!) \vdash \mathsf{ret}\ x : \mathbb{C}\ pc\ \perp\ (\!|\tau|\!)}\ \text{CG-ret}$$

2. FC-lam:

$$\frac{\Gamma, x : \tau_1 \vdash_{\ell_e} e : \tau_2 \rightsquigarrow e_{c1}}{\Gamma \vdash_{pc} \lambda x.e : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\perp} \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\lambda x.e_{c1}))}\ \text{FC-lam}$$

$T_0 = \mathbb{C}\ pc\ \perp\ (\!|(\tau_1 \xrightarrow{\ell_e} \tau_2)^{\perp}|\!) = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \perp\ (\!|(\tau_1 \xrightarrow{\ell_e} \tau_2)|\!)$

$T_1 = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \perp\ (\!|\tau_1|\!) \rightarrow \mathbb{C}\ \ell_e\ \perp\ (\!|\tau_2|\!)$

$T_{1.0} = \mathsf{Labeled}\ \perp\ (\!|\tau_1|\!) \rightarrow \mathbb{C}\ \ell_e\ \perp\ (\!|\tau_2|\!)$

$T_{1.1} = (\!|\tau_1|\!) \to \mathbb{C}\ \ell_e \perp (\!|\tau_2|\!)$

$T_{1.2} = \mathbb{C}\ \ell_e \perp (\!|\tau_2|\!)$

P1:

$$\dfrac{\dfrac{P2}{(\!|\Gamma|\!), x : (\!|\tau_1|\!) \vdash e_{c1} : T_{1.2}}\ \text{IH}}{(\!|\Gamma|\!) \vdash \lambda x.e_{c1} : T_{1.1}}\ \text{CG-lam}$$

Main derivation:

$$\dfrac{\dfrac{P1}{(\!|\Gamma|\!) \vdash (\mathsf{Lb}(\lambda x.e_{c1})) : T_{1.0}}\ \text{CG-label}}{(\!|\Gamma|\!) \vdash \mathsf{ret}(\mathsf{Lb}(\lambda x.e_{c1})) : T_1}\ \text{CG-ret}$$

3. FC-app:

$$\dfrac{\Gamma \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell} \rightsquigarrow e_{c1} \qquad \Gamma \vdash_{pc} e_2 : \tau_1 \rightsquigarrow e_{c2} \qquad \mathcal{L} \vdash \ell \sqcup pc \sqsubseteq \ell_e \qquad \mathcal{L} \vdash \tau_2 \searrow \ell}{\Gamma \vdash_{pc} e_1\ e_2 : \tau_2 \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b)))))}\ \text{FC-app}$$

$T_0 = \mathbb{C}\ pc \perp (\!|(\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell}|\!) = \mathbb{C}\ pc \perp \mathsf{Labeled}\ \ell\ (\!|(\tau_1 \xrightarrow{\ell_e} \tau_2)|\!)$

$T_1 = \mathbb{C}\ pc \perp \mathsf{Labeled}\ \ell\ (\!|\tau_1|\!) \to \mathbb{C}\ \ell_e \perp (\!|\tau_2|\!)$

$T_{1.1} = \mathsf{Labeled}\ \ell\ (\!|\tau_1|\!) \to \mathbb{C}\ \ell_e \perp (\!|\tau_2|\!)$

$T_{1.2} = \mathbb{C} \top \ell\ (\!|\tau_1|\!) \to \mathbb{C}\ \ell_e \perp (\!|\tau_2|\!)$

$T_{1.3} = (\!|\tau_1|\!) \to \mathbb{C}\ \ell_e \perp (\!|\tau_2|\!)$

$T_{1.4} = \mathbb{C}\ \ell_e \perp (\!|\tau_2|\!)$

$T_{1.5} = \mathbb{C}\ \ell_e\ \ell\ (\!|\tau_2|\!)$

$T_{1.6} = \mathbb{C}\ pc\ \ell\ (\!|\mathsf{A}^{\ell_i}|\!)$

$T_{1.7} = \mathbb{C}\ pc\ \ell\ \mathsf{Labeled}\ (\ell_i)\ (\!|\mathsf{A}|\!)$

$T_{1.9} = \mathbb{C}\ pc \perp \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{1.10} = \mathbb{C}\ pc \perp (\!|\tau_2|\!)$

$T_2 = \mathbb{C}\ pc \perp (\!|\tau_1|\!)$

$T_{c4} = \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c3} = \mathbb{C} \top \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c2} = \mathbb{C}\ pc\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c1} = \mathbb{C}\ pc \perp \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c0} = \mathbb{C}\ pc\ \ell\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_c = T_{c0} \to T_{c1}$

Pc2:

$$\dfrac{\dfrac{}{(\!|\Gamma|\!), x : T_{c0}, y : T_{c4} \vdash y : T_{c4}}\ \text{CG-var}}{(\!|\Gamma|\!), x : T_{c0}, y : T_{c4} \vdash \mathsf{unlabel}(y) : T_{c3}}\ \text{CG-unlabel}$$

Pc1:

$$\dfrac{}{(\!|\Gamma|\!), x : T_{c0} \vdash x : T_{c0}}\ \text{CG-var}$$

Pc0:

$$\dfrac{Pc1 \qquad Pc2 \qquad \dfrac{P0}{\mathcal{L} \models \ell \sqsubseteq \ell_i}}{\dfrac{\llparenthesis \Gamma \rrparenthesis, x : T_{c0} \vdash \mathsf{bind}(x, y.\mathsf{unlabel}(y)) : T_{c2}}{\llparenthesis \Gamma \rrparenthesis, x : T_{c0} \vdash \mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_{c1}}\ \text{CG-tolabeled}}\ \text{CG-bind}$$

Pc:

$$\dfrac{\dfrac{Pc0}{\llparenthesis \Gamma \rrparenthesis \vdash \lambda x.\mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_c}\ \text{CG-lam}}{\llparenthesis \Gamma \rrparenthesis \vdash \texttt{coerce\_taint} : T_c}\ \text{From Definition of } \texttt{coerce\_taint}$$

P6:

$$\dfrac{}{\llparenthesis \Gamma \rrparenthesis, a : T_{1.1}, b : \llparenthesis \tau_1 \rrparenthesis, c : T_{1.3} \vdash b : \llparenthesis \tau_1 \rrparenthesis}\ \text{CG-var}$$

P5:

$$\dfrac{}{\llparenthesis \Gamma \rrparenthesis, a : T_{1.1}, b : \llparenthesis \tau_1 \rrparenthesis, c : T_{1.3} \vdash c : T_{1.3}}\ \text{CG-var}$$

P4:

$$\dfrac{\dfrac{P5 \qquad P6}{\llparenthesis \Gamma \rrparenthesis, a : T_{1.1}, b : \llparenthesis \tau_2 \rrparenthesis, c : T_{1.3} \vdash c\ b : T_{1.4}}\ \text{CG-app}}{\llparenthesis \Gamma \rrparenthesis, a : T_{1.1}, b : \llparenthesis \tau_2 \rrparenthesis, c : T_{1.3} \vdash c\ b : T_{1.5}}\ \text{CGSub-monad}$$

P3:

$$\dfrac{}{\llparenthesis \Gamma \rrparenthesis, a : T_{1.1}, b : \llparenthesis \tau_1 \rrparenthesis \vdash a : T_{1.1}}\ \text{CG-var}$$

P2:

$$\dfrac{\dfrac{P3}{\llparenthesis \Gamma \rrparenthesis, a : T_{1.1}, b : \llparenthesis \tau_1 \rrparenthesis \vdash \mathsf{unlabel}\ a : T_{1.2}}\ \text{CG-unlabel} \qquad P4}{\llparenthesis \Gamma \rrparenthesis, a : T_{1.1}, b : \llparenthesis \tau_1 \rrparenthesis \vdash \mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b)) : T_{1.6}}\ \text{CG-bind}$$

P1:

$$\dfrac{\dfrac{}{\llparenthesis \Gamma \rrparenthesis, a : T_{1.1} \vdash e_{c2} : T_2}\ \text{IH2, Weakening} \qquad P2}{\llparenthesis \Gamma \rrparenthesis, a : T_{1.1} \vdash \mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b))) : T_{1.6}}\ \text{CG-bind}$$

P0:

$$\dfrac{\dfrac{}{\mathcal{L} \vdash A^{\ell_i} \searrow \ell}\ \text{Given, } \tau_2 = \mathsf{A}^{\ell_i}}{\mathcal{L} \vdash \ell \sqsubseteq \ell_i}\ \text{By inversion}$$

Main derivation:

$$\dfrac{\dfrac{Pc \qquad \dfrac{\dfrac{}{\llparenthesis \Gamma \rrparenthesis \vdash e_{c1} : T_1}\ \text{IH1} \qquad P1}{\llparenthesis \Gamma \rrparenthesis \vdash \mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b)))) : T_{1.7}}\ \text{CG-bind}}{\llparenthesis \Gamma \rrparenthesis \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b))))) : T_{1.9}}\ \text{CG-app}}{\llparenthesis \Gamma \rrparenthesis \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b))))) : T_{1.10}}\ \text{Definition 5.19}$$

4. FC-FI:

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash_{\ell_e} e : \tau \rightsquigarrow e_c}{\Sigma; \Psi; \Gamma \vdash_{pc} \Lambda e : (\forall \alpha.(\ell_e, \tau))^{\perp} \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\Lambda e_c))} \text{ FC-FI}$$

$T_0 = \mathbb{C}\ pc\ \perp\ (\!|(\forall \alpha.(\ell_e, \tau))^{\perp}|\!) = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \perp\ (\!|(\forall \alpha.(\ell_e, \tau))|\!)$

$T_1 = \mathbb{C}\ pc\ \perp\ (\mathsf{Labeled}\ \perp\ (\forall \alpha.\mathbb{C}\ \ell_e\ \perp\ (\!|\tau|\!)))$

$T_{1.0} = \mathsf{Labeled}\ \perp\ (\forall \alpha.\mathbb{C}\ \ell_e\ \perp\ (\!|\tau|\!))$

$T_{1.1} = \forall \alpha.\mathbb{C}\ \ell_e\ \perp\ (\!|\tau|\!)$

P1:

$$\frac{\dfrac{P2}{\Sigma, \alpha; \Psi; (\!|\Gamma|\!) \vdash e_c : (\!|\tau|\!)} \text{ IH}}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \Lambda e_c : T_{1.1}} \text{ CG-lam}$$

Main derivation:

$$\frac{\dfrac{P1}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \mathsf{Lb}(\Lambda e_c) : T_{1.0}} \text{ CG-label}}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \mathsf{ret}(\mathsf{Lb}(\Lambda e_c)) : T_1} \text{ CG-ret,CG-sub}$$

5. FC-FE:

$$\frac{FV(\ell') \subseteq \Sigma \qquad \begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e : (\forall \alpha.(\ell_e, \tau))^{\ell} \rightsquigarrow e_c \\ \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e[\ell'/\alpha]\end{array} \qquad \Sigma; \Psi \vdash \tau[\ell'/\alpha] \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e\ [] : \tau[\ell'/\alpha] \rightsquigarrow \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b[]))))} \text{ FG-FE}$$

$T_0 = \mathbb{C}\ pc\ \perp\ (\!|(\forall \alpha.(\ell_e, \tau))^{\ell}|\!) = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \ell\ (\!|(\forall \alpha.(\ell_e, \tau))|\!)$

$T_1 = \mathbb{C}\ pc\ \perp\ (\mathsf{Labeled}\ \ell\ (\forall \alpha.\mathbb{C}\ \ell_e\ \perp\ (\!|\tau|\!)))$

$T_{1.1} = (\mathsf{Labeled}\ \ell\ (\forall \alpha.\mathbb{C}\ \ell_e\ \perp\ (\!|\tau|\!)))$

$T_{1.9} = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \ell_i[\ell'/\alpha]\ (\!|\mathsf{A}|\!)[\ell'/\alpha]$

$T_{1.10} = \mathbb{C}\ pc\ \perp\ (\!|\tau[\ell'/\alpha]|\!)$

$T_2 = \mathbb{C}\ \top\ \ell\ (\forall \alpha.\mathbb{C}\ \ell_e\ \perp\ (\!|\tau|\!))$

$T_{2.1} = \forall \alpha.\mathbb{C}\ \ell_e\ \perp\ (\!|\tau|\!)$

$T_{2.2} = (\mathbb{C}\ \ell_e\ \perp\ (\!|\tau|\!))[\ell'/\alpha]$

$T_{2.3} = \mathbb{C}\ \ell_e[\ell'/\alpha]\ \perp\ (\!|\tau|\!)[\ell'/\alpha]$

$T_{2.4} = \mathbb{C}\ pc\ \ell\ (\!|\mathsf{A}^{\ell_i}|\!)[\ell'/\alpha]$

$T_{2.5} = \mathbb{C}\ pc\ \ell\ \mathsf{Labeled}\ (\ell_i[\ell'/\alpha])\ (\!|\mathsf{A}|\!)[\ell'/\alpha]$

$T_{c4} = \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c3} = \mathbb{C}\ \top\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c2} = \mathbb{C}\ pc\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c1} = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c0} = \mathbb{C}\ pc\ \ell\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_c = T_{c0} \to T_{c1}$

Pc2:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!), x : T_{c0}, y : T_{c4} \vdash y : T_{c4}}\ \text{CG-var}}{\Sigma; \Psi; (\!|\Gamma|\!), x : T_{c0}, y : T_{c4} \vdash \mathsf{unlabel}(y) : T_{c3}}\ \text{CG-unlabel}$$

Pc1:

$$\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!), x : T_{c0} \vdash x : T_{c0}}\ \text{CG-var}$$

Pc0:

$$\dfrac{\dfrac{Pc1 \qquad Pc2 \qquad \dfrac{P0}{\mathcal{L} \models \ell \sqsubseteq \ell_i}}{\Sigma; \Psi; (\!|\Gamma|\!), x : T_{c0} \vdash \mathsf{bind}(x, y.\mathsf{unlabel}(y)) : T_{c2}}\ \text{CG-bind}}{\Sigma; \Psi; (\!|\Gamma|\!), x : T_{c0} \vdash \mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_{c1}}\ \text{CG-tolabeled}$$

Pc:

$$\dfrac{\dfrac{Pc0}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \lambda x.\mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_c}\ \text{CG-lam}}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \texttt{coerce\_taint} : T_c}\ \text{From Definition of } \texttt{coerce\_taint}$$

P4:

$$\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!), a : T_{1.1}, b : T_{2.1} \vdash b[] : T_{2.3}}\ \text{CG-FE}$$

P1:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!), a : T_{1.1} \vdash \mathsf{unlabel}\ a : T_2} \qquad P2}{\Sigma; \Psi; (\!|\Gamma|\!), a : T_{1.1} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.(b[])) : T_{2.5}}\ \text{CG-bind}$$

P0:

$$\dfrac{\dfrac{}{\mathcal{L} \vdash A^{\ell_i} \searrow \ell}\ \text{Given, } \tau_2 = \mathsf{A}^{\ell_i}}{\mathcal{L} \vdash \ell \sqsubseteq \ell_i}\ \text{By inversion}$$

Main derivation:

$$\dfrac{\dfrac{Pc \qquad \dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash e_c : T_1}\ \text{IH1} \qquad P1}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash (\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b[])))) : T_{2.5}}\ \text{CG-bind}}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b[])))) : T_{1.9}}\ \text{CG-app}}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b[])))) : T_{1.10}}\ \text{Lemma 5.24 and Def 5.19}$$

6. FC-CI:

$$\dfrac{\Sigma; \Psi, c; \Gamma \vdash_{\ell_e} e : \tau \rightsquigarrow e_c}{\Sigma; \Psi; \Gamma \vdash_{pc} \nu\ e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\perp} \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\nu e_c))}\ \text{FG-CI}$$

$T_0 = \mathbb{C}\ pc \perp (\!|(c \overset{\ell_e}{\Rightarrow} \tau)^{\perp}|\!) = \mathbb{C}\ pc \perp (\mathsf{Labeled} \perp (\!|(c \overset{\ell_e}{\Rightarrow} \tau)|\!))$

$T_1 = \mathbb{C}\ pc\ \bot\ (\textsf{Labeled}\ \bot\ (c \Rightarrow \mathbb{C}\ \ell_e\ \bot\ (\!|\tau|\!)))$

$T_{1.0} = \textsf{Labeled}\ \bot\ (c \Rightarrow \mathbb{C}\ \ell_e\ \bot\ (\!|\tau|\!))$

$T_{1.1} = c \Rightarrow \mathbb{C}\ \ell_e\ \bot\ (\!|\tau|\!)$

P1:

$$\dfrac{\dfrac{P2}{\Sigma; \Psi, c; (\!|\Gamma|\!) \vdash e_c : (\!|\tau|\!)}\ \text{IH}}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \nu e_c : T_{1.1}}\ \text{CG-CI}$$

Main derivation:

$$\dfrac{\dfrac{P1}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \textsf{Lb}(\nu e_c) : T_{1.0}}\ \text{CG-label}}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \textsf{ret}(\textsf{Lb}(\nu e_c)) : T_1}\ \text{CG-ret,CG-sub}$$

7. FC-CE:

$$\dfrac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell} \rightsquigarrow e_c \qquad \Sigma; \Psi \vdash c \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e \qquad \Sigma; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e\ \bullet : \tau \rightsquigarrow \texttt{coerce\_taint}(\textsf{bind}(e_c, a.\textsf{bind}(\textsf{unlabel}\ a, b.(b\bullet))))}\ \text{FG-CE}$$

$T_0 = \mathbb{C}\ pc\ \bot\ (\!|(c \overset{\ell_e}{\Rightarrow} \tau)^{\ell}|\!) = \mathbb{C}\ pc\ \bot\ \textsf{Labeled}\ \ell\ (\!|(c \overset{\ell_e}{\Rightarrow} \tau)|\!)$

$T_1 = \mathbb{C}\ pc\ \bot\ (\textsf{Labeled}\ \ell\ (c \Rightarrow \mathbb{C}\ \ell_e\ \bot\ (\!|\tau|\!)))$

$T_{1.1} = (\textsf{Labeled}\ \ell\ (c \Rightarrow \mathbb{C}\ \ell_e\ \bot\ (\!|\tau|\!)))$

$T_{1.9} = \mathbb{C}\ pc\ \bot\ \textsf{Labeled}\ \ell_i\ (\!|\textsf{A}|\!)$

$T_{1.10} = \mathbb{C}\ pc\ \bot\ (\!|\tau|\!)$

$T_2 = \mathbb{C}\ \top\ \ell\ (c \Rightarrow \mathbb{C}\ \ell_e\ \bot\ (\!|\tau|\!))$

$T_{2.1} = c \Rightarrow \mathbb{C}\ \ell_e\ \bot\ (\!|\tau|\!)$

$T_{2.2} = \mathbb{C}\ \ell_e\ \bot\ (\!|\tau|\!)$

$T_{2.4} = \mathbb{C}\ pc\ \ell\ (\!|\textsf{A}^{\ell_i}|\!)$

$T_{2.5} = \mathbb{C}\ pc\ \ell\ \textsf{Labeled}\ (\ell_i)\ (\!|\textsf{A}|\!)$

$T_{c4} = \textsf{Labeled}\ \ell_i\ (\!|\textsf{A}|\!)$

$T_{c3} = \mathbb{C}\ \top\ \ell_i\ (\!|\textsf{A}|\!)$

$T_{c2} = \mathbb{C}\ pc\ \ell_i\ (\!|\textsf{A}|\!)$

$T_{c1} = \mathbb{C}\ pc\ \bot\ \textsf{Labeled}\ \ell_i\ (\!|\textsf{A}|\!)$

$T_{c0} = \mathbb{C}\ pc\ \ell\ \textsf{Labeled}\ \ell_i\ (\!|\textsf{A}|\!)$

$T_c = T_{c0} \rightarrow T_{c1}$

Pc2:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!), x : T_{c0}, y : T_{c4} \vdash y : T_{c4}}\ \text{CG-var}}{\Sigma; \Psi; (\!|\Gamma|\!), x : T_{c0}, y : T_{c4} \vdash \textsf{unlabel}(y) : T_{c3}}\ \text{CG-unlabel}$$

Pc1:

$$\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!), x : T_{c0} \vdash x : T_{c0}}\ \text{CG-var}$$

Pc0:

$$\dfrac{Pc1 \qquad Pc2 \qquad \dfrac{P0}{\mathcal{L} \models \ell \sqsubseteq \ell_i}}{\dfrac{\Sigma; \Psi; (\!|\Gamma|\!), x : T_{c0} \vdash \mathsf{bind}(x, y.\mathsf{unlabel}(y)) : T_{c2}}{\Sigma; \Psi; (\!|\Gamma|\!), x : T_{c0} \vdash \mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_{c1}} \text{CG-tolabeled}} \text{CG-bind}$$

Pc:

$$\dfrac{\dfrac{Pc0}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \lambda x.\mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_c} \text{CG-lam}}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \mathtt{coerce\_taint} : T_c} \text{From Definition of } \mathtt{coerce\_taint}$$

P4:

$$\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!), a : T_{1.1}, b : T_{2.1} \vdash b\bullet : T_{2.2}} \text{CG-CE}$$

P1:

$$\dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!), a : T_{1.1} \vdash \mathsf{unlabel}\ a : T_2} \qquad P2}{\Sigma; \Psi; (\!|\Gamma|\!), a : T_{1.1} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.(b\bullet)) : T_{2.5}} \text{CG-bind}$$

P0:

$$\dfrac{\dfrac{}{\mathcal{L} \vdash A^{\ell_i} \searrow \ell} \text{Given, } \tau_2 = \mathsf{A}^{\ell_i}}{\mathcal{L} \vdash \ell \sqsubseteq \ell_i} \text{By inversion}$$

Main derivation:

$$\dfrac{\dfrac{Pc \qquad \dfrac{\dfrac{}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash e_c : T_1} \text{IH1} \qquad P1}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b\bullet))) : T_{2.5}} \text{CG-bind}}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b\bullet)))) : T_{1.9}} \text{CG-app}}{\Sigma; \Psi; (\!|\Gamma|\!) \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b\bullet)))) : T_{1.10}} \text{Definition 5.19}$$

8. FC-prod:

$$\dfrac{\Gamma \vdash_{pc} e_1 : \tau_1 \rightsquigarrow e_{c1} \qquad \Gamma \vdash_{pc} e_2 : \tau_2 \rightsquigarrow e_{c2}}{\Gamma \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^{\perp} \rightsquigarrow \mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{ret}(\mathsf{Lb}(a, b))))} \text{FC-prod}$$

$T_1 = \mathbb{C}\ pc\ \perp\ (\!|(\tau_1 \times \tau_2)^{\perp}|\!)$

$T_2 = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \perp\ (\!|(\tau_1 \times \tau_2)|\!)$

$T_3 = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \perp\ (\!|\tau_1|\!) \times (\!|\tau_2|\!)$

$T_{3.1} = \mathsf{Labeled}\ \perp\ (\!|\tau_1|\!) \times (\!|\tau_2|\!)$

$T_4 = \mathbb{C}\ pc\ \perp\ (\!|\tau_1|\!)$

$T_5 = \mathbb{C}\ pc\ \perp\ (\!|\tau_2|\!)$

P4:

$$\dfrac{}{(\!|\Gamma|\!), a : (\!|\tau_1|\!), b : (\!|\tau_1|\!) \vdash a : (\!|\tau_1|\!)} \text{CG-var}$$

P3:

$$\dfrac{}{(\!|\Gamma|\!), a : (\!|\tau_1|\!), b : (\!|\tau_1|\!) \vdash b : (\!|\tau_2|\!)} \text{ CG-var}$$

P2:

$$\dfrac{\dfrac{\dfrac{P3 \qquad P4}{(\!|\Gamma|\!), a : (\!|\tau_1|\!), b : (\!|\tau_1|\!) \vdash (a, b) : (\!|\tau_1|\!) \times (\!|\tau_2|\!)} \text{ CG-prod}}{(\!|\Gamma|\!), a : (\!|\tau_1|\!), b : (\!|\tau_2|\!) \vdash \mathsf{Lb}(a, b) : T_{3.1}} \text{ CG-label}}{(\!|\Gamma|\!), a : (\!|\tau_1|\!), b : (\!|\tau_2|\!) \vdash \mathsf{ret}(\mathsf{Lb}(a, b)) : T_3} \text{ CG-ret}$$

P1:

$$\dfrac{\dfrac{}{(\!|\Gamma|\!), a : (\!|\tau_1|\!) \vdash e_{c2} : T_5} \text{ IH2} \qquad P2}{(\!|\Gamma|\!), a : (\!|\tau_1|\!) \vdash \mathsf{bind}(e_{c2}, b.\mathsf{ret}(\mathsf{Lb}(a, b))) : T_3} \text{ CG-bind}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{}{(\!|\Gamma|\!) \vdash e_{c1} : T_4} \text{ IH1} \qquad P1}{(\!|\Gamma|\!) \vdash \mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{ret}(\mathsf{Lb}(a, b)))) : T_3} \text{ CG-bind}}{(\!|\Gamma|\!) \vdash \mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{ret}(\mathsf{Lb}(a, b)))) : T_1} \text{ Definition 5.19}$$

9. FC-fst:

$$\dfrac{\Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^\ell \rightsquigarrow e_c \qquad \mathcal{L} \vdash \tau_1 \searrow \ell}{\Gamma \vdash_{pc} \mathsf{fst}(e) : \tau_1 \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))} \text{ FC-fst}$$

$T_1 = \mathbb{C}\ pc\ \bot\ (\!|\tau_1|\!)$

$T_2 = \mathbb{C}\ pc\ \bot\ (\!|(\tau_1 \times \tau_2)^\ell|\!)$

$T_{2.1} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell\ (\!|(\tau_1 \times \tau_2)|\!)$

$T_{2.2} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell\ (\!|\tau_1|\!) \times (\!|\tau_2|\!)$

$T_{2.3} = \mathsf{Labeled}\ \ell\ (\!|\tau_1|\!) \times (\!|\tau_2|\!)$

$T_{2.4} = (\!|\tau_1|\!) \times (\!|\tau_2|\!)$

$T_{2.5} = \mathbb{C}\ \top\ \ell\ (\!|\tau_1|\!) \times (\!|\tau_2|\!)$

$T_3 = \mathbb{C}\ \top\ \ell\ (\!|\tau_1|\!)$

$T_{3.1} = \mathbb{C}\ pc\ \ell\ (\!|\tau_1|\!)$

$T_{3.2} = \mathbb{C}\ pc\ \ell\ (\!|\mathsf{A}^{\ell_i}|\!)$

$T_{3.3} = \mathbb{C}\ pc\ \ell\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{3.5} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{3.6} = \mathbb{C}\ pc\ \bot\ (\!|\mathsf{A}^{\ell_i}|\!)$

$T_{c4} = \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c3} = \mathbb{C}\ \top\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c2} = \mathbb{C}\ pc\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c1} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c0} = \mathbb{C}\ pc\ \ell\ \mathsf{Labeled}\ \ell_i\ \llparenthesis \mathsf{A} \rrparenthesis$

$T_c = T_{c0} \to T_{c1}$

Pg:

$$\dfrac{\dfrac{}{\mathcal{L} \vdash A^{\ell_i} \searrow \ell}\ \text{Given, } \tau_1 = \mathsf{A}^{\ell_i}}{\mathcal{L} \vdash \ell \sqsubseteq \ell_i}\ \text{By inversion}$$

Pc2:

$$\dfrac{\dfrac{}{\llparenthesis \Gamma \rrparenthesis, x : T_{c0}, y : T_{c4} \vdash y : T_{c4}}\ \text{CG-var}}{\llparenthesis \Gamma \rrparenthesis, x : T_{c0}, y : T_{c4} \vdash \mathsf{unlabel}(y) : T_{c3}}\ \text{CG-unlabel}$$

Pc1:

$$\dfrac{}{\llparenthesis \Gamma \rrparenthesis, x : T_{c0} \vdash x : T_{c0}}\ \text{CG-var}$$

Pc0:

$$\dfrac{\dfrac{Pc1 \qquad Pc2 \qquad \dfrac{Pg}{\mathcal{L} \models \ell \sqsubseteq \ell_i}}{\llparenthesis \Gamma \rrparenthesis, x : T_{c0} \vdash \mathsf{bind}(x, y.\mathsf{unlabel}(y)) : T_{c2}}\ \text{CG-bind}}{\llparenthesis \Gamma \rrparenthesis, x : T_{c0} \vdash \mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_{c1}}\ \text{CG-tolabeled}$$

Pc:

$$\dfrac{\dfrac{Pc0}{\llparenthesis \Gamma \rrparenthesis \vdash \lambda x.\mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_c}\ \text{CG-lam}}{\llparenthesis \Gamma \rrparenthesis \vdash \texttt{coerce\_taint} : T_c}\ \text{From Definition of } \texttt{coerce\_taint}$$

