

The Transitive Composability of Relation Transition Systems

Technical Appendix

Chung-Kil Hur Georg Neis Derek Dreyer Viktor Vafeiadis
Max Planck Institute for Software Systems (MPI-SWS)
{gil,neis,dreyer,viktor}@mpi-sws.org

January 2012

Contents

1	Language	3
1.1	Syntax	3
1.2	Dynamic Semantics	3
1.3	Static Semantics	3
1.4	Contextual Equivalence	5
2	Model	6
2.1	Definitions	6
2.2	Basic Properties	10
2.3	Compatibility	21
2.4	Soundness	33
2.5	Symmetry	34
3	Examples	37
3.1	World Generator	37
3.2	Substitutivity	40
3.3	Expansion	40
3.4	Beta Law	41
3.5	Awkward Example	41
3.6	Well-Bracketed State Change	43
3.7	Twin Abstraction	45
4	Weak Isomorphism Theorem	48
4.1	Weak Isomorphisms	48
4.2	Global Knowledge Constructions	48
4.3	Category of Worlds	50
4.4	Isomorphism Theorem	50
4.5	Examples	53

5	Transitivity	55
5.1	Constructing a Full World That Relates e_1 and e_3	55
5.1.1	Type Decomposition	55
5.1.2	World Construction	57
5.1.3	Transitivity of Value Equivalence	58
5.1.4	Transitivity of Term Equivalence	61
5.1.5	Transitivity w.r.t. the Full World	63
5.2	Constructing an Isomorphic Lifted World	64
5.2.1	Stability	66
5.2.2	Isomorphism	69
5.2.3	Transitivity	71

1 Language

We define the language F^μ .

1.1 Syntax

$$\begin{aligned}
\ell &\in \text{Loc} \\
x &\in \text{Var} \\
\alpha &\in \text{TyVar} \\
\sigma \in \text{Typ} &::= \alpha \mid \text{unit} \mid \text{int} \mid \text{bool} \mid \sigma_1 \times \sigma_2 \mid \sigma_1 + \sigma_2 \mid \sigma_1 \rightarrow \sigma_2 \mid \mu\alpha. \sigma \mid \forall\alpha. \sigma \mid \exists\alpha. \sigma \mid \text{ref } \sigma \\
v \in \text{Val} &::= x \mid \langle \rangle \mid n \mid \text{tt} \mid \text{ff} \mid \langle v_1, v_2 \rangle \mid \text{inj}^1 v \mid \text{inj}^2 v \mid \text{roll } v \mid \\
&\quad \text{fix } f(x). e \mid \Lambda. e \mid \text{pack } v \mid \ell \\
e \in \text{Exp} &::= v \mid \text{if } e_0 \text{ then } e_1 \text{ else } e_2 \mid \langle e_1, e_2 \rangle \mid e.1 \mid e.2 \mid \text{inj}^1 e \mid \text{inj}^2 e \mid \\
&\quad (\text{case } e \text{ of } \text{inj}^1 x \Rightarrow e_1 \mid \text{inj}^2 x \Rightarrow e_2) \mid \text{roll } e \mid \text{unroll } e \mid e_1 e_2 \mid e[] \mid \text{pack } e \mid \\
&\quad \text{unpack } e_1 \text{ as } x \text{ in } e_2 \mid \text{ref } e \mid !e \mid e_1 := e_2 \mid e_1 == e_2 \\
K \in \text{Cont} &::= \bullet \mid \text{if } K \text{ then } e_1 \text{ else } e_2 \mid \langle K, e \rangle \mid \langle v, K \rangle \mid K.1 \mid K.2 \mid \text{inj}^1 K \mid \text{inj}^2 K \mid \\
&\quad \text{case } K \text{ of } [\text{inj}^i x \Rightarrow e_i] \mid \text{roll } K \mid \text{unroll } K \mid K e \mid v K \mid K[] \mid \text{pack } K \mid \\
&\quad \text{unpack } K \text{ as } x \text{ in } e \mid \text{ref } K \mid !K \mid K := e \mid v := K \mid K == e \mid v == K \\
p \in \text{Prog} &::= x \mid \langle \rangle \mid n \mid \text{tt} \mid \text{ff} \mid \text{if } p_0 \text{ then } p_1 \text{ else } p_2 \mid \langle p_1, p_2 \rangle \mid p.1 \mid p.2 \mid \text{inj}_\sigma^1 p \mid \text{inj}_\sigma^2 p \mid \\
&\quad (\text{case } p \text{ of } \text{inj}^1 x \Rightarrow p_1 \mid \text{inj}^2 x \Rightarrow p_2) \mid \text{roll}_\sigma p \mid \text{unroll } p \mid \text{fix } f(x:\sigma_1):\sigma_2. p \mid p_1 p_2 \mid \Lambda\alpha. p \mid \\
&\quad p[\sigma] \mid \text{pack } \langle \sigma, p \rangle \text{ as } \exists\alpha. \sigma' \mid \text{unpack } p_1 \text{ as } \langle \alpha, x \rangle \text{ in } p_2 \mid \text{ref } p \mid !p \mid p_1 := p_2 \mid p_1 == p_2 \\
h \in \text{Heap} &::= \text{Loc} \xrightarrow{\text{fin}} \text{CVal}
\end{aligned}$$

1.2 Dynamic Semantics

$$\begin{aligned}
h, \text{if } \text{tt} \text{ then } e_1 \text{ else } e_2 &\hookrightarrow h, e_1 \\
h, \text{if } \text{ff} \text{ then } e_1 \text{ else } e_2 &\hookrightarrow h, e_2 \\
h, \langle v_1, v_2 \rangle.i &\hookrightarrow h, v_i \\
h, \text{case } \text{inj}^j v \text{ of } [\text{inj}^i x \Rightarrow e_i] &\hookrightarrow h, e_j[v/x] \\
h, (\text{fix } f(x). e) v &\hookrightarrow h, e[(\text{fix } f(x). e)/f, v/x] \\
h, (\Lambda. e)[] &\hookrightarrow h, e \\
h, \text{unpack } (\text{pack } v) \text{ as } x \text{ in } e &\hookrightarrow h, e[v/x] \\
h, \text{unroll } (\text{roll } v) &\hookrightarrow h, v \\
h, \text{ref } v &\hookrightarrow h \uplus [\ell \mapsto v], \ell \quad \text{where } \ell \notin \text{dom}(h) \\
h \uplus [\ell \mapsto v], !\ell &\hookrightarrow h \uplus [\ell \mapsto v], v \\
h \uplus [\ell \mapsto v], \ell := v' &\hookrightarrow h \uplus [\ell \mapsto v'], \langle \rangle \\
h, \ell == \ell &\hookrightarrow h, \text{tt} \\
h, \ell == \ell' &\hookrightarrow h, \text{ff} \quad \text{where } \ell \neq \ell' \\
h, K[e] &\hookrightarrow h', K[e'] \quad \text{where } h, e \hookrightarrow h', e'
\end{aligned}$$

1.3 Static Semantics

$$\begin{aligned}
\text{Type environments } \Delta &::= \cdot \mid \Delta, \alpha \\
\text{Term environments } \Gamma &::= \cdot \mid \Gamma, x:\sigma
\end{aligned}$$

$$\boxed{\Delta \vdash \sigma}$$

$$\frac{\text{fv}(\sigma) \subseteq \Delta \quad \text{names}(\sigma) = \emptyset}{\Delta \vdash \sigma}$$

$$\boxed{\Delta \vdash \Gamma}$$

$$\frac{\forall x:\sigma \in \Gamma. \Delta \vdash \sigma}{\Delta \vdash \Gamma}$$

$\Delta; \Gamma \vdash p : \sigma$

$$\begin{array}{c}
\frac{\Delta \vdash \Gamma \quad x : \sigma \in \Gamma}{\Delta; \Gamma \vdash x : \sigma} \quad \frac{\Delta \vdash \Gamma}{\Delta; \Gamma \vdash c : \tau_{\text{base}}} \\
\\
\frac{\Delta; \Gamma \vdash p_1 : \sigma_1 \quad \Delta; \Gamma \vdash p_2 : \sigma_2}{\Delta; \Gamma \vdash \langle p_1, p_2 \rangle : \sigma_1 \times \sigma_2} \quad \frac{\Delta; \Gamma \vdash p : \sigma_1 \times \sigma_2}{\Delta; \Gamma \vdash p.1 : \sigma_1} \quad \frac{\Delta; \Gamma \vdash p : \sigma_1 \times \sigma_2}{\Delta; \Gamma \vdash p.2 : \sigma_2} \\
\\
\frac{\Delta; \Gamma, x : \sigma_1 \vdash p : \sigma_2}{\Delta; \Gamma \vdash \lambda x : \sigma_1. p : \sigma_1 \rightarrow \sigma_2} \quad \frac{\Delta; \Gamma \vdash p_1 : \sigma_1 \rightarrow \sigma_2 \quad \Delta; \Gamma \vdash p_2 : \sigma_1}{\Delta; \Gamma \vdash p_1 p_2 : \sigma_2} \\
\\
\frac{\Delta, \alpha; \Gamma \vdash p : \sigma}{\Delta; \Gamma \vdash \Lambda \alpha. p : \forall \alpha. \sigma} \quad \frac{\Delta; \Gamma \vdash p : \forall \alpha. \sigma_1 \quad \Delta \vdash \sigma_2}{\Delta; \Gamma \vdash p[\sigma_2] : \sigma_1[\sigma_2/\alpha]} \\
\\
\frac{\Delta \vdash \sigma_1 \quad \Delta; \Gamma \vdash p : \sigma_2[\sigma_1/\alpha]}{\Delta; \Gamma \vdash \text{pack } \langle \sigma_1, p \rangle \text{ as } \exists \alpha. \sigma_2 : \exists \alpha. \sigma_2} \quad \frac{\Delta; \Gamma \vdash p_1 : \exists \alpha. \sigma_1 \quad \Delta, \alpha; \Gamma, x : \sigma_1 \vdash p_2 : \sigma_2 \quad \Delta \vdash \sigma_2}{\Delta; \Gamma \vdash \text{unpack } p_1 \text{ as } \langle \alpha, x \rangle \text{ in } p_2 : \sigma_2} \\
\\
\frac{\Delta; \Gamma \vdash p : \sigma[\mu \alpha. \sigma/\alpha]}{\Delta; \Gamma \vdash \text{roll}_{\mu \alpha. \sigma} p : \mu \alpha. \sigma} \quad \frac{\Delta; \Gamma \vdash p : \mu \alpha. \sigma}{\Delta; \Gamma \vdash \text{unroll } p : \sigma[\mu \alpha. \sigma/\alpha]} \\
\\
\frac{\Delta; \Gamma \vdash p : \sigma}{\Delta; \Gamma \vdash \text{ref } p : \text{ref } \sigma} \quad \frac{\Delta; \Gamma \vdash p_1 : \text{ref } \sigma \quad \Delta; \Gamma \vdash p_2 : \sigma}{\Delta; \Gamma \vdash p_1 := p_2 : \text{unit}} \\
\\
\frac{\Delta; \Gamma \vdash p : \text{ref } \sigma}{\Delta; \Gamma \vdash !p : \sigma} \quad \frac{\Delta; \Gamma \vdash p_1 : \text{ref } \sigma \quad \Delta; \Gamma \vdash p_2 : \text{ref } \sigma}{\Delta; \Gamma \vdash p_1 == p_2 : \text{bool}}
\end{array}$$

...