P2:

$$\dfrac{\dfrac{\dfrac{}{\llparenthesis \Gamma \rrparenthesis, a : T_{2.3}, b : T_{2.4} \vdash b : T_{2.4}}\ \text{CG-var}}{\llparenthesis \Gamma \rrparenthesis, a : T_{2.3}, b : T_{2.4} \vdash \mathsf{fst}(b) : \llparenthesis \tau_1 \rrparenthesis}\ \text{CG-fst}}{\llparenthesis \Gamma \rrparenthesis, a : T_{2.3}, b : T_{2.4} \vdash \mathsf{ret}(\mathsf{fst}(b)) : T_3}\ \text{CG-ret}$$

P1:

$$\dfrac{\dfrac{}{\llparenthesis \Gamma \rrparenthesis, a : T_{2.3} \vdash \mathsf{unlabel}\ (a) : T_{2.5}}\ \text{CG-unlabel} \qquad P2}{\llparenthesis \Gamma \rrparenthesis, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b))) : T_{3.1}}\ \text{CG-bind}$$

P0:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\llparenthesis \Gamma \rrparenthesis \vdash e_c : T_{2.2}}\ \text{IH} \qquad P1}{\llparenthesis \Gamma \rrparenthesis \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))) : T_{3.1}}\ \text{CG-bind}}{\llparenthesis \Gamma \rrparenthesis \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))) : T_{3.2}}}{\llparenthesis \Gamma \rrparenthesis \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))) : T_{3.3}}\ \text{Definition 5.19}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{Pc \qquad P0}{\llparenthesis \Gamma \rrparenthesis \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b))))) : T_{3.5}}\ \text{CG-app}}{\llparenthesis \Gamma \rrparenthesis \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b))))) : T_{3.6}}\ \text{Definition 5.19}}{\llparenthesis \Gamma \rrparenthesis \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b))))) : T_1}$$

10. FC-snd:

$$\frac{\Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^{\ell} \rightsquigarrow e_c \qquad \mathcal{L} \vdash \tau_2 \searrow \ell}{\Gamma \vdash_{pc} \mathsf{snd}(e) : \tau_2 \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b)))))} \text{FC-snd}$$

$T_1 = \mathbb{C}\ pc \perp (\!|\tau_2|\!)$
$T_2 = \mathbb{C}\ pc \perp (\!|(\tau_1 \times \tau_2)^{\ell}|\!)$
$T_{2.1} = \mathbb{C}\ pc \perp \mathsf{Labeled}\ \ell\ (\!|(\tau_1 \times \tau_2)|\!)$
$T_{2.2} = \mathbb{C}\ pc \perp \mathsf{Labeled}\ \ell\ (\!|\tau_1|\!) \times (\!|\tau_2|\!)$
$T_{2.3} = \mathsf{Labeled}\ \ell\ (\!|\tau_1|\!) \times (\!|\tau_2|\!)$
$T_{2.4} = (\!|\tau_1|\!) \times (\!|\tau_2|\!)$
$T_{2.5} = \mathbb{C}\ \top\ \ell\ (\!|\tau_1|\!) \times (\!|\tau_2|\!)$
$T_3 = \mathbb{C}\ \top\ \ell\ (\!|\tau_2|\!)$
$T_{3.1} = \mathbb{C}\ pc\ \ell\ (\!|\tau_2|\!)$
$T_{3.2} = \mathbb{C}\ pc\ \ell\ (\!|\mathsf{A}^{\ell_i}|\!)$
$T_{3.3} = \mathbb{C}\ pc\ \ell\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$
$T_{3.5} = \mathbb{C}\ pc \perp \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$
$T_{3.6} = \mathbb{C}\ pc \perp (\!|\mathsf{A}^{\ell_i}|\!)$
$T_{c4} = \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$
$T_{c3} = \mathbb{C}\ \top\ \ell_i\ (\!|\mathsf{A}|\!)$
$T_{c2} = \mathbb{C}\ pc\ \ell_i\ (\!|\mathsf{A}|\!)$
$T_{c1} = \mathbb{C}\ pc \perp \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$
$T_{c0} = \mathbb{C}\ pc\ \ell\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$
$T_c = T_{c0} \rightarrow T_{c1}$

Pg:

$$\frac{\dfrac{}{\mathcal{L} \vdash A^{\ell_i} \searrow \ell} \text{Given, } \tau_2 = \mathsf{A}^{\ell_i}}{\mathcal{L} \vdash \ell \sqsubseteq \ell_i} \text{By inversion}$$

Pc2:

$$\frac{\dfrac{}{(\!|\Gamma|\!), x : T_{c0}, y : T_{c4} \vdash y : T_{c4}} \text{CG-var}}{(\!|\Gamma|\!), x : T_{c0}, y : T_{c4} \vdash \mathsf{unlabel}(y) : T_{c3}} \text{CG-unlabel}$$

Pc1:

$$\frac{}{(\!|\Gamma|\!), x : T_{c0} \vdash x : T_{c0}} \text{CG-var}$$

Pc0:

$$\frac{\dfrac{Pc1 \qquad Pc2 \qquad \dfrac{Pg}{\mathcal{L} \models \ell \sqsubseteq \ell_i}}{(\!|\Gamma|\!), x : T_{c0} \vdash \mathsf{bind}(x, y.\mathsf{unlabel}(y)) : T_{c2}} \text{CG-bind}}{(\!|\Gamma|\!), x : T_{c0} \vdash \mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_{c1}} \text{CG-tolabeled}$$

Pc:

$$\dfrac{\dfrac{Pc0}{(\!|\Gamma|\!) \vdash \lambda x.\mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_c}\text{CG-lam}}{(\!|\Gamma|\!) \vdash \texttt{coerce\_taint} : T_c}\text{From Definition of } \texttt{coerce\_taint}$$

P2:

$$\dfrac{\dfrac{\dfrac{}{(\!|\Gamma|\!), a : T_{2.3}, b : T_{2.4} \vdash b : T_{2.4}}\text{CG-var}}{(\!|\Gamma|\!), a : T_{2.3}, b : T_{2.4} \vdash \mathsf{snd}(b) : (\!|\tau_2|\!)}\text{CG-snd}}{(\!|\Gamma|\!), a : T_{2.3}, b : T_{2.4} \vdash \mathsf{ret}(\mathsf{snd}(b)) : T_3}\text{CG-ret}$$

P1:

$$\dfrac{\dfrac{}{(\!|\Gamma|\!), a : T_{2.3} \vdash \mathsf{unlabel}\ (a) : T_{2.5}}\text{CG-unlabel} \qquad P2}{(\!|\Gamma|\!), a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b))) : T_{3.1}}\text{CG-bind}$$

P0:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{(\!|\Gamma|\!) \vdash e_c : T_{2.2}}\text{IH} \qquad P1}{(\!|\Gamma|\!) \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b)))) : T_{3.1}}\text{CG-bind}}{(\!|\Gamma|\!) \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b)))) : T_{3.2}}}{(\!|\Gamma|\!) \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b)))) : T_{3.3}}\text{Definition 5.19}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{Pc \qquad P0}{(\!|\Gamma|\!) \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b))))) : T_{3.5}}\text{CG-app}}{(\!|\Gamma|\!) \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b))))) : T_{3.6}}\text{Definition 5.19}}{(\!|\Gamma|\!) \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{snd}(b))))) : T_1}$$

11. FC-inl:

$$\dfrac{\Gamma \vdash_{pc} e : \tau_1 \rightsquigarrow e_c}{\Gamma \vdash_{pc} \mathsf{inl}(e) : (\tau_1 + \tau_2)^{\perp} \rightsquigarrow \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinl}(a)))}\text{FC-inl}$$

$T_1 = \mathbb{C}\ pc \perp (\!|(\tau_1 + \tau_2)^{\perp}|\!)$

$T_{1.1} = \mathbb{C}\ pc \perp \mathsf{Labeled} \perp (\!|(\tau_1 + \tau_2)|\!)$

$T_{1.2} = \mathbb{C}\ pc \perp \mathsf{Labeled} \perp (\!|\tau_1|\!) + (\!|\tau_2|\!)$

$T_{1.3} = \mathsf{Labeled} \perp (\!|\tau_1|\!) + (\!|\tau_2|\!)$

$T_2 = \mathbb{C}\ pc \perp (\!|\tau_1|\!)$

P1:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{(\!|\Gamma|\!), a : (\!|\tau_1|\!) \vdash a : (\!|\tau_1|\!)}\text{CG-var}}{(\!|\Gamma|\!), a : (\!|\tau_1|\!) \vdash \mathsf{inl}(a) : (\!|\tau_1|\!) + (\!|\tau_2|\!)}\text{CG-inl}}{(\!|\Gamma|\!), a : (\!|\tau_1|\!) \vdash \mathsf{Lbinl}(a) : T_{1.3}}\text{CG-label}}{(\!|\Gamma|\!), a : (\!|\tau_1|\!) \vdash \mathsf{ret}(\mathsf{Lbinl}(a)) : T_{1.2}}\text{CG-ret}$$

Main derivation:

$$\dfrac{\dfrac{}{(\!|\Gamma|\!) \vdash e_c : T_2}\text{IH} \qquad P1}{\dfrac{(\!|\Gamma|\!) \vdash \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinl}(a))) : T_{1.2}}{(\!|\Gamma|\!) \vdash \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinl}(a))) : T_1}\text{Definition 5.19}}\text{CG-bind}$$

12. FC-inr:

$$\dfrac{\Gamma \vdash_{pc} e : \tau_2 \rightsquigarrow e_c}{\Gamma \vdash_{pc} \mathsf{inr}(e) : (\tau_1 + \tau_2)^{\perp} \rightsquigarrow \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinr}(a)))}\text{FC-inr}$$

$T_1 = \mathbb{C}\ pc\ \perp\ (\!|(\tau_1 + \tau_2)^{\perp}|\!)$

$T_{1.1} = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \perp\ (\!|(\tau_1 + \tau_2)|\!)$

$T_{1.2} = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \perp\ (\!|\tau_1|\!) + (\!|\tau_2|\!)$

$T_{1.3} = \mathsf{Labeled}\ \perp\ (\!|\tau_1|\!) + (\!|\tau_2|\!)$

$T_2 = \mathbb{C}\ pc\ \perp\ (\!|\tau_2|\!)$

P1:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{(\!|\Gamma|\!), a : (\!|\tau_2|\!) \vdash a : (\!|\tau_2|\!)}\text{CG-var}}{(\!|\Gamma|\!), a : (\!|\tau_2|\!) \vdash \mathsf{inr}(a) : (\!|\tau_1|\!) + (\!|\tau_2|\!)}\text{CG-inr}}{(\!|\Gamma|\!), a : (\!|\tau_2|\!) \vdash \mathsf{Lbinr}(a) : T_{1.3}}\text{CG-label}}{(\!|\Gamma|\!), a : (\!|\tau_2|\!) \vdash \mathsf{ret}(\mathsf{Lbinr}(a)) : T_{1.2}}\text{CG-ret}$$

Main derivation:

$$\dfrac{\dfrac{}{(\!|\Gamma|\!) \vdash e_c : T_2}\text{IH} \qquad P1}{\dfrac{(\!|\Gamma|\!) \vdash \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinr}(a))) : T_{1.2}}{(\!|\Gamma|\!) \vdash \mathsf{bind}(e_c, a.\mathsf{ret}(\mathsf{Lbinr}(a))) : T_1}\text{Definition 5.19}}\text{CG-bind}$$

13. FC-case:

$$\dfrac{\begin{array}{c}\Gamma \vdash_{pc} e : (\tau_1 + \tau_2)^{\ell} \rightsquigarrow e_c \\ \Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_1 : \tau \rightsquigarrow e_{c1} \qquad \Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_2 : \tau \rightsquigarrow e_{c2} \qquad \mathcal{L} \vdash \tau \searrow \ell\end{array}}{\Gamma \vdash_{pc} \mathsf{case}(e, x.e_1, y.e_2) : \tau \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2}))))}\text{FC-case}$$

$T_1 = \mathbb{C}\ pc\ \perp\ (\!|\tau|\!)$

$T_2 = \mathbb{C}\ pc\ \perp\ (\!|(\tau_1 + \tau_2)^{\ell}|\!)$

$T_{2.1} = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \ell\ (\!|\tau_1 + \tau_2|\!)$

$T_{2.2} = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \ell\ ((\!|\tau_1|\!) + (\!|\tau_2|\!))$

$T_{2.3} = \mathsf{Labeled}\ \ell\ ((\!|\tau_1|\!) + (\!|\tau_2|\!))$

$T_{2.4} = \mathbb{C}\ \top\ \ell\ ((\!|\tau_1|\!) + (\!|\tau_2|\!))$

$T_{2.5} = (\!|\tau_1|\!) + (\!|\tau_2|\!)$

$T_3 = \mathbb{C}\ (pc \sqcup \ell)\ \perp\ (\!|\tau|\!)$

$T_4 = \mathbb{C}\ (pc \sqcup \ell)\ \ell\ (\!|\tau|\!)$

$T_5 = \mathbb{C}\ (pc)\ \ell\ (\!|\mathsf{A}^{\ell_i}|\!)$

$T_{5.1} = \mathbb{C}\ (pc)\ \ell\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{5.3} = \mathbb{C}\ (pc)\ (\bot)\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{5.4} = \mathbb{C}\ (pc)\ (\bot)\ (\!|\mathsf{A}^{\ell_i}|\!)$

$T_{c4} = \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c3} = \mathbb{C}\ \top\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c2} = \mathbb{C}\ pc\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c1} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c0} = \mathbb{C}\ pc\ \ell\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_c = T_{c0} \to T_{c1}$

Pg:

$$\dfrac{\dfrac{}{\mathcal{L} \vdash A^{\ell_i} \searrow \ell}\ \text{Given, } \tau = \mathsf{A}^{\ell_i}}{\mathcal{L} \vdash \ell \sqsubseteq \ell_i}\ \text{By inversion}$$

Pc2:

$$\dfrac{\dfrac{}{(\!|\Gamma|\!), x : T_{c0}, y : T_{c4} \vdash y : T_{c4}}\ \text{CG-var}}{(\!|\Gamma|\!), x : T_{c0}, y : T_{c4} \vdash \mathsf{unlabel}(y) : T_{c3}}\ \text{CG-unlabel}$$

Pc1:

$$\dfrac{}{(\!|\Gamma|\!), x : T_{c0} \vdash x : T_{c0}}\ \text{CG-var}$$

Pc0:

$$\dfrac{\dfrac{Pc1 \qquad Pc2 \qquad \dfrac{Pg}{\mathcal{L} \models \ell \sqsubseteq \ell_i}}{(\!|\Gamma|\!), x : T_{c0} \vdash \mathsf{bind}(x, y.\mathsf{unlabel}(y)) : T_{c2}}\ \text{CG-bind}}{(\!|\Gamma|\!), x : T_{c0} \vdash \mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_{c1}}\ \text{CG-tolabeled}$$

Pc:

$$\dfrac{\dfrac{Pc0}{(\!|\Gamma|\!) \vdash \lambda x.\mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_c}\ \text{CG-lam}}{(\!|\Gamma|\!) \vdash \texttt{coerce\_taint} : T_c}\ \text{From Definition of } \texttt{coerce\_taint}$$

P2:

$$\dfrac{\dfrac{}{(\!|\Gamma|\!), a : T_{2.3}, b : T_{2.5} \vdash b : T_{2.5}}\ \text{CG-var} \quad \dfrac{}{(\!|\Gamma|\!), a : T_{2.3}, b : T_{2.5}, x : (\!|\tau_1|\!) \vdash e_{c1} : T_3}\ \text{IH2, Weakening} \quad \dfrac{}{(\!|\Gamma|\!), a : T_{2.3}, b : T_{2.5}, y : (\!|\tau_2|\!) \vdash e_{c2} : T_3}\ \text{IH3, Weakening}}{(\!|\Gamma|\!), a : T_{2.3}, b : T_{2.5} \vdash \mathsf{case}(b, x.e_{c1}, y.e_{c2}) : T_3}\ \text{CG-case}$$

P1:

$$\dfrac{\dfrac{}{(\!|\Gamma|\!), a : T_{2.3} \vdash \mathsf{unlabel}\ a : T_{2.4}}\text{ CG-unlabel} \qquad P2}{\dfrac{(\!|\Gamma|\!), a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2})) : T_3}{(\!|\Gamma|\!), a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2})) : T_4}\text{ CG-sub}}\text{ CG-bind}$$

P0:

$$\dfrac{\dfrac{}{(\!|\Gamma|\!) \vdash e_c : T_{2.2}}\text{ IH1} \qquad P1}{(\!|\Gamma|\!) \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2}))) : T_5}\text{ CG-bind}$$

P0.2:

$$\dfrac{P0}{(\!|\Gamma|\!) \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2}))) : T_{5.1}}\text{ Definition 5.19}$$

P0.1:

$$\dfrac{\dfrac{Pc \qquad P0.2}{(\!|\Gamma|\!) \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2})))) : T_{5.3}}}{(\!|\Gamma|\!) \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2}))))T_{5.4}}\text{ Definition 5.19}$$

Main derivation:

$$\dfrac{P0.1}{(\!|\Gamma|\!) \vdash \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{c1}, y.e_{c2})))) : T_1}$$

14. FC-ref:

$$\dfrac{\Gamma \vdash_{pc} e : \tau \rightsquigarrow e_c \qquad \mathcal{L} \vdash \tau \searrow pc}{\Gamma \vdash_{pc} \mathsf{new}\ (e) : (\mathsf{ref}\ \tau)^{\perp} \rightsquigarrow \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{L}b b)))}\text{ FC-ref}$$

$T_1 = \mathbb{C}\ pc\ \perp\ (\!|(\mathsf{ref}\ \tau)^{\perp}|\!)$

$T_{1.1} = \mathbb{C}\ pc\ \perp\ (\!|(\mathsf{ref}\ \mathsf{A}^{\ell_i})^{\perp}|\!)$

$T_{1.2} = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \perp\ (\!|(\mathsf{ref}\ \mathsf{A}^{\ell_i})|\!)$

$T_{1.3} = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \perp\ \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_2 = \mathbb{C}\ pc\ \perp\ (\!|\tau|\!)$

$T_{2.1} = \mathbb{C}\ pc\ \perp\ (\!|\mathsf{A}^{\ell_i}|\!)$

$T_{2.2} = \mathbb{C}\ pc\ \perp\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{2.3} = \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{2.4} = \mathbb{C}\ pc\ \perp\ \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{2.5} = \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{2.51} = \mathsf{Labeled}\ \perp\ \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)$

P2:

$$\dfrac{\dfrac{\dfrac{}{(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5} \vdash b : T_{2.5}}\text{ CG-var}}{(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5} \vdash \mathsf{L}b b : T_{2.51}}\text{ CG-label}}{(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3}, b : T_{2.5} \vdash \mathsf{ret}(\mathsf{L}b b) : T_{1.3}}\text{ CG-ret}$$

P1:

$$\dfrac{\dfrac{}{(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3} \vdash \mathsf{new}\ (a) : T_{2.4}}\text{CG-new} \qquad P2}{(\!|\Gamma|\!)_{\vec{\beta'}}, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{L}b b)) : T_{1.3}}\text{CG-bind}$$

Main derivation:

$$\dfrac{\dfrac{\dfrac{}{(\!|\Gamma|\!)_{\vec{\beta'}} \vdash e_c : T_{2.2}}\text{IH} \qquad P1}{(\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{L}b b))) : T_{1.3}}\text{CG-bind}}{(\!|\Gamma|\!)_{\vec{\beta'}} \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{L}b b))) : T_1}\text{Definition 5.19}$$

15. FC-deref:

$$\dfrac{\Gamma \vdash_{pc} e : (\mathsf{ref}\ \tau)^{\ell} \rightsquigarrow e_c \qquad \mathcal{L} \vdash \tau <: \tau' \qquad \mathcal{L} \vdash \tau' \searrow \ell}{\Gamma \vdash_{pc} !e : \tau \rightsquigarrow \mathtt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))}\text{FC-deref}$$

$T_1 = \mathbb{C}\ pc\ \bot\ (\!|\tau'|\!)$

$T_{1.1} = \mathbb{C}\ pc\ \bot\ (\!|\mathsf{A}'^{\ell'_i}|\!)$

$T_{1.2} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell'_i\ (\!|\mathsf{A}'|\!)$

$T_2 = \mathbb{C}\ pc\ \bot\ (\!|(\mathsf{ref}\ \tau)^{\ell}|\!)$

$T_{2.1} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell\ (\!|(\mathsf{ref}\ \tau)|\!)$

$T_{2.2} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell\ (\!|(\mathsf{ref}\ \mathsf{A}^{\ell_i})|\!)$

$T_{2.3} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell\ (\mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!))$

$T_{2.4} = \mathsf{Labeled}\ \ell\ (\mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!))$

$T_{2.5} = \mathbb{C}\ \top\ \ell\ (\mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!))$

$T_{2.6} = \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{2.7} = \mathbb{C}\ \top\ \bot\ (\mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!))$

$T_{2.8} = \mathbb{C}\ \top\ \ell\ (\mathsf{Labeled}\ \ell'_i\ (\!|\mathsf{A}'|\!))$

$T_{2.9} = \mathbb{C}\ pc\ \ell\ (\mathsf{Labeled}\ \ell'_i\ (\!|\mathsf{A}'|\!))$

$T_{c4} = \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c3} = \mathbb{C}\ \top\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c2} = \mathbb{C}\ pc\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c1} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{c0} = \mathbb{C}\ pc\ \ell\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_c = T_{c0} \to T_{c1}$

Pg:

$$\dfrac{\dfrac{}{\mathcal{L} \vdash A^{\ell_i} \searrow \ell}\text{Given, } \tau' = \mathsf{A}^{\ell_i}}{\mathcal{L} \vdash \ell \sqsubseteq \ell_i}\text{By inversion}$$

Pc2:

$$\dfrac{\dfrac{}{(\!|\Gamma|\!), x : T_{c0}, y : T_{c4} \vdash y : T_{c4}}\text{CG-var}}{(\!|\Gamma|\!), x : T_{c0}, y : T_{c4} \vdash \mathsf{unlabel}(y) : T_{c3}}\text{CG-unlabel}$$

Pc1:

$$\frac{}{(\!|\Gamma|\!), x : T_{c0} \vdash x : T_{c0}} \text{ CG-var}$$

Pc0:

$$\frac{\frac{Pc1 \qquad Pc2 \qquad \frac{Pg}{\mathcal{L} \models \ell \sqsubseteq \ell_i}}{(\!|\Gamma|\!), x : T_{c0} \vdash \mathsf{bind}(x, y.\mathsf{unlabel}(y)) : T_{c2}} \text{ CG-bind}}{(\!|\Gamma|\!), x : T_{c0} \vdash \mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_{c1}} \text{ CG-tolabeled}$$

Pc:

$$\frac{\frac{Pc0}{(\!|\Gamma|\!) \vdash \lambda x.\mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y))) : T_c} \text{ CG-lam}}{(\!|\Gamma|\!) \vdash \texttt{coerce\_taint} : T_c} \text{ From Definition of } \texttt{coerce\_taint}$$

P2:

$$\frac{\frac{\frac{}{(\!|\Gamma|\!), a : T_{2.4}, b : T_{2.6} \vdash b : T_{2.6}} \text{ CG-var}}{(\!|\Gamma|\!), a : T_{2.4}, b : T_{2.6} \vdash !b : T_{2.7}} \text{ CG-deref}}{(\!|\Gamma|\!), a : T_{2.4}, b : T_{2.6} \vdash !b : T_{2.8}} \text{ CG-sub, Lemma 5.21}$$

P1:

$$\frac{\frac{}{(\!|\Gamma|\!), a : T_{2.4} \vdash \mathsf{unlabel}\ a : T_{2.5}} \text{ CG-unlabel} \qquad P2}{(\!|\Gamma|\!), a : T_{2.4} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.!b) : T_{2.8}} \text{ CG-bind}$$

P0:

$$\frac{\frac{}{(\!|\Gamma|\!) \vdash e_c : T_{2.3}} \qquad P1}{(\!|\Gamma|\!) \vdash \mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)) : T_{2.9}} \text{ CG-bind}$$

Main derivation:

$$\frac{\frac{Pc \qquad P0}{(\!|\Gamma|\!) \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b))) : T_{1.2}} \text{ CG-app}}{(\!|\Gamma|\!) \vdash \texttt{coerce\_taint}(\mathsf{bind}(e_c, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b))) : T_{1.1}} \text{ Definition 5.19}$$

16. FC-assign:

$$\frac{\Gamma \vdash_{pc} e_1 : (\mathsf{ref}\ \tau)^{\ell} \rightsquigarrow e_{c1} \qquad \Gamma \vdash_{pc} e_2 : \tau \rightsquigarrow e_{c2} \qquad \tau \searrow (pc \sqcup \ell)}{\begin{array}{c}\Gamma \vdash_{pc} e_1 := e_2 : \mathsf{unit} \rightsquigarrow \\ \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())\end{array}} \text{ FC-assign}$$

$T_1 = \mathbb{C}\ pc\ \bot\ (\!|\mathsf{unit}|\!)$

$T_{1.1} = \mathbb{C}\ pc\ \bot\ \mathsf{unit}$

$T_2 = \mathbb{C}\ pc\ \bot\ (\!|(\mathsf{ref}\ \tau)^{\ell}|\!)$

$T_{2.1} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell\ (\!|(\mathsf{ref}\ \tau)|\!)$

$T_{2.2} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell\ (\!|(\mathsf{ref}\ \mathsf{A}^{\ell_i})|\!)$

$T_{2.3} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell\ \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{2.4} = \mathsf{Labeled}\ \ell\ \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{2.5} = \mathbb{C}\ \top\ (\ell)\ \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{2.6} = \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{2.7} = \mathbb{C}\ (pc \sqcup \ell)\ \bot\ \mathsf{unit}$

$T_{2.71} = \mathbb{C}\ (pc \sqcup \ell)\ \ell\ \mathsf{unit}$

$T_{2.8} = \mathbb{C}\ pc\ (\ell)\ \mathsf{unit}$

$T_{2.9} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell\ \mathsf{unit}$

$T_3 = \mathbb{C}\ pc\ \bot\ (\!|\tau|\!)$

$T_{3.1} = \mathbb{C}\ pc\ \bot\ (\!|\mathsf{A}^{\ell_i}|\!)$

$T_{3.2} = \mathbb{C}\ pc\ \bot\ \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

$T_{3.3} = \mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!)$

P4:

$$\frac{}{(\!|\Gamma|\!), a : T_{2.4}, b : T_{3.3}, c : T_{2.6} \vdash c : T_{2.6}}\ \text{CG-var}$$

P5:

$$\frac{}{(\!|\Gamma|\!), a : T_{2.4}, b : T_{3.3}, c : T_{2.6} \vdash b : T_{3.3}}\ \text{CG-var}$$

P3:

$$\frac{\dfrac{P4 \qquad P5 \qquad \dfrac{\dfrac{}{\mathcal{L} \vdash \tau \searrow (pc \sqcup \ell)}\ \text{Given}}{\mathcal{L} \vdash (pc \sqcup \ell) \sqsubseteq \ell_i}\ \text{By inversion}}{(\!|\Gamma|\!), a : T_{2.4}, b : T_{3.3}, c : T_{2.6} \vdash c := b : T_{2.7}}\ \text{CG-assign}}{(\!|\Gamma|\!), a : T_{2.4}, b : T_{3.3}, c : T_{2.6} \vdash c := b : T_{2.71}}\ \text{CGsub-monad}$$

P2:

$$\frac{\dfrac{}{(\!|\Gamma|\!), a : T_{2.4}, b : T_{3.3} \vdash \mathsf{unlabel}\ a : T_{2.5}}\ \text{CG-unlabel} \qquad P3}{(\!|\Gamma|\!), a : T_{2.4}, b : T_{3.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, c.c := b) : T_{2.8}}\ \text{CG-bind}$$

P1:

$$\frac{\dfrac{}{(\!|\Gamma|\!), a : T_{2.4} \vdash e_{c2} : T_{3.2}}\ \text{IH2} \qquad P2}{(\!|\Gamma|\!), a : T_{2.4} \vdash \mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b))) : T_{2.8}}\ \text{CG-bind}$$

P0:

$$\frac{\dfrac{}{(\!|\Gamma|\!) \vdash e_{c1} : T_{2.3}}\ \text{IH1} \qquad P1}{(\!|\Gamma|\!) \vdash \mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b))) : T_{2.8}}\ \text{CG-bind}$$

P0.1:

$$\frac{P0}{(\!|\Gamma|\!) \vdash \mathsf{toLabeled}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))) : T_{2.9}}\ \text{CG-toLabeled}$$

Main derivation:

$$\frac{P0.1 \qquad \dfrac{}{(\!|\Gamma|\!), d : \mathsf{Labeled}\ \ell\ \mathsf{unit} \vdash \mathsf{ret}() : T_{1.1}}}{(\!|\Gamma|\!) \vdash \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{c1}, a.\mathsf{bind}(e_{c2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}()) : T_{1.1}}$$

$\square$

Lemma 5.21 (Subtyping - Type preservation)**.** $\forall \Sigma; \Psi$.
The following holds:

1. $\forall \tau, \tau'$.
   $\Sigma; \Psi \vdash \tau <: \tau' \implies \Sigma; \Psi \vdash (\!|\tau|\!) <: (\!|\tau'|\!)$

2. $\forall \mathsf{A}, \mathsf{A}'$.
   $\Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}' \implies \Sigma; \Psi \vdash (\!|\mathsf{A}|\!) <: (\!|\mathsf{A}'|\!)$

Proof. Proof by simultaneous induction on $\tau <: \tau$ and $\mathsf{A} <: \mathsf{A}$

Proof of statement (1)

Let $\tau = \mathsf{A}_1^{\ell_1}$ and $\tau' = \mathsf{A}_2^{\ell_2}$

P2:

$$\dfrac{\dfrac{\dfrac{}{\mathsf{A}_1^{\ell_1} <: \mathsf{A}_2^{\ell_2}}\text{ Given}}{\Sigma; \Psi \vdash \mathsf{A}_1 <: \mathsf{A}_2}\text{ By inversion} \qquad P1}{\Sigma; \Psi \vdash ((\!|\mathsf{A}_1|\!)) <: ((\!|\mathsf{A}_2|\!))}\text{ IH(2) on } \mathsf{A}_1 <: \mathsf{A}_2$$

P1:

$$\dfrac{\dfrac{}{\mathsf{A}_1^{\ell_1} <: \mathsf{A}_2^{\ell_2}}\text{ Given}}{\Sigma; \Psi \vdash \ell_1 \sqsubseteq \ell_2}\text{ By inversion}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad P2}{\Sigma; \Psi \vdash \mathsf{Labeled}\ \ell_1\ ((\!|\mathsf{A}_1|\!)) <: \mathsf{Labeled}\ \ell_2\ ((\!|\mathsf{A}_2|\!))}\text{ CGsub-labeled}}{\Sigma; \Psi \vdash (\!|\mathsf{A}_1^{\ell_1}|\!) <: (\!|\mathsf{A}_2^{\ell_2}|\!)}$$

Proof of statement (2)

We proceed by cases on $\mathsf{A} <: \mathsf{A}$

1. FGsub-base:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{b} <: \mathsf{b}}\text{ CG-refl}}{\Sigma; \Psi \vdash (\!|\mathsf{b}|\!) <: (\!|\mathsf{b}|\!)}\text{ Definition 5.19}$$

2. FGsub-ref:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!) <: \mathsf{ref}\ \ell_i\ (\!|\mathsf{A}|\!)}\text{ CG-refl}}{\Sigma; \Psi \vdash (\!|\mathsf{ref}\ \mathsf{A}^{\ell_i}|\!) <: (\!|\mathsf{ref}\ \mathsf{A}^{\ell_i}|\!)}\text{ Definition 5.19}$$

3. FGsub-prod:

   P1:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}\text{ Given}}{\Sigma; \Psi \vdash \tau_1 <: \tau_1'}\text{ By inversion}}{\Sigma; \Psi \vdash (\!|\tau_1|\!) <: (\!|\tau_1'|\!)}\text{ IH(1) on } \tau_1 <: \tau_1'$$

P2:

$$\dfrac{\dfrac{\overline{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}\ \text{Given}}{\Sigma; \Psi \vdash \tau_2 <: \tau_2'}\ \text{By inversion}}{\Sigma; \Psi \vdash (\!|\tau_2|\!) <: (\!|\tau_2'|\!)}\ \text{IH(1) on } \tau_2 <: \tau_2'$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad P2}{\Sigma; \Psi \vdash (\!|\tau_1|\!) \times (\!|\tau_2|\!) <: (\!|\tau_1'|\!) \times (\!|\tau_2'|\!)}\ \text{CGsub-prod}}{\Sigma; \Psi \vdash (\!|\tau_1 \times \tau_2|\!) <: (\!|\tau_1' \times \tau_2'|\!)}\ \text{Definition 5.19}$$

4. FGsub-sum:

P1:

$$\dfrac{\dfrac{\overline{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'}\ \text{Given}}{\Sigma; \Psi \vdash \tau_1 <: \tau_1'}\ \text{By inversion}}{\Sigma; \Psi \vdash (\!|\tau_1|\!) <: (\!|\tau_1'|\!)}\ \text{IH(1) on } \tau_1 <: \tau_1'$$

P2:

$$\dfrac{\dfrac{\overline{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'}\ \text{Given}}{\Sigma; \Psi \vdash \tau_2 <: \tau_2'}\ \text{By inversion}}{\Sigma; \Psi \vdash (\!|\tau_2|\!) <: (\!|\tau_2'|\!)}\ \text{IH(1) on } \tau_2 <: \tau_2'$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad P2}{\Sigma; \Psi \vdash (\!|\tau_1|\!) + (\!|\tau_2|\!) <: (\!|\tau_1'|\!) + (\!|\tau_2'|\!)}\ \text{CGsub-prod}}{\Sigma; \Psi \vdash (\!|\tau_1 + \tau_2|\!) <: (\!|\tau_1' + \tau_2'|\!)}\ \text{Definition 5.19}$$

5. FGsub-arrow:

$T_1 = (\!|\tau_1|\!) \to \mathbb{C}\ \ell_e \perp (\!|\tau_2|\!)$

$T_2 = (\!|\tau_1'|\!) \to \mathbb{C}\ \ell_e' \perp (\!|\tau_2'|\!)$

P2:

$$\dfrac{\dfrac{\overline{\Sigma; \Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'}\ \text{Given}}{\Sigma; \Psi \vdash \tau_2 <: \tau_2'}\ \text{By inversion, Weakening} \qquad \dfrac{\overline{\Sigma; \Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'}\ \text{Given}}{\Sigma; \Psi \vdash \ell_e' \sqsubseteq \ell_e}\ \text{By inversion, Weakening}}{\Sigma; \Psi \vdash \mathbb{C}\ \ell_e \perp (\!|\tau_2|\!) <: \mathbb{C}\ \ell_e' \perp (\!|\tau_2'|\!)}\ \text{IH(1), CGsub-monad}$$

P1:

$$\dfrac{\dfrac{\overline{\Sigma; \Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'}\ \text{Given}}{\Sigma; \Psi \vdash \tau_1' <: \tau_1}\ \text{By inversion, Weakening}}{\Sigma; \Psi \vdash (\!|\tau_1'|\!) <: (\!|\tau_1|\!)}\ \text{IH(1)}$$

Main derivation:

$$\dfrac{P1 \qquad P2}{\Sigma; \Psi \vdash (\!|\tau_1 \xrightarrow{\ell_e} \tau_2|\!) <: (\!|\tau_1' \xrightarrow{\ell_e'} \tau_2'|\!)} \text{ Definition 5.19}$$

6. FGsub-forall:

P1:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \forall\alpha.(\ell_e, \tau) <: \forall\alpha.(\ell_e', \tau')} \text{ Given}}{\Sigma, \alpha; \Psi \vdash \tau <: \tau'} \text{ By inversion}}{\Sigma, \alpha; \Psi \vdash (\!|\tau|\!) <: (\!|\tau'|\!)} \text{ IH(1)}$$

$$\dfrac{\Sigma, \alpha; \Psi \vdash (\!|\tau|\!) <: (\!|\tau'|\!) \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash \forall\alpha.(\ell_e, \tau) <: \forall\alpha.(\ell_e', \tau')} \text{ Given}}{\Sigma, \alpha; \Psi \vdash \ell_e' \sqsubseteq \ell_e} \text{ By inversion}}{\Sigma, \alpha; \Psi \vdash \mathbb{C}\ \ell_e \perp (\!|\tau|\!) <: \mathbb{C}\ \ell_e' \perp (\!|\tau'|\!)} \text{ CGsub-monad}$$

Main derivation:

$$\dfrac{\dfrac{P1}{\Sigma; \Psi \vdash \forall\alpha.\mathbb{C}\ \ell_e \perp (\!|\tau|\!) <: \forall\alpha.\mathbb{C}\ \ell_e' \perp (\!|\tau'|\!)}}{\Sigma; \Psi \vdash (\!|\forall\alpha.(\ell_e, \tau)|\!) <: (\!|\forall\alpha.(\ell_e', \tau')|\!)} \text{ Definition 5.19}$$

7. FGsub-constraint:

P1:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash c \overset{\ell_e}{\Rightarrow} \tau <: c' \overset{\ell_e'}{\Rightarrow} \tau'} \text{ Given}}{\Sigma; \Psi \vdash \tau <: \tau'} \text{ By inversion}}{\Sigma; \Psi \vdash (\!|\tau|\!) <: (\!|\tau'|\!)} \text{ IH(1)}$$

$$\dfrac{\Sigma; \Psi \vdash (\!|\tau|\!) <: (\!|\tau'|\!) \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash c \overset{\ell_e}{\Rightarrow} \tau <: c' \overset{\ell_e'}{\Rightarrow} \tau'} \text{ Given}}{\Sigma; \Psi \vdash \ell_e' \sqsubseteq \ell_e} \text{ By inversion}}{\Sigma; \Psi \vdash \mathbb{C}\ \ell_e \perp (\!|\tau|\!) <: \mathbb{C}\ \ell_e' \perp (\!|\tau'|\!)} \text{ CGsub-monad}$$

P0:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash c \overset{\ell_e}{\Rightarrow} \tau <: c' \overset{\ell_e'}{\Rightarrow} \tau'} \text{ Given}}{\Sigma; \Psi \vdash c' \implies c} \text{ By inversion}$$

Main derivation:

$$\dfrac{\dfrac{P0 \qquad P1}{\Sigma; \Psi \vdash c \Rightarrow \mathbb{C}\ \ell_e \perp (\!|\tau|\!) <: c' \Rightarrow \mathbb{C}\ \ell_e' \perp (\!|\tau'|\!)}}{\Sigma; \Psi \vdash (\!|c \overset{\ell_e}{\Rightarrow} \tau|\!) <: (\!|c' \overset{\ell_e'}{\Rightarrow} \tau'|\!)} \text{ Definition 5.19}$$

8. FGsub-unit:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}} \text{ CGsub-unit}}{\Sigma; \Psi \vdash (\!|\mathsf{unit}|\!) <: (\!|\mathsf{unit}|\!)} \text{ Definition 5.19}$$

□

Lemma 5.22 (FG $\rightsquigarrow$ CG: Preservation of well-formedness)**.** *Forall* Σ*,* Ψ *the following hold:*

1. $\forall \tau.\ \Sigma; \Psi \vdash \tau\ WF \implies \Sigma; \Psi \vdash (\!|\tau|\!)\ WF$
2. $\forall \mathsf{A}.\ \Sigma; \Psi \vdash \mathsf{A}\ WF \implies \Sigma; \Psi \vdash (\!|\mathsf{A}|\!)\ WF$

Proof. Proof by simulataneous induction on the WF relation of FG

Proof of statement (1)

Let $\tau = \mathsf{A}^{\ell'}$

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash (\!|\mathsf{A}|\!)\ WF}\ \text{IH(2) on } \mathsf{A} \qquad \dfrac{}{\text{FV}(\ell') \in \Sigma}\ \text{By inversion}}{\Sigma; \Psi \vdash \mathsf{Labeled}\ \ell'\ (\!|\mathsf{A}|\!)\ WF}\ \text{CG-wff-labeled}$$

Proof of statement (2)

We proceed by case analyzing the last rule of given WF judgment.

1. FG-wff-base:

$$\dfrac{}{\Sigma; \Psi \vdash \mathsf{b}\ WF}\ \text{CG-wff-base}$$

2. FG-wff-unit:

$$\dfrac{}{\Sigma; \Psi \vdash \mathsf{unit}\ WF}\ \text{CG-wff-unit}$$

3. FG-wff-arrow:

P0:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash (\!|\tau_2|\!)\ WF}\ \text{IH(1) on } \tau_2 \qquad \dfrac{}{\text{FV}(\ell_e) \in \Sigma}\ \text{By inversion}}{\Sigma; \Psi \vdash \mathbb{C}\ \ell_e \perp (\!|\tau_2|\!)\ WF}\ \text{CG-wff-monad}$$

Main derivation:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash (\!|\tau_1|\!)\ WF}\ \text{IH(1) on } \tau_1 \qquad P0}{\Sigma; \Psi \vdash ((\!|\tau_1|\!) \to \mathbb{C}\ \ell_e \perp (\!|\tau_2|\!))\ WF}\ \text{CG-wff-arrow}$$

4. FG-wff-prod:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash (\!|\tau_1|\!)\ WF}\ \text{IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash (\!|\tau_2|\!)\ WF}\ \text{IH(1) on } \tau_2}{\Sigma; \Psi \vdash (\!|\tau_1|\!) \times (\!|\tau_2|\!)\ WF}\ \text{CG-wff-prod}$$

5. FG-wff-sum:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash (\!|\tau_1|\!)\ WF}\ \text{IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash (\!|\tau_2|\!)\ WF}\ \text{IH(1) on } \tau_2}{\Sigma; \Psi \vdash (\!|\tau_1|\!) + (\!|\tau_2|\!)\ WF}\ \text{CG-wff-prod}$$

6. FG-wff-ref:
   Let $\tau = \mathsf{A}^{\ell'}$

$$\dfrac{\dfrac{\dfrac{}{\mathrm{FV}(\mathsf{A}) = \emptyset}\text{ By inversion} \qquad \dfrac{}{\mathrm{FV}(\ell') = \emptyset}\text{ By inversion}}{\mathrm{FV}((\!|\mathsf{A}|\!)) = \emptyset}\text{ Lemma 5.23}}{\Sigma; \Psi \vdash \mathsf{ref}\ \ell'\ (\!|\mathsf{A}|\!)\ WF}\text{ CG-wff-ref}$$

7. FG-wff-forall:

$$\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha; \Psi \vdash (\!|\tau|\!)\ WF}\text{ IH(1) on }\tau \qquad \dfrac{}{\mathrm{FV}(\ell_e) \in \Sigma \cup \{\alpha\}}\text{ By inversion}}{\Sigma, \alpha; \Psi \vdash \mathbb{C}\ \ell_e \perp (\!|\tau|\!)\ WF}\text{ CG-wff-monad}}{\Sigma; \Psi \vdash (\forall \alpha.\mathbb{C}\ \ell_e \perp (\!|\tau|\!))\ WF}\text{ CG-wff-forall}$$

8. FG-wff-constraint:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi, c \vdash (\!|\tau|\!)\ WF}\text{ IH(1) on }\tau \qquad \dfrac{}{\mathrm{FV}(\ell_e) \in \Sigma}\text{ By inversion}}{\Sigma; \Psi, c \vdash \mathbb{C}\ \ell_e \perp (\!|\tau|\!)\ WF}\text{ CG-wff-monad}}{\Sigma; \Psi \vdash c \Rightarrow \mathbb{C}\ \ell_e \perp (\!|\tau|\!)\ WF}\text{ CG-wff-constraint}$$

□

Lemma 5.23 (FG ⇝ CG: Free variable lemma)**.** $\forall \tau, \mathsf{A}$. *The following hold*

1. $FV((\!|\tau|\!)) \subseteq FV(\tau)$
2. $FV((\!|\mathsf{A}|\!)) \subseteq FV(\mathsf{A})$

Proof. Proof by simultaneous induction on τ and A

Proof for (1)

Let $\tau = \mathsf{A}^{\ell_i}$

	$\mathrm{FV}((\!|\mathsf{A}^{\ell_i}|\!))$	
$=$	$\mathrm{FV}(\mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!))$	Definition 5.19
$=$	$\mathrm{FV}(\ell_i) \cup \mathrm{FV}((\!|\mathsf{A}|\!))$	
$\subseteq$	$\mathrm{FV}(\ell_i) \cup \mathrm{FV}(\mathsf{A})$	IH(2) on A
$=$	$\mathrm{FV}(\mathsf{A}^{\ell_i})$	

Proof for (2)

1. $\mathsf{A} = \mathsf{b}$:

	$\mathrm{FV}((\!|\mathsf{b}|\!))$	
$=$	$\mathrm{FV}(\mathsf{b})$	Definition 5.19
$\subseteq$	$\mathrm{FV}(\mathsf{b})$	

2. $\mathsf{A} = \mathsf{unit}$:

	$\mathrm{FV}((\!|\mathsf{unit}|\!))$	
$=$	$\mathrm{FV}(\mathsf{unit})$	Definition 5.19
$\subseteq$	$\mathrm{FV}(\mathsf{unit})$	

3. $\mathsf{A} = \tau_1 \xrightarrow{\ell_e} \tau_2$:

$$\begin{array}{lll} & FV((\!|\tau_1 \xrightarrow{\ell_e} \tau_2|\!)) & \\ = & FV((\!|\tau_1|\!) \rightarrow \mathbb{C}\ \ell_e \perp (\!|\tau_2|\!)) & \text{Definition 5.19} \\ = & FV((\!|\tau_1|\!)) \cup FV(\ell_e) \cup FV((\!|\tau_2|\!)) & \\ \subseteq & FV(\tau_1) \cup FV(\ell_e) \cup FV(\tau_2) & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\ = & FV(\tau_1 \xrightarrow{\ell_e} \tau_2) & \end{array}$$

4. $\mathsf{A} = \tau_1 \times \tau_2$:

$$\begin{array}{lll} & FV((\!|\tau_1 \times \tau_2|\!)) & \\ = & FV((\!|\tau_1|\!) \times (\!|\tau_2|\!)) & \text{Definition 5.19} \\ = & FV((\!|\tau_1|\!)) \cup FV((\!|\tau_2|\!)) & \\ \subseteq & FV(\tau_1) \cup FV(\tau_2) & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\ = & FV(\tau_1 \times \tau_2) & \end{array}$$

5. $\mathsf{A} = \tau_1 + \tau_2$:

$$\begin{array}{lll} & FV((\!|\tau_1 + \tau_2|\!)) & \\ = & FV((\!|\tau_1|\!) + (\!|\tau_2|\!)) & \text{Definition 5.19} \\ = & FV((\!|\tau_1|\!)) \cup FV((\!|\tau_2|\!)) & \\ \subseteq & FV(\tau_1) \cup FV(\tau_2) & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\ = & FV(\tau_1 + \tau_2) & \end{array}$$

6. $\mathsf{A} = \mathsf{ref}\ \tau_i$:

   Let $\tau_i = \mathsf{A}_i^{\ell_i}$

$$\begin{array}{lll} & FV((\!|\mathsf{ref}\ \tau_i|\!)) & \\ = & FV(\mathsf{ref}\ \ell_i\ (\!|\mathsf{A}_i|\!)) & \text{Definition 5.19} \\ = & FV(\ell_i) \cup FV((\!|\mathsf{A}_i|\!)) & \\ \subseteq & FV(\ell_i) \cup FV(\mathsf{A}_i) & \text{IH(2) on } \mathsf{A}_i \\ = & FV(\mathsf{ref}\ \mathsf{A}_i^{\ell_i}) & \\ = & FV(\mathsf{ref}\ \tau_i) & \end{array}$$

7. $\mathsf{A} = \forall \alpha.(\ell_e, \tau_i)$:

$$\begin{array}{lll} & FV((\!|\forall \alpha.(\ell_e, \tau_i)|\!)) & \\ = & FV(\forall \alpha.\mathbb{C}\ \ell_e \perp (\!|\tau_i|\!)) & \text{Definition 5.19} \\ = & FV(\ell_e) \cup FV((\!|\tau_i|\!)) & \\ \subseteq & FV(\ell_e) \cup FV(\tau_i) & \text{IH(1) on } \tau_i \\ = & FV(\forall \alpha.(\ell_e, \tau_i)) & \end{array}$$

8. $\mathsf{A} = c \overset{\ell_e}{\Rightarrow} \tau_i$:

$$\begin{array}{lll} & FV((\!|c \overset{\ell_e}{\Rightarrow} \tau_i|\!)) & \\ = & FV(c) \cup FV(\mathbb{C}\ \ell_e \perp (\!|\tau|\!)) & \text{Definition 5.19} \\ = & FV(c) \cup FV(\ell_e) \cup FV((\!|\tau_i|\!)) & \\ \subseteq & FV(c) \cup FV(\ell_e) \cup FV(\tau_i) & \text{IH(1) on } \tau_i \\ = & FV(c \overset{\ell_e}{\Rightarrow} \tau_i) & \end{array}$$

□

Lemma 5.24 (FG ⇝ CG: Substitution lemma)**.** *$\forall \tau, \mathsf{A}$ s.t $\vdash \tau$ WF and $\vdash \mathsf{A}$ WF. The following hold*

1. $(\!|\tau|\!)[\ell/\alpha] = (\!|(\tau[\ell/\alpha])|\!)$

2. $(\!|\mathsf{A}|\!)[\ell/\alpha] = (\!|\mathsf{A}[\ell/\alpha]|\!)$

Proof. Proof by simultaneous induction on τ and A

Proof for (1)

Let $\tau = \mathsf{A}^{\ell_i}$

$$\begin{array}{lll} & ((\!|\mathsf{A}^{\ell_i}|\!))[\ell/\alpha] & \\ = & (\mathsf{Labeled}\ \ell_i\ (\!|\mathsf{A}|\!))[\ell/\alpha] & \text{Definition 5.19} \\ = & (\mathsf{Labeled}\ \ell_i[\ell/\alpha]\ (\!|\mathsf{A}|\!)[\ell/\alpha]) & \\ = & (\mathsf{Labeled}\ \ell_i[\ell/\alpha]\ (\!|\mathsf{A}[\ell/\alpha]|\!)) & \text{IH(2) on } \mathsf{A} \\ = & (\!|\mathsf{A}[\ell/\alpha]^{\ell_i[\ell/\alpha]}|\!) & \\ = & (\!|\mathsf{A}^{\ell_i}[\ell/\alpha]|\!) & \end{array}$$

Proof for (2)

1. $\mathsf{A} = \mathsf{b}$:

$$\begin{array}{lll} & ((\!|\mathsf{b}|\!))[\ell/\alpha] & \\ = & (\mathsf{b})[\ell/\alpha] & \text{Definition 5.19} \\ = & (\mathsf{b}) & \\ = & (\!|\mathsf{b}|\!) & \\ = & (\!|\mathsf{b}[\ell/\alpha]|\!) & \end{array}$$

2. $\mathsf{A} = \mathsf{unit}$:

$$\begin{array}{lll} & ((\!|\mathsf{unit}|\!))[\ell/\alpha] & \\ = & (\mathsf{unit})[\ell/\alpha] & \text{Definition 5.19} \\ = & (\mathsf{unit}) & \\ = & (\!|\mathsf{unit}|\!) & \\ = & (\!|\mathsf{unit}[\ell/\alpha]|\!) \subseteq & (\mathsf{unit}) \end{array}$$

3. $\mathsf{A} = \tau_1 \xrightarrow{\ell_e} \tau_2$:

$$\begin{array}{lll} & ((\!|\tau_1 \xrightarrow{\ell_e} \tau_2|\!))[\ell/\alpha] & \\ = & ((\!|\tau_1|\!) \to \mathbb{C}\ \ell_e \perp (\!|\tau_2|\!))[\ell/\alpha] & \text{Definition 5.19} \\ = & ((\!|\tau_1|\!)[\ell/\alpha] \to \mathbb{C}\ \ell_e[\ell/\alpha] \perp (\!|\tau_2|\!)[\ell/\alpha]) & \\ = & ((\!|\tau_1[\ell/\alpha]|\!) \to \mathbb{C}\ \ell_e[\ell/\alpha] \perp (\!|\tau_2[\ell/\alpha]|\!)) & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\ = & (\!|(\tau_1[\ell/\alpha] \xrightarrow{\ell_e[\ell/\alpha]} \tau_2[\ell/\alpha])|\!) & \\ = & (\!|(\tau_1 \xrightarrow{\ell_e} \tau_2)[\ell/\alpha]|\!) & \end{array}$$

4. $\mathsf{A} = \tau_1 \times \tau_2$:

$$\begin{array}{lll} & ((\!|\tau_1 \times \tau_2|\!))[\ell/\alpha] & \\ = & ((\!|\tau_1|\!)[\ell/\alpha] \times (\!|\tau_2|\!)[\ell/\alpha]) & \text{Definition 5.19} \\ = & ((\!|\tau_1[\ell/\alpha]|\!) \times (\!|\tau_2[\ell/\alpha]|\!)) & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\ = & (\!|(\tau_1[\ell/\alpha] \times \tau_2[\ell/\alpha])|\!) & \\ = & (\!|(\tau_1 \times \tau_2)[\ell/\alpha]|\!) & \end{array}$$

5. $\mathsf{A} = \tau_1 + \tau_2$:

$$\begin{array}{lll} & ((\!|\tau_1 + \tau_2|\!))[\ell/\alpha] & \\ = & ((\!|\tau_1|\!)[\ell/\alpha] + (\!|\tau_2|\!)[\ell/\alpha]) & \text{Definition 5.19} \\ = & ((\!|\tau_1[\ell/\alpha]|\!) + (\!|\tau_2[\ell/\alpha]|\!)) & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\ = & (\!|(\tau_1[\ell/\alpha] + \tau_2[\ell/\alpha])|\!) & \\ = & (\!|(\tau_1 + \tau_2)[\ell/\alpha]|\!) & \end{array}$$

6. $\mathsf{A} = \mathsf{ref}\ \tau_i$:

Let $\tau_i = \mathsf{A}_i^{\ell_i}$

$$
\begin{array}{lll}
 & ((\!|\mathsf{ref}\ \tau_i|\!))[\ell/\alpha] & \\
= & (\mathsf{ref}\ \ell_i\ (\!|\mathsf{A}_i|\!))[\ell/\alpha] & \text{Definition 5.19} \\
= & (\mathsf{ref}\ \ell_i\ (\!|\mathsf{A}_i|\!)) & \text{Lemma 5.22} \\
= & (\mathsf{ref}\ \mathsf{A}_i^{\ell_i}) & \text{since} \vdash \mathsf{ref}\ \tau_i\ WF \\
= & (\!|(\mathsf{ref}\ \tau_i[\ell/\alpha])|\!) & \\
= & (\!|(\mathsf{ref}\ \tau_i)[\ell/\alpha]|\!) &
\end{array}
$$

7. $\mathsf{A} = \forall\alpha.(\ell_e, \tau_i)$:

$$
\begin{array}{lll}
 & ((\!|\forall\alpha.(\ell_e, \tau_i)|\!))[\ell/\alpha] & \\
= & (\forall\alpha.\mathbb{C}\ \ell_e \perp (\!|\tau_i|\!))[\ell/\alpha] & \text{Definition 5.19} \\
= & (\forall\alpha.\mathbb{C}\ \ell_e[\ell/\alpha] \perp (\!|\tau_i|\!)[\ell/\alpha]) & \\
= & (\forall\alpha.\mathbb{C}\ \ell_e[\ell/\alpha] \perp (\!|\tau_i[\ell/\alpha]|\!)) & \text{IH(1) on } \tau_i \\
= & (\!|(\forall\alpha.(\ell_e[\ell/\alpha], \tau_i[\ell/\alpha]))|\!) & \\
= & (\!|(\forall\alpha.(\ell_e, \tau_i))[\ell/\alpha]|\!) &
\end{array}
$$

8. $\mathsf{A} = c \overset{\ell_e}{\Rightarrow} \tau_i$:

$$
\begin{array}{lll}
 & ((\!|c \overset{\ell_e}{\Rightarrow} \tau_i|\!))[\ell/\alpha] & \\
= & (c \Rightarrow \mathbb{C}\ \ell_e \perp (\!|\tau|\!))[\ell/\alpha] & \text{Definition 5.19} \\
= & c[\ell/\alpha] \Rightarrow (\mathbb{C}\ \ell_e[\ell/\alpha] \perp (\!|\tau|\!)[\ell/\alpha]) & \\
= & c[\ell/\alpha] \Rightarrow (\mathbb{C}\ \ell_e[\ell/\alpha] \perp (\!|\tau[\ell/\alpha]|\!)) & \text{IH(1) on } \tau_i \\
= & (\!|(c \overset{\ell_e}{\Rightarrow} \tau_i)[\ell/\alpha]|\!) &
\end{array}
$$

□

5.2.3 Model for FG to CG translation

Definition 5.25 (${}^s\theta_2$ extends ${}^s\theta_1$). ${}^s\theta_1 \sqsubseteq {}^s\theta_2 \triangleq$
$\forall a \in {}^s\theta_1.{}^s\theta_1(a) = \tau \implies {}^s\theta_2(a) = \tau$

Definition 5.26 ($\hat{\beta}_2$ extends $\hat{\beta}_1$). $\hat{\beta}_1 \sqsubseteq \hat{\beta}_2 \triangleq$
$\forall (a_1, a_2) \in \hat{\beta}_1.(a_1, a_2) \in \hat{\beta}_2$

Definition 5.27 (Unary value relation).