$\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma')$

$$\begin{array}{c}
\frac{\Delta \subseteq \Delta' \quad \Gamma \subseteq \Gamma'}{\vdash \bullet : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma)} \\
\\
\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1) \quad \Delta'; \Gamma' \vdash p_2 : \sigma_2}{\vdash \langle C, p_2 \rangle : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1 \times \sigma_2)} \\
\\
\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1 \times \sigma_2)}{\vdash C.1 : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1)} \quad \frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1 \times \sigma_2)}{\vdash C.2 : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_2)} \\
\\
\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma', x : \sigma_1; \sigma_2)}{\vdash \lambda x : \sigma_1. C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1 \rightarrow \sigma_2)} \\
\\
\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1 \rightarrow \sigma_2) \quad \Delta'; \Gamma' \vdash p_2 : \sigma_1}{\vdash C p_2 : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_2)} \\
\\
\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1) \quad \Delta'; \Gamma' \vdash p_1 : \sigma_1 \rightarrow \sigma_2}{\vdash p_1 C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_2)}
\end{array}$$

$$\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta', \alpha; \Gamma'; \sigma_1)}{\vdash \Lambda\alpha. C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \forall\alpha. \sigma_1)} \quad \frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \forall\alpha. \sigma_1)}{\vdash C[\sigma_2] : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1[\sigma_2/\alpha])}$$

$$\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1[\alpha])}{\vdash \text{pack } \langle \sigma_1, C \rangle \text{ as } \exists\alpha. \sigma_2 : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \exists\alpha. \sigma_2)}$$

$$\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \exists\alpha. \sigma_1) \quad \Delta', \alpha; \Gamma', x:\sigma_1 \vdash p_2 : \sigma_2 \quad \Delta' \vdash \sigma_2}{\vdash \text{unpack } C \text{ as } \langle \alpha, x \rangle \text{ in } p_2 : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_2)}$$

$$\frac{\Delta'; \Gamma' \vdash p_1 : \exists\alpha. \sigma_1 \quad \vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta', \alpha; \Gamma', x:\sigma_1; \sigma_2) \quad \Delta' \vdash \sigma_2}{\vdash \text{unpack } p_1 \text{ as } \langle \alpha, x \rangle \text{ in } C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_2)}$$

$$\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1[\mu\alpha. \sigma_1/\alpha])}{\vdash \text{roll}_{\mu\alpha. \sigma_1} C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \mu\alpha. \sigma_1)}$$

$$\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \mu\alpha. \sigma_1)}{\vdash \text{unroll } C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1[\mu\alpha. \sigma_1/\alpha])}$$

$$\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1)}{\vdash \text{ref } C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \text{ref } \sigma_1)}$$

$$\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \text{ref } \sigma_1) \quad \Delta'; \Gamma' \vdash p_2 : \sigma_1}{\vdash C := p_2 : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \text{unit})}$$

$$\frac{\Delta'; \Gamma' \vdash p_1 : \text{ref } \sigma_1 \quad \vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1)}{\vdash p_1 := C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \text{unit})}$$

$$\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \text{ref } \sigma_1)}{\vdash !C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1)}$$

$$\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \text{ref } \sigma_1) \quad \Delta'; \Gamma' \vdash p_2 : \text{ref } \sigma_1}{\vdash C == p_2 : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \text{bool})}$$

$$\frac{\Delta'; \Gamma' \vdash p_1 : \text{ref } \sigma_1 \quad \vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \text{ref } \sigma_1)}{\vdash p_1 == C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \text{bool})}$$

...

1.4 Contextual Equivalence

Definition 1 (Contextual equivalence).

Let $\Delta; \Gamma \vdash p_1 : \sigma$ and $\Delta; \Gamma \vdash p_2 : \sigma$. Then:

$$\Delta; \Gamma \vdash p_1 \sim_{\text{ctx}} p_2 : \sigma := \forall C, h, \tau. \vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\cdot; \cdot; \tau) \implies (h, |C[p_1]| \uparrow \iff h, |C[p_2]| \uparrow)$$

2 Model

2.1 Definitions

Various Relations.

$$\begin{aligned} \text{beta}(e) &:= \begin{cases} e' & \text{if } \forall h. h, e \hookrightarrow^1 h, e' \\ \text{undef} & \text{otherwise} \end{cases} \\ \text{FunVal} &:= \{ f \in \text{CVal} \mid \forall v. \text{beta}(f v) \text{ defined} \} \\ \text{TyFunVal} &:= \{ v \in \text{CVal} \mid \text{beta}(v[]) \text{ defined} \} \end{aligned}$$

$\mathbf{n} \in \text{TyNam}$

$$\begin{aligned} \text{Names} &:= \{ \mathcal{N} \in \mathbb{P}(\text{TyNam}) \mid \mathcal{N} \text{ is countably infinite} \} \\ \sigma \in \text{Type} &::= \mathbf{n} \mid \alpha \mid \text{unit} \mid \text{int} \mid \text{bool} \mid \sigma_1 \times \sigma_2 \mid \sigma_1 + \sigma_2 \mid \sigma_1 \rightarrow \sigma_2 \mid \mu\alpha. \sigma \mid \forall\alpha. \sigma \mid \exists\alpha. \sigma \mid \text{ref } \sigma \\ \text{CType} &:= \{ \tau \in \text{Type} \mid \text{ftv}(\tau) = \emptyset \} \\ \text{CTypeF} &:= \{ (\tau_1 \rightarrow \tau_2) \in \text{CType} \} \cup \{ \text{ref } \tau \in \text{CType} \} \cup \{ (\forall\alpha. \sigma) \in \text{CType} \} \cup \text{TyNam} \\ \text{VRelF} &:= \text{CTypeF} \rightarrow \mathbb{P}(\text{CVal} \times \text{CVal}) \\ \text{VRel} &:= \text{CType} \rightarrow \mathbb{P}(\text{CVal} \times \text{CVal}) \\ \text{ERel} &:= \text{CType} \rightarrow \mathbb{P}(\text{CExp} \times \text{CExp}) \\ \text{KRel} &:= \text{CType} \times \text{CType} \rightarrow \mathbb{P}(\text{CCont} \times \text{CCont}) \\ \text{HRel} &:= \mathbb{P}(\text{Heap} \times \text{Heap}) \end{aligned}$$

Note that as a notational convention we use σ to range over possibly open types and τ over closed types.

Value Closure. We define the closure $\bar{R} \in \text{VRel}$ for $R \in \text{VRelF}$ as the least fixpoint of the following equation.

$$\begin{aligned} \bar{R}(\tau_{\text{base}}) &:= \text{ID}_{\tau_{\text{base}}} \\ \bar{R}(\tau_1 \times \tau_2) &:= \{ ((v_1, v'_1), (v_2, v'_2)) \mid (v_1, v_2) \in \bar{R}(\tau_1) \wedge (v'_1, v'_2) \in \bar{R}(\tau_2) \} \\ \bar{R}(\tau_1 + \tau_2) &:= \{ (\text{inj}^1 v_1, \text{inj}^1 v_2) \mid (v_1, v_2) \in \bar{R}(\tau_1) \} \cup \{ (\text{inj}^2 v_1, \text{inj}^2 v_2) \mid (v_1, v_2) \in \bar{R}(\tau_2) \} \\ \bar{R}(\mu\alpha. \sigma) &:= \{ (\text{roll } v_1, \text{roll } v_2) \mid (v_1, v_2) \in \bar{R}(\sigma[\mu\alpha. \sigma/\alpha]) \} \\ \bar{R}(\exists\alpha. \sigma) &:= \{ (\text{pack } v_1, \text{pack } v_2) \mid \exists \tau \in \text{CType}. (v_1, v_2) \in \bar{R}(\sigma[\tau/\alpha]) \} \\ \bar{R}(\tau_1 \rightarrow \tau_2) &:= R(\tau_1 \rightarrow \tau_2) \\ \bar{R}(\text{ref } \tau) &:= R(\text{ref } \tau) \\ \bar{R}(\mathbf{n}) &:= R(\mathbf{n}) \\ \bar{R}(\forall\alpha. \sigma) &:= R(\forall\alpha. \sigma) \end{aligned}$$

Dependent World. For a preordered set $P = (\mathbf{S}_P, \sqsubseteq_P)$ we define

$$\begin{aligned} \text{DepWorld}(P) &:= \\ &\{ (\mathbf{N}, \mathbf{S}, \sqsubseteq, \sqsubseteq_{\text{pub}}, \mathbf{L}, \mathbf{H}) \\ &\quad \in \mathbb{P}(\text{TyNam}) \times \text{Set} \times \mathbb{P}(\mathbf{S} \times \mathbf{S}) \times \mathbb{P}(\mathbf{S} \times \mathbf{S}) \times \\ &\quad (\mathbf{S}_P \rightarrow \mathbf{S} \rightarrow \text{VRelF} \rightarrow \text{VRelF}) \times (\mathbf{S}_P \rightarrow \mathbf{S} \rightarrow \text{VRelF} \rightarrow \text{HRel}) \mid \\ &\quad \sqsubseteq, \sqsubseteq_{\text{pub}} \text{ are preorders } \wedge \\ &\quad \sqsubseteq_{\text{pub}} \text{ is a subset of } \sqsubseteq \wedge \\ &\quad \mathbf{L} \text{ is monotone in the first argument w.r.t. } \sqsubseteq_P, \text{ in the second w.r.t. } \sqsubseteq, \text{ in the third w.r.t. } \leq \wedge \\ &\quad \mathbf{H} \text{ is monotone in the third argument w.r.t. } \leq \wedge \\ &\quad (\forall s_1, s_2. \forall R. \forall \mathbf{n} \notin \mathbf{N}. \mathbf{L}(s_1)(s_2)(R)(\mathbf{n}) = \emptyset) \wedge \\ &\quad (\forall s_1, s_2. \forall R. \forall (\tau_1 \rightarrow \tau_2, f_1, f_2) \in \mathbf{L}(s_1)(s_2)(R). f_1, f_2 \in \text{FunVal}) \wedge \\ &\quad (\forall s_1, s_2. \forall R. \forall (\forall\alpha. \sigma, v_1, v_2) \in \mathbf{L}(s_1)(s_2)(R). v_1, v_2 \in \text{TyFunVal}) \quad \} \end{aligned}$$

Here we write \leq for the pointwise lifting of the usual subset ordering \subseteq to function spaces.