$$
\begin{array}{lcl}
\lfloor \mathsf{b} \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, {}^sv, {}^tv) \mid {}^sv \in [\![\mathsf{b}]\!] \wedge {}^tv \in [\![\mathsf{b}]\!] \wedge {}^sv = {}^tv\} \\
\lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, {}^sv, {}^tv) \mid {}^sv \in [\![\mathsf{unit}]\!] \wedge {}^tv \in [\![\mathsf{unit}]\!]\} \\
\lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, ({}^sv_1, {}^sv_2), ({}^tv_1, {}^tv_2)) \mid \\
 & & ({}^s\theta, m, {}^sv_1, {}^tv_1) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}} \wedge ({}^s\theta, m, {}^sv_2, {}^tv_2) \in \lfloor \tau_2 \rfloor_V^{\hat{\beta}}\} \\
\lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, \mathsf{inl}\ {}^sv, \mathsf{inl}\ {}^tv) \mid ({}^s\theta, m, {}^sv, {}^tv) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}}\} \cup \\
 & & \{({}^s\theta, m, \mathsf{inr}\ {}^sv, \mathsf{inr}\ {}^tv) \mid ({}^s\theta, m, {}^sv, {}^tv) \in \lfloor \tau_2 \rfloor_V^{\hat{\beta}}\} \\
\lfloor \tau_1 \xrightarrow{\ell_e} \tau_2 \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, \lambda x.e_s, \lambda x.e_t) \mid \\
 & & \forall {}^s\theta' \sqsupseteq {}^s\theta, {}^sv, {}^tv, j < m, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, {}^sv, {}^tv) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}'} \implies \\
 & & ({}^s\theta', j, e_s[{}^sv/x], e_t[{}^tv/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}'}\} \\
\lfloor \forall \alpha.(\ell_e, \tau) \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, \Lambda e_s, \Lambda e_t) \mid \\
 & & \forall {}^s\theta' \sqsupseteq {}^s\theta, j < m, \hat{\beta} \sqsubseteq \hat{\beta}', \ell' \in \mathcal{L}.({}^s\theta', j, e_s, e_t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}'}\} \\
\lfloor c \overset{\ell_e}{\Rightarrow} \tau \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, \nu e_s, \nu e_t) \mid \\
 & & \mathcal{L} \models c \implies \forall {}^s\theta' \sqsupseteq {}^s\theta, j < m, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, e_s, e_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}'}\} \\
\lfloor \mathsf{ref}\ \tau \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, a_s, a_t) \mid {}^s\theta(a_s) = \tau \wedge ({}^sa, {}^ta) \in \hat{\beta}\} \\
\lfloor \mathsf{A}^{\ell'} \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, m, {}^sv, \mathsf{Lb}({}^tv)) \mid ({}^s\theta, m, {}^sv, {}^tv) \in \lfloor \mathsf{A} \rfloor_V^{\hat{\beta}}\}
\end{array}
$$

Definition 5.28 (Unary expression relation).

$$
\begin{array}{lcl}
\lfloor \tau \rfloor_E^{\hat{\beta}} & \triangleq & \{({}^s\theta, n, e_s, e_t) \mid \\
 & & \forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv.(H_s, e_s) \Downarrow_i (H_s', {}^sv) \implies \\
 & & \exists H_t', {}^tv.(H_t, e_t) \Downarrow^f (H_t', {}^tv) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \\
 & & \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor \tau \rfloor_V^{\hat{\beta}'}\}
\end{array}
$$

Definition 5.29 (Unary heap well formedness).

$$
\begin{array}{lcl}
(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta & \triangleq & dom({}^s\theta) \subseteq dom(H_s) \wedge \\
 & & \hat{\beta} \subseteq (dom({}^s\theta) \times dom(H_t)) \wedge \\
 & & \forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a_1) \rfloor_V^{\hat{\beta}}
\end{array}
$$

Definition 5.30 (Value substitution). $\delta^s : Var \mapsto Val$, $\delta^t : Var \mapsto Val$

Definition 5.31 (Unary interpretation of Γ).

$$
\begin{array}{lcl}
\lfloor \Gamma \rfloor_V^{\hat{\beta}} & \triangleq & \{({}^s\theta, n, \delta^s, \delta^t) \mid dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t) \wedge \\
 & & \forall x \in dom(\Gamma).({}^s\theta, n, \delta^s(x), \delta^t(x)) \in \lfloor \Gamma(x) \rfloor_V^{\hat{\beta}}\}
\end{array}
$$

5.2.4 Soundness proof for FG to CG translation

Lemma 5.32 (Monotonicity). $\forall {}^s\theta, {}^s\theta', n, {}^sv, {}^tv, n', \beta, \beta'$.

1. $\forall \mathsf{A}.\ ({}^s\theta, n, {}^sv, {}^tv) \in \lfloor \mathsf{A} \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n \implies ({}^s\theta', n', {}^sv, {}^tv) \in \lfloor \mathsf{A} \rfloor_V^{\hat{\beta}'}$

2. $\forall \tau.\ ({}^s\theta, n, {}^sv, {}^tv) \in \lfloor \tau \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n \implies ({}^s\theta', n', {}^sv, {}^tv) \in \lfloor \tau \rfloor_V^{\hat{\beta}'}$

Proof. Proof by simultaneous induction on A and τ

Proof of statement (1)

We case analyze A in the last step

1. Case b:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{b} \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{b} \rfloor_V^{\hat{\beta}'}$

   Since $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{b} \rfloor_V^{\hat{\beta}}$ therefore from Definition 5.27 we know that ${}^s v \in [\![\mathsf{b}]\!] \wedge {}^t v \in [\![\mathsf{b}]\!]$ and ${}^s v = {}^t v$

   Therefore from Definition 5.27 we get the desired

2. Case unit:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}'}$

   Since $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}}$ therefore from Definition 5.27 we know that ${}^s v \in [\![\mathsf{unit}]\!] \wedge {}^t v \in [\![\mathsf{unit}]\!]$

   Therefore from Definition 5.27 we get the desired

3. Case $\tau_1 \times \tau_2$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}'}$

   From Definition 5.27 we know that ${}^s v = ({}^s v_1, {}^s v_2)$ and ${}^t v = ({}^t v_1, {}^t v_2)$.

   We also know that $({}^s\theta, n, {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}}$ and $({}^s\theta, n, {}^s v_2, {}^t v_2) \in \lfloor \tau_2 \rfloor_V^{\hat{\beta}}$

   IH1: $({}^s\theta', n', {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}'}$ (From Statement (2))

   IH2: $({}^s\theta', n', {}^s v_2, {}^t v_2) \in \lfloor \tau_2 \rfloor_V^{\hat{\beta}'}$ (From Statement (2))

   Therefore from Definition 5.27, IH1 and IH2 we get

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 \times \tau_2 \rfloor_V^{\hat{\beta}'}$

4. Case $\tau_1 + \tau_2$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}'}$

   From Definition 5.27 two cases arise

   (a) ${}^s v = \mathsf{inl}({}^s v')$ and ${}^t v = \mathsf{inl}({}^t v')$:
   IH: $({}^s\theta', n', {}^s v', {}^t v') \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}'}$ (From Statement (2))
   Therefore from Definition 5.27 and IH we get
   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 + \tau_2 \rfloor_V^{\hat{\beta}'}$

   (b) ${}^s v = \mathsf{inr}({}^s v')$ and ${}^t v = \mathsf{inr}({}^t v')$:
   Symmetric reasosning as in the previous case

5. Case $\tau_1 \xrightarrow{\ell_e} \tau_2$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau_1 \xrightarrow{\ell_e} \tau_2 \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \tau_1 \xrightarrow{\ell_e} \tau_2 \rfloor_V^{\hat{\beta}'}$

   From Definition 5.27 we know that

   ${}^s v$ is of the form $\lambda x.e_s$ (for some e_s) and ${}^t v$ is of the form $\lambda x.e_t$ (for some e_t) s.t

   $\forall {}^s\theta' \sqsupseteq {}^s\theta, {}^s v_1, {}^t v_1, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'_1.({}^s\theta', j, {}^s v_1, {}^t v_1) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}'_1} \implies$
   $({}^s\theta', j, e_s[{}^s v_1/x], e_t[{}^t v_1/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}'_1}$ (A0)

   Similarly from Definition 5.27 we are required to prove

   $\forall {}^s\theta'' \sqsupseteq {}^s\theta', {}^s v_2, {}^t v_2, k < n', \hat{\beta}' \sqsubseteq \hat{\beta}''.({}^s\theta'', k, {}^s v_2, {}^t v_2) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}''} \implies$
   $({}^s\theta'', k, e_s[{}^s v_2/x], e_t[{}^t v_2/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}''}$

   This means we are given some

   ${}^s\theta'' \sqsupseteq {}^s\theta', {}^s v_2, {}^t v_2, k < n', \hat{\beta}' \sqsubseteq \hat{\beta}''$ s.t $({}^s\theta'', k, {}^s v_2, {}^t v_2) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}''}$
   and we are required to prove

   $({}^s\theta'', k, e_s[{}^s v_2/x], e_t[{}^t v_2/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}''}$

   Instantiating (A0) with ${}^s\theta'', {}^s v_2, {}^t v_2, k, \hat{\beta}''$ since
   ${}^s\theta'' \sqsupseteq {}^s\theta' \sqsupseteq {}^s\theta$, $k < n' < n$ and $\hat{\beta} \sqsubseteq \hat{\beta}' \sqsubseteq \hat{\beta}''$ therefore we get
   $({}^s\theta'', k, e_s[{}^s v_2/x], e_t[{}^t v_2/x]) \in \lfloor \tau_2 \rfloor_E^{\hat{\beta}''}$

6. Case $\forall \alpha.(\ell_e, \tau)$:

Given:

$({}^s\theta, n, {}^sv, {}^tv) \in \lfloor \forall \alpha.(\ell_e, \tau) \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

To prove:

$({}^s\theta', n', {}^sv, {}^tv) \in \lfloor \forall \alpha.(\ell_e, \tau) \rfloor_V^{\hat{\beta}'}$

From Definition 5.27 we know that

${}^sv$ is of the form Λe_s (for some e_s) and ${}^tv$ is of the form Λe_t (for some e_t) s.t

$$\forall {}^s\theta' \sqsupseteq {}^s\theta, {}^sv_1, {}^tv_1, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'_1, \ell' \in \mathcal{L}.({}^s\theta', j, e_s, e_t) \in \lfloor \tau[\ell'/\alpha] \rfloor_E^{\hat{\beta}'_1} \quad \text{(F0)}$$

Similarly from Definition 5.27 we are required to prove

$\forall {}^s\theta'' \sqsupseteq {}^s\theta', {}^sv_2, {}^tv_2, k < n', \hat{\beta}' \sqsubseteq \hat{\beta}'', \ell'' \in \mathcal{L}.({}^s\theta'', k, e_s, e_t) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\hat{\beta}''}$

This means we are given some

${}^s\theta'' \sqsupseteq {}^s\theta', {}^sv_2, {}^tv_2, k < n', \hat{\beta}' \sqsubseteq \hat{\beta}'', \ell'' \in \mathcal{L}$

and we are required to prove

$({}^s\theta'', k, e_s, e_t) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\hat{\beta}''}$

Instantiating (F0) with ${}^s\theta'', {}^sv_2, {}^tv_2, k, \hat{\beta}'', \ell''$ since

${}^s\theta'' \sqsupseteq {}^s\theta' \sqsupseteq {}^s\theta$, $k < n' < n$ and $\hat{\beta} \sqsubseteq \hat{\beta}' \sqsubseteq \hat{\beta}''$ therefore we get

$({}^s\theta'', k, e_s, e_t) \in \lfloor \tau[\ell''/\alpha] \rfloor_E^{\hat{\beta}''}$

7. Case $c \stackrel{\ell_e}{\Rightarrow} \tau$:

Given:

$({}^s\theta, n, {}^sv, {}^tv) \in \lfloor c \stackrel{\ell_e}{\Rightarrow} \tau \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

To prove:

$({}^s\theta', n', {}^sv, {}^tv) \in \lfloor c \stackrel{\ell_e}{\Rightarrow} \tau \rfloor_V^{\hat{\beta}'}$

From Definition 5.27 we know that

${}^sv$ is of the form νe_s (for some e_s) and ${}^tv$ is of the form νe_t (for some e_t) s.t

$$\forall {}^s\theta' \sqsupseteq {}^s\theta, {}^sv_1, {}^tv_1, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'_1.\mathcal{L} \models c \implies ({}^s\theta', j, e_s, e_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}'_1} \quad \text{(C0)}$$

Similarly from Definition 5.27 we are required to prove

$\forall {}^s\theta'' \sqsupseteq {}^s\theta', {}^sv_2, {}^tv_2, k < n', \hat{\beta}' \sqsubseteq \hat{\beta}''.\mathcal{L} \models c \implies ({}^s\theta'', k, e_s, e_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}''}$

This means we are given some

${}^s\theta'' \sqsupseteq {}^s\theta', {}^sv_2, {}^tv_2, k < n', \hat{\beta}' \sqsubseteq \hat{\beta}''$ s.t $\mathcal{L} \models c$

and we are required to prove

$({}^s\theta'', k, e_s, e_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}''}$

Instantiating (C0) with ${}^s\theta'', {}^s v_2, {}^t v_2, k, \hat{\beta}''$ since
${}^s\theta'' \sqsupseteq {}^s\theta' \sqsupseteq {}^s\theta$, $k < n' < n$ and $\hat{\beta} \sqsubseteq \hat{\beta}' \sqsubseteq \hat{\beta}''$ therefore we get
$({}^s\theta'', k, e_s, e_t) \in \lfloor \tau \rfloor_E^{\hat{\beta}''}$

8. Case $\mathsf{ref}\ \tau$:

   Given:

   $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{ref}\ \tau \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

   To prove:

   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{ref}\ \tau \rfloor_V^{\hat{\beta}'}$

   From Definition 5.27 we know that ${}^s v = a_s$ and ${}^t v = a_t$. We also know that ${}^s\theta(a_s) = \tau \wedge (a_s, a_t) \in \hat{\beta}$

   From Definition 5.27, Definition 5.25 and Definition 5.26 we get
   $({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{ref}\ \tau \rfloor_V^{\hat{\beta}'}$

Proof of Statement (2)
Let $\tau = \mathsf{A}^{\ell''}$:

Given:
$({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \mathsf{A}^{\ell''} \rfloor_V^{\hat{\beta}} \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \wedge n' < n$

From Definition 5.27 we know that
$\exists {}^t v_i . {}^t v = \mathsf{Lb}({}^t v_i)$ and $({}^s\theta, n, {}^s v, {}^t v_i) \in \lfloor \mathsf{A} \rfloor_V^{\hat{\beta}}$

To prove:
$({}^s\theta', n', {}^s v, {}^t v) \in \lfloor \mathsf{A}^{\ell''} \rfloor_V^{\hat{\beta}'}$

This means from Definition 5.27 we need to prove
$({}^s\theta', n', {}^s v, {}^t v_i) \in \lfloor \mathsf{A} \rfloor_V^{\hat{\beta}'}$

IH: $({}^s\theta', n', {}^s v, {}^t v_i) \in \lfloor \mathsf{A} \rfloor_V^{\hat{\beta}'}$ (From Statement (1))

Therefore we get the desired directly from IH.

□

Lemma 5.33 (Unary monotonicity for Γ)**.** $\forall \theta, \theta', \delta, \Gamma, n, n', \hat{\beta}, \hat{\beta}'$.
$(\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}} \wedge n' < n \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}' \implies (\theta', n', \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}'}$

Proof. Given: $(\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}} \wedge n' < n \wedge {}^s\theta \sqsubseteq {}^s\theta' \wedge \hat{\beta} \sqsubseteq \hat{\beta}'$
To prove: $(\theta', n', \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}'}$

From Definition 5.31 it is given that
$dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t) \wedge \forall x_i \in dom(\Gamma).({}^s\theta, n, \delta^s(x_i), \delta^t(x_i)) \in \lfloor \Gamma(x_i) \rfloor_V^{\hat{\beta}}$

And again from Definition 5.31 we are required to prove that
$dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t) \wedge \forall x_i \in dom(\Gamma).({}^s\theta', n', \delta^s(x_i), \delta^t(x_i)) \in \lfloor \Gamma(x_i) \rfloor_V^{\hat{\beta}'}$

- $dom(\Gamma) \subseteq dom(\delta^s) \wedge dom(\Gamma) \subseteq dom(\delta^t)$:

  Given

- $\forall x_i \in dom(\Gamma).({}^s\theta', n', \delta^s(x_i), \delta^t(x_i)) \in \lfloor \Gamma(x_i) \rfloor_V^{\hat{\beta}'}$:

  Since we know that $\forall x_i \in dom(\Gamma).({}^s\theta, n, \delta^s(x_i), \delta^t(x_i)) \in \lfloor \Gamma(x_i) \rfloor_V^{\hat{\beta}}$ (given)

  Therefore from Lemma 5.32 we get

  $\forall x_i \in dom(\Gamma).({}^s\theta', n', \delta^s(x_i), \delta^t(x_i)) \in \lfloor \Gamma(x_i) \rfloor_V^{\hat{\beta}'}$

□

Lemma 5.34 (Unary monotonicity for H)**.** $\forall {}^s\theta, H_s, H_t, n, n', \hat{\beta}$.
$(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge n' < n \implies (n', H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$

Proof. Given: $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge n' < n$

To prove: $(n', H_s, H_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta$

From Definition 5.29 it is given that
$dom({}^s\theta) \subseteq dom(H_S) \wedge \hat{\beta} \subseteq (dom({}^s\theta) \times dom(H_t)) \wedge \forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$

And again from Definition 5.29 we are required to prove that
$dom({}^s\theta) \subseteq dom(H_S) \wedge \hat{\beta} \subseteq (dom({}^s\theta) \times dom(H_t)) \wedge \forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n'-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$

- $dom({}^s\theta) \subseteq dom(H_S)$:

  Given

- $\hat{\beta} \subseteq (dom({}^s\theta) \times dom(H_t))$:

  Given

- $\forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n'-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$:

  Since we know that $\forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$ (given)

  Therefore from Lemma 5.32 we get

  $\forall (a_1, a_2) \in \hat{\beta}.({}^s\theta, n'-1, H_s(a_1), H_t(a_2)) \in \lfloor {}^s\theta(a) \rfloor_V^{\hat{\beta}}$

□

Lemma 5.35 (Coercion lemma)**.** $\forall H, e, v$.
$(H, e) \Downarrow_{-}^{f} (H', \mathsf{Lb}\, v) \implies$
$(H, \texttt{coerce\_taint}\ e) \Downarrow_{-}^{f} (H', \mathsf{Lb}\, v)$

Proof. Given: $(H, e) \Downarrow_{-}^{f} (H', \mathsf{Lb}\, v)$

To prove: $(H, \texttt{coerce\_taint}\ e) \Downarrow_{-}^{f} (H', \mathsf{Lb}\, v)$

From Definition of `coerce_taint`and cg-app it suffices to prove that
$(H, \mathsf{toLabeled}(\mathsf{bind}(e, y.\mathsf{unlabel}(y)))) \Downarrow_{-}^{f} (H', \mathsf{Lb}\, v)$

From cg-tolabeled it suffices to prove that
$(H, \mathsf{bind}(e, y.\mathsf{unlabel}(y))) \Downarrow^f_- (H', v)$

From cg-bind it suffices to prove that

1. $(H, e) \Downarrow^f_- (H'_1, v_1)$:

   We are given that $(H, e) \Downarrow^f_- (H', v)$ therefore we have $H'_1 = H'$ and $v'_1 = \mathsf{Lb}\, v$

2. $(H'_1, \mathsf{unlabel}(y)[v_1/y]) \Downarrow^f_- (H', v)$:
   It sufffices to prove that
   $(H', \mathsf{unlabel}(\mathsf{Lb}\, v)) \Downarrow^f_- (H', v)$:
   We get this directly from cg-unlabel

□

Theorem 5.36 (Fundamental theorem)**.** $\forall \Sigma, \Psi, \Gamma, \tau, e_s, e_t, pc, \mathcal{L}, \delta^s, \delta^t, \sigma, {}^s\theta, n, \hat{\beta}$.
$\Sigma; \Psi; \Gamma \vdash_{pc} e_s : \tau \rightsquigarrow e_t \wedge$
$\mathcal{L} \models \Psi\ \sigma \wedge ({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma\ \sigma \rfloor_V^{\hat{\beta}}$
$\Longrightarrow$
$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

Proof. Proof by induction on the $\rightsquigarrow$ relation

1. FC-var:

$$\frac{}{\Gamma, x : \tau \vdash_{pc} x : \tau \rightsquigarrow \mathsf{ret}\ x}\ \text{FC-var}$$

   Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor (\Gamma \cup \{x \mapsto \tau\})\ \sigma \rfloor_V^{\hat{\beta}}$

   To prove: $({}^s\theta, n, x\ \delta^s, \mathsf{ret}(x)\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

   From Definition 5.28 it suffices to prove that

   $\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, x\ \delta^s) \Downarrow_i (H'_s, {}^s v) \implies$
   $\exists H'_t, {}^t v.(H_t, \mathsf{ret}(x)\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge$
   $({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$

   This means given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^s v$ s.t $(H_s, x\ \delta^s) \Downarrow_i (H'_s, {}^s v)$
   From fg-val we know that $i = 0$, ${}^s v = x\ \delta^s$. Also from cg-ret we know that ${}^t v = x\ \delta^t$ and $H'_t = H_t$

   And we are required to prove

   $$\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsubseteq \hat{\beta}.(n, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'} \qquad \text{(F-V0)}$$

   We choose ${}^s\theta'$ as ${}^s\theta$ and $\hat{\beta}'$ as $\hat{\beta}$

(a) $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$: Given

(b) $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}}$:

Since we are given $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor (\Gamma \cup \{x \mapsto \tau\})\ \sigma \rfloor_V^{\hat{\beta}}$, therefore from Definition 5.31 we get $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}}$

2. FC-lam:

$$\frac{\Gamma, x : \tau_1 \vdash_{\ell_e} e_s : \tau_2 \leadsto e_t}{\Gamma \vdash_{pc} \lambda x.e_s : (\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp \leadsto \mathsf{ret}(\mathsf{Lb}\lambda x.e_t)} \text{FC-lam}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, (\lambda x.e_s)\ \delta^s, \mathsf{ret}(\mathsf{Lb}\lambda x.e_t)\ \delta^t) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 5.28 it suffices to prove

$$\begin{aligned}
&\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, (\lambda x.e_s)\ \delta^s) \Downarrow_i (H_s', {}^s v) \implies \\
&\exists H_t', {}^t v.(H_t, \mathsf{ret}(\mathsf{Lb}(\lambda x.e_t)))\ \delta^t) \Downarrow^f (H_t', {}^t v) \wedge \\
&\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}
\end{aligned}$$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $(H_s, (\lambda x.e_s)\ \delta^s) \Downarrow_i (H_s', {}^s v)$

From fg-val we know that ${}^s v = (\lambda x.e_s)\ \delta^s$, $H_s' = H_s$ and $i = 0$. Also from cg-ret, cg-label and cg-FI we know that $H_t' = H_t$ and ${}^t v = (\mathsf{Lb}(\lambda x.e_t))\ \delta^t$

It suffices to prove that

$$\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n, H_s, H_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n, {}^s v, {}^t v) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$$

We choose ${}^s\theta'$ as ${}^s\theta$ and $\hat{\beta}'$ as $\hat{\beta}$

(a) $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$: Given

(b) $({}^s\theta, n, \lambda x.e_s\ \delta^s, \mathsf{Lb}(\lambda x.e_t)\ \delta^t) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp\ \sigma \rfloor_V^{\hat{\beta}}$:

From Definition 5.27 it suffices to prove that

$({}^s\theta, n, \lambda x.e_s\ \delta^s, (\lambda x.e_t)\ \delta^t) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma \rfloor_V^{\hat{\beta}}$

Again from Definition 5.27 it suffices to prove that

$$\begin{aligned}
&\forall {}^s\theta' \sqsupseteq {}^s\theta, {}^s v_d, {}^t v_d, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.({}^s\theta', j, {}^s v_d, {}^t v_d) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'} \implies \\
&({}^s\theta', j, e_s[{}^s v_d/x]\ \delta^s, e_t[{}^t v_d/x]\ \delta^t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}'}
\end{aligned}$$

This further means that given ${}^s\theta' \sqsupseteq {}^s\theta, {}^s v_d, {}^t v_d, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t $({}^s\theta', j, {}^s v_d, {}^t v_d) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'}$

And we a re required to prove

$$({}^s\theta', j, e_s[{}^s v_d/x]\ \delta^s, e_t[{}^t v_d/x]\ \delta^t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}'} \qquad \text{(F-L0)}$$

Since we are given $({}^s\theta', j, {}^s v_d, {}^t v_d) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'}$, therefore from Definition 5.31 and Lemma 5.33 we have
$({}^s\theta', j, \delta^s \cup \{x \mapsto {}^s v_d\}, \delta^t \cup \{x \mapsto {}^t v_d\}) \in \lfloor (\Gamma \cup \{x \mapsto \tau_1\})\ \sigma \rfloor_V^{\hat{\beta}'}$.
Therefore from IH we get
$({}^s\theta', j, e_s\ \delta^s \cup \{x \mapsto {}^s v_d\}, e_t\ \delta^t \cup \{x \mapsto {}^t v_d\}) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}'}$

We get (F-L0) directly from IH

3. FC-app:

$$\frac{\Gamma \vdash_{pc} e_{s1} : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell} \rightsquigarrow e_{t1} \qquad \Gamma \vdash_{pc} e_{s2} : \tau_1 \rightsquigarrow e_{t2} \qquad \mathcal{L} \vdash \ell \sqcup pc \sqsubseteq \ell_e \qquad \mathcal{L} \vdash \tau \searrow \ell}{\Gamma \vdash_{pc} e_{s1}\ e_{s2} : \tau_2 \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c\ b))))} \text{FC-app}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove:

$({}^s\theta, n, (e_{s1}\ e_{s2})\ \delta^s, \texttt{coerce\_taint}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c\ b))))\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, (e_{s1}\ e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \texttt{coerce\_taint}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c\ b))))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge$
$\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\rhd} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'}$

This further means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta$ and given some $i < n, {}^s v$ s.t $(H_s, (e_{s1}\ e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$

And we need to prove
$\exists H'_t, {}^t v.(H_t, \texttt{coerce\_taint}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c\ b))))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge$
$\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\rhd} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-A0)

<u>IH1:</u>

$({}^s\theta, n, e_{s1}\ \delta^s, e_{t1}\ \delta^t) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell}\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\rhd} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_{s1}) \Downarrow_j (H'_{s1}, {}^s v_1) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.(n - j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\rhd} {}^s\theta'_1 \wedge$
$({}^s\theta'_1, n - j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell}\ \sigma \rfloor_V^{\hat{\beta}'_1}$

We instantiate with H_s, H_t. And since we know that $(H_s, (e_{s1}\ e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists j < i < n$ s.t $(H_{s1}, e_{s1}) \Downarrow_j (H'_{s1}, {}^s v_1)$.

This means we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s \theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor(\tau_1 \xrightarrow{\ell_e} \tau_2)^\ell\ \sigma\rfloor_V^{\hat{\beta}'_1}$ (F-A1.0)

Since we know that $({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor(\tau_1 \xrightarrow{\ell_e} \tau_2)^\ell\ \sigma\rfloor_V^{\hat{\beta}'_1}$ therefore from Definition 5.27 we know that $\exists^t v_i.{}^t v_1 = \mathsf{Lb}({}^t v_i)$ s.t

$({}^s\theta'_1, n-j, {}^s v_1, {}^t v_i) \in \lfloor(\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma\rfloor_V^{\hat{\beta}'_1}$ (F-A1.1)

From Definition 5.27 we know that ${}^s v_1 = \lambda x.e'_s$ and ${}^t v_i = \lambda x.e'_t$ s.t
$\forall^s\theta''_1 \sqsupseteq {}^s\theta'_1, {}^s v', {}^t v', l < (n-j), \hat{\beta}'_1 \sqsubseteq \hat{\beta}''_1.$
$({}^s\theta''_1, l, {}^s v', {}^t v') \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}''_1} \implies ({}^s\theta''_1, l, e'_s[{}^s v'/x], e'_t[{}^t v'/x]) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}''_1}$ (F-A1)

<u>IH2:</u>

$({}^s\theta'_1, n-j, e_{s2}\ \delta^s, e_{t2}\ \delta^t) \in \lfloor\tau_1\ \sigma\rfloor_E^{\hat{\beta}'_1}$

This means from Definition 5.28 we have

$\forall H_{s2}, H_{t2}.(n-j, H_{s2}, H_{t2}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta \wedge \forall k < n-j, {}^s v_2.(H_{s2}, e_{s2}\ \delta^s) \Downarrow_j (H'_{s2}, {}^s v_2) \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t2}) \Downarrow^f (H'_{t2}, {}^t v_2 \delta^t) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_1.(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}'_2}$

We instantiate with $H'_{s1}, H'_{t1},$. And since we know that $(H_s, (e_{s1}\ e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists k < i-j < n-j$ s.t $(H'_{s1}, e_{s2}\ \delta^s) \Downarrow_k (H'_{s2}, {}^s v_2)$.