Full World. We define

$$\text{World} := \{ W \in \text{DepWorld}(\{*\}, \{(*, *)\}) \}$$

and for $W \in \text{World}$ and $s \in W.\mathbf{S}$ often write just $W.\mathbf{H}(s)$ for $W.\mathbf{H}(*)(s)$ (and similar for the \mathbf{L} component).

World for Mutable References. We define the reference world $W_{\text{ref}} \in \text{World}$ as follows.

$$\begin{aligned} W_{\text{ref}}.\mathbf{N} &:= \emptyset \\ W_{\text{ref}}.\mathbf{S} &:= \{ s_{\text{rf}} \in \mathbb{P}_{\text{fin}}(\text{CType} \times \text{Loc} \times \text{Loc}) \mid \\ &\quad \forall (\tau, \ell_1, \ell_2), (\tau', \ell'_1, \ell'_2) \in s_{\text{rf}}. \\ &\quad (\ell_1 = \ell'_1 \implies \tau = \tau' \wedge \ell_2 = \ell'_2) \wedge (\ell_2 = \ell'_2 \implies \tau = \tau' \wedge \ell_1 = \ell'_1) \} \\ s'_{\text{rf}} \sqsupseteq s_{\text{rf}} &\text{ iff } s'_{\text{rf}} \supseteq s_{\text{rf}} \\ s'_{\text{rf}} \sqsupseteq_{\text{pub}} s_{\text{rf}} &\text{ iff } s'_{\text{rf}} \supseteq s_{\text{rf}} \\ W_{\text{ref}}.\mathbf{L}(s_{\text{rf}})(R) &:= \{ (\text{ref } \tau, \ell_1, \ell_2) \mid (\tau, \ell_1, \ell_2) \in s_{\text{rf}} \} \\ W_{\text{ref}}.\mathbf{H}(s_{\text{rf}})(R) &:= \{ (h_1, h_2) \mid \text{dom}(h_1) = \text{dom}_{[1]}(s_{\text{rf}}) \wedge \text{dom}(h_2) = \text{dom}_{[2]}(s_{\text{rf}}) \wedge \\ &\quad \forall (\tau, \ell_1, \ell_2) \in s_{\text{rf}}. (\tau, h_1(\ell_1), h_2(\ell_2)) \in R \} \end{aligned}$$

where

$$\begin{aligned} \text{dom}_{[1]}(s) &:= \{ \ell_1 \mid \exists \tau, \ell_2. (\tau, \ell_1, \ell_2) \in s \}, \\ \text{dom}_{[2]}(s) &:= \{ \ell_2 \mid \exists \tau, \ell_1. (\tau, \ell_1, \ell_2) \in s \}. \end{aligned}$$

Local World. We define

$$\text{LWorld} := \{ w \in \text{DepWorld}(W_{\text{ref}}.\mathbf{S}, W_{\text{ref}}.\sqsubseteq) \mid \forall s_{\text{rf}}, s, R, \tau. w.\mathbf{L}(s_{\text{rf}})(s)(R)(\text{ref } \tau) = \emptyset \}$$

Product World. For $w_1, w_2 \in \text{LWorld}$, we define $w_1 \otimes w_2 \in \text{LWorld}$ as follows.

$$\begin{aligned} \mathbf{N} &:= w_1.\mathbf{N} \uplus w_2.\mathbf{N} \\ \mathbf{S} &:= w_1.\mathbf{S} \times w_2.\mathbf{S} \\ (s'_1, s'_2) \sqsupseteq (s_1, s_2) &\text{ iff } s'_1 \sqsupseteq s_1 \wedge s'_2 \sqsupseteq s_2 \\ (s'_1, s'_2) \sqsupseteq_{\text{pub}} (s_1, s_2) &\text{ iff } s'_1 \sqsupseteq_{\text{pub}} s_1 \wedge s'_2 \sqsupseteq_{\text{pub}} s_2 \\ \mathbf{L}(s_{\text{rf}})(s_1, s_2)(R) &:= w_1.\mathbf{L}(s_{\text{rf}})(s_1)(R) \cup w_2.\mathbf{L}(s_{\text{rf}})(s_2)(R) \\ \mathbf{H}(s_{\text{rf}})(s_1, s_2)(R) &:= w_1.\mathbf{H}(s_{\text{rf}})(s_1)(R) \otimes w_2.\mathbf{H}(s_{\text{rf}})(s_2)(R) \end{aligned}$$

where

$$H_1 \otimes H_2 := \{ (h_1 \uplus h'_1, h_2 \uplus h'_2) \mid (h_1, h_2) \in H_1 \wedge (h'_1, h'_2) \in H_2 \}$$

Note that $w_1 \otimes w_2$ is undefined iff $w_1.\mathbf{N}$ and $w_2.\mathbf{N}$ is not disjoint.

Lifting of a Local World. For $w \in \text{LWorld}$, we define $w \uparrow \in \text{World}$ as follows.

$$\begin{aligned} \mathbf{N} &:= w.\mathbf{N} \\ \mathbf{S} &:= W_{\text{ref}}.\mathbf{S} \times w.\mathbf{S} \\ (s'_{\text{rf}}, s') \sqsupseteq (s_{\text{rf}}, s) &\text{ iff } s'_{\text{rf}} \sqsupseteq s_{\text{rf}} \wedge s' \sqsupseteq s \\ (s'_{\text{rf}}, s') \sqsupseteq_{\text{pub}} (s_{\text{rf}}, s) &\text{ iff } s'_{\text{rf}} \sqsupseteq_{\text{pub}} s_{\text{rf}} \wedge s' \sqsupseteq_{\text{pub}} s \\ \mathbf{L}(s_{\text{rf}}, s)(R) &:= W_{\text{ref}}.\mathbf{L}(s_{\text{rf}})(R) \cup w.\mathbf{L}(s_{\text{rf}})(s)(R) \\ \mathbf{H}(s_{\text{rf}}, s)(R) &:= W_{\text{ref}}.\mathbf{H}(s_{\text{rf}})(R) \otimes w.\mathbf{H}(s_{\text{rf}})(s)(R) \end{aligned}$$

Single-State Worlds. Given a local knowledge $L \in \text{VRelF} \xrightarrow{\text{mon}} \text{VRelF}$ and a heap relation $H \in \text{VRelF} \xrightarrow{\text{mon}} \text{HRel}$ such that

$$\begin{aligned} \forall R. \forall (\tau_1 \rightarrow \tau_2, f_1, f_2) \in L(R). f_1, f_2 \in \text{FunVal} \wedge \\ \forall R. \forall (\forall \alpha. \tau, f_1, f_2) \in L(R). f_1, f_2 \in \text{TyFunVal} \end{aligned}$$

we define the single-state local world $w_{\text{single}}(L, H) \in \text{LWorld}$ as follows.

$$\begin{aligned} w_{\text{single}}(L, H).N &:= \emptyset \\ w_{\text{single}}(L, H).S &:= \{ * \} \\ * &\sqsupseteq * \\ * &\sqsupseteq_{\text{pub}} * \\ w_{\text{single}}(L, H).L(s_{\text{rf}})(*)(R) &:= \{ (\tau' \rightarrow \tau, f_1, f_2) \in L(R) \} \cup \{ (\forall \alpha. \tau, f_1, f_2) \in L(R) \} \\ w_{\text{single}}(L, H).H(s_{\text{rf}})(*)(R) &:= H(R) \end{aligned}$$

Global Knowledge. We define the ref-name-preserving order $\geq_{\text{ref}}^{\mathcal{N}}$ between $R, R' \in \text{VRelF}$ as follows.

$$\begin{aligned} R' \geq_{\text{ref}}^{\mathcal{N}} R \quad \text{iff} \quad &\forall \tau. R'(\tau) \sqsupseteq R(\tau) \wedge \\ &\forall \tau. R'(\text{ref } \tau) = R(\text{ref } \tau) \wedge \\ &\forall \mathbf{n} \in \mathcal{N}. R'(\mathbf{n}) = R(\mathbf{n}) \end{aligned}$$

Note that $R' \geq_{\text{ref}}^{\mathcal{N}} R \implies R' \geq R$.

We define $\text{GK}(W)$ for $W \in \text{World}$ as follows.

$$\text{GK}(W) := \{ G \in W.S \rightarrow \text{VRelF} \mid G \text{ is monotone w.r.t. } \sqsupseteq \wedge \forall s. G(s) \geq_{\text{ref}}^{W.N} W.L(s)(G(s)) \}$$

Expression and Continuation Equivalence. We define the following notation.

$$s' \sqsupseteq [s_0, s] \quad \text{iff} \quad s' \sqsupseteq_{\text{pub}} s_0 \wedge s' \sqsupseteq s$$

For $W \in \text{World}$, we coinductively define $\mathbf{E}_W \in \text{GK}(W) \rightarrow W.S \times W.S \rightarrow \text{ERel}$ and $\mathbf{K}_W \in \text{GK}(W) \rightarrow W.S \times W.S \rightarrow \text{KRel}$ as follows.

$$\begin{aligned} \mathbf{E}_W(G)(s_0, s)(\tau) &:= \{ (e_1, e_2) \mid \forall (h_1, h_2) \in W.H(s)(G(s)). \forall h_1^F, h_2^F. \\ &\quad ((h_1, h_1^F, e_1), (h_2, h_2^F, e_2)) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s_0, s)(\tau) \} \\ \mathbf{K}_W(G)(s_0, s)(\tau_1, \tau_2) &:= \{ (K_1, K_2) \mid \forall (v_1, v_2) \in \overline{G(s)}(\tau_1). (K_1[v_1], K_2[v_2]) \in \mathbf{E}_W(G)(s_0, s)(\tau_2) \} \\ \mathbf{O}_W(R^K)(G)(s_0, s)(\tau) &:= \{ ((h_1, h_1^F, e_1), (h_2, h_2^F, e_2)) \mid h_1 \uplus h_1^F \text{ defined} \wedge h_2 \uplus h_2^F \text{ defined} \implies \\ &\quad (h_1 \uplus h_1^F, e_1 \uparrow \wedge h_2 \uplus h_2^F, e_2 \uparrow) \\ &\quad \vee (\exists h'_1, h'_2, v_1, v_2. h_1 \uplus h_1^F, e_1 \hookrightarrow^* h'_1 \uplus h_1^F, v_1 \wedge h_2 \uplus h_2^F, e_2 \hookrightarrow^* h'_2 \uplus h_2^F, v_2 \wedge \\ &\quad \exists s' \sqsupseteq [s_0, s]. (h'_1, h'_2) \in W.H(s')(G(s')) \wedge (v_1, v_2) \in \overline{G(s')}(v)) \\ &\quad \vee (\exists h'_1, h'_2, \tau', K_1, K_2, e'_1, e'_2. \\ &\quad h_1 \uplus h_1^F, e_1 \hookrightarrow^* h'_1 \uplus h_1^F, K_1[e'_1] \wedge h_2 \uplus h_2^F, e_2 \hookrightarrow^* h'_2 \uplus h_2^F, K_2[e'_2] \wedge \\ &\quad \exists s' \sqsupseteq s. (h'_1, h'_2) \in W.H(s')(G(s')) \wedge (\tau', e'_1, e'_2) \in \mathbf{S}(G(s'), G(s')) \wedge \\ &\quad \forall s'' \sqsupseteq_{\text{pub}} s'. \forall G' \geq G. (K_1, K_2) \in R^K(G')(s_0, s'')(v_1, v_2)) \} \\ \mathbf{S}(R_f, R_v) &:= \{ (\tau, f_1, v_1, f_2, v_2) \mid \exists \tau'. (f_1, f_2) \in R_f(\tau' \rightarrow \tau) \wedge (v_1, v_2) \in \overline{R_v}(\tau') \} \\ &\quad \cup \{ (\sigma[\tau/\alpha], f_1[], f_2[]) \mid \tau \in \text{CType} \wedge (f_1, f_2) \in R_f(\forall \alpha. \sigma) \} \end{aligned}$$

Program Equivalence.