This means we have

$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t2}) \Downarrow^f (H'_{t2}, {}^t v_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_1.(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}'_2}$ (F-A2)

We instantiate (F-A1) with θ''_1 as θ'_2, ${}^s v'$ as ${}^s v_2$, ${}^t v'$ as ${}^t v_2$, l as $n-j-k$ and $\hat{\beta}''_1$ as $\hat{\beta}'_2$. Therefore we get

$({}^s\theta'_2, n-j-k, e'_s[{}^s v_2/x], e'_t[{}^t v_2/x]) \in \lfloor\tau_2\ \sigma\rfloor_E^{\hat{\beta}'_2}$

From Definition 5.28 we have

$\forall H_s, H_t.(n-j-k, H_s, H_t) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge \forall a < n-j-k, {}^s v.(H_s, e'_s[{}^s v_2/x]) \Downarrow_i (H'_{s3}, {}^s v_3) \implies$
$\exists H'_{t3}, {}^t v_3.(H_t, e'_t[{}^t v_2/x]) \Downarrow^f (H'_{t3}, {}^t v_3) \wedge \exists^s\theta'_3 \sqsupseteq {}^s\theta'_2, \hat{\beta}'_3 \sqsupseteq \hat{\beta}'_2.$
$(n-j-k-a, H'_{s3}, H'_{t3}) \overset{\hat{\beta}'_3}{\triangleright} {}^s\theta'_3 \wedge ({}^s\theta'_3, n-j-k-a, {}^s v_3, {}^t v_3) \in \lfloor\tau_2\ \sigma\rfloor_V^{\hat{\beta}'_3}$

Instantiating with H'_{s2}, H'_{t2}. since we know that $(H_s, (e_{s1}\ e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists a < i-j-k < n-j-k$ s.t $(H'_{s2}, e'_s[{}^s v/x]\ \delta^s) \Downarrow_a (H'_{s3}, {}^s v_3)$

Therefore we have

$\exists H'_{t3}, {}^t v_3.(H_t, e'_t[{}^t v_2/x]) \Downarrow^f (H'_{t3}, {}^t v_3) \wedge \exists^s\theta'_3 \sqsupseteq {}^s\theta'_2, \hat{\beta}'_3 \sqsupseteq \hat{\beta}'_2.$
$(n - j - k - a, H'_{s3}, H'_{t3}) \overset{\hat{\beta}'_3}{\triangleright} {}^s\theta'_3 \wedge ({}^s\theta'_3, n - j - k - a, {}^s v_3, {}^t v_3) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'_3}$ (F-A3)

Let $\tau_2 = \mathsf{A}_2^{\ell_i}$, since $\tau_2 \searrow \ell$ therefore $\ell \sqsubseteq \ell_i$ and
$({}^s\theta'_3, n - j - k - a, {}^s v_3, {}^t v_3) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'_3}$
Therefore from Definition 5.27 we know that
$({}^s\theta'_3, n - j - k - a, {}^s v_3, \mathsf{Lb}{}^t v_{3i}) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'_3}$ (F-A3.1)

In order to prove (F-A0) we choose H'_t as H'_{t3} and ${}^t v$ as $\mathsf{Lb}({}^t v_{3i})$. We need to prove:

(a) $(H_t, \texttt{coerce\_taint}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c\ b))))\ \delta^t) \Downarrow^f (H'_{t3}, \mathsf{Lb}({}^t v_{3i}))$:

From Lemma 5.35 it suffices to prove that
$(H_t, \mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c\ b)))\ \delta^t) \Downarrow^f (H'_{t3}, \mathsf{Lb}\ ({}^t v_3))$

From cg-bind it further suffices to show that

- $(H_t, e_{t1}\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1)$:
  We get this directly from (F-A1.0)
- $(H'_{t1}, \mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c\ b))[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t3}, \mathsf{Lb}({}^t v_{3i}))$:
  From cg-bind it suffices to prove that
  - $(H'_{t1}, e_{t2}\ \delta^t) \Downarrow^f (H'_{t2}, {}^t v_2)$:
    We get this directly from (F-A2)
  - $(H'_{t2}, \mathsf{bind}(\mathsf{unlabel}\ a, c.c\ b)[{}^t v_1/a][{}^t v_2/b]\delta^t) \Downarrow^f (H'_{t3}, \mathsf{Lb}({}^t v_{3i}))$:
    From cg-bind again it suffices to prove
    * $(H'_{t2}, (\mathsf{unlabel}\ a)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t31}, {}^t v_{t2})$:
      Since from (F-A1.1) we know that $\exists^t v_i.{}^t v_1 = \mathsf{Lb}({}^t v_i)$

      Therefore from cg-unlabel and (F-A1) we know that $H'_{t31} = H'_{t2}$ and ${}^t v_{t2} = {}^t v_i = \lambda x.e'_t$
    * $((c\ b)[{}^t v_2/b][{}^t v_{t2}/c]\ \delta^t) \Downarrow {}^t v_{t21}$:
      It suffices to prove that
      $((\lambda x.e'_t)\ {}^t v_2\ \delta^t) \Downarrow {}^t v_{t21}$

      From cg-app we know that
      ${}^t v_{t21} = e'_t[{}^t v_2/x]\ \delta^t$
    * $(H'_{t2}, {}^t v_{21}) \Downarrow^f (H'_{t3}, \mathsf{Lb}({}^t v_{3i}))$:
      From (F-A3) and (F-A3.1) we get the desired

(b) $\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta'_3$ and $\hat{\beta}'$ as $\hat{\beta}'_3$. From fg-app we know that $i = j + k + a + 1$, ${}^s v = {}^s v_3$ and $H'_s = H'_{s3}$. Also from the termination proof (previous point) we know that $H'_t = H'_{t3}$ and ${}^t v = \mathsf{Lb}\ ({}^t v_3)$

We get $(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta'$ from (F-A3) and Lemma 5.34

Since ${}^t v = \mathsf{Lb}({}^t v_3)$ therefore from Definition 5.27 it suffices to prove that
$({}^s\theta'_3, n - j - k - a - 1, {}^s v_3, {}^t v_3) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'_3}$

We get this directly from (F-A3) and Lemma 5.32

4. FC-FI:

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash_{\ell_e} e_s : \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash_{pc} \Lambda e_s : (\forall \alpha.(\ell_e, \tau))^{\perp} \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\Lambda e_t))} \text{ FC-FI}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, (\Lambda e_s)\ \delta^s, \mathsf{ret}(\mathsf{Lb}\Lambda e_t)\ \delta^t) \in \lfloor (\forall \alpha.(\ell_e, \tau))^{\perp}\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 5.28 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, (\Lambda e_s)\ \delta^s) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{ret}(\mathsf{Lb}(\Lambda e_t)))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge$
$\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor (\forall \alpha.(\ell_e, \tau))^{\perp}\ \sigma \rfloor_V^{\hat{\beta}'}$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $(H_s, (\Lambda e_s)\ \delta^s) \Downarrow_i (H'_s, {}^s v)$

From fg-val we know that ${}^s v = (\Lambda e_s)\ \delta^s$, $H'_s = H_s$ and $i = 0$. Also from cg-ret, cg-label and cg-val we know that $H'_t = H_t$ and ${}^t v = (\mathsf{Lb}(\Lambda e_t))\ \delta^t$

It suffices to prove that

$\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n, H_s, H_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n, {}^s v, {}^t v) \in \lfloor (\forall \alpha.(\ell_e, \tau))^{\perp}\ \sigma \rfloor_V^{\hat{\beta}'}$

We choose ${}^s\theta'$ as ${}^s\theta$ and $\hat{\beta}'$ as $\hat{\beta}$

(a) $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$: Given

(b) $({}^s\theta, n, \Lambda e_s\ \delta^s, \mathsf{Lb}(\Lambda e_t)\ \delta^t) \in \lfloor (\forall \alpha.(\ell_e, \tau))^{\perp}\ \sigma \rfloor_V^{\hat{\beta}}$:
From Definition 5.27 it suffices to prove that
$({}^s\theta, n, \Lambda e_s\ \delta^s, (\Lambda e_t)\ \delta^t) \in \lfloor (\forall \alpha.(\ell_e, \tau))\ \sigma \rfloor_V^{\hat{\beta}}$

Again from Definition 5.27 it suffices to prove that
$\forall {}^s\theta' \sqsupseteq {}^s\theta, {}^s v_d, {}^t v_d, j < n, \hat{\beta} \sqsubseteq \hat{\beta}', \ell' \in \mathcal{L}.({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_E^{\hat{\beta}'}$

This further means that given ${}^s\theta' \sqsupseteq {}^s\theta, {}^s v_d, {}^t v_d, j < n, \hat{\beta} \sqsubseteq \hat{\beta}', \ell' \in \mathcal{L}$

And we are required to prove
$({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_E^{\hat{\beta}'}$ (F-F0)

We get (F-F0) directly from IH

5. FC-FE:

$$\frac{\text{FV}(\ell') \subseteq \Sigma \qquad \begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e_s : (\forall \alpha.(\ell_e, \tau))^{\ell} \rightsquigarrow e_t \\ \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e[\ell'/\alpha]\end{array} \qquad \Sigma; \Psi \vdash \tau[\ell'/\alpha] \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e_s\ []: \tau[\ell'/\alpha] \rightsquigarrow \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b[]))))} \text{ FG-FE}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove:

$({}^s\theta, n, (e_s\ [])\ \delta^s, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b[]))))\ \delta^t) \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, (e_s\ [])\ \delta^s) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b[]))))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_V^{\hat{\beta}'}$

This further means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $(H_s, (e_s\ [])\ \delta^s) \Downarrow_i (H'_s, {}^s v)$

And we need to prove
$\exists H'_t, {}^t v.(H_t, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b[]))))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-F0)

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\forall \alpha.(\ell_e, \tau))^\ell\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_s) \Downarrow_j (H'_{s1}, {}^s v_1) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge$
$({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\forall \alpha.(\ell_e, \tau))^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$

We instantiate with H_s, H_t. And since we know that $(H_s, (e_s\ [])\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists j < i < n, H'_{s1}$ s.t $(H_s, e_s) \Downarrow_j (H'_{s1}, {}^s v_1)$.

This means we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\forall \alpha.(\ell_e, \tau))^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-F1.0)

Since we know that $({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\forall \alpha.(\ell_e, \tau))^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$ therefore from Definition 5.27 we know that $\exists {}^t v_i.{}^t v_1 = \mathsf{Lb}({}^t v_i)$ s.t

$({}^s\theta'_1, n-j, {}^s v_1, {}^t v_i) \in \lfloor (\forall \alpha.(\ell_e, \tau))\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-F1.1)

From Definition 5.27 we know that ${}^s v_1 = \Lambda e'_s$ and ${}^t v_i = \Lambda e'_t$ s.t

$\forall {}^s\theta''_1 \sqsupseteq {}^s\theta'_1, l < (n-j), \hat{\beta}'_1 \sqsubseteq \hat{\beta}''_1, \ell'' \in \mathcal{L}.({}^s\theta''_1, l, e'_s, e'_t) \in \lfloor \tau[\ell''/\alpha]\ \sigma \rfloor_E^{\hat{\beta}''_1}$ (F-F1)

Therefore we instantiate (F-F1) with θ''_1 as θ'_1, l as $(n-j-1)$, $\hat{\beta}''_1$ as $\hat{\beta}'_1$ and ℓ'' as ℓ'. Therefore we get

$({}^s\theta_1', n-j-1, e_s', e_t') \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_E^{\hat{\beta}_2'}$

From Definition 5.28 we have

$\forall H_s, H_t.(n-j-1, H_s, H_t) \overset{\hat{\beta}_2'}{\triangleright} {}^s\theta_1' \wedge \forall a < n-j-1, {}^s v.(H_s, e_s') \Downarrow_a (H_{s2}', {}^s v_2) \implies$
$\exists H_{t2}', {}^t v_2.(H_t, e_t') \Downarrow^f (H_{t2}', {}^t v_2) \wedge \exists^s \theta_2' \sqsupseteq {}^s\theta_2', \hat{\beta}_2' \sqsupseteq \hat{\beta}_2'.$
$(n-j-1-a, H_{s2}', H_{t2}') \overset{\hat{\beta}_2'}{\triangleright} {}^s\theta_2' \wedge ({}^s\theta_2', n-j-1-a, {}^s v_2, {}^t v_2) \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_V^{\hat{\beta}_2'}$

Since we know that $(H_s, (e_s\ [])\ \delta^s) \Downarrow_i (H_s', {}^s v)$ therefore $\exists k = i-j-1$ s.t $(H_{s1}, e_s') \Downarrow_k (H_{s2}', {}^s v_2)$. We know that $k = i-j-1 < n-j-1$. Therefore instantiating with H_{s1}', H_{t1}', k we get

$\exists H_{t2}', {}^t v_2.(H_{t1}', e_t') \Downarrow^f (H_{t2}', {}^t v_2) \wedge \exists^s \theta_2' \sqsupseteq {}^s\theta_2', \hat{\beta}_2' \sqsupseteq \hat{\beta}_2'.$
$(n-j-1-k, H_{s2}', H_{t2}') \overset{\hat{\beta}_2'}{\triangleright} {}^s\theta_2' \wedge ({}^s\theta_2', n-j-1-a, {}^s v_2, {}^t v_2) \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_V^{\hat{\beta}_2'}$ (F-F3)

Let $\tau[\ell'/\alpha] = \mathsf{A}_2^{\ell_i}$, since $\tau[\ell'/\alpha] \searrow \ell$ therefore $\ell \sqsubseteq \ell_i$ and

$({}^s\theta_2', n-j-1-k, {}^s v_2, {}^t v_2) \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_V^{\hat{\beta}_2'}$
Therefore from Definition 5.27 we know that
$({}^s\theta_2', n-j-1-k, {}^s v_2, \mathsf{Lb}^t v_{2i}) \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_V^{\hat{\beta}_2'}$ (F-F3.1)

In order to prove (F-F0) we choose H_t' as H_{t2}' and ${}^t v$ as $\mathsf{Lb}({}^t v_{2i})$. We need to prove:

(a) $(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b[]))))\ \delta^t) \Downarrow^f (H_{t2}', \mathsf{Lb}({}^t v_{2i}))$:

From Lemma 5.35 it suffices to prove that
$(H_t, \mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b[])))\ \delta^t) \Downarrow^f (H_{t2}', \mathsf{Lb}\ ({}^t v_{2i}))$

From cg-bind it further suffices to show that

- $(H_t, e_t\ \delta^t) \Downarrow^f (H_{t1}', {}^t v_1)$:
  We get this directly from (F-F1.0)
- $(H_{t1}', \mathsf{bind}(\mathsf{unlabel}\ a, b.(b[]))[{}^t v_1/a]\ \delta^t) \Downarrow^f (H_{t2}', \mathsf{Lb}({}^t v_{2i}))$:
  From cg-bind it suffices to prove that
  - $(H_{t1}', (\mathsf{unlabel}\ a)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H_{t11}', {}^t v_{t2})$:
    Since from (F-F1.1) we know that $\exists^t v_i.{}^t v_1 = \mathsf{Lb}({}^t v_i)$

    Therefore from cg-unlabel and (F-F1) we know that $H_{t11}' = H_{t1}'$ and ${}^t v_{t2} = {}^t v_i = \Lambda e_t'$
  - $((b\ [])[{}^t v_{t2}/b]\ \delta^t) \Downarrow {}^t v_{t21}$:
    It suffices to prove that
    $((\Lambda e_t')\ []\ \delta^t) \Downarrow {}^t v_{t21}$

    From cg-FE and cg-val we know that
    ${}^t v_{t21} = e_t'\ \delta^t$
  - $(H_{t1}', {}^t v_{21}) \Downarrow^f (H_{t2}', \mathsf{Lb}({}^t v_{2i}))$:
    From (F-F3) we get the desired

(b) $\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta'_2$ and $\hat{\beta}'$ as $\hat{\beta}'_2$. From fg-FE we know that $i = j+k+1$, ${}^sv = {}^sv_2$ and $H'_s = H'_{s2}$. Also from the termination proof (previous point) we know that $H'_t = H'_{t2}$ and ${}^tv = \mathsf{Lb}\ ({}^tv_{2i})$

We get $(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta'$ from (F-F3) and Lemma 5.34

Since ${}^tv = {}^tv_2 = \mathsf{Lb}({}^tv_{2i})$ therefore from Definition 5.27 it suffices to prove that $({}^s\theta'_3, n-j-k-1, {}^sv_2, {}^tv_2) \in \lfloor \tau[\ell'/\alpha]\ \sigma \rfloor_V^{\hat{\beta}'_3}$

We get this directly from (F-F3) and Lemma 5.32

6. FC-CI:

$$\frac{\Sigma; \Psi, c; \Gamma \vdash_{\ell_e} e_s : \tau \rightsquigarrow e_t}{\Sigma; \Psi; \Gamma \vdash_{pc} \nu\ e_s : (c \overset{\ell_e}{\Rightarrow} \tau)^\perp \rightsquigarrow \mathsf{ret}(\mathsf{Lb}(\nu e_t))} \text{ FG-CI}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, (\nu e_s)\ \delta^s, \mathsf{ret}(\mathsf{Lb}\nu e_t)\ \delta^t) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\perp\ \sigma \rfloor_E^{\hat{\beta}}$

From Definition 5.28 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv.(H_s, (\nu e_s)\ \delta^s) \Downarrow_i (H'_s, {}^sv) \implies$
$\exists H'_t, {}^tv.(H_t, \mathsf{ret}(\mathsf{Lb}(\nu e_t)))\ \delta^t) \Downarrow^f (H'_t, {}^tv) \wedge$
$\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor (\forall\alpha.(\ell_e, \tau))^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^sv$ s.t $(H_s, (\nu e_s)\ \delta^s) \Downarrow_i (H'_s, {}^sv)$

From fg-val we know that ${}^sv = (\nu e_s)\ \delta^s$, $H'_s = H_s$ and $i = 0$. Also from cg-ret, cg-label and cg-val we know that $H'_t = H_t$ and ${}^tv = (\mathsf{Lb}(\nu e_t))\ \delta^t$

It suffices to prove that

$\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n, H_s, H_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n, {}^sv, {}^tv) \in \lfloor (\forall\alpha.(\ell_e, \tau))^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$

We choose ${}^s\theta'$ as ${}^s\theta$ and $\hat{\beta}'$ as $\hat{\beta}$

(a) $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$: Given

(b) $({}^s\theta, n, \nu e_s\ \delta^s, \mathsf{Lb}(\nu e_t)\ \delta^t) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\perp\ \sigma \rfloor_V^{\hat{\beta}}$:
From Definition 5.27 it suffices to prove that
$({}^s\theta, n, \nu e_s\ \delta^s, (\nu e_t)\ \delta^t) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)\ \sigma \rfloor_V^{\hat{\beta}}$

Again from Definition 5.27 it suffices to prove that
$\forall^s\theta' \sqsupseteq {}^s\theta, {}^sv_d, {}^tv_d, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'.\mathcal{L} \models c \implies ({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'}$

This further means that given ${}^s\theta' \sqsupseteq {}^s\theta, {}^sv_d, {}^tv_d, j < n, \hat{\beta} \sqsubseteq \hat{\beta}'$ s.t $\mathcal{L} \models c \implies$

And we are required to prove

$({}^s\theta', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'}$ (F-C0)

We get (F-C0) directly from IH

7. FC-CE:

$$\frac{\Sigma;\Psi;\Gamma \vdash_{pc} e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell} \rightsquigarrow e_t \qquad \Sigma;\Psi \vdash c \qquad \Sigma;\Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e \qquad \Sigma;\Psi \vdash \tau \searrow \ell}{\Sigma;\Psi;\Gamma \vdash_{pc} e\ \bullet : \tau \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b\bullet))))} \text{FG-CE}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove:

$({}^s\theta, n, (e_s\ \bullet)\ \delta^s, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b\bullet))))\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 it suffices to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, (e_s\ \bullet)\ \delta^s) \Downarrow_i (H_s', {}^s v) \implies$
$\exists H_t', {}^t v.(H_t, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b\bullet))))\ \delta^t) \Downarrow^f (H_t', {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$

This further means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ and given some $i < n, {}^s v$ s.t $(H_s, (e_s\ \bullet)\ \delta^s) \Downarrow_i (H_s', {}^s v)$

And we need to prove

$\exists H_t', {}^t v.(H_t, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b\bullet))))\ \delta^t) \Downarrow^f (H_t', {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-C0)

IH:

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell}\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_s) \Downarrow_j (H_{s1}', {}^s v_1) \implies$
$\exists H_{t1}', {}^t v_1.(H_{t1}, e_t) \Downarrow^f (H_{t1}', {}^t v_1) \wedge \exists {}^s\theta_1' \sqsupseteq {}^s\theta, \hat{\beta}_1' \sqsupseteq \hat{\beta}.(n-j, H_{s1}', H_{t1}') \overset{\hat{\beta}_1'}{\triangleright} {}^s\theta_1' \wedge$
$({}^s\theta_1', n-j, {}^s v_1, {}^t v_1) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell}\ \sigma \rfloor_V^{\hat{\beta}_1'}$

We instantiate with H_s, H_t. And since we know that $(H_s, (e_s\ \bullet)\ \delta^s) \Downarrow_i (H_s', {}^s v)$ therefore $\exists j < i < n, H_{s1}'$ s.t $(H_s, e_s) \Downarrow_j (H_{s1}', {}^s v_1)$.

This means we have

$\exists H_{t1}', {}^t v_1.(H_{t1}, e_t) \Downarrow^f (H_{t1}', {}^t v_1) \wedge \exists {}^s\theta_1' \sqsupseteq {}^s\theta, \hat{\beta}_1' \sqsupseteq \hat{\beta}.(n-j, H_{s1}', H_{t1}') \overset{\hat{\beta}_1'}{\triangleright} {}^s\theta_1' \wedge ({}^s\theta_1', n-j, {}^s v_1, {}^t v_1) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell}\ \sigma \rfloor_V^{\hat{\beta}_1'}$ (F-C1.0)

Since we know that $({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$ therefore from Definition 5.27 we know that $\exists^t v_i.{}^t v_1 = \mathsf{Lb}({}^t v_i)$ s.t

$({}^s\theta'_1, n-j, {}^s v_1, {}^t v_i) \in \lfloor (c \overset{\ell_e}{\Rightarrow} \tau)\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-C1.1)

From Definition 5.27 we know that ${}^s v_1 = \nu e'_s$ and ${}^t v_i = \nu e'_t$ s.t

$\forall^s\theta''_1 \sqsupseteq {}^s\theta'_1, l < (n-j), \hat{\beta}'_1 \sqsubseteq \hat{\beta}''_1, \ell'' \in \mathcal{L}.({}^s\theta''_1, l, e'_s, e'_t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}''_1}$ (F-C1)

Therefore we instantiate (F-C1) with θ''_1 as θ'_1, l as $(n-j-1)$, $\hat{\beta}''_1$ as $\hat{\beta}'_1$ and ℓ'' as ℓ'. Therefore we get

$({}^s\theta'_1, n-j-1, e'_s, e'_t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'_2}$

From Definition 5.28 we have

$\forall H_s, H_t.(n-j-1, H_s, H_t) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_1 \wedge \forall a < n-j-1, {}^s v.(H_s, e'_s) \Downarrow_a (H'_{s2}, {}^s v_2) \implies$
$\exists H'_{t2}, {}^t v_2.(H_t, e'_t) \Downarrow^f (H'_{t2}, {}^t v_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_2, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_2.$
$(n-j-1-a, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n-j-1-a, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_2}$

Since we know that $(H_s, (e_s\ \bullet)\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists k = i-j-1$ s.t $(H_{s1}, e'_s) \Downarrow_k (H'_{s2}, {}^s v_2)$. We know that $k = i-j-1 < n-j-1$. Therefore instantiating with H'_{s1}, H'_{t1}, k we get

$\exists H'_{t2}, {}^t v_2.(H'_{t1}, e'_t) \Downarrow^f (H'_{t2}, {}^t v_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_2, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_2.$
$(n-j-1-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n-j-1-a, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_2}$ (F-C3)

Let $\tau = \mathsf{A}_2^{\ell_i}$, since $\tau \searrow \ell$ therefore $\ell \sqsubseteq \ell_i$ and

$({}^s\theta'_2, n-j-1-k, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_2}$

Therefore from Definition 5.27 we know that

$({}^s\theta'_2, n-j-1-k, {}^s v_2, \mathsf{Lb}^t v_{2i}) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_2}$ (F-C3.1)

In order to prove (F-C0) we choose H'_t as H'_{t2} and ${}^t v$ as $\mathsf{Lb}({}^t v_{2i})$. We need to prove:

(a) $(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b\bullet))))\ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}({}^t v_{2i}))$:

From Lemma 5.35 it suffices to prove that
$(H_t, \mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.(b\bullet)))\ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}\ ({}^t v_{2i}))$

From cg-bind it further suffices to show that

- $(H_t, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1)$:
  We get this directly from (F-C1.0)
- $(H'_{t1}, \mathsf{bind}(\mathsf{unlabel}\ a, b.(b\bullet))[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}({}^t v_{2i}))$:
  From cg-bind it suffices to prove that

- $(H'_{t1}, (\mathsf{unlabel}\ a)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t11}, {}^t v_{t2})$:
  Since from (F-C1.1) we know that $\exists^t v_i.{}^t v_1 = \mathsf{Lb}({}^t v_i)$

  Therefore from cg-unlabel and (F-C1) we know that $H'_{t11} = H'_{t1}$ and ${}^t v_{t2} = {}^t v_i = \nu e'_t$

- $((b\ \bullet)[{}^t v_{t2}/b]\ \delta^t) \Downarrow {}^t v_{t21}$:
  It suffices to prove that
  $((\nu e'_t)\ \bullet\ \delta^t) \Downarrow {}^t v_{t21}$

  From cg-CE and cg-val we know that
  ${}^t v_{t21} = e'_t\ \delta^t$
- $(H'_{t1}, {}^t v_{21}) \Downarrow^f (H'_{t2}, \mathsf{Lb}({}^t v_{2i}))$:
  From (F-C3) we get the desired

(b) $\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta'_2$ and $\hat{\beta}'$ as $\hat{\beta}'_2$. From fg-CE we know that $i = j+k+1$, ${}^s v = {}^s v_2$ and $H'_s = H'_{s2}$. Also from the termination proof (previous point) we know that $H'_t = H'_{t2}$ and ${}^t v = \mathsf{Lb}\ ({}^t v_{2i})$

We get $(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta'$ from (F-C3) and Lemma 5.34

Since ${}^t v = {}^t v_2 = \mathsf{Lb}({}^t v_{2i})$ therefore from Definition 5.27 it suffices to prove that
$({}^s\theta'_3, n-j-k-1, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_3}$

We get this directly from (F-C3) and Lemma 5.32

8. FC-prod:

$$\frac{\Gamma \vdash_{pc} e_{s1} : \tau_1 \rightsquigarrow e_{t1} \qquad \Gamma \vdash_{pc} e_{s2} : \tau_2 \rightsquigarrow e_{t2}}{\Gamma \vdash_{pc} (e_{s1}, e_{s2}) : (\tau_1 \times \tau_2)^\perp \rightsquigarrow \mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{ret}(\mathsf{Lb}(a, b))))} \text{prod}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, (e_{s1}, e_{s2})\ \delta^s, (\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{ret}(\mathsf{Lb}(a, b)))))\ \delta^t) \in \lfloor (\tau_1 \times \tau_2)^\perp\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v_1, {}^s v_2.(H_s, (e_{s1}, e_{s2})) \Downarrow_i (H'_s, ({}^s v_1, {}^s v_2)) \implies$
$\exists H'_t, {}^t v.(H_t, (\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{ret}(\mathsf{Lb}(a, b)))))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \in \lfloor (\tau_1 \times \tau_2)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^s v_1, {}^s v_2$ s.t $(H_s, (e_{s1}, e_{s2})) \Downarrow_i (H'_s, ({}^s v_1, {}^s v_2))$

And we need to prove
$\exists H'_t, {}^t v.(H_t, (\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{ret}(\mathsf{Lb}(a, b)))))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, ({}^s v_1, {}^s v_2), {}^t v) \in \lfloor (\tau_1 \times \tau_2)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-P0)

<u>IH1:</u>

$({}^s\theta, n, e_{s1}\ \delta^s, e_{t1}\ \delta^t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we need to prove

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_{s1}\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-j, {}^s v_1, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'_1}$

Instantiating with H_s, H_t and since we know that $(H_s, (e_{s1}, e_{s2})) \Downarrow_i (H'_s, ({}^s v_1, {}^s v_2))$ therefore $\exists j < i < n$ s.t $(H_{s1}, e_{s1}\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1)$

Therefore we have
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1)) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-P1)

<u>IH2:</u>

$({}^s\theta'_1, n-j, e_{s2}\ \delta^s, e_{t2}\ \delta^t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}'_1}$

This means from Definition 5.28 we need to prove

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}}{\triangleright} {}^s\theta'_1 \wedge \forall k < n-j, {}^s v_1.(H_{s2}, e_{s2}\ \delta^s) \Downarrow_j (H'_{s2}, {}^s v_1) \implies$
$\exists H'_{t2}, {}^t v_1.(H_{t2}, e_{t2}) \Downarrow^f (H'_{t2}, {}^t v_1) \wedge \exists {}^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_1.$
$(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_1, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'_2}$

Instantiating with H'_{s1}, H'_{t1} and since we know that $(H_s, (e_{s1}, e_{s2})) \Downarrow_i (H'_s, ({}^s v_1, {}^s v_2))$ therefore $\exists k < i-j < n-j$ s.t $(H_{s2}, e_{s2}\ \delta^s) \Downarrow_k (H'_{s2}, {}^s v_2)$

Therefore we have
$\exists H'_{t2}, {}^t v_1.(H_{t2}, e_{t2}) \Downarrow^f (H'_{t2}, {}^t v_2) \wedge \exists {}^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_1.$
$(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}'_2}$ (F-P2)

In order to prove (F-P0) we choose H_t as H'_{t2} and ${}^t v$ as $\mathsf{Lb}({}^t v_1, {}^t v_2)$

(a) $(H_t, (\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{ret}(\mathsf{Lb}(a,b))))) \ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}({}^t v_1, {}^t v_2))$:
From cg-bind it suffices to prove that
- $(H_t, e_{t1}\ \delta^t) \Downarrow^f (H'_{tb1}, {}^t v_{tb1})$:
  From (F-P1) we know that $H'_{tb1} = H'_{t1}$ and ${}^t v_{tb1} = {}^t v_1$
- $(H'_{t1}, \mathsf{bind}(e_{t2}, b.\mathsf{ret}(\mathsf{Lb}(a,b)))[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}({}^t v_1, {}^t v_2))$:
  From cg-bind it suffices to prove that
  - $(H'_{t1}, e_{t2}\ \delta^t) \Downarrow^f (H'_{tb2}, {}^t v_{tb2})$:
    From (F-P2) we know that $H'_{tb2} = H'_{t2}$ and ${}^t v_{tb2} = {}^t v_2$
  - $(H'_{t2}, \mathsf{ret}(\mathsf{Lb}(a,b))[{}^t v_1/a][{}^t v_2/b]\ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}({}^t v_1, {}^t v_2))$:
    We get this from cg-ret, (F-P1) and (F-P2)

(b) $\exists^s\theta' \sqsupseteq {^s\theta}, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {^s\theta'} \wedge ({^s\theta'}, n-i, ({^s v_1}, {^s v_2}), {^t v}) \in \lfloor(\tau_1 \times \tau_2)^{\perp}\ \sigma\rfloor_V^{\hat{\beta}'}$:
We choose ${^s\theta'}$ as ${^s\theta'_2}$ and $\hat{\beta}'$ as $\hat{\beta}'_2$ and since from fg-prod $i = j+k+1$ and $H'_s = H'_{s2}$. Therefore from (F-P2) and Lemma 5.34 we get

$(n-i, H'_s, H'_{t2}) \overset{\hat{\beta}'}{\triangleright} {^s\theta'}$

In order to prove $({^s\theta'}, n-i, ({^s v_1}, {^s v_2}), {^t v}) \in \lfloor(\tau_1 \times \tau_2)^{\perp}\ \sigma\rfloor_V^{\hat{\beta}'}$
From Definition 5.27 it suffices to prove

$\exists^t v_i.{^t v} = \mathsf{Lb}({^t v_i}) \wedge ({^s\theta'}, n-i, ({^s v_1}, {^s v_2}), {^t v_i}) \in \lfloor(\tau_1 \times \tau_2)\ \sigma\rfloor_V^{\hat{\beta}'_2}$

Since ${^t v} = \mathsf{Lb}({^t v_1}, {^t v_2})$ therefore we get the desired from (F-P1), (F-P2), Definition 5.27 and Lemma 5.32

9. FC-fst:

$$\frac{\Gamma \vdash_{pc} e_s : (\tau_1 \times \tau_2)^{\ell} \rightsquigarrow e_t \qquad \mathcal{L} \vdash \tau_1 \searrow \ell}{\Gamma \vdash_{pc} \mathsf{fst}(e_s) : \tau_1 \rightsquigarrow \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))}\ \text{fst}$$

Also given is: $({^s\theta}, n, \delta^s, \delta^t) \in \lfloor\Gamma\rfloor_V^{\hat{\beta}}$
To prove: $({^s\theta}, n, \mathsf{fst}(e_s)\ \delta^s, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))\ \delta^t) \in \lfloor\tau_1\ \sigma\rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {^s\theta} \wedge \forall i < n, {^s v}.(H_s, \mathsf{fst}(e_s)) \Downarrow_i (H'_s, {^s v}) \implies$
$\exists H'_t, {^t v}.(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))) \Downarrow^f (H'_t, {^t v}) \wedge$
$\exists^s\theta' \sqsupseteq {^s\theta}, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {^s\theta'} \wedge ({^s\theta'}, n-i, {^s v}, {^t v}) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}'}$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\gamma,\hat{\beta}}{\triangleright} {^s\theta}$. Also given some $i < n, {^s v}$ s.t $(H_s, \mathsf{fst}(e_s)) \Downarrow_i (H'_s, {^s v})$
We need to prove

$\exists H'_t, {^t v}.(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))) \Downarrow^f (H'_t, {^t v}) \wedge$
$\exists^s\theta' \sqsupseteq {^s\theta}, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {^s\theta'} \wedge ({^s\theta'}, n-i, {^s v}, {^t v}) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}'}$ (F-F0)

<u>IH:</u>

$({^s\theta}, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor(\tau_1 \times \tau_2)^{\ell}\ \sigma\rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {^s\theta} \wedge \forall i < n, {^s v_1}.(H_{s1}, e_s) \Downarrow_j (H'_{s1}, {^s v_1}) \implies$
$\exists H'_{t1}, {^t v}.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {^t v_1}) \wedge \exists^s\theta'_1 \sqsupseteq {^s\theta}, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {^s\theta'_1} \wedge ({^s\theta'_1}, n-j, {^s v_1}, {^t v_1}) \in \lfloor(\tau_1 \times \tau_2)^{\ell}\ \sigma\rfloor_V^{\hat{\beta}'_1}$

Instantiating with H_s, H_t and since we know that $(H_s, \mathsf{fst}(e_s)) \Downarrow_i (H'_s, {^s v})$ therefore $\exists j < i < n$ s.t $(H_s, e_s) \Downarrow_j (H'_{s1}, {^s v_1})$

This means we have

$\exists H'_{t1}, {}^t v.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$

$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 \times \tau_2)^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-F1)

Since we know that $({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 \times \tau_2)^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$ therefore from Definition 5.27 we know that ${}^t v_1 = \mathsf{Lb}({}^t v_i)$ s.t

$({}^s\theta'_1, n-j, {}^s v_1, {}^t v_i) \in \lfloor (\tau_1 \times \tau_2)\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-F1.1)

From Definition 5.27 we know that ${}^s v_1 = ({}^s v_{i1}, {}^s v_{i2})$ and ${}^t v_i = ({}^t v_{i1}, {}^t v_{i2})$ s.t

$({}^s\theta'_1, n-j, {}^s v_{i1}, {}^t v_{i1}) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-F1.2)

Let $\tau_1 = \mathsf{A}_1^{\ell_i}$, since $\tau_1 \searrow \ell$ therefore $\ell \sqsubseteq \ell_i$ and

$({}^s\theta'_1, n-j, {}^s v_{i1}, {}^t v_{i1}) \in \lfloor \mathsf{A}_1^{\ell_i} \rfloor_V^{\hat{\beta}}$

Therefore from Definition 5.27 we know that

$({}^s\theta'_1, n-j, {}^s v_{i1}, \mathsf{Lb}\,{}^t v_{i11}) \in \lfloor \mathsf{A}_1 \rfloor_V^{\hat{\beta}'_1}$ (F-F1.3)

In order to prove (F-F0) we choose H'_t as H'_{t1} and ${}^t v$ as ${}^t v_{i1} (= \mathsf{Lb}\,{}^t v_{i11})$ as we need to prove

(a) $(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))))) \Downarrow^f (H'_{t1}, \mathsf{Lb}\,{}^t v_{i11})$:
From Lemma 5.35 it suffices to prove that
$(H_t, \mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b))))) \Downarrow^f (H'_{t1}, \mathsf{Lb}\ ({}^t v_{i11}))$
From cg-bind it suffices to prove that

- $(H_t, e_t\ \delta^t) \Downarrow^f (H'_{t11}, {}^t v_{t11})$:
  From (F-F1) we know that $H'_{t11} = H'_{t1}$ and ${}^t v_{t11} = {}^t v_1 = \mathsf{Lb}({}^t v_i)$
- $(H'_{t1}, \mathsf{bind}(\mathsf{unlabel}\ (a), b.\mathsf{ret}(\mathsf{fst}(b)))[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t1}, \mathsf{Lb}\,{}^t v_{i11})$:
  Again from cg-bind it suffices to prove that
  - $(H'_{t1}, \mathsf{unlabel}\ (a)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t21}, {}^t v_{t21})$:
    Since ${}^t v_1 = \mathsf{Lb}({}^t v_{i1}, {}^t v_{i2})$ from (F-F1.1) and (F-F1.2) therefore we get the desired from cg-unlabel

    So, $H_{t21} = H'_{t1}$ and ${}^t v_{t21} = ({}^t v_{i1}, {}^t v_{i2})$
  - $(H'_{t1}, \mathsf{ret}(\mathsf{fst}(b))[({}^t v_{i1}, {}^t v_{i2})/b]\ \delta^t) \Downarrow^f (H'_{t1}, \mathsf{Lb}\,{}^t v_{i11})$:
    We get the desired from cg-fst and cg-ret and (F-F1.3)

(b) $\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_{t1}) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v_{i1}) \in \lfloor \tau_1 \rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta'_1$ and $\hat{\beta}'$ as $\hat{\beta}'_1$. And from fg-fst we know that $i = j+1$ and $H'_s = H'_{s1}$ therefore from (F-F1) and Lemma 5.34 we get

$(n-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1$

Since from fg-fst we know that ${}^s v = {}^s v_{i1}$ therefore from (F-F1.2) and Lemma 5.32 we get

$({}^s\theta', n-i, {}^s v_{i1}, {}^t v_{i1}) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'_1}$

10. FC-snd:

Symmetric reasoning as in the FC-fst case

11. FC-inl:

$$\frac{\Gamma \vdash_{pc} e : \tau_1 \leadsto e_t}{\Gamma \vdash_{pc} \mathsf{inl}(e_s) : (\tau_1 + \tau_2)^{\perp} \leadsto \mathsf{bind}(e_t, a.\mathsf{ret}(\mathsf{Lbinl}(a)))} \text{ inl}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{inl}(e_s)\ \delta^s, \mathsf{bind}(e_t, a.\mathsf{ret}(\mathsf{Lbinl}(a)))\delta^t) \in \lfloor (\tau_1 + \tau_2)^{\perp}\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we have

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\rhd} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, \mathsf{inl}(e_s)) \Downarrow_i (H_s', {}^s v) \implies$
$\exists H_t', {}^t v.(H_t, \mathsf{bind}(e_t, a.\mathsf{ret}(\mathsf{Lbinl}(a)))\ \delta^t) \Downarrow^f (H_t', {}^t v) \wedge \exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n - i, H_s', H_t') \overset{\hat{\beta}'}{\rhd} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$

This means that we are given some H_s, H_t s.t $(n, H_s, H_t) \overset{\gamma,\hat{\beta}}{\rhd} {}^s\theta$. Also given some $i < n, {}^s v$ s.t $(H_s, \mathsf{inl}(e_s)) \Downarrow_i (H_s', {}^s v)$

And we need to prove

$\exists H_t', {}^t v.(H_t, \mathsf{bind}(e_t, a.\mathsf{ret}(\mathsf{Lbinl}(a)))\delta^t) \Downarrow^f (H_t', {}^t v) \wedge \exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n - i, H_s', H_t') \overset{\hat{\beta}'}{\rhd} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor (\tau_1 + \tau_2)^{\perp}\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-IL0)

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we need to prove

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\rhd} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_s\ \delta^s) \Downarrow_j (H_{s1}', {}^s v_1) \implies$
$\exists H_{t1}', {}^t v_1.(H_{t1}, e_t) \Downarrow^f (H_{t1}', {}^t v_1) \wedge \exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}_1' \sqsupseteq \hat{\beta}.$
$(n - j, H_{s1}', H_{t1}') \overset{\hat{\beta}_1'}{\rhd} {}^s\theta' \wedge ({}^s\theta', n - j, {}^s v_1, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}_1'}$

Instantiating with H_s, H_t and since we know that $(H_s, \mathsf{inl}(e_s)) \Downarrow_i (H_s', {}^s v)$ therefore $\exists j < i < n$ s.t $(H_s, e_s\ \delta^s) \Downarrow_j (H_{s1}', {}^s v_1)$

Therefore we have

$\exists H_{t1}', {}^t v_1.(H_t, e_{t1}) \Downarrow^f (H_{t1}', {}^t v_1) \wedge \exists^s\theta_1' \sqsupseteq {}^s\theta, \hat{\beta}_1' \sqsupseteq \hat{\beta}.$
$(n - j, H_{s1}', H_{t1}') \overset{\hat{\beta}_1'}{\rhd} {}^s\theta_1' \wedge ({}^s\theta_1', n - j, {}^s v_1, {}^t v_1)) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}_1'}$ (F-IL1)

In order to prove (F-IL0) we choose H_t' as H_{t1}' and ${}^t v$ as $(\mathsf{Lb}\ \mathsf{inl}({}^t v_1))$ and we need to prove:

(a) $(H_t, \mathsf{bind}(e_t, a.\mathsf{ret}(\mathsf{Lbinl}(a)))\ \delta^t) \Downarrow^f (H_{t1}', (\mathsf{Lb}\ \mathsf{inl}({}^t v_1)))$:
   From cg-bind it suffices to prove that
   i. $(H_t, e_t\ \delta^t) \Downarrow^f (H_{t11}', {}^t v_{t11})$:
      From (F-IL1) we know that $H_{t11}' = H_{t1}'$ and ${}^t v_{t11} = {}^t v_1$
   ii. $(H_{t1}', \mathsf{ret}(\mathsf{Lbinl}(a))[{}^t v_1/a]\ \delta^t) \Downarrow^f (H_{t1}', (\mathsf{Lb}\ \mathsf{inl}({}^t v_1)))$:
      From cg-ret and (F-IL1)

(b) $\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor(\tau_1+\tau_2)^\perp\ \sigma\rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta_1'$ and $\hat{\beta}'$ as $\hat{\beta}_1'$. Since from fg-inl we know that $i = j+1$ and $H_s' = H_{s1}'$ therefore from (F-IL1) and Lemma 5.34 we get

$(n-i, H_{s1}', H_{t1}') \overset{\hat{\beta}_1'}{\triangleright} {}^s\theta_1'$

Now we need to prove $({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor(\tau_1+\tau_2)^\perp\ \sigma\rfloor_V^{\hat{\beta}'}$
Since ${}^sv = \mathsf{inl}\ {}^sv_1$ and ${}^tv = \mathsf{Lb}(\mathsf{inl}({}^tv_1))$ therefore from Definition 5.27 it suffices to prove that
$({}^s\theta', n-i, \mathsf{inl}\ {}^sv_1, \mathsf{inl}\ {}^tv_1) \in \lfloor(\tau_1+\tau_2)\ \sigma\rfloor_V^{\hat{\beta}'}$

Since from (F-IL1) we know that $({}^s\theta', n-j, {}^sv_1, {}^tv_1) \in \lfloor\tau_1\ \sigma\rfloor_V^{\hat{\beta}'}$
Therefore from Lemma 5.32 and Definition 5.27 we get
$({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor(\tau_1+\tau_2)\ \sigma\rfloor_V^{\hat{\beta}'}$

12. FC-inr:

Symmetric reasoning as in the FC-inl case

13. FC-case:

$$\frac{\Gamma \vdash_{pc} e_s : (\tau_1+\tau_2)^\ell \rightsquigarrow e_t \qquad \Gamma, x:\tau_1 \vdash_{pc\sqcup\ell} e_{s1} : \tau \rightsquigarrow e_{t1} \qquad \Gamma, x:\tau_1 \vdash_{pc\sqcup\ell} e_{s2} : \tau \rightsquigarrow e_{t2} \qquad \mathcal{L} \vdash \tau \searrow \ell}{\Gamma \vdash_{pc} \mathsf{case}(e_s, x.e_{s1}, y.e_{s2}) : \tau \rightsquigarrow \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{t1}, y.e_{t2}))))}\ \text{case}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor\Gamma\ \sigma\rfloor_V^{\hat{\beta}}$

To prove:

$({}^s\theta, n, \mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{t1}, y.e_{t2}))))\ \delta^t) \in \lfloor\tau\ \sigma\rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^sv.(H_s, \mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s) \Downarrow_i (H_s', {}^sv) \implies$
$\exists H_t', {}^tv.(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{t1}, y.e_{t2}))))\ \delta^t) \Downarrow^f (H_t', {}^tv) \wedge$

$\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}'}$

This means we are given some H_s, H_t s.t $(n, H_s, H_t) \overset{\gamma,\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^sv$ s.t $(H_s, \mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s) \Downarrow_i (H_s', {}^sv)$
And we need to prove
$\exists H_t', {}^tv.(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{t1}, y.e_{t2}))))\ \delta^t) \Downarrow^f (H_t', {}^tv) \wedge$

$\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^sv, {}^tv) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}'}$ (F-C0)

<u>IH1:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\tau_1 + \tau_2)^\ell\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_s) \Downarrow_j (H'_{s1}, {}^s v_1) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n - j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n - j, {}^s v_1, {}^t v_1) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_1}$

Instantiating with H_s, H_t and since we know that $(H_s, \mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists j < i < n$ s.t $(H_{s1}, e_s) \Downarrow_j (H'_{s1}, {}^s v_1)$
Therefore we have
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n - j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n - j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 + \tau_2)^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-C1)

Since from (F-C1) we have $({}^s\theta'_1, n - j, {}^s v_1, {}^t v_1) \in \lfloor (\tau_1 + \tau_2)^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$ therefore from Definition 5.27 we know that
$\exists^t v_i.{}^t v_1 = \mathsf{Lb}({}^t v_i) \wedge ({}^s\theta'_1, n - j, {}^s v_1, {}^t v_i) \in \lfloor (\tau_1 + \tau_2)\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-C1.1)

2 cases arise

(a) ${}^s v_1 = \mathsf{inl}({}^s v_{i1})$ and ${}^t v_i = \mathsf{inl}({}^t v_{i1})$:

Also from Lemma 5.33 and Definition 5.31 we know that
$({}^s\theta'_1, n - j, \delta^s \cup \{x \mapsto {}^s v_1\}, \delta^t \cup \{x \mapsto {}^t v_{i1}\}) \in \lfloor (\Gamma, \{x \mapsto {}^s v_1\}) \rfloor_V^{\hat{\beta}'_1}$
<u>IH2:</u>
$({}^s\theta'_1, n - j, e_{s1}\ \delta^s \cup \{x \mapsto {}^s v_1\}, e_{t1}\ \delta^t \cup \{x \mapsto {}^t v_{i1}\}) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'_1}$

This means from Definition 5.28 we have
$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge \forall k < n - j, {}^s v_2.(H_{s2}, e_{s1}\ \delta^s \cup \{x \mapsto {}^s v_1\}) \Downarrow_j (H'_{s2}, {}^s v_2) \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t1}\ \delta^t \cup \{x \mapsto {}^t v_{i1}\}) \Downarrow^f (H'_{t2}, {}^t v_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_1.$
$(n - j - k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n - j - k, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_2}$

Instantiating with H'_{s1}, H'_{t1} and since we know that $(H_s, \mathsf{case}(e_s, x.e_{s1}, y.e_{s2})\ \delta^s \cup \{x \mapsto {}^s v_1\}) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists k < i - j < n - j$ s.t $(H'_{s1}, e_{s1}) \Downarrow_k (H'_{s2}, {}^s v_2)$
Therefore we have
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t1}\ \delta^t \cup \{x \mapsto {}^t v_1\}) \Downarrow^f (H'_{t2}, {}^t v_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_1.$
$(n - j - k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n - j - k, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_2}$ (F-C2)

Let $\tau = \mathsf{A}^{\ell_i}$ and since we know that $\tau \searrow \ell$ therefore we have $\ell \sqsubseteq \ell_i$

Since we have $({}^s\theta'_2, n - j - k, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_2}$
Therefore from Definition 5.27 we have
$({}^s\theta'_2, n - j - k, {}^s v_2, \mathsf{Lb}\,{}^t v_{2i}) \in \lfloor \mathsf{A}^{\ell_i} \rfloor_V^{\hat{\beta}'_2}$ (F-C2.1)

In order to prove (F-C0) we choose H'_t as H'_{t2} and ${}^t v$ as ${}^t v_2 = \mathsf{Lb}\,{}^t v_{2i}$
And we need to prove:

i. $(H_t, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{t1}, y.e_{t2})))) \ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}\,{}^t v_{2i})$:
From Lemma 5.35 it suffices to prove that
$(H_t, (\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{t1}, y.e_{t2})))) \ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}\,{}^t v_{2i})$

From cg-bind it suffices to prove that

- $(H_t, e_t \ \delta^t) \Downarrow^f (H'_{t11}, {}^t v_{t11})$:
  From (F-C1) we know that $H'_{t11} = H'_{t1}$ and ${}^t v_{t11} = {}^t v_1$
- $(H'_{t1}, \mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{case}(b, x.e_{t1}, y.e_{t2}))[{}^t v_1/a] \ \delta^t) \Downarrow^f (H'_{t2}, \mathsf{Lb}\,{}^t v_{2i})$:
  From cg-bind it suffices to prove that
  - $(H'_{t1}, (\mathsf{unlabel}\ a)[{}^t v_1/a] \ \delta^t) \Downarrow^f (H'_{t21}, {}^t v_{t21})$:
    Since from (F-C1.1) we know that ${}^t v_1 = \mathsf{Lb}({}^t v_i)$ therefore from cg-unlabel we know that
    $H'_{t21} = H'_{t1}$ and ${}^t v_{t21} = {}^t v_i$
  - $(\mathsf{case}(b, x.e_{t1}, y.e_{t2})[{}^t v_i/b]\delta^t) \Downarrow {}^t v_{t22}$:
    Since we know that in this case ${}^t v_i = \mathsf{inl}({}^t v_{i1})$
    Therefore from cg-case we know that ${}^t v_{t22} = e_{t1}[{}^t v_{i1}/x] \ \delta^t$
  - $(H'_{t1}, e_{t1}[{}^t v_{i1}/x] \ \delta^t) \Downarrow (H'_{t2}, \mathsf{Lb}\,{}^t v_{2i})$:
    From (F-C2) and (F-C2.1) we get the desired

ii. $\exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau \ \sigma \rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta'_2$ and $\hat{\beta}'$ as $\hat{\beta}'_2$. Since from fg-case we know that $i = j + k + 1$ and $H'_s = H'_{s2}$ therefore from (F-C2) and Lemma 5.34 we get
$(n-i, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2$

Now we need to prove $({}^s\theta'_2, n-i, {}^s v, {}^t v) \in \lfloor \tau \ \sigma \rfloor_V^{\hat{\beta}'_2}$
Since ${}^s v = {}^s v_2$ and ${}^t v = {}^t v_2$ and since from (F-C2) we know that
$({}^s\theta'_2, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau \ \sigma \rfloor_V^{\hat{\beta}'_2}$
Therefore from Lemma 5.32 and Definition 5.27 we get
$({}^s\theta'_2, n-i, {}^s v_2, {}^t v_2) \in \lfloor \tau \ \sigma \rfloor_V^{\hat{\beta}'_2}$

(b) ${}^s v_1 = \mathsf{inr}({}^s v_{i1})$ and ${}^t v_1 = \mathsf{inr}({}^t v_{i1})$:
Symmetric reasoning as in the previous case

14. FC-ref:

$$\frac{\Gamma \vdash_{pc} e_s : \tau \rightsquigarrow e_t \qquad \mathcal{L} \vdash \tau \searrow pc}{\Gamma \vdash_{pc} \mathsf{new}\ (e_s) : (\mathsf{ref}\ \tau)^{\perp} \rightsquigarrow \mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb} b)))} \text{ ref}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, \mathsf{new}\ (e_s) \ \delta^s, \mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb} b)) \ \delta^t) \ \delta^t) \in \lfloor (\mathsf{ref}\ \tau)^{\perp} \ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we have

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, \mathsf{new}\ (e_s) \ \delta^s) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb} b))) \ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor (\mathsf{ref}\ \tau)^{\perp} \ \sigma \rfloor_V^{\hat{\beta}'}$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\gamma,\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^s v$ s.t $(H_s, \mathsf{new}\ (e_s)\ \delta^s) \Downarrow_i (H'_s, {}^s v)$.

And we are required to prove

$\exists H'_t, {}^t v.(H_t, \mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb} b)))\ \delta^t) \Downarrow^f (H'_t, {}^t v) \wedge \exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor (\mathsf{ref}\ \tau)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-R0)

IH:

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we have

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_s\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n - j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n - j, {}^s v_1, {}^t v_1) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_1}$

Instantiating with H_s, H_t and since we know that $(H_s, \mathsf{new}\ (e_s)\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore we know that $\exists j < n$ s.t $(H_s, e_s\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1)$.