For $w \in \text{LWorld}$, we define:

$$\begin{aligned} \text{stable}(w) &:= \forall G \in \text{GK}(w \uparrow). \forall s_{\text{rf}}, s. \forall (h_1, h_2) \in w.H(s_{\text{rf}})(s)(G(s_{\text{rf}}, s)). \\ &\quad \forall s'_{\text{rf}} \sqsupseteq s_{\text{rf}}. \forall (h^1_{\text{ref}}, h^2_{\text{ref}}) \in W_{\text{ref}}.H(s'_{\text{rf}})(G(s'_{\text{rf}}, s)). h^1_{\text{ref}} \uplus h_1 \text{ defined} \wedge h^2_{\text{ref}} \uplus h_2 \text{ defined} \implies \\ &\quad \exists s' \sqsupseteq_{\text{pub}} s. (h_1, h_2) \in w.H(s'_{\text{rf}})(s')(G(s'_{\text{rf}}, s')) \end{aligned}$$

For $W \in \text{World}$, we define:

$$\begin{aligned} \text{inhabited}(W) &:= \forall G \in \mathbf{GK}(W). \exists s_0. (\emptyset, \emptyset) \in W.H(s_0)(G(s_0)) \\ \text{consistent}(W) &:= \forall G \in \mathbf{GK}(W). \forall s. \forall (\tau, e_1, e_2) \in \mathbf{S}(W.L(s)(G(s)), G(s)). \\ &\quad (\tau, \text{beta}(e_1), \text{beta}(e_2)) \in \mathbf{E}_W(G)(s, s) \end{aligned}$$

We define program equivalence $\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma$.

$$\begin{aligned} \text{TyEnv}(\Delta) &:= \{ \delta \mid \delta \in \Delta \rightarrow \text{CType} \} \\ \text{Env}(\Gamma, R) &:= \{ (\gamma_1, \gamma_2) \mid \gamma_1, \gamma_2 \in \text{dom}(\Gamma) \rightarrow \text{CVal} \wedge \forall x. (\Gamma(x), \gamma_1(x), \gamma_2(x)) \in \bar{R} \} \\ \Delta; \Gamma \vdash e_1 \sim_W e_2 : \sigma &:= \text{inhabited}(W) \wedge \text{consistent}(W) \wedge \\ &\quad \forall G \in \mathbf{GK}(W). \forall s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s)). \\ &\quad (\delta\sigma, \gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_W(G)(s, s) \\ \Delta; \Gamma \vdash e_1 \sim_w e_2 : \sigma &:= \text{stable}(w) \wedge \Delta; \Gamma \vdash e_1 \sim_{w\uparrow} e_2 : \sigma \\ \Delta; \Gamma \vdash e_1 \sim e_2 : \sigma &:= \forall \mathcal{N} \in \text{Names}. \exists w \in \text{LWorld}. w.N \subseteq \mathcal{N} \wedge \Delta; \Gamma \vdash e_1 \sim_w e_2 : \sigma \end{aligned}$$

2.2 Basic Properties

Notation. For a monotone function $F \in \text{VRelF} \rightarrow \text{VRelF}$ and $R \in \text{VRelF}$, we define $[F]_R^*$ as the least fixpoint of the monotone function $F(-) \cup R$:

$$[F]_R^* := \mu X. F(X) \cup R.$$

For $W \in \text{World}$, we define $[W] \in W.S \rightarrow \text{VRelF}$ as follows:

$$[W](s) := [W.L(s)]_{\emptyset}^*.$$

Lemma 1. If $G' \geq G$ and $s' \sqsupseteq s$, then:

1. $G'(s') \geq G(s)$
2. $\text{Env}(\Gamma, G'(s')) \supseteq \text{Env}(\Gamma, G(s))$

Proof.

1. By definition of GK we know $G'(s') \geq G'(s)$. And since $G' \geq G$ we also know $G'(s) \geq G(s)$.
2. Follows immediately from (1).

□

Lemma 2. $\forall W \in \text{World}. [W] \in \text{GK}(W)$

Proof. We must establish four properties:

- a) To show: $[W]$ is monotone w.r.t. \sqsubseteq .
Follows from monotonicity of $W.L$.
- b) To show: $\forall s, \tau. [W](s)(\tau) \supseteq W.L(s)([W](s))(\tau)$.
Immediate after unrolling fixpoint once.
- c) To show: $\forall s, \tau. [W](s)(\text{ref } \tau) = W.L(s)([W](s))(\text{ref } \tau)$.
Easy fixpoint induction.
- d) To show: $\forall s, \mathbf{n} \in W.N. [W](s)(\mathbf{n}) = W.L(s)([W](s))(\mathbf{n})$.
Easy fixpoint induction.

□

Lemma 3. $\forall W \in \text{World}, G \in \text{GK}(W). [W] \leq G$

Proof. Easy fixpoint induction.

□

Lemma 4. If

- $h_1 \uplus h_1^f, e_1 \hookrightarrow^* h'_1 \uplus h_1^f, e'_1,$
- $h_2 \uplus h_2^f, e_2 \hookrightarrow^* h'_2 \uplus h_2^f, e'_2,$
- $s' \sqsupseteq s,$ and
- $(\tau, (h'_1, h_1^f, e'_1), (h'_2, h_2^f, e'_2)) \in \mathbf{O}_W(R^K)(s_0, s'),$

then $(\tau, (h_1, h_1^f, e_1), (h_2, h_2^f, e_2)) \in \mathbf{O}_W(R^K)(s_0, s)$.

Proof. Follows easily from the definition of \mathbf{O}_W .

□

Lemma 5. $G(s) \leq \overline{G(s)} \leq \mathbf{E}_W(G)(s, s)$

Proof. The first inclusion holds immediately by definition; the second by choosing the final state to be s . \square

Lemma 6. $(\tau, \tau, \bullet, \bullet) \in \mathbf{K}_W(G)(s, s)$

Proof. We need to show $(\tau, v_1, v_2) \in \mathbf{E}_W(G)(s, s)$ for $(\tau, v_1, v_2) \in \overline{G(s)}$, which holds by Lemma 5. \square

Lemma 7. If $s'_0 \sqsupseteq_{\text{pub}} s_0$, then:

1. $\mathbf{E}_W(G)(s'_0, s) \leq \mathbf{E}_W(G)(s_0, s)$
2. $\mathbf{K}_W(G)(s'_0, s) \leq \mathbf{K}_W(G)(s_0, s)$

Proof. We define \mathbf{E}'_W and \mathbf{K}'_W as follows:

$$\begin{aligned} \mathbf{E}'_W(G)(s_0, s) &= \{ (\tau, e_1, e_2) \mid \exists s'_0. s'_0 \sqsupseteq_{\text{pub}} s_0 \wedge (\tau, e_1, e_2) \in \mathbf{E}_W(G)(s'_0, s) \} \\ \mathbf{K}'_W(G)(s_0, s) &= \{ (\tau_1, \tau_2, K_1, K_2) \mid \exists s'_0. s'_0 \sqsupseteq_{\text{pub}} s_0 \wedge (\tau_1, \tau_2, K_1, K_2) \in \mathbf{K}_W(G)(s'_0, s) \} \end{aligned}$$

If $\mathbf{E}'_W \leq \mathbf{E}_W$ and $\mathbf{K}'_W \leq \mathbf{K}_W$, then for $s'_0 \sqsupseteq_{\text{pub}} s_0$ we have

$$\mathbf{E}_W(G)(s'_0, s) \leq \mathbf{E}'_W(G)(s_0, s) \leq \mathbf{E}_W(G)(s_0, s)$$

(and similar for \mathbf{K}_W).

We now prove $\mathbf{E}'_W \leq \mathbf{E}_W$ and $\mathbf{K}'_W \leq \mathbf{K}_W$ by coinduction. Concretely, we have to show:

1. $\forall e_1, e_2, G, s_0, s, \tau.$
 $(e_1, e_2) \in \mathbf{E}'_W(G)(s_0, s)(\tau) \implies$
 $\forall (h_1, h_2) \in W.H(s)(G(s)). \forall h_1^F, h_2^F. ((h_1, h_1^F, e_1), (h_2, h_2^F, e_2)) \in \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0, s)(\tau)$
2. $\forall K_1, K_2, G, s_0, s, \tau', \tau.$
 $(K_1, K_2) \in \mathbf{K}'_W(G)(s_0, s)(\tau', \tau) \implies$
 $\forall (v_1, v_2) \in \overline{G(s)}(\tau'). (K_1[v_1], K_2[v_2]) \in \mathbf{E}'_W(G)(s_0, s)(\tau)$

For (1):

- Suppose $(e_1, e_2) \in \mathbf{E}'_W(G)(s_0, s)(\tau)$ and $(h_1, h_2) \in W.H(s)(G(s))$.
- We must show $((h_1, h_1^F, e_1), (h_2, h_2^F, e_2)) \in \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0, s)(\tau)$.
- By definition of \mathbf{E}'_W we know $(e_1, e_2) \in \mathbf{E}_W(G)(s'_0, s)(\tau)$ for some $s'_0 \sqsupseteq_{\text{pub}} s_0$.
- Hence $((h_1, h_1^F, e_1), (h_2, h_2^F, e_2)) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s'_0, s)(\tau)$.
- It is easy to see that this implies $((h_1, h_1^F, e_1), (h_2, h_2^F, e_2)) \in \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0, s)(\tau)$.

For (2):

- Suppose $(K_1, K_2) \in \mathbf{K}'_W(G)(s_0, s)(\tau', \tau)$ and $(v_1, v_2) \in \overline{G(s)}(\tau')$.
- We must show $(K_1[v_1], K_2[v_2]) \in \mathbf{E}'_W(G)(s_0, s)(\tau)$.
- By definition of \mathbf{K}'_W we know $(K_1, K_2) \in \mathbf{K}_W(G)(s'_0, s)(\tau', \tau)$ for some $s'_0 \sqsupseteq_{\text{pub}} s_0$.
- Hence $(K_1[v_1], K_2[v_2]) \in \mathbf{E}_W(G)(s'_0, s)(\tau) \subseteq \mathbf{E}'_W(G)(s_0, s)(\tau)$.