Therefore we have

$\exists H'_{t1}, {}^t v_1.(H_t, e_t\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n - j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n - j, {}^s v_1, {}^t v_1) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-R1)

In order to prove (F-R0) we choose H'_t as $H'_1 \cup \{a_t \mapsto {}^t v_1\}$, ${}^t v = \mathsf{Lb}(a_t)$, ${}^s\theta'$ as ${}^s\theta'_1 \cup \{a_s \mapsto \tau\}$ and $\hat{\beta}'$ as $\hat{\beta}'_1 \cup \{(a_s, a_t)\}$

And we need to prove:

(a) $(H_t, \mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb}\ b)))\ \delta^t) \Downarrow^f (H'_t, {}^t v)$:
From cg-bind it suffices to prove that
- $(H_t, e_t\ \delta^t) \Downarrow^f (H'_{t11}, {}^t v_{t1})$:
From (F-R1) we know that $H'_{t11} = H'_{t1}$ and ${}^t v_{t1} = {}^t v_1$
- $(H'_{t1}, \mathsf{bind}(\mathsf{new}\ (a), b.\mathsf{ret}(\mathsf{Lb}\ b))[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_t, {}^t v)$:
From cg-bind it suffices to prove that
  i. $(H'_{t1}, \mathsf{new}\ (a)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_t, {}^t v_{t2})$:
  From cg-new we know that $H'_t = H'_{t1} \cup \{a_t \mapsto {}^t v_1\}$ and ${}^t v = a_t$
  ii. $(H'_1 \cup \{a_t \mapsto {}^t v_1\}, \mathsf{ret}(\mathsf{Lb} b))[{}^t v_1/a][a_t/b]\ \delta^t) \Downarrow^f (H'_t, {}^t v_t)$:
  From cg-ret we know that $H'_t = H'_{t1} \cup \{a_t \mapsto {}^t v_1\}$ and ${}^t v_t = \mathsf{Lb}(a_t)$

(b) $\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor (\mathsf{ref}\tau)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$:

From (F-R1) we know that $(n - j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1$ and since $H'_s = H'_{s1} \cup \{a_s \mapsto {}^s v_1\}$, $H'_t = H'_{t1} \cup \{a_t \mapsto {}^t v_1\}$, ${}^s\theta' = {}^s\theta'_1 \cup \{a_s \mapsto \tau\}$

Therefore from Definition 5.29 and Lemma 5.34 we get $(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta'$

To prove: $({}^s\theta', n - i, {}^s v, {}^t v) \in \lfloor (\mathsf{ref}\ \tau)^\perp\ \sigma \rfloor_V^{\hat{\beta}'}$

Since we know that ${}^s v = a_s$ and ${}^t v = \mathsf{Lb}\ a_t$ therefore we need to prove

$({}^s\theta', n-i, a_s, \mathsf{Lb}(a_t)) \in \lfloor (\mathsf{ref}\ \tau)^{\perp}\ \sigma \rfloor_V^{\hat{\beta}'}$

From Definition 5.27 it suffices to prove that

$({}^s\theta', n-i, a_s, a_t) \in \lfloor (\mathsf{ref}\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'}$

Again from Definition 5.27 it suffices to prove that

${}^s\theta'(a_s) = \tau \wedge (a_s, a_t) \in \hat{\beta}'$

We get this by construction

15. FC-deref:

$$\frac{\Gamma \vdash_{pc} e_s : (\mathsf{ref}\ \tau)^{\ell} \rightsquigarrow e_t \qquad \mathcal{L} \vdash \tau <: \tau' \qquad \mathcal{L} \vdash \tau' \searrow \ell}{\Gamma \vdash_{pc} !e_s : \tau' \rightsquigarrow \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))}\ \text{deref}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove: $({}^s\theta, n, !e\ \delta^s, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))\delta^t) \in \lfloor \tau'\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we need to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, !e_s) \Downarrow_i (H_s', {}^s v) \implies$
$\exists H_t', {}^t v.(H_t, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))) \Downarrow^f (H_t', {}^t v) \wedge \exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}'}$

This means that we are given some H_s, H_t s.t $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^s v$ s.t $(H_s, !e_s) \Downarrow_i (H_s', {}^s v)$

And we need to prove

$\exists H_t', {}^t v.(H_t, \texttt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))) \Downarrow^f (H_t', {}^t v) \wedge \exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-i, H_s', H_t') \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}'}$ (F-DR0)

<u>IH:</u>

$({}^s\theta, n, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor (\mathsf{ref}\ \tau)^{\ell}\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we need to prove

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_s) \Downarrow_j (H_{s1}', {}^s v_1) \implies$
$\exists H_{t1}', {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H_{t1}', {}^t v_1) \wedge \exists^s\theta_1' \sqsupseteq {}^s\theta, \hat{\beta}_1' \sqsupseteq \hat{\beta}.$
$(n-j, H_{s1}', H_{t1}') \overset{\hat{\beta}_1'}{\triangleright} {}^s\theta_1' \wedge ({}^s\theta_1', n-j, {}^s v_1, {}^t v_1) \in \lfloor (\mathsf{ref}\ \tau)^{\ell}\ \sigma \rfloor_V^{\hat{\beta}_1'}$

Instantiating with H_s, H_t and since we know that $(H_s, !e_s) \Downarrow_i (H_s', {}^s v)$ therefore $\exists j < n$ s.t $(H_{s1}, e_s) \Downarrow_j (H_{s1}', {}^s v)$

Therefore we have

$\exists H_{t1}', {}^t v_1.(H_{t1}, e_t\ \delta^t) \Downarrow^f (H_{t1}', {}^t v_1) \wedge \exists^s\theta_1' \sqsupseteq {}^s\theta, \hat{\beta}_1' \sqsupseteq \hat{\beta}.$
$(n-j, H_{s1}', H_{t1}') \overset{\hat{\beta}_1'}{\triangleright} {}^s\theta_1' \wedge ({}^s\theta_1', n-j, {}^s v_1, {}^t v_1) \in \lfloor (\mathsf{ref}\ \tau)^{\ell}\ \sigma \rfloor_V^{\hat{\beta}_1'}$ (F-DR1)

From (F-DR1) we have $({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor(\mathsf{ref}\ \tau)^\ell\ \sigma\rfloor_V^{\hat{\beta}'_1}$

From Definition 5.27 we have
$\exists^t v_i.{}^t v_1 = \mathsf{Lb}({}^t v_i) \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_i) \in \lfloor(\mathsf{ref}\ \tau)\ \sigma\rfloor_V^{\hat{\beta}'_1}$ (F-DR1.1)

From Definition 5.27 we know that ${}^s v_1 = a_s$ and ${}^t v_i = a_t$
${}^s\theta'_1(a_s) = \tau \wedge (a_s, a_t) \in \hat{\beta}'_1$ (F-DR1.2)

Since we are given that $(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta$ therefore from Definition 5.29 we know that
$({}^s\theta, n-1, H_s(a_s), H_t(a_t)) \in \lfloor {}^s\theta(a_s)\rfloor_V^{\hat{\beta}}$
which means we have
$({}^s\theta, n-1, H_s(a_s), H_t(a_t)) \in \lfloor \tau\ \sigma\rfloor_V^{\hat{\beta}}$

From Lemma 5.37 we know that
$({}^s\theta, n-1, H_s(a_s), H_t(a_t)) \in \lfloor \tau'\ \sigma\rfloor_V^{\hat{\beta}}$

Let $\tau' = \mathsf{A}'^{\ell_i}$ since $\tau' \searrow \ell$ therefore $\ell \sqsubseteq \ell_i$
Let $v_g = H_t(a_t)$ therefore from Definition 5.27 we have
$({}^s\theta, n-1, H_s(a_s), \mathsf{Lb}\, v_{gi}) \in \lfloor \tau'\ \sigma\rfloor_V^{\hat{\beta}}$ (F-DR1.3)

In order to prove (F-DR0) we choose H'_t as H'_{t1} and ${}^t v$ as $H'_{t1}(a_t) = v_g = \mathsf{Lb}\, v_{gi}$

(a) $(H_t, \mathtt{coerce\_taint}(\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))\ \delta^t) \Downarrow^f (H'_{t1}, \mathsf{Lb}\, v_{gi})$:

From Lemma 5.35 it suffices to prove that
$(H_t, (\mathsf{bind}(e_t, a.\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))\ \delta^t) \Downarrow^f (H'_{t1}, \mathsf{Lb}\, v_{gi})$
From cg-bind it suffices to prove

i. $(H_t, e_t\ \delta^t) \Downarrow^f (H'_{t11}, {}^t v_{t1})$:
From (F-DR1) we know that $H'_{t11} = H'_{t1}$ and ${}^t v_{t1} = {}^t v_1$

ii. $(H'_{t1}, \mathsf{bind}(\mathsf{unlabel}\ a, b.!b)[{}^t v_1/a]\delta^t) \Downarrow^f (H'_{t1}, \mathsf{Lb}\, v_{gi})$:
From cg-bind it suffices to prove that

A. $(H'_{t1}, (\mathsf{unlabel}\ a)[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t21}, {}^t v_{t21})$:
From (F-DR1.1) we know that ${}^t v_1 = \mathsf{Lb}({}^t v_i)$
Therefore from cg-unlabel we know that $H'_{t21} = H'_{t1}$ and ${}^t v_{t21} = {}^t v_i$

B. $(H'_{t1}, (!b)[{}^t v_1/a][{}^t v_i/b]\ \delta^t) \Downarrow^f (H'_{t1}, \mathsf{Lb}\, v_{gi})$:
We get the desired from CG-deref, (F-DR1.2) and (F-DR1.3)

(b) $\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, \mathsf{Lb}\, v_{gi}) \in \lfloor \tau'\ \sigma\rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta'_1$ and $\hat{\beta}'$ as $\hat{\beta}'_1$

Therefore from (F-DR1) we get $(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1$ and snce $i = j+1$ therefore from Lemma 5.34 we get $(n-i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1$

Since from (F-DR1.2) we know that $(a_s, a_t) \in \hat{\beta}'_1$ and ${}^s\theta'_1(a_s) = \tau$. Also from (F-DR1) we have $(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1$. Therefore from Definition 5.28 we have $(n - j - 1, H'_{s1}(a_s), H'_{t1}(a_t)) \in \lfloor {}^s\theta'_1(a_s) \rfloor_V^{\hat{\beta}'_1}$

Since $i = j + 1$, ${}^s\theta'_1(a_s) = \tau$, $H'_{s1}(a_s) = {}^s v$ and $H'_{t1}(a_t) = {}^t v_g = \mathsf{Lb}\, v_{gi}$

Therefore we get $({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau' \rfloor_V^{\hat{\beta}'}$

from (F-DR1.3) and Lemma 5.32

16. FC-assign:

$$\frac{\Gamma \vdash_{pc} e_{s1} : (\mathsf{ref}\ \tau)^\ell \rightsquigarrow e_{t1} \qquad \Gamma \vdash_{pc} e_{s2} : \tau \rightsquigarrow e_{t2} \qquad \mathcal{L} \vdash \tau \searrow (pc \sqcup \ell)}{\begin{array}{c}\Gamma \vdash_{pc} e_{s1} := e_{s2} : \mathsf{unit} \rightsquigarrow \\ \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())\end{array}} \text{ assign}$$

Also given is: $({}^s\theta, n, \delta^s, \delta^t) \in \lfloor \Gamma \rfloor_V^{\hat{\beta}}$

To prove:

$({}^s\theta, n, (e_{s1} := e_{s2})\ \delta^s, \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())\ \delta^t) \in \lfloor \mathsf{unit} \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we are required to prove

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, (e_{s1} := e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())\ \delta^t) \Downarrow^f$
$(H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}'}$

This means that given some H_s, H_t s.t $(n, H_s, H_t) \overset{\gamma,\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $i < n, {}^s v$ s.t $(H_s, (e_{s1} := e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$

And we need to prove

$\exists H'_t, {}^t v.(H_t, \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())\ \delta^t) \Downarrow^f$
$(H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}'}$ (F-AN0)

<u>IH1:</u>

$({}^s\theta, n, e_{s1}\ \delta^s, e_{t1}\ \delta^t) \in \lfloor (\mathsf{ref}\tau)^\ell\ \sigma \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we are required to prove

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\gamma,\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_{s1}\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\mathsf{ref}\ \tau)^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$

Instantiating with H_s, H_t and since we know that $(H_s, (e_{s1} := e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists j < n$ s.t $(H_{s1}, e_{s1}\ \delta^s) \Downarrow_j (H'_{s1}, {}^s v_1)$

Therefore we have

$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_{t1}\ \delta^t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\mathsf{ref}\ \tau)^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-AN1)

Since from (F-AN1) we know that $({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor (\mathsf{ref}\ \tau)^\ell\ \sigma \rfloor_V^{\hat{\beta}'_1}$ therefore from Definition 5.27 we have

$\exists^t v_i. {}^t v_1 = \mathsf{Lb}({}^t v_i) \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_i) \in \lfloor (\mathsf{ref}\ \tau)\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (F-AN1.1)

From Definition 5.27 this further means that

${}^s\theta'_1(a_s) = \tau \wedge (a_s, a_t) \in \hat{\beta}'_1$ where ${}^s v_1 = a_s$ and ${}^t v_1 = a_t$ (F-AN1.2)

IH2:

$({}^s\theta'_1, n-j, e_{s2}\ \delta^s, e_{t2}\ \delta^t) \in \lfloor \tau\ \sigma \rfloor_E^{\hat{\beta}'_1}$

This means from Definition 5.28 we are required to prove

$\forall H_{s2}, H_{t2}.(n, H_{s2}, H_{t2}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge \forall k < n-j, {}^s v_2.(H_{s2}, e_{s2}\ \delta^s) \Downarrow_k (H'_{s2}, {}^s v_2) \implies$
$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t2}\ \delta^t) \Downarrow^f (H'_{t2}, {}^t v_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_1.$
$(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_2}$

Instantiating with H'_{s1}, H'_{t1} and since we know that $(H_s, (e_{s2} := e_{s2})\ \delta^s) \Downarrow_i (H'_s, {}^s v)$ therefore $\exists k < n-j$ s.t $(H_{s2}, e_{s2}\ \delta^s) \Downarrow_k (H'_{s2}, {}^s v_2)$

Therefore we have

$\exists H'_{t2}, {}^t v_2.(H_{t2}, e_{t2}\ \delta^t) \Downarrow^f (H'_{t2}, {}^t v_2) \wedge \exists^s\theta'_2 \sqsupseteq {}^s\theta'_1, \hat{\beta}'_2 \sqsupseteq \hat{\beta}'_1.$
$(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\triangleright} {}^s\theta'_2 \wedge ({}^s\theta'_2, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_2}$ (F-AN2)

In order to prove (F-AN0) we choose H'_t as $H'_{t2}[a_t \mapsto {}^s v_2]$, ${}^t v$ as ()

We need to prove

(a) $(H_t, \mathsf{bind}(\mathsf{toLabeled}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))), d.\mathsf{ret}())\ \delta^t) \Downarrow^f (H'_t, {}^t v)$:
From cg-bind it suffices to prove that
- $(H_t, \mathsf{toLabeled}(\mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b))))\ \delta^t) \Downarrow^f (H'_T, {}^t v_T)$:

From cg-toLabeled it suffices to prove that
$(H_t, \mathsf{bind}(e_{t1}, a.\mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)))\delta^t) \Downarrow^f (H'_T, {}^t v_{Ti})$
where ${}^t v_T = \mathsf{Lb}\, {}^t v_{Ti}$
From cg-bind it further suffices to prove that:

- $(H_t, e_{t1}\ \delta^t) \Downarrow^f (H'_{t11}, {}^t v_{t11})$:
  From (F-AN1) we know that $H'_{t11} = H'_{t1}$ and ${}^t v_{t11} = {}^t v_1$
- $(H'_{t1}, \mathsf{bind}(e_{t2}, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b))[{}^t v_1/a]\ \delta^t) \Downarrow^f (H'_{t12}, {}^t v_{t12})$:
  From cg-bind it suffices to prove
  - $(H'_{t1}, e_{t2}\ \delta^t) \Downarrow^f (H'_{t13}, {}^t v_{t13})$:
    From (F-AN2) we know that $H'_{t13} = H'_{t2}$ and ${}^t v_{t13} = {}^t v_2$

– $(H'_{t1}, \mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)[{}^t v_1/a][{}^t v_2/b]\ \delta^t) \Downarrow^f (H'_t, {}^t v_{t12})$:
From cg-bind it suffices to prove that

∗ $(H'_{t1}, \mathsf{unlabel}\ a[{}^t v_1/a][{}^t v_2/b]\ \delta^t) \Downarrow^f (H'_{t21}, {}^t v_{t21})$:
From (F-AN1.1) we know that
${}^t v_1 = \mathsf{Lb}({}^t v_i) \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_i) \in \lfloor(\mathsf{ref}\ \tau)\ \sigma\rfloor_V^{\hat{\beta}'_1}$
Therefore from cg-unlabel we know that $H'_{t21} = H'_{t1}$ and ${}^t v_{t21} = {}^t v_i = a_t$

∗ $(H'_{t1}, (c := b)[{}^t v_1/a][{}^t v_2/b][{}^t v_i/c]\ \delta^t) \Downarrow^f (H'_t, {}^t v)$:
From cg-assign we know that $H'_t = H'_{t1}[a_t \mapsto {}^t v_2]$ and ${}^t v_{t12} = ()$

Since ${}^t v_{t12} = {}^t v_{Ti} = ()$ therefore ${}^t v_T = \mathsf{Lb}()$
- $(H'_T, \mathsf{ret}()[{}^t v_T/d])\ \delta^t) \Downarrow^f (H'_t, ())$:
From cg-ret and cg-val

(b) $\exists^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\rhd} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}'}$:
We choose ${}^s\theta'$ as ${}^s\theta'_2$ and $\hat{\beta}'$ as $\hat{\beta}'_2$

In order to prove $(n-i, H'_s, H'_t) \overset{\hat{\beta}'_2}{\rhd} {}^s\theta'_2$ it suffices to prove

- $dom({}^s\theta'_2) \subseteq dom(H'_s)$:

  Since from (F-AN2) we know that $(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\rhd} {}^s\theta'_2$ therefore from Definition 5.29 we get $dom({}^s\theta'_2) \subseteq dom(H'_s)$
- $\hat{\beta}'_2 \subseteq (dom({}^s\theta'_2) \times dom(H'_t))$:

  Since from (F-AN2) we know that $(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\rhd} {}^s\theta'_2$ therefore from Definition 5.29 we get
  $\hat{\beta}'_2 \subseteq (dom({}^s\theta'_2) \times dom(H'_t))$
- $\forall (a_1, a_2) \in \hat{\beta}'_2.({}^s\theta'_2, n-i-1, H'_s(a_1), H'_t(a_2)) \in \lfloor {}^s\theta'_2(a_1)\rfloor_V^{\hat{\beta}}$:
  $\forall (a_1, a_2) \in \hat{\beta}'_2$.
  – $a_1 = a_s$ and $a_1 = a_t$:
    Since from (F-AN2) we know that $({}^s\theta'_2, n-j-k, {}^s v_2, {}^t v_2) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}'_2}$
    Also from (F-AN1.2) and Definition 5.25 we know that ${}^s\theta'_2(a_1) = \tau$
    Therefore from Lemma 5.32 we get
    $({}^s\theta'_2, n-i-1, {}^s v_2, {}^t v_2) \in \lfloor\tau\ \sigma\rfloor_V^{\hat{\beta}'_2}$
  – $a_1 \neq a_s$ and $a_1 \neq a_t$:
    From (F-AN2) since we know that $(n-j-k, H'_{s2}, H'_{t2}) \overset{\hat{\beta}'_2}{\rhd} {}^s\theta'_2$ therefore from Definition 5.29 we get
    $({}^s\theta'_2, n-j-k-1, H'_{s2}(a_1), H'_{t2}(a_2)) \in \lfloor {}^s\theta'_2(a_1)\rfloor_V^{\hat{\beta}'_2}$
    Since $i = j+k+1$ therefore from Lemma 5.32 we get
    $({}^s\theta'_2, n-i-1, H'_{s2}(a_1), H'_{t2}(a_2)) \in \lfloor {}^s\theta'_2(a_1)\rfloor_V^{\hat{\beta}'_2}$
  – $a_1 = a_s$ and $a_1 \neq a_t$:
    This case cannot arise
  – $a_1 \neq a_s$ and $a_1 = a_t$:
    This case cannot arise

And in order to prove $({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor\mathsf{unit}\rfloor_V^{\hat{\beta}'}$
Since we know that ${}^s v = ()$ and ${}^t v = ()$ therefore from Definition 5.27 we get $({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor\mathsf{unit}\rfloor_V^{\hat{\beta}'}$

□

Lemma 5.37 (Subtyping lemma). *The following holds:*
$\forall \Sigma, \Psi, \sigma, \mathcal{L}, \hat{\beta}$.

1. $\forall \mathsf{A}, \mathsf{A}'$.

   (a) $\Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor (\mathsf{A}\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\mathsf{A}'\ \sigma) \rfloor_V^{\hat{\beta}}$

2. $\forall \tau, \tau'$.

   (a) $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor (\tau\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau'\ \sigma) \rfloor_V^{\hat{\beta}}$

   (b) $\Sigma; \Psi \vdash \tau <: \tau' \wedge \mathcal{L} \models \Psi\ \sigma \implies \lfloor (\tau\ \sigma) \rfloor_E^{\hat{\beta}} \subseteq \lfloor (\tau'\ \sigma) \rfloor_E^{\hat{\beta}}$

Proof. Proof by simultaneous induction on $\mathsf{A} <: \mathsf{A}'$ and $\tau <: \tau'$
Proof of statement 1(a)
We analyse the different cases of $\mathsf{A} <: \mathsf{A}'$ in the last step:

1. FGsub-arrow:

   Given:
   $$\frac{\mathcal{L} \vdash \tau_1' <: \tau_1 \qquad \mathcal{L} \vdash \tau_2 <: \tau_2' \qquad \mathcal{L} \vdash \ell_e' \sqsubseteq \ell_e}{\mathcal{L} \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'}\ \text{FGsub-arrow}$$

   To prove: $\lfloor ((\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor ((\tau_1' \xrightarrow{\ell_e'} \tau_2')\ \sigma) \rfloor_V^{\hat{\beta}}$

   IH1: $\lfloor (\tau_1'\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau_1\ \sigma) \rfloor_V^{\hat{\beta}}$ (Statement 2(a))

   It suffices to prove: $\forall ({}^s\theta, m, \lambda x.e_s, (\lambda x.e_t)) \in \lfloor ((\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$.
   $({}^s\theta, m, \lambda x.e_s, (\lambda x.e_t)) \in \lfloor ((\tau_1' \xrightarrow{\ell_e'} \tau_2')\ \sigma) \rfloor_V^{\hat{\beta}}$

   This means that given some ${}^s\theta, m$ and $\lambda x.e_s, (\lambda x.e_t)$ s.t
   $({}^s\theta, m, \lambda x.e_s, (\lambda x.e_t)) \in \lfloor ((\tau_1 \xrightarrow{\ell_e} \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$
   Therefore from Definition 5.27 we are given:
   $\forall {}^s\theta_1' \sqsupseteq {}^s\theta, {}^s v_1, {}^t v_1, j < m, \hat{\beta} \sqsubseteq \hat{\beta}_1'.({}^s\theta_1', j, {}^s v_1, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}_1'} \implies$
   $({}^s\theta_1', j, e_s[{}^s v_1/x]\ \delta^s, e_t[{}^t v_1/x]\ \delta^t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}_1'}$ (S-L0)

   And it suffices to prove: $({}^s\theta, m, \lambda x.e_s, (\lambda x.e_t)) \in \lfloor ((\tau_1' \xrightarrow{\ell_e'} \tau_2')\ \sigma) \rfloor_V^{\hat{\beta}}$

   Again from Definition 5.27, it suffices to prove:
   $\forall {}^s\theta_2' \sqsupseteq {}^s\theta, {}^s v_2, {}^t v_2, k < m, \hat{\beta} \sqsubseteq \hat{\beta}_2'.({}^s\theta_2', k, {}^s v_2, {}^t v_2) \in \lfloor \tau_1'\ \sigma \rfloor_V^{\hat{\beta}_2'} \implies$
   $({}^s\theta_2', k, e_s[{}^s v_2/x]\ \delta^s, e_t[{}^t v_2/x]\ \delta^t) \in \lfloor \tau_2'\ \sigma \rfloor_E^{\hat{\beta}_2'}$ (S-L1)

   This means that given ${}^s\theta_2' \sqsupseteq {}^s\theta, {}^s v_2, {}^t v_2, k < m, \hat{\beta} \sqsubseteq \hat{\beta}_2'$ s.t $({}^s\theta_2', k, {}^s v_2, {}^t v_2) \in \lfloor \tau_1'\ \sigma \rfloor_V^{\hat{\beta}_2'}$
   And we need to prove

$({}^s\theta'_2, k, e_s[{}^s v_2/x]\ \delta^s, e_t[{}^t v_2/x]\ \delta^t) \in \lfloor \tau'_2\ \sigma \rfloor_E^{\hat{\beta}'_2}$ (S-L2)

Instantiating (S-L0) with ${}^s\theta'_2, {}^s v_2, {}^t v_2, k, \hat{\beta}'_2$. Since we have $({}^s\theta'_2, k, {}^s v_2, {}^t v_2) \in \lfloor \tau'_1\ \sigma \rfloor_V^{\hat{\beta}'_2}$ therefore from IH1 we also have

$({}^s\theta'_2, k, {}^s v_2, {}^t v_2) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}'_2}$

Therefore we get

$({}^s\theta'_2, k, e_s[{}^s v_2/x]\ \delta^s, e_t[{}^t v_2/x]\ \delta^t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}'_2}$

IH2: $\lfloor (\tau_2\ \sigma) \rfloor_E^{\hat{\beta}} \subseteq \lfloor (\tau'_2\ \sigma) \rfloor_E^{\hat{\beta}}$ (Statement 2(b))

Finally using IH2 we get

$({}^s\theta'_2, k, e_s[{}^s v_2/x]\ \delta^s, e_t[{}^t v_2/x]\ \delta^t) \in \lfloor \tau'_2\ \sigma \rfloor_E^{\hat{\beta}'_2}$

2. FGsub-forall:

   Given:

$$\frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2 \qquad \Sigma, \alpha; \Psi \vdash \ell'_e \sqsubseteq \ell_e}{\Sigma; \Psi \vdash \forall \alpha.(\ell_e, \tau_1) <: \forall \alpha.(\ell'_e, \tau_2)} \text{FGsub-forall}$$

   To prove: $\lfloor (\forall \alpha.(\ell_e, \tau_1)\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\forall \alpha.(\ell'_e, \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

   It suffices to prove: $\forall ({}^s\theta, m, \Lambda e_s, (\Lambda e_t)) \in \lfloor (\forall \alpha.(\ell_e, \tau_1)\ \sigma) \rfloor_V^{\hat{\beta}}$.
   $({}^s\theta, m, \Lambda e_s, (\Lambda e_t)) \in \lfloor (\forall \alpha.(\ell'_e, \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

   This means that given some ${}^s\theta, m$ and $\Lambda e_s, (\Lambda e_t)$ s.t

   $({}^s\theta, m, \Lambda e_s, (\Lambda e_t)) \in \lfloor (\forall \alpha.(\ell_e, \tau_1)\ \sigma) \rfloor_V^{\hat{\beta}}$
   Therefore from Definition 5.27 we are given:

   $\forall {}^s\theta'_1 \sqsupseteq {}^s\theta, j < m, \hat{\beta} \sqsubseteq \hat{\beta}'_1, \ell'_1 \in \mathcal{L}.({}^s\theta'_1, j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau_1[\ell'_1/\alpha]\ \sigma \rfloor_E^{\hat{\beta}'_1}$ (S-F0)

   And it suffices to prove: $({}^s\theta, m, \Lambda e_s, (\Lambda e_t)) \in \lfloor (\forall \alpha.(\ell'_e, \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

   Again from Definition 5.27, it suffices to prove:

   $\forall {}^s\theta'_2 \sqsupseteq {}^s\theta, k < m, \hat{\beta} \sqsubseteq \hat{\beta}'_2, \ell'_2 \in \mathcal{L}.({}^s\theta'_2, k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau_2[\ell'_2/\alpha]\ \sigma \rfloor_E^{\hat{\beta}'_2}$ (S-F1)

   This means that given ${}^s\theta'_2 \sqsupseteq {}^s\theta, k < m, \hat{\beta} \sqsubseteq \hat{\beta}'_2, \ell'_2 \in \mathcal{L}$
   And we need to prove

   $({}^s\theta'_2, k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau_2[\ell'_2/\alpha]\ \sigma \rfloor_E^{\hat{\beta}'_2}$ (S-F2)

   Instantiating (S-F0) with ${}^s\theta'_2, k, \hat{\beta}'_2, \ell'_2$ we get

   $({}^s\theta'_2, k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau_1[\ell'_2/\alpha]\ \sigma \rfloor_E^{\hat{\beta}'_2}$

   IH: $\lfloor (\tau_1[\ell'_2/\alpha]\ \sigma) \rfloor_E^{\hat{\beta}'_2} \subseteq \lfloor (\tau_2[\ell'_2/\alpha]\ \sigma) \rfloor_E^{\hat{\beta}'_2}$ (Statement 2(b))
   Finally using IH we get the desired.

3. FGsub-constraint:

Given:

$$\frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi \vdash \tau_1 <: \tau_2 \qquad \Sigma; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash c_1 \stackrel{\ell_e}{\Rightarrow} \tau_1 <: c_2 \stackrel{\ell_e'}{\Rightarrow} \tau_2} \text{ FGsub-constraint}$$

To prove: $\lfloor (c_1 \stackrel{\ell_e}{\Rightarrow} \tau_1)\ \sigma \rfloor_V^{\hat{\beta}} \subseteq \lfloor (c_2 \stackrel{\ell_e'}{\Rightarrow} \tau_2)\ \sigma \rfloor_V^{\hat{\beta}}$

It suffices to prove: $\forall ({}^s\theta, m, \nu e_s, (\nu e_t)) \in \lfloor (c_1 \stackrel{\ell_e}{\Rightarrow} \tau_1)\ \sigma \rfloor_V^{\hat{\beta}}$.
$({}^s\theta, m, \nu e_s, (\nu e_t)) \in \lfloor (c_2 \stackrel{\ell_e'}{\Rightarrow} \tau_2)\ \sigma \rfloor_V^{\hat{\beta}}$

This means that given some ${}^s\theta, m$ and $\nu e_s, (\nu e_t)$ s.t
$({}^s\theta, m, \nu e_s, (\nu e_t)) \in \lfloor (c_1 \stackrel{\ell_e}{\Rightarrow} \tau_1)\ \sigma \rfloor_V^{\hat{\beta}}$
Therefore from Definition 5.27 we are given:
$\forall {}^s\theta_1' \sqsupseteq {}^s\theta, j < m, \hat{\beta} \sqsubseteq \hat{\beta}_1'.\mathcal{L} \models c_1 \implies ({}^s\theta_1', j, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}_1'}$ (S-C0)

And it suffices to prove: $({}^s\theta, m, \nu e_s, (\nu e_t)) \in \lfloor (c_2 \stackrel{\ell_e'}{\Rightarrow} \tau_2)\ \sigma \rfloor_V^{\hat{\beta}}$

Again from Definition 5.27, it suffices to prove:
$\forall {}^s\theta_2' \sqsupseteq {}^s\theta, k < m, \hat{\beta} \sqsubseteq \hat{\beta}_2'.\mathcal{L} \models c_2 \implies ({}^s\theta_2', k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}_2'}$ (S-C1)

This means that given ${}^s\theta_2' \sqsupseteq {}^s\theta, k < m, \hat{\beta} \sqsubseteq \hat{\beta}_2'$ s.t $\mathcal{L} \models c_2$
And we need to prove

$({}^s\theta_2', k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau_2\ \sigma \rfloor_E^{\hat{\beta}_2'}$ (S-C2)

Instantiating (S-C0) with ${}^s\theta_2', k, \hat{\beta}_2'$ and since we know that $\mathcal{L} \models c_2\ \sigma \implies c_1\ \sigma$ therefore we get
$({}^s\theta_2', k, e_s\ \delta^s, e_t\ \delta^t) \in \lfloor \tau_1\ \sigma \rfloor_E^{\hat{\beta}_2'}$

IH: $\lfloor (\tau_1\ \sigma) \rfloor_E^{\hat{\beta}_2'} \subseteq \lfloor (\tau_2\ \sigma) \rfloor_E^{\hat{\beta}_2'}$ (Statement 2(b))
Finally using IH we get the desired.