\square

Lemma 8. If $w_1, w_2 \in \text{LWorld}$, then $\forall G \in \text{GK}((w_1 \otimes w_2)\uparrow). \forall s_2 \in w_2.S. G(-, -, s_2) \in \text{GK}(w_1\uparrow)$.

Proof. We must establish four properties:

a) To show: $G(-, -, s_2)$ is monotone w.r.t. \sqsubseteq .

This follows directly from the definition of \uparrow, \otimes and the monotonicity of G .

b) To show: $\forall s_{\text{rf}}, s_1, \tau. G(s_{\text{rf}}, s_1, s_2)(\tau) \supseteq w_1 \uparrow. \mathbf{L}(s_{\text{rf}}, s_1)(G(s_{\text{rf}}, s_1, s_2))(\tau)$.

We know $G(s_{\text{rf}}, s_1, s_2)(\tau) \supseteq (w_1 \otimes w_2) \uparrow. \mathbf{L}(s_{\text{rf}}, s_1, s_2)(G(s_{\text{rf}}, s_1, s_2))(\tau)$.

By definition, the latter equals $w_1 \uparrow. \mathbf{L}(s_{\text{rf}}, s_1)(G(s_{\text{rf}}, s_1, s_2))(\tau) \cup w_2. \mathbf{L}(s_{\text{rf}})(s_2)(G(s_{\text{rf}}, s_1, s_2))(\tau)$.

c) To show: $\forall s_{\text{rf}}, s_1, \tau. G(s_{\text{rf}}, s_1, s_2)(\text{ref } \tau) = w_1 \uparrow. \mathbf{L}(s_{\text{rf}}, s_1)(G(s_{\text{rf}}, s_1, s_2))(\text{ref } \tau)$.

We know $G(s_{\text{rf}}, s_1, s_2)(\text{ref } \tau) = (w_1 \otimes w_2) \uparrow. \mathbf{L}(s_{\text{rf}}, s_1, s_2)(G(s_{\text{rf}}, s_1, s_2))(\text{ref } \tau)$.

By definition, the latter equals $w_1 \uparrow. \mathbf{L}(s_{\text{rf}}, s_1)(G(s_{\text{rf}}, s_1, s_2))(\text{ref } \tau) \cup w_2. \mathbf{L}(s_{\text{rf}})(s_2)(G(s_{\text{rf}}, s_1, s_2))(\text{ref } \tau)$.

Since $w_2 \in \text{LWorld}$, we are done.

d) To show: $\forall s_{\text{rf}}, s_1, \mathbf{n} \in w_1 \uparrow. \mathbf{N}. G(s_{\text{rf}}, s_1, s_2)(\mathbf{n}) = w_1 \uparrow. \mathbf{L}(s_{\text{rf}}, s_1)(G(s_{\text{rf}}, s_1, s_2))(\mathbf{n})$.

We know $G(s_{\text{rf}}, s_1, s_2)(\mathbf{n}) = (w_1 \otimes w_2) \uparrow. \mathbf{L}(s_{\text{rf}}, s_1, s_2)(G(s_{\text{rf}}, s_1, s_2))(\mathbf{n})$.

By definition, the latter equals $w_1 \uparrow. \mathbf{L}(s_{\text{rf}}, s_1)(G(s_{\text{rf}}, s_1, s_2))(\mathbf{n}) \cup w_2. \mathbf{L}(s_{\text{rf}})(s_2)(G(s_{\text{rf}}, s_1, s_2))(\mathbf{n})$.

Since $\mathbf{n} \notin w_2. \mathbf{N}$ by definition of \uparrow, \otimes , we are done.

□

Lemma 9. If $w_1, w_2 \in \text{LWorld}$, then $\forall G \in \text{GK}((w_1 \otimes w_2) \uparrow). \forall s_1 \in w_1. \mathbf{S}. G(-, s_1, -) \in \text{GK}(w_2 \uparrow)$.

Proof. Similar to Lemma 8.

□

Lemma 10. If $w = w_1 \otimes w_2$ with $w_1, w_2 \in \text{LWorld}$ and *stable*(w_2), then for all $G \in \text{GK}(w \uparrow)$ and for all $s_{\text{rf}}^0, s_{\text{rf}} \in W_{\text{ref}}. \mathbf{S}, s_1^0, s_1 \in w_1. \mathbf{S}, s_2^0, s_2 \in w_2. \mathbf{S}$ with $s_2 \sqsupseteq_{\text{pub}} s_2^0$:

$$1. \mathbf{E}_{w_1 \uparrow}(G(-, -, s_2))((s_{\text{rf}}^0, s_1^0), (s_{\text{rf}}, s_1)) \leq \mathbf{E}_{w \uparrow}(G)((s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2))$$

$$2. \mathbf{K}_{w_1 \uparrow}(G(-, -, s_2))((s_{\text{rf}}^0, s_1^0), (s_{\text{rf}}, s_1)) \leq \mathbf{K}_{w \uparrow}(G)((s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2))$$

Proof. We define $\mathbf{E}'_{w \uparrow}$ and $\mathbf{K}'_{w \uparrow}$ as follows:

$$\mathbf{E}'_{w \uparrow}(G)((s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2)) = \{ (\tau, e_1, e_2) \mid s_2 \sqsupseteq_{\text{pub}} s_2^0 \wedge (\tau, e_1, e_2) \in \mathbf{E}_{w_1 \uparrow}(G(-, -, s_2))((s_{\text{rf}}^0, s_1^0), (s_{\text{rf}}, s_1)) \}$$

$$\mathbf{K}'_{w \uparrow}(G)((s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2)) = \{ (\tau', \tau, K_1, K_2) \mid s_2 \sqsupseteq_{\text{pub}} s_2^0 \wedge (\tau', \tau, K_1, K_2) \in \mathbf{K}_{w_1 \uparrow}(G(-, -, s_2))((s_{\text{rf}}^0, s_1^0), (s_{\text{rf}}, s_1)) \}$$

We now prove $\mathbf{E}'_{w \uparrow} \leq \mathbf{E}_{w \uparrow}$ and $\mathbf{K}'_{w \uparrow} \leq \mathbf{K}_{w \uparrow}$ by coinduction. Concretely, we have to show:

1. $\forall e_1, e_2, G, s_{\text{rf}}^0, s_{\text{rf}}, s_1^0, s_2^0, s_1, s_2, \tau.$

$$(e_1, e_2) \in \mathbf{E}'_{w \uparrow}(G)((s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2))(\tau) \implies \forall (h_1, h_2) \in w \uparrow. \mathbf{H}(s_{\text{rf}}, s_1, s_2)(G(s_{\text{rf}}, s_1, s_2)). \forall h_1^F, h_2^F. ((h_1, h_1^F, e_1), (h_2, h_2^F, e_2)) \in \mathbf{O}_{w \uparrow}(\mathbf{K}'_{w \uparrow})(G)((s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2))(\tau)$$

2. $\forall K_1, K_2, G, s_{\text{rf}}^0, s_{\text{rf}}, s_1^0, s_2^0, s_1, s_2, \tau', \tau.$

$$(K_1, K_2) \in \mathbf{K}'_{w \uparrow}(G)((s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2))(\tau', \tau) \implies \forall (v_1, v_2) \in G(s_{\text{rf}}, s_1, s_2)(\tau'). (K_1[v_1], K_2[v_2]) \in \mathbf{E}'_{w \uparrow}(G)((s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2))(\tau)$$

For (1):

- Suppose $(e_1, e_2) \in \mathbf{E}'_{w \uparrow}(G)((s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2))(\tau)$ and $(h_1, h_2) \in w \uparrow. \mathbf{H}(s_{\text{rf}}, s_1, s_2)(G(s_{\text{rf}}, s_1, s_2))$.
- By definition of $\mathbf{E}'_{w \uparrow}$ we know $s_2 \sqsupseteq_{\text{pub}} s_2^0$ and $(e_1, e_2) \in \mathbf{E}_{w_1 \uparrow}(G(-, -, s_2))((s_{\text{rf}}^0, s_1^0), (s_{\text{rf}}, s_1))(\tau)$.
- We must show $((h_1, h_1^F, e_1), (h_2, h_2^F, e_2)) \in \mathbf{O}_{w \uparrow}(\mathbf{K}'_{w \uparrow})(G)((s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2))(\tau)$.

- So suppose defined($h_1 \uplus h_1^F$) and defined($h_2 \uplus h_2^F$).
- From $(h_1, h_2) \in w\uparrow.\mathbf{H}(s_{\text{rf}}, s_1, s_2)(G(s_{\text{rf}}, s_1, s_2))$ and the definition of \uparrow, \otimes , we know $h_1 = h'_1 \uplus h''_1$ and $h_2 = h'_2 \uplus h''_2$ with $(h'_1, h'_2) \in w_1\uparrow.\mathbf{H}(s_{\text{rf}}, s_1)(G(s_{\text{rf}}, s_1, s_2))$ and $(h''_1, h''_2) \in w_2.\mathbf{H}(s_{\text{rf}})(s_2)(G(s_{\text{rf}}, s_1, s_2))$.
- Hence $((h'_1, h''_1 \uplus h_1^F, e_1), (h'_2, h''_2 \uplus h_2^F, e_2)) \in \mathbf{O}_{w_1\uparrow}(\mathbf{K}_{w_1\uparrow})(G(-, -, s_2))((s_{\text{rf}}^0, s_1^0), (s_{\text{rf}}, s_1))(\tau)$.
- Consequently at least one of the following three properties holds:
 - A) $h_1 \uplus h_1^F, e_1 \uparrow$ and $h_2 \uplus h_2^F, e_2 \uparrow$
 - B) (a) $h_1 \uplus h_1^F, e_1 \hookrightarrow^* \widetilde{h}'_1 \uplus h''_1 \uplus h_1^F, v_1$ and $h_2 \uplus h_2^F, e_2 \hookrightarrow^* \widetilde{h}'_2 \uplus h''_2 \uplus h_2^F, v_2$
 (b) $(\widetilde{s}_{\text{rf}}, \widetilde{s}_1) \sqsupseteq [(s_{\text{rf}}^0, s_1^0), (s_{\text{rf}}, s_1)]$
 (c) $(\widetilde{h}'_1, \widetilde{h}'_2) \in w_1\uparrow.\mathbf{H}(\widetilde{s}_{\text{rf}}, \widetilde{s}_1)(G(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, s_2))$
 (d) $(v_1, v_2) \in \overline{G(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, s_2)}(\tau)$
 - C) (a) $h_1 \uplus h_1^F, e_1 \hookrightarrow^* \widetilde{h}'_1 \uplus h''_1 \uplus h_1^F, K_1[e'_1]$ and $h_2 \uplus h_2^F, e_2 \hookrightarrow^* \widetilde{h}'_2 \uplus h''_2 \uplus h_2^F, K_2[e'_2]$
 (b) $(\widetilde{s}_{\text{rf}}, \widetilde{s}_1) \sqsupseteq (s_{\text{rf}}, s_1)$
 (c) $(\widetilde{h}'_1, \widetilde{h}'_2) \in w_1\uparrow.\mathbf{H}(\widetilde{s}_{\text{rf}}, \widetilde{s}_1)(G(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, s_2))$
 (d) $(e'_1, e'_2) \in \mathbf{S}(G(\widetilde{s}_{\text{rf}}, \widetilde{s}, s_2), G(\widetilde{s}_{\text{rf}}, \widetilde{s}, s_2))(\widetilde{\tau})$
 (e) $\forall (\widetilde{s}_{\text{rf}}, \widehat{s}_1) \sqsupseteq_{\text{pub}} (\widetilde{s}_{\text{rf}}, \widetilde{s}_1). \forall G' \geq G(-, -, s_2). (K_1, K_2) \in \mathbf{K}_{w_1\uparrow}(G')((s_{\text{rf}}^0, s_1^0), (\widehat{s}_{\text{rf}}, \widehat{s}_1))(\widetilde{\tau}, \tau)$

• If (A) holds, then we are done.