4. FGsub-prod:

Given:

$$\frac{\mathcal{L} \vdash \tau_1 <: \tau_1' \qquad \mathcal{L} \vdash \tau_2 <: \tau_2'}{\mathcal{L} \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'} \text{ FGsub-prod}$$

To prove: $\lfloor ((\tau_1 \times \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor ((\tau_1' \times \tau_2')\ \sigma) \rfloor_V^{\hat{\beta}}$

IH1: $\lfloor (\tau_1\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau_1'\ \sigma) \rfloor_V^{\hat{\beta}}$ (Statement 2(a))

IH2: $\lfloor (\tau_2\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau_2'\ \sigma) \rfloor_V^{\hat{\beta}}$ (Statement 2(a))

It suffices to prove:

$\forall ({}^s\theta, m, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \in \lfloor ((\tau_1 \times \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}.\ \ ({}^s\theta, m, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \in \lfloor ((\tau_1' \times \tau_2')\ \sigma) \rfloor_V^{\hat{\beta}}$

This means that given some ${}^s\theta, n$ and ${}^s v_1, {}^s v_2, {}^t v_1, {}^t v_2$ s.t
$({}^s\theta, m, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \in \lfloor ((\tau_1 \times \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$
Therefore from Definition 5.27 we are given:
$({}^s\theta, m, {}^s v_1, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}} \wedge ({}^s\theta, m, {}^s v_2, {}^t v_2) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}}$ (S-P0)

And it suffices to prove: $({}^s\theta, m, ({}^s v_1, {}^s v_2), ({}^t v_1, {}^t v_2)) \in \lfloor ((\tau_1' \times \tau_2')\ \sigma) \rfloor_V^{\hat{\beta}}$

Again from Definition 5.27, it suffices to prove:
$({}^s\theta, m, {}^s v_1, {}^t v_1) \in \lfloor \tau_1'\ \sigma \rfloor_V^{\hat{\beta}} \wedge ({}^s\theta, m, {}^s v_2, {}^t v_2) \in \lfloor \tau_2'\ \sigma \rfloor_V^{\hat{\beta}}$ (S-P1)

Since from (S-P0) we know that $({}^s\theta, m, {}^s v_1, {}^t v_1) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}}$ therefore from IH1 we have $({}^s\theta, m, {}^s v_1, {}^t v_1) \in \lfloor \tau_1'\ \sigma \rfloor_V^{\hat{\beta}}$
Similarly since we have $({}^s\theta, m, {}^s v_2, {}^t v_2) \in \lfloor \tau_2\ \sigma \rfloor_V^{\hat{\beta}}$ from (S-P0) therefore from IH2 we have $({}^s\theta, m, {}^s v_2, {}^t v_2) \in \lfloor \tau_2'\ \sigma \rfloor_V^{\hat{\beta}}$

5. FGsub-sum:
   Given:

$$\frac{\mathcal{L} \vdash \tau_1 <: \tau_1' \qquad \mathcal{L} \vdash \tau_2 <: \tau_2'}{\mathcal{L} \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'}\ \text{FGsub-sum}$$

   To prove: $\lfloor ((\tau_1 + \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor ((\tau_1' + \tau_2')\ \sigma) \rfloor_V^{\hat{\beta}}$

   IH1: $\lfloor (\tau_1\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau_1'\ \sigma) \rfloor_V^{\hat{\beta}}$ (Statement 2(a))
   IH2: $\lfloor (\tau_2\ \sigma) \rfloor_V^{\hat{\beta}} \subseteq \lfloor (\tau_2'\ \sigma) \rfloor_V^{\hat{\beta}}$ (Statement 2(a))
   It suffices to prove: $\forall ({}^s\theta, n, {}^s v, {}^t v) \in \lfloor ((\tau_1 + \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}.\ ({}^s\theta, n, {}^s v, {}^t v) \in \lfloor ((\tau_1' + \tau_2')\ \sigma) \rfloor_V^{\hat{\beta}}$

   This means that given: $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor ((\tau_1 + \tau_2)\ \sigma) \rfloor_V^{\hat{\beta}}$

   And it suffices to prove: $({}^s\theta, n, {}^s v, {}^t v) \in \lfloor ((\tau_1' + \tau_2')\ \sigma) \rfloor_V^{\hat{\beta}}$

   2 cases arise

   (a) ${}^s v = \mathsf{inl}\ {}^s v_i$ and ${}^t v = \mathsf{inl}\ {}^t v_i$:
       From Definition 5.27 we are given:
       $({}^s\theta, n, {}^s v_i, {}^t v_i) \in \lfloor \tau_1\ \sigma \rfloor_V^{\hat{\beta}}$ (S-S0)

       And we are required to prove that:
       $({}^s\theta, n, {}^s v_i, {}^t v_i) \in \lfloor \tau_1'\ \sigma \rfloor_V^{\hat{\beta}}$
       From (S-S0) and IH1 get this

(b) ${}^{s}v = \mathsf{inr}\ {}^{s}v_i$ and ${}^{t}v = \mathsf{inr}\ {}^{t}v_i$:
Symmetric reasoning as in the previous case

6. FGsub-ref:
Given:

$$\frac{}{\mathcal{L} \vdash \mathsf{ref}\ \tau <: \mathsf{ref}\ \tau}\ \text{FGsub-ref}$$

To prove: $\lfloor((\mathsf{ref}\ \tau)\ \sigma)\rfloor_V^{\hat{\beta}} \subseteq \lfloor((\mathsf{ref}\ \tau)\ \sigma)\rfloor_V^{\hat{\beta}}$

It suffices to prove: $\forall({}^{s}\theta, n, a_s, a_t) \in \lfloor((\mathsf{ref}\ \tau)\ \sigma)\rfloor_V^{\hat{\beta}}.\ ({}^{s}\theta, n, a_s, a_t) \in \lfloor((\mathsf{ref}\ \tau)\ \sigma)\rfloor_V^{\hat{\beta}}$
We get this directly from Definition 5.27

7. FGsub-base:
Given:

$$\frac{}{\mathcal{L} \vdash \mathsf{b} <: \mathsf{b}}\ \text{FGsub-base}$$

To prove: $\lfloor((\mathsf{b}))\rfloor_V^{\hat{\beta}} \subseteq \lfloor((\mathsf{b}))\rfloor_V^{\hat{\beta}}$

Directly from Definition 5.27

8. FGsub-unit:
Given:

$$\frac{}{\mathcal{L} \vdash \mathsf{unit} <: \mathsf{unit}}\ \text{FGsub-unit}$$

To prove: $\lfloor((\mathsf{unit}))\rfloor_V^{\hat{\beta}} \subseteq \lfloor((\mathsf{unit}))\rfloor_V^{\hat{\beta}}$

Directly from Definition 5.27

Proof of statement 2(a)
Given:

$$\frac{\mathcal{L} \vdash \ell' \sqsubseteq \ell'' \qquad \mathcal{L} \vdash \mathsf{A} <: \mathsf{A}'}{\mathcal{L} \vdash \mathsf{A}^{\ell'} <: \mathsf{A}'^{\ell''}}\ \text{FGsub-label}$$

To prove: $\lfloor((\mathsf{A}^{\ell'}))\rfloor_V^{\hat{\beta}} \subseteq \lfloor((\mathsf{A}'^{\ell''}))\rfloor_V^{\hat{\beta}}$
This means from Definition 5.27 we need to prove
$\forall({}^{s}\theta, n, {}^{s}v, \mathsf{Lb}({}^{t}v_i)) \in \lfloor \mathsf{A}^{\ell'} \rfloor_V^{\hat{\beta}}.({}^{s}\theta, n, {}^{s}v, \mathsf{Lb}({}^{t}v_i)) \in \lfloor \mathsf{A}'^{\ell''} \rfloor_V^{\hat{\beta}}$

This means that given $({}^{s}\theta, n, {}^{s}v, \mathsf{Lb}({}^{t}v_i)) \in \lfloor \mathsf{A}^{\ell'} \rfloor_V^{\hat{\beta}}$
From Definition 5.27 it further means that we are given
$({}^{s}\theta, n, {}^{s}v, {}^{t}v_i) \in \lfloor \mathsf{A} \rfloor_V^{\hat{\beta}}$ (S-LB0)

And we need to prove
$({}^{s}\theta, n, {}^{s}v, \mathsf{Lb}({}^{t}v_i)) \in \lfloor \mathsf{A}'^{\ell''} \rfloor_V^{\hat{\beta}}$

Again from Definition 5.27 it suffices to prove that

$({}^s\theta, n, {}^s v, {}^t v_i) \in \lfloor \mathsf{A}' \rfloor_V^{\hat{\beta}}$

Since $\ell' \sqsubseteq \ell''$ and $\mathsf{A}' <: \mathsf{A}''$ therefore from IH (Statement 1(a)) and (S-LB0) we get the desired

Proof of statement 2(b)
Given: $\mathcal{L} \vdash \tau <: \tau'$
To prove: $\lfloor (\tau\ \sigma) \rfloor_E^{\hat{\beta}} \subseteq \lfloor (\tau'\ \sigma) \rfloor_E^{\hat{\beta}}$
This means we need to prove that
$\forall (\theta, n, e_s, e_t) \in \lfloor (\tau\ \sigma) \rfloor_E^{\hat{\beta}}.\ (\theta, n, e_s, e_t) \in \lfloor (\tau'\ \sigma) \rfloor_E^{\hat{\beta}}$

This means given $(\theta, n, e_s, e_t) \in \lfloor (\tau\ \sigma) \rfloor_E^{\hat{\beta}}$

This means from Definition 5.28 we have

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall i < n, {}^s v.(H_s, e_s) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v.(H_t, e_t) \Downarrow^f (H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n-i, {}^s v, {}^t v) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'}$ (S-E0)

And it suffices to prove that $({}^s\theta, n, e_s, e_t) \in \lfloor (\tau'\ \sigma) \rfloor_E^{\hat{\beta}}$

Again from Definition 5.28 it means we need to prove

$\forall H_{s1}, H_{t1}.(n, H_{s1}, H_{t1}) \overset{\hat{\beta}}{\triangleright} {}^s\theta \wedge \forall j < n, {}^s v_1.(H_{s1}, e_s) \Downarrow_j (H'_{s1}, {}^s v_1) \implies$
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}'_1}$

This means that given some H_{s1}, H_{t1} s.t $(n, H_{s1}, H_{t1}) \overset{\ell_2,\hat{\beta}}{\triangleright} {}^s\theta$. Also given some $j < n, {}^s v_1$ s.t $(H_{s1}, e_s) \Downarrow_j (H'_{s1}, {}^s v_1)$
And we need to prove
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}'_1}$ (S-E1)
Instantiating (S-E0) with H_{s1}, H_{t1} and with $j, {}^s v_1$. Then we get
$\exists H'_t, {}^t v.(H_t, e_t) \Downarrow^f (H'_t, {}^t v) \wedge \exists {}^s\theta' \sqsupseteq {}^s\theta, \hat{\beta}' \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_t) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor \tau\ \sigma \rfloor_V^{\hat{\beta}'_1}$
Since we have $\tau <: \tau'$. Therefore from IH (Statement 2(a)) we get
$\exists H'_{t1}, {}^t v_1.(H_{t1}, e_t) \Downarrow^f (H'_{t1}, {}^t v_1) \wedge \exists {}^s\theta'_1 \sqsupseteq {}^s\theta, \hat{\beta}'_1 \sqsupseteq \hat{\beta}.$
$(n-j, H'_{s1}, H'_{t1}) \overset{\hat{\beta}'_1}{\triangleright} {}^s\theta'_1 \wedge ({}^s\theta'_1, n-j, {}^s v_1, {}^t v_1) \in \lfloor \tau'\ \sigma \rfloor_V^{\hat{\beta}'_1}$

□

Theorem 5.38 (Deriving FG NI via compilation)**.** $\forall e_s, {}^s v_1, {}^s v_2, n_1, n_2, H'_{s1}, H'_{s2}, \perp.$
Let $\mathsf{bool} = (\mathsf{unit} + \mathsf{unit})$
$x : \mathsf{bool}^\top \vdash_\perp e_s : \mathsf{bool}^\perp \wedge$
$\emptyset \vdash_\perp {}^s v_1 : \mathsf{bool}^\top \wedge \emptyset \vdash_\perp {}^s v_2 : \mathsf{bool}^\top \wedge$
$(\emptyset, e_s[{}^s v_1/x]) \Downarrow_{n_1} (H'_{s1}, {}^s v'_1) \wedge$
$(\emptyset, e_s[{}^s v_2/x]) \Downarrow_{n_2} (H'_{s2}, {}^s v'_2) \wedge$
$\implies$
${}^s v'_1 = {}^s v'_2$

Proof. From the FG to CG translation we know that $\exists e_t$ s.t
$x : \mathsf{bool}^\top \vdash e_s : \mathsf{bool}^\bot \rightsquigarrow e_t$
Similarly we also know that $\exists {}^t v_1, {}^t v_2$ s.t
$\emptyset \vdash {}^s v_1 : \mathsf{bool}^\top \rightsquigarrow {}^t v_1$ and $\emptyset \vdash {}^s v_2 : \mathsf{bool}^\top \rightsquigarrow {}^t v_2$ (NI-0)

From type preservation theorem (choosing $\alpha = \overline{\beta} = \bot$) we know that
$x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e_t : \mathbb{C}\ \bot\ \bot\ \mathsf{Labeled}\ \bot\ \mathsf{bool}$
$\emptyset \vdash {}^t v_1 : \mathbb{C}\ \bot\ \bot\ \mathsf{Labeled}\ \top\ \mathsf{bool}$
$\emptyset \vdash {}^t v_2 : \mathbb{C}\ \bot\ \bot\ \mathsf{Labeled}\ \top\ \mathsf{bool}$ (NI-1)

Since we have $\emptyset \vdash {}^s v_1 : \mathsf{bool}^\top \rightsquigarrow {}^t v_1$
And since ${}^s v_1$ and ${}^t v_1$ are closed terms (from given and NI-1)
Therefore from Theorem 5.36 we have (we choose $n > n_1$ and $n > n_2$)
$(\emptyset, n, {}^s v_1, {}^t v_1) \in \lfloor \mathsf{bool}^\top \rfloor_E^\emptyset$ (NI-2)

Therefore from Definition 5.28 we have
$\forall H_s, H_t.(n, H_s, H_t) \overset{\emptyset}{\triangleright} \emptyset \wedge \forall i < n, {}^s v.(H_s, {}^s v_1) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v_{11}.(H_t, {}^t v_1) \Downarrow^f (H'_t, {}^t v_{11}) \wedge \exists {}^s\theta' \sqsupseteq \emptyset, \hat{\beta}' \sqsupseteq \emptyset.$
$(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v_{11}) \in \lfloor \mathsf{bool}^\top \rfloor_V^{\hat{\beta}'}$

Instantiating with $\emptyset, \emptyset$ and from fg-val we know that $H'_s = H_s = \emptyset$, ${}^s v = {}^s v_1$. Therefore we have
$\exists H'_t, {}^t v_{11}.(H_t, {}^t v_1) \Downarrow^f (H'_t, {}^t v_{11}) \wedge \exists {}^s\theta' \sqsupseteq \emptyset, \hat{\beta}' \sqsupseteq \emptyset.$
$(n, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n, {}^s v_1, {}^t v_{11}) \in \lfloor \mathsf{bool}^\top \rfloor_V^{\hat{\beta}'}$ (NI-2.1)

From Definition 5.27 we know that
${}^t v_{11} = \mathsf{Lb}({}^t v_{i11}) \wedge ({}^s\theta', n, {}^s v_1, {}^t v_{i11}) \in \lfloor (\mathsf{unit} + \mathsf{unit}) \rfloor_V^{\hat{\beta}'}$

Again from Definition 5.27 we know that
Either a) ${}^s v_1 = \mathsf{inl}()$ and ${}^t v_{i11} = \mathsf{inl}()$ or b)${}^s v_1 = \mathsf{inr}()$ and ${}^t v_{i11} = \mathsf{inr}()$
But in either case we have that $\emptyset \vdash {}^t v_{i11} : (\mathsf{unit} + \mathsf{unit})$ (NI-2.2)

As a result we have $\emptyset \vdash {}^t v_{11} : \mathsf{Labeled}\ \top\ (\mathsf{unit} + \mathsf{unit})$ (NI-2.3)
We give it typing derivation

$$\dfrac{\dfrac{}{\emptyset \vdash {}^t v_{i11} : (\mathsf{unit} + \mathsf{unit})}\ \text{(NI-2.2)}}{\emptyset \vdash \mathsf{Lb}({}^t v_{i11}) : \mathsf{Labeled}\ \top\ (\mathsf{unit} + \mathsf{unit})}$$

From Definition 5.31 and (NI-2.1) we know that
$(\emptyset, n, (x \mapsto {}^s v_1), (x \mapsto {}^t v_{11})) \in \lfloor x \mapsto \mathsf{bool}^\top \rfloor_V^{\hat{\beta}'}$

Therefore we can apply Theorem 5.36 to get
$(\emptyset, n, e_s[{}^s v_1/x], e_t[{}^t v_{11}/x]) \in \lfloor \mathsf{bool}^\bot \rfloor_E^{\hat{\beta}'}$ (NI-2.4)

From Definition 5.28 we get
$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}'}{\triangleright} \emptyset \wedge \forall i < n, {}^s v''_1.(H_s, e_s[{}^s v_1/x]) \Downarrow_i (H'_{s1}, {}^s v''_1) \implies$
$\exists H'_{t1}, {}^t v''_1.(H_t, e_t[{}^t v_{11}/x]) \Downarrow^f (H'_{t1}, {}^t v''_1) \wedge \exists {}^s\theta' \sqsupseteq \emptyset, \hat{\beta}'' \sqsupseteq \hat{\beta}'.$
$(n - i, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v''_1, {}^t v''_1) \in \lfloor \mathsf{bool}^\bot \rfloor_V^{\hat{\beta}''}$

Instantiating with $\emptyset, \emptyset, n_1, {}^s v'_1$ we get

$\exists H'_{t1}, {}^t v''_1.(H_t, e_t[{}^t v_{11}/x]) \Downarrow^f (H'_{t1}, {}^t v''_1) \wedge \exists^s \theta' \sqsupseteq {}^s\theta, \hat{\beta}'' \sqsupseteq \hat{\beta}'.$

$(n - n_1, H'_{s1}, H'_{t1}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - n_1, {}^s v'_1, {}^t v''_1) \in \lfloor \mathsf{bool}^{\perp} \rfloor_V^{\hat{\beta}''}$ (NI-2.5)

Since we have $({}^s\theta', n - n_1, {}^s v'_1, {}^t v''_1) \in \lfloor \mathsf{bool}^{\perp} \rfloor_V^{\hat{\beta}''}$ therefore from Definition 5.27 we have
$\exists^t v_{i1}.{}^t v'' = \mathsf{Lb}({}^t v_{i1}) \wedge ({}^s\theta', n - n_1, {}^s v'_1, {}^t v_{i1}) \in \lfloor \mathsf{bool} \rfloor_V^{\hat{\beta}''}$
Since $({}^s\theta', n - n_1, {}^s v'_1, {}^t v_{i1}) \in \lfloor (\mathsf{unit} + \mathsf{unit}) \rfloor_V^{\hat{\beta}''}$ therefore from Definition 5.27 two cases arise

- ${}^s v'_1 = \mathsf{inl}\ {}^s v_{i11}$ and ${}^t v_{i1} = \mathsf{inl}^t v_{i11}$:
  From Definition 5.27 we have
  $({}^s\theta', n - n_1, {}^s v_{i11}, {}^t v_{i11}) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}''}$
  which means we have ${}^s v_{i11} = {}^t v_{i11}$
- ${}^s v'_1 = \mathsf{inr}\ {}^s v_{i11}$ and ${}^t v_{i1} = \mathsf{inr}^t v_{i11}$:
  Symmetric reasoning as in the previous case

So no matter which case arise we have ${}^s v'_1 = {}^t v_{i1}$

Similarly with other substitution we have $(\emptyset, n, {}^s v_2, {}^t v_2) \in \lfloor \mathsf{bool}^{\top} \rfloor_E^{\emptyset}$ (NI-3)

Therefore from Definition 5.28 we have
$\forall H_s, H_t.(n, H_s, H_t) \overset{\emptyset}{\triangleright} \emptyset \wedge \forall i < n, {}^s v.(H_s, {}^s v_2) \Downarrow_i (H'_s, {}^s v) \implies$
$\exists H'_t, {}^t v_{22}.(H_t, {}^t v_2) \Downarrow^f (H'_t, {}^t v_{22}) \wedge \exists^s \theta' \sqsupseteq \emptyset, \hat{\beta}' \sqsupseteq \emptyset.$
$(n - i, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v, {}^t v_{22}) \in \lfloor \mathsf{bool}^{\top} \rfloor_V^{\hat{\beta}'}$

Instantiating with $\emptyset, \emptyset$ and from fg-val we know that $H'_s = H_s = \emptyset$, ${}^s v = {}^s v_1$. Therefore we have
$\exists H'_t, {}^t v_{22}.(H_t, {}^t v_2) \Downarrow^f (H'_t, {}^t v_{22}) \wedge \exists^s \theta' \sqsupseteq \emptyset, \hat{\beta}' \sqsupseteq \emptyset.$
$(n, H'_s, H'_t) \overset{\hat{\beta}'}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n, {}^s v_1, {}^t v_{22}) \in \lfloor \mathsf{bool}^{\top} \rfloor_V^{\hat{\beta}'}$ (NI-3.1)

From Definition 5.27 we know that
${}^t v_2 = \mathsf{Lb}({}^t v_{i22}) \wedge ({}^s\theta', n, {}^s v_1, {}^t v_{i22}) \in \lfloor (\mathsf{unit} + \mathsf{unit}) \rfloor_V^{\hat{\beta}'}$

Again from Definition 5.27 we know that
Either a) ${}^s v_2 = \mathsf{inl}()$ and ${}^t v_{i22} = \mathsf{inl}()$ or b)${}^s v_2 = \mathsf{inr}()$ and ${}^t v_{i22} = \mathsf{inr}()$
But in either case we have that $\emptyset \vdash {}^t v_{i22} : (\mathsf{unit} + \mathsf{unit})$ (NI-3.2)

As a result we have $\emptyset \vdash {}^t v_{22} : \mathsf{Labeled}\ \top\ (\mathsf{unit} + \mathsf{unit})$ (NI-3.3)
We give it typing derivation

$$\dfrac{\dfrac{}{\emptyset \vdash {}^t v_{i22} : (\mathsf{unit} + \mathsf{unit})}\ \text{(NI-3.2)}}{\emptyset \vdash \mathsf{Lb}({}^t v_{i22}) : \mathsf{Labeled}\ \top\ (\mathsf{unit} + \mathsf{unit})}$$

From Definition 5.31 and (NI-3.1) we know that
$(\emptyset, n, (x \mapsto {}^s v_2), (x \mapsto {}^t v_{22})) \in \lfloor x \mapsto \mathsf{bool}^{\top} \rfloor_V^{\hat{\beta}'}$

Therefore we can apply Theorem 5.36 to get
$(\emptyset, n, e_s[{}^s v_2/x], e_t[{}^t v_{22}/x]) \in \lfloor \mathsf{bool}^{\perp} \rfloor_E^{\hat{\beta}'}$ (NI-3.4)

From Definition 5.28 we get

$\forall H_s, H_t.(n, H_s, H_t) \overset{\hat{\beta}'}{\triangleright} \emptyset \wedge \forall i < n, {}^s v_2''.(H_s, e_s[{}^s v_2/x]) \Downarrow_i (H'_{s2}, {}^s v_2'') \implies$
$\exists H'_{t2}, {}^t v_2''.(H_t, e_t[{}^t v_{22}/x]) \Downarrow^f (H'_{t2}, {}^t v_2'') \wedge \exists^s \theta' \sqsupseteq \emptyset, \hat{\beta}'' \sqsupseteq \hat{\beta}'.$
$(n - i, H'_{s2}, H'_{t2}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - i, {}^s v_2'', {}^t v_2'') \in \lfloor \mathsf{bool}^{\perp} \rfloor_V^{\hat{\beta}''}$

Instantiating with $\emptyset, \emptyset, n_2, {}^s v_2'$ we get
$\exists H'_{t2}, {}^t v_2''.(H_t, e_t[{}^t v_{22}/x]) \Downarrow^f (H'_{t2}, {}^t v_2'') \wedge \exists^s \theta' \sqsupseteq {}^s\theta, \hat{\beta}'' \sqsupseteq \hat{\beta}'.$
$(n - n_1, H'_s, H'_{t2}) \overset{\hat{\beta}''}{\triangleright} {}^s\theta' \wedge ({}^s\theta', n - n_1, {}^s v_2', {}^t v_2'') \in \lfloor \mathsf{bool}^{\perp} \rfloor_V^{\hat{\beta}''}$ (NI-3.5)

Since we have $({}^s\theta', n - n_2, {}^s v_2', {}^t v_2'') \in \lfloor \mathsf{bool}^{\perp} \rfloor_V^{\hat{\beta}''}$ therefore from Definition 5.27 we have
$\exists^t v_{i2}.{}^t v_2'' = \mathsf{Lb}({}^t v_{i2}) \wedge ({}^s\theta', n - n_2, {}^s v_2', {}^t v_{i2}) \in \lfloor \mathsf{bool} \rfloor_V^{\hat{\beta}''}$
Since $({}^s\theta', n - n_2, {}^s v_2', {}^t v_{i2}) \in \lfloor (\mathsf{unit} + \mathsf{unit}) \rfloor_V^{\hat{\beta}''}$ therefore from Definition 5.27 two cases arise

- ${}^s v_2' = \mathsf{inl}\ {}^s v_{i22}$ and ${}^t v_{i2} = \mathsf{inl}^t v_{i22}$:
  From Definition 5.27 we have
  $({}^s\theta', n - n_2, {}^s v_{i22}, {}^t v_{i22}) \in \lfloor \mathsf{unit} \rfloor_V^{\hat{\beta}''}$
  which means we have ${}^s v_{i22} = {}^t v_{i22}$
- ${}^s v_1' = \mathsf{inr}\ {}^s v_{i22}$ and ${}^t v_{i2} = \mathsf{inr}^t v_{i22}$:
  Symmetric reasoning as in the previous case

So no matter which case arise we have ${}^s v_2' = {}^t v_{i2}$

We know that $\emptyset \vdash {}^t v_{11} : \mathsf{Labeled}\ \top\ \mathsf{bool}$ (NI-2.3)

Also we have $\emptyset \vdash {}^t v_{22} : \mathsf{Labeled}\ \top\ \mathsf{bool}$ (NI-3.3)

Let $e_T = \mathsf{bind}(e_t, y.\mathsf{unlabel}(y))$
We show that $x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e_T : \mathbb{C}\ \perp\ \perp\ \mathsf{bool}$ by giving a typing derivation
P2:

$$\dfrac{\dfrac{}{x : \mathsf{Labeled}\ \top\ \mathsf{bool}, y : \mathsf{Labeled}\ \perp\ \mathsf{bool} \vdash y : \mathsf{Labeled}\ \perp\ \mathsf{bool}}\ \text{CG-var}}{x : \mathsf{Labeled}\ \top\ \mathsf{bool}, y : \mathsf{Labeled}\ \perp\ \mathsf{bool} \vdash \mathsf{unlabel}(y) : \mathbb{C}\ \perp\ \perp\ \mathsf{bool}}\ \text{CG-unlabel}$$

P1:

$$\dfrac{}{x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash e_t : \mathbb{C}\ \perp\ \perp\ \mathsf{Labeled}\ \perp\ \mathsf{bool}}\ \text{From (NI-1)}$$

Main derivation:

$$\dfrac{P1 \qquad P2}{x : \mathsf{Labeled}\ \top\ \mathsf{bool} \vdash \mathsf{bind}(e_t, y.\mathsf{unlabel}(y)) : \mathbb{C}\ \perp\ \perp\ \mathsf{bool}}$$

Say $e_t[{}^t v_{11}/x]$ reduces in n_{t1} steps in (NI-2.5) and $e_t[{}^t v_{22}/x]$ reduces in n_{t2} steps in (NI-3.5)
We instantiate Theorem 5.18 with $e_T, {}^t v_{11}, {}^t v_{22}, {}^t v_{i1}, {}^t v_{i2}, n_{t1} + 2, n_{t2} + 2, H'_{t1}, H'_{t2}$ and from (NI-2.5) and (NI-3.5) we have ${}^t v_{i1} = {}^t v_{i2}$ and thus ${}^s v_1' = {}^s v_2'$

□