• If (B) holds:

– By *stable*(w_2) there is $\widetilde{s}_2 \sqsupseteq_{\text{pub}} s_2$ such that

$$(h''_1, h''_2) \in w_2.\mathbf{H}(\widetilde{s}_{\text{rf}})(\widetilde{s}_2)(G(s_{\text{rf}}, s_1, s_2)) .$$

– By monotonicity of $w_2.\mathbf{H}$, from $G(s_{\text{rf}}, s_1, s_2) \subseteq G(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, \widetilde{s}_2)$, we have

$$(h''_1, h''_2) \in w_2.\mathbf{H}(\widetilde{s}_{\text{rf}})(\widetilde{s}_2)(G(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, \widetilde{s}_2)) .$$

– From (Bc) and monotonicity we also know $(\widetilde{h}'_1, \widetilde{h}'_2) \in w_1\uparrow.\mathbf{H}(\widetilde{s}_{\text{rf}}, \widetilde{s}_1)(G(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, \widetilde{s}_2))$.

– Thus by the definition of \uparrow, \otimes , we get $(\widetilde{h}'_1 \uplus h''_1, \widetilde{h}'_2 \uplus h''_2) \in w\uparrow.\mathbf{H}(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, \widetilde{s}_2)(G(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, \widetilde{s}_2))$.

– From (Bb) and the definition of \uparrow, \otimes , we get $(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, \widetilde{s}_2) \sqsupseteq [(s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2)]$.

– Together with (Ba) (Bd) we are done.

• If (C) holds:

– By *stable*(w_2) there is $\widetilde{s}_2 \sqsupseteq_{\text{pub}} s_2$ such that

$$(h''_1, h''_2) \in w_2.\mathbf{H}(\widetilde{s}_{\text{rf}})(\widetilde{s}_2)(G(s_{\text{rf}}, s_1, s_2)) .$$

– By monotonicity of $w_2.\mathbf{H}$, from $G(s_{\text{rf}}, s_1, s_2) \subseteq G(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, \widetilde{s}_2)$, we have

$$(h''_1, h''_2) \in w_2.\mathbf{H}(\widetilde{s}_{\text{rf}})(\widetilde{s}_2)(G(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, \widetilde{s}_2)) .$$

– From (Cc) and monotonicity we also know $(\widetilde{h}'_1, \widetilde{h}'_2) \in w_1\uparrow.\mathbf{H}(\widetilde{s}_{\text{rf}}, \widetilde{s}_1)(G(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, \widetilde{s}_2))$.

– Thus by the definition of \uparrow, \otimes , we get $(\widetilde{h}'_1 \uplus h''_1, \widetilde{h}'_2 \uplus h''_2) \in w\uparrow.\mathbf{H}(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, \widetilde{s}_2)(G(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, \widetilde{s}_2))$.

– From (Cb) and the definition of \uparrow, \otimes , we get $(\widetilde{s}_{\text{rf}}, \widetilde{s}_1, \widetilde{s}_2) \sqsupseteq [(s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2)]$.

– Now it remains to show:

$$\forall (\widehat{s}_{\text{rf}}, \widehat{s}_1, \widehat{s}_2) \sqsupseteq_{\text{pub}} (\widetilde{s}_{\text{rf}}, \widetilde{s}_1, \widetilde{s}_2). \forall G' \geq G. (K_1, K_2) \in \mathbf{K}'_{w\uparrow}(G')((s_{\text{rf}}^0, s_1^0, s_2^0), (\widehat{s}_{\text{rf}}, \widehat{s}_1, \widehat{s}_2))(\widetilde{\tau}, \tau)$$

– So suppose $(\widehat{s}_{\text{rf}}, \widehat{s}_1, \widehat{s}_2) \sqsupseteq_{\text{pub}} (\widetilde{s}_{\text{rf}}, \widetilde{s}_1, \widetilde{s}_2)$ and $G' \geq G$.

– Note that $(\widehat{s}_{\text{rf}}, \widehat{s}_1) \sqsupseteq_{\text{pub}} (\widetilde{s}_{\text{rf}}, \widetilde{s}_1)$ and, by monotonicity, $G'(-, -, \widehat{s}_2) \geq G(-, -, s_2)$.

– From (Ce) we therefore get $(K_1, K_2) \in \mathbf{K}'_{w_1\uparrow}(G'(-, -, \widehat{s}_2))((s_{\text{rf}}^0, s_1^0), (\widehat{s}_{\text{rf}}, \widehat{s}_1))(\widetilde{\tau}, \tau)$.

– By definition of $\mathbf{K}'_{w\uparrow}$ this implies

$$(K_1, K_2) \in \mathbf{K}'_{w\uparrow}(G')((s_{\text{rf}}^0, s_1^0, s_2^0), (\widehat{s}_{\text{rf}}, \widehat{s}_1, \widehat{s}_2))(\widetilde{\tau}, \tau)$$

For (2):

- Suppose $(K_1, K_2) \in \mathbf{K}'_{w\uparrow}(G)((s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2))(\tau', \tau)$ and $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s_1, s_2)}(\tau')$.
- By definition of $\mathbf{K}'_{w\uparrow}$ we know $s_2 \sqsupseteq_{\text{pub}} s_2^0$ and $(K_1, K_2) \in \mathbf{K}'_{w_1\uparrow}(G(-, -, s_2))((s_{\text{rf}}^0, s_1^0), (s_{\text{rf}}, s_1))(\tau', \tau)$.
- We must show $(K_1[v_1], K_2[v_2]) \in \mathbf{E}'_{w\uparrow}(G)((s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2))(\tau)$.
- By definition of $\mathbf{E}'_{w\uparrow}$ it suffices to show

$$(K_1[v_1], K_2[v_2]) \in \mathbf{E}_{w_1\uparrow}(G(-, -, s_2))((s_{\text{rf}}^0, s_1^0), (s_{\text{rf}}, s_1))(\tau).$$

- Since $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s_1, s_2)}(\tau')$, we are done. □

Lemma 11. If $w = w_1 \otimes w_2$ with $w_1, w_2 \in \text{LWorld}$ and $\text{stable}(w_1)$, then for all $G \in \text{GK}(w\uparrow)$ and for all $s_{\text{rf}}^0, s_{\text{rf}} \in W_{\text{ref}}.\mathcal{S}$, $s_1^0, s_1 \in w_1.\mathcal{S}$, $s_2^0, s_2 \in w_2.\mathcal{S}$ with $s_1 \sqsupseteq_{\text{pub}} s_1^0$:

1. $\mathbf{E}_{w_2\uparrow}(G(-, s_1, -))((s_{\text{rf}}^0, s_2^0), (s_{\text{rf}}, s_2)) \leq \mathbf{E}_{w\uparrow}(G)((s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2))$
2. $\mathbf{K}_{w_2\uparrow}(G(-, s_1, -))((s_{\text{rf}}^0, s_2^0), (s_{\text{rf}}, s_2)) \leq \mathbf{K}_{w\uparrow}(G)((s_{\text{rf}}^0, s_1^0, s_2^0), (s_{\text{rf}}, s_1, s_2))$

Proof. Similar to Lemma 10. □

Lemma 12. If $w = w_1 \otimes w_2$ with $w_1, w_2 \in \text{LWorld}$ and $\text{stable}(w_1)$, $\text{stable}(w_2)$, then:

1. $\text{stable}(w)$
2. If $\text{inhabited}(w_1\uparrow)$ and $\text{inhabited}(w_2\uparrow)$, then $\text{inhabited}(w\uparrow)$.
3. If $\text{consistent}(w_1\uparrow)$ and $\text{consistent}(w_2\uparrow)$, then $\text{consistent}(w\uparrow)$.

Proof.

1. • Suppose $G \in \text{GK}((w_1 \otimes w_2)\uparrow)$, $(h_1, h_2) \in (w_1 \otimes w_2).\mathbf{H}(s_{\text{rf}})(s_1, s_2)(G(s_{\text{rf}}, s_1, s_2))$ and $s'_{\text{rf}} \sqsupseteq s_{\text{rf}}$.
- Further suppose $(h'_1, h'_2) \in W_{\text{ref}}.\mathbf{H}(s'_{\text{rf}})(G(s'_{\text{rf}}, s))$ and $\text{defined}(h'_1 \uplus h_1)$ and $\text{defined}(h'_2 \uplus h_2)$.
- We must show that there is $(s'_1, s'_2) \sqsupseteq_{\text{pub}} (s_1, s_2)$ such that

$$(h_1, h_2) \in (w_1 \otimes w_2).\mathbf{H}(s'_{\text{rf}})(s'_1, s'_2)(G(s'_{\text{rf}}, s'_1, s'_2)).$$

- Decomposing $(w_1 \otimes w_2).\mathbf{H}$ gives us $h_1^1, h_2^1, h_1^2, h_2^2$ such that:
 - $h_1 = h_1^1 \uplus h_1^2$ and $h_2 = h_2^1 \uplus h_2^2$
 - $(h_1^1, h_2^1) \in w_1.\mathbf{H}(s_{\text{rf}})(s_1)(G(s_{\text{rf}}, s_1, s_2))$

- defined($h'_1 \uplus h_1^1$) and defined($h'_2 \uplus h_2^1$)
- $(h_1^2, h_2^2) \in w_2.H(s_{\text{rf}})(s_2)(G(s_{\text{rf}}, s_1, s_2))$
- defined($h'_1 \uplus h_1^2$) and defined($h'_2 \uplus h_2^2$)
- From this, Lemmas 8–11, and the assumptions, we get $s'_1 \sqsupseteq_{\text{pub}} s_1$ and $s'_2 \sqsupseteq_{\text{pub}} s_2$ such that:
 - (a) $(h_1^1, h_2^1) \in w_1.H(s'_{\text{rf}})(s'_1)(G(s'_{\text{rf}}, s'_1, s_2))$
 - (b) $(h_1^2, h_2^2) \in w_2.H(s'_{\text{rf}})(s'_2)(G(s'_{\text{rf}}, s_1, s'_2))$
- Using monotonicity and then composing this gives us

$$(h_1, h_2) \in (w_1 \otimes w_2).H(s'_{\text{rf}})(s'_1, s'_2)(G(s'_{\text{rf}}, s'_1, s'_2)).$$

2. • Suppose $G \in \text{GK}(w\uparrow)$.
 - From the assumptions, Lemma 2, and definition of \uparrow and W_{ref} we get s_1, s_2 such that
 - $(\emptyset, \emptyset) \in w_1.H(\emptyset)(s_1)([w_1\uparrow](\emptyset, s_1))$ and
 - $(\emptyset, \emptyset) \in w_2.H(\emptyset)(s_2)([w_2\uparrow](\emptyset, s_2))$.
 - From Lemmas 2, 3, 8, 9, we know $[w_1\uparrow] \leq [w\uparrow](-, (-, s_2))$ and $[w_2\uparrow] \leq [w\uparrow](-, (s_1, -))$.
 - Hence $(\emptyset, \emptyset) \in w\uparrow.H(\emptyset, (s_1, s_2))([w\uparrow](\emptyset, (s_1, s_2)))$ by monotonicity and definition of \otimes, \uparrow .
3. • We suppose
 - (a) $s = (s_{\text{rf}}, s_1, s_2) \in w\uparrow.S$
 - (b) $G \in \text{GK}(w\uparrow)$
 - (c) $(\tau, e_1, e_2) \in \mathbf{S}(w\uparrow.L(s)(G(s)), G(s))$
 and must show $(\tau, \text{beta}(e_1), \text{beta}(e_2)) \in \mathbf{E}_{w\uparrow}(G)(s, s)$.
 - From (c) and the definitions of \uparrow, \otimes and \mathbf{S} we know:

$$\begin{aligned} (\tau, e_1, e_2) &\in \mathbf{S}(W_{\text{ref}}.L(s_{\text{rf}})(G(s)), G(s)) \vee \\ (\tau, e_1, e_2) &\in \mathbf{S}(w_1.L(s_{\text{rf}})(s_1)(G(s)), G(s)) \vee \\ (\tau, e_1, e_2) &\in \mathbf{S}(w_2.L(s_{\text{rf}})(s_2)(G(s)), G(s)) \end{aligned}$$

- This implies:

$$\begin{aligned} (\tau, e_1, e_2) &\in \mathbf{S}(w_1\uparrow.L(s_{\text{rf}}, s_1)(G(s)), G(s)) \vee \\ (\tau, e_1, e_2) &\in \mathbf{S}(w_2\uparrow.L(s_{\text{rf}}, s_2)(G(s)), G(s)) \end{aligned}$$

- If the former is true, the goal follows from *consistent*($w_1\uparrow$) with the help of Lemmas 8 and 10.
- If the latter is true, the goal follows from *consistent*($w_2\uparrow$) with the help of Lemmas 9 and 11.

□

Lemma 13. For $G \in \text{GK}(W)$, $s_0, s'_0, s \in W.S$, $\tau, \tau' \in \text{CType}$, $K_1, K_2 \in \text{Cont}$, if

$$\forall s' \sqsupseteq [s'_0, s]. \forall G' \geq G. (\tau', \tau, K_1, K_2) \in \mathbf{K}_W(G')(s_0, s'),$$

then:

1. $(\tau', e_1, e_2) \in \mathbf{E}_W(G)(s'_0, s)$ implies $(\tau, K_1[e_1], K_2[e_2]) \in \mathbf{E}_W(G)(s_0, s)$.
2. $(\tau'', \tau', K'_1, K'_2) \in \mathbf{K}_W(G)(s'_0, s)$ implies $(\tau'', \tau, K_1[K'_1], K_2[K'_2]) \in \mathbf{K}_W(G)(s_0, s)$.

Proof. We define \mathbf{E}'_W and \mathbf{K}'_W as follows:

$$\begin{aligned} \mathbf{E}'_W(G)(s_0, s) &= \{ (\tau, K_1[e_1], K_2[e_2]) \mid \exists \tau', s'_0. (\tau', e_1, e_2) \in \mathbf{E}_W(G)(s'_0, s) \wedge \\ &\quad \forall s' \sqsupseteq [s'_0, s]. \forall G' \geq G. (\tau', \tau, K_1, K_2) \in \mathbf{K}_W(G')(s_0, s') \} \end{aligned}$$

$$\begin{aligned} \mathbf{K}'_W(G)(s_0, s) &= \{ (\tau'', \tau, K_1[K'_1], K_2[K'_2]) \mid \exists \tau', s'_0. (\tau'', \tau', K'_1, K'_2) \in \mathbf{K}_W(G)(s'_0, s) \wedge \\ &\quad \forall s' \sqsupseteq [s'_0, s]. \forall G' \geq G. (\tau', \tau, K_1, K_2) \in \mathbf{K}_W(G')(s_0, s') \} \end{aligned}$$

It suffices to show $\mathbf{E}'_W \leq \mathbf{E}_W$ and $\mathbf{K}'_W \leq \mathbf{K}_W$, which we do by coinduction. Concretely, we have to show:

1. $\forall K_1, K_2, e_1, e_2, G, s_0, s, \tau.$
 $(K_1[e_1], K_2[e_2]) \in \mathbf{E}'_W(G)(s_0, s)(\tau) \implies$
 $\forall (h_1, h_2) \in W.H(s)(G(s)). \forall h_1^F, h_2^F.$
 $((h_1, h_1^F, K_1[e_1]), (h_2, h_2^F, K_2[e_2])) \in \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0, s)(\tau)$
2. $\forall K_1, K_2, K'_1, K'_2, G, s_0, s, \tau'', \tau.$
 $(K_1[K'_1], K_2[K'_2]) \in \mathbf{K}'_W(G)(s_0, s)(\tau'', \tau) \implies$
 $\forall (v_1, v_2) \in \overline{G}(s)(\tau''). (K_1[K'_1][v_1], K_2[K'_2][v_2]) \in \mathbf{E}'_W(G)(s_0, s)(\tau)$

For (1):

- Suppose $(K_1[e_1], K_2[e_2]) \in \mathbf{E}'_W(G)(s_0, s)(\tau)$ and $(h_1, h_2) \in W.H(s)(G(s)).$
- By definition of \mathbf{E}'_W we know $(e_1, e_2) \in \mathbf{E}_W(G)(s'_0, s)(\tau')$ and

$$\forall s' \supseteq [s'_0, s]. \forall G' \geq G. (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau)$$

for some s'_0 and τ' .

- We must show $((h_1, h_1^F, K_1[e_1]), (h_2, h_2^F, K_2[e_2])) \in \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0, s)(\tau).$
- So suppose defined $(h_1 \uplus h_1^F)$ and defined $(h_2 \uplus h_2^F).$
- We know $((h_1, h_1^F, e_1), (h_2, h_2^F, e_2)) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s'_0, s)(\tau').$
- Hence at least one of the following three properties holds:

- A) $h_1 \uplus h_1^F, e_1 \uparrow$ and $h_2 \uplus h_2^F, e_2 \uparrow$
- B) (a) $h_1 \uplus h_1^F, e_1 \hookrightarrow^* h'_1 \uplus h_1^F, v_1$ and $h_2 \uplus h_2^F, e_2 \hookrightarrow^* h'_2 \uplus h_2^F, v_2$
(b) $s' \supseteq [s'_0, s]$
(c) $(h'_1, h'_2) \in W.H(s')(G(s'))$
(d) $(v_1, v_2) \in \overline{G}(s')(\tau')$
- C) (a) $h_1 \uplus h_1^F, e_1 \hookrightarrow^* h'_1 \uplus h_1^F, K'_1[e'_1]$ and $h_2 \uplus h_2^F, e_2 \hookrightarrow^* h'_2 \uplus h_2^F, K'_2[e'_2]$
(b) $s' \supseteq s$
(c) $(h'_1, h'_2) \in W.H(s')(G(s'))$
(d) $(e'_1, e'_2) \in \mathbf{S}(G(s'), G(s'))(\tilde{\tau})$
(e) $\forall s'' \supseteq_{\text{pub}} s'. \forall G' \geq G. (K'_1, K'_2) \in \mathbf{K}_W(G')(s'_0, s'')(\tilde{\tau}, \tau')$

- If (A) holds:

– Then $h_1 \uplus h_1^F, K_1[e_1] \uparrow$ and $h_2 \uplus h_2^F, K_2[e_2] \uparrow$, so we are done.

- If (B) holds:

- Then $h_1 \uplus h_1^F, K_1[e_1] \hookrightarrow^* h'_1 \uplus h_1^F, K_1[v_1]$ and $h_2 \uplus h_2^F, K_2[e_2] \hookrightarrow^* h'_2 \uplus h_2^F, K_2[v_2]$ from (Ba).
- Since $(K_1, K_2) \in \mathbf{K}_W(G)(s_0, s')(\tau', \tau)$ from (Bb), we get $(K_1[v_1], K_2[v_2]) \in \mathbf{E}_W(G)(s_0, s')(\tau)$ from (Bd).
- Using (Bc), this implies $((h'_1, h_1^F, K_1[v_1]), (h'_2, h_2^F, K_2[v_2])) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s_0, s')(\tau).$
- We show $\mathbf{O}_W(\mathbf{K}_W)(G)(s_0, s')(\tau) \subseteq \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0, s')(\tau):$
 - * It suffices to show $\mathbf{K}_W \leq \mathbf{K}'_W.$
 - * By definition of the latter, this follows from Lemmas 7 and 6.
- Consequently, $((h'_1, h_1^F, K_1[v_1]), (h'_2, h_2^F, K_2[v_2])) \in \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0, s')(\tau).$
- We are done by (Bb) and Lemma 4.

- If (C) holds:

- Then $h_1 \uplus h_1^{\mathbb{F}}, e_1 \hookrightarrow^* h'_1 \uplus h_1^{\mathbb{F}}, K_1[K'_1][e'_1]$ and $h_2 \uplus h_2^{\mathbb{F}}, e_2 \hookrightarrow^* h'_2 \uplus h_2^{\mathbb{F}}, K_2[K'_2][e'_2]$ from (Ca).
- Due to (Cb–d) it remains to show:

$$\forall s'' \sqsupseteq_{\text{pub}} s'. \forall G' \geq G. (K_1[K'_1], K_2[K'_2]) \in \mathbf{K}'_W(G')(s_0, s'')(\tilde{\tau}, \tau)$$

- So suppose $s'' \sqsupseteq_{\text{pub}} s'$ and $G' \geq G$.
- By definition of \mathbf{K}'_W it suffices to show $(K'_1, K'_2) \in \mathbf{K}_W(G')(s'_0, s'')(\tilde{\tau}, \tau')$ and

$$\forall s''' \sqsupseteq [s'_0, s'']. \forall G'' \geq G'. (K_1, K_2) \in \mathbf{K}_W(G'')(s_0, s''')(\tau', \tau).$$

- The former follows from (Ce).
- For the latter, recall that

$$\forall s' \sqsupseteq [s'_0, s]. \forall G' \geq G. (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau).$$

- Since $s'' \sqsupseteq_{\text{pub}} s' \sqsupseteq s$ and $G'' \geq G' \geq G$, we are done.

For (2):

- Suppose $(K_1[K'_1], K_2[K'_2]) \in \mathbf{K}'_W(G)(s_0, s)(\tau'', \tau)$ and $(v_1, v_2) \in \overline{G(s)}(\tau'')$.
- By definition of \mathbf{K}'_W we know $(K'_1, K'_2) \in \mathbf{K}_W(G)(s'_0, s)(\tau'', \tau')$ and

$$\forall s' \sqsupseteq [s'_0, s]. \forall G' \geq G. (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau)$$

for some s'_0 and τ' .

- We must show $(K_1[K'_1][v_1], K_2[K'_2][v_2]) \in \mathbf{E}'_W(G)(s_0, s)(\tau)$.
- By definition of \mathbf{E}'_W it suffices to show $(K'_1[v_1], K'_2[v_2]) \in \mathbf{E}_W(G)(s'_0, s)(\tau')$ and

$$\forall s' \sqsupseteq [s'_0, s]. \forall G' \geq G. (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau).$$

- The latter is given and the former follows from $(K'_1, K'_2) \in \mathbf{K}_W(G)(s'_0, s)(\tau'', \tau')$ and $(v_1, v_2) \in \overline{G(s)}(\tau'')$.

□

Lemma 14. If $\text{inhabited}(w_2 \uparrow)$, $\text{consistent}(w_2 \uparrow)$, $\text{stable}(w_2)$, and $\text{defined}(w_1 \otimes w_2)$, then:

$$\Delta; \Gamma \vdash e_1 \sim_{w_1} e_2 : \sigma \implies \Delta; \Gamma \vdash e_1 \sim_{w_1 \otimes w_2} e_2 : \sigma$$

Proof.

- Using the assumptions and Lemma 12, we get $\text{inhabited}((w_1 \otimes w_2) \uparrow)$ and $\text{consistent}((w_1 \otimes w_2) \uparrow)$ as well as $\text{stable}(w_1 \otimes w_2)$.
- Now suppose $G \in \text{GK}((w_1 \otimes w_2) \uparrow)$ and $\delta \in \text{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_{\text{rf}}, s, s'))$.
- We must show $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{(w_1 \otimes w_2) \uparrow}(G)((s_{\text{rf}}, s, s'), (s_{\text{rf}}, s, s'))(\delta\sigma)$.
- From $\Delta; \Gamma \vdash e_1 \sim_{w_1} e_2 : \sigma$ and Lemma 8 we know:

$$(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{w_1 \uparrow}(G(-, -, s'))((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\delta\sigma)$$

- We are done by Lemma 10. □

Lemma 15. If $\forall w. (\forall i \in \{1 \dots n\}. \Delta_i; \Gamma_i \vdash e_i \sim_w e'_i : \sigma_i) \implies \Delta; \Gamma \vdash e \sim_{w\uparrow} e' : \sigma$, then

$$(\forall i \in \{1 \dots n\}. \Delta_i; \Gamma_i \vdash e_i \sim e'_i : \sigma_i) \implies \Delta; \Gamma \vdash e \sim e' : \sigma .$$

Proof.

- Suppose $\forall w. (\forall i \in \{1 \dots n\}. \Delta_i; \Gamma_i \vdash e_i \sim_w e'_i : \sigma_i) \implies \Delta; \Gamma \vdash e \sim_{w\uparrow} e' : \sigma$ and $\forall i \in \{1 \dots n\}. \Delta_i; \Gamma_i \vdash e_i \sim e'_i : \sigma_i$.
- Given $\mathcal{N} \in \text{Names}$, since \mathcal{N} is countably infinite, we can split it into \mathcal{N}_i 's such that $\mathcal{N} = \mathcal{N}_1 \uplus \dots \uplus \mathcal{N}_n$.
- Thus by the premise we have w_i 's such that for all i , $w_i.\mathbf{N} \subseteq \mathcal{N}_i$ and $\Delta_i; \Gamma_i \vdash e_i \sim_{w_i} e'_i : \sigma_i$.
- Since $w_i.\mathbf{N}$'s are disjoint, by applying Lemma 14 repeatedly, we have $\Delta_i; \Gamma_i \vdash e_i \sim_{w_1 \otimes \dots \otimes w_n} e'_i : \sigma_i$ for all i .
- By the assumption we thus have $\Delta; \Gamma \vdash e \sim_{(w_1 \otimes \dots \otimes w_n)\uparrow} e' : \sigma$.
- Using Lemma 12 we get $\text{stable}(w_1 \otimes \dots \otimes w_n)$ and thus $\Delta; \Gamma \vdash e \sim_{w_1 \otimes \dots \otimes w_n} e' : \sigma$
- By definition of \otimes , we have $(w_1 \otimes \dots \otimes w_n).\mathbf{N} \subseteq \mathcal{N}_1 \uplus \dots \uplus \mathcal{N}_n = \mathcal{N}$, and thus $\Delta; \Gamma \vdash e \sim e' : \sigma$. □

Lemma 16. If $\forall W. (\forall i \in \{1 \dots n\}. \Delta_i; \Gamma_i \vdash e_i \sim_W e'_i : \sigma_i) \implies \Delta; \Gamma \vdash e \sim_W e' : \sigma$, then:

$$(\forall i \in \{1 \dots n\}. \Delta_i; \Gamma_i \vdash e_i \sim e'_i : \sigma_i) \implies \Delta; \Gamma \vdash e \sim e' : \sigma$$

Proof. Immediate consequence of Lemma 15. □

Lemma 17. If $\forall G, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s)). (\gamma_1 K_1, \gamma_2 K_2) \in \mathbf{K}_W(G)(s, s)(\delta\sigma', \delta\sigma)$ then

$$\Delta; \Gamma \vdash e_1 \sim_W e_2 : \sigma' \implies \Delta; \Gamma \vdash K_1[e_1] \sim_W K_2[e_2] : \sigma$$

Proof.

- Suppose $G \in \text{GK}(W)$, $\delta \in \text{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s))$.
- We must show $((\gamma_1 K_1)[\gamma_1 e_1], (\gamma_2 K_2)[\gamma_2 e_2]) \in \mathbf{E}_W(G)(s, s)(\delta\sigma)$.
- From the premise we get $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_W(G)(s, s)(\delta\sigma')$.
- By Lemma 13 it suffices to show

$$(\gamma_1 K_1, \gamma_2 K_2) \in \mathbf{K}_W(G')(s, s^\circ)(\delta\sigma', \delta\sigma)$$

for $s^\circ \sqsupseteq_{\text{pub}} s$ and $G' \geq G$.

- By Lemma 7 it then suffices to show

$$(\gamma_1 K_1, \gamma_2 K_2) \in \mathbf{K}_W(G')(s^\circ, s^\circ)(\delta\sigma', \delta\sigma),$$

which follows from Lemma 1 and the assumption. □

Lemma 18 (External call). For any $G \in \text{GK}(W)$ and $\mathcal{R} \in W.S \rightarrow \text{VRelF}$, if

$$\text{consistent}(W) \wedge \forall s. G(s) = W.L(s)(G(s)) \cup \mathcal{R}(s),$$

then we have

$$\begin{aligned} & \forall (\tau, e_1, e_2) \in \mathbf{E}_W(G)(s_0, s). \forall (h_1, h_2) \in W.H(s)(G(s)). \\ & \forall h_1^F, h_2^F. h_1 \uplus h_1^F \text{ defined} \wedge h_2 \uplus h_2^F \text{ defined} \implies \\ & \quad (h_1 \uplus h_1^F, e_1 \uparrow \wedge h_2 \uplus h_2^F, e_2 \uparrow) \\ & \quad \vee (\exists h'_1, h'_2, v_1, v_2. h_1 \uplus h_1^F, e_1 \hookrightarrow^* h'_1 \uplus h_1^F, v_1 \wedge h_2 \uplus h_2^F, e_2 \hookrightarrow^* h'_2 \uplus h_2^F, v_2 \wedge \\ & \quad \exists s' \sqsupseteq [s_0, s]. (h'_1, h'_2) \in W.H(s')(G(s')) \wedge (v_1, v_2) \in G(s')(\tau)) \\ & \quad \vee (\exists h'_1, h'_2, \tau', K_1, K_2, e'_1, e'_2. \\ & \quad h_1 \uplus h_1^F, e_1 \hookrightarrow^* h'_1 \uplus h_1^F, K_1[e'_1] \wedge h_2 \uplus h_2^F, e_2 \hookrightarrow^* h'_2 \uplus h_2^F, K_2[e'_2] \wedge \\ & \quad \exists s' \sqsupseteq s. (h'_1, h'_2) \in W.H(s')(G(s')) \wedge (\tau', e'_1, e'_2) \in \mathbf{S}(\mathcal{R}(s'), G(s')) \wedge \\ & \quad \forall s'' \sqsupseteq_{\text{pub}} s'. \forall G' \geq G. (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s'')(\tau', \tau)) \end{aligned}$$

Proof.

- We prove the following proposition by induction on n .

$$\begin{aligned} & \forall (\tau, e_1, e_2) \in \mathbf{E}_W(G)(s_0, s). \forall (h_1, h_2) \in W.H(s)(G(s)). \\ & \forall h_1^F, h_2^F. h_1 \uplus h_1^F \text{ defined} \wedge h_2 \uplus h_2^F \text{ defined} \implies \\ & \quad (h_1 \uplus h_1^F, e_1 \uparrow^n \wedge h_2 \uplus h_2^F, e_2 \uparrow^n) \\ & \quad \vee (\exists h'_1, h'_2, v_1, v_2. h_1 \uplus h_1^F, e_1 \hookrightarrow^* h'_1 \uplus h_1^F, v_1 \wedge h_2 \uplus h_2^F, e_2 \hookrightarrow^* h'_2 \uplus h_2^F, v_2 \wedge \\ & \quad \exists s' \sqsupseteq [s_0, s]. (h'_1, h'_2) \in W.H(s')(G(s')) \wedge (v_1, v_2) \in G(s')(\tau)) \tag{1} \\ & \quad \vee (\exists h'_1, h'_2, \tau', K_1, K_2, e'_1, e'_2. \\ & \quad h_1 \uplus h_1^F, e_1 \hookrightarrow^* h'_1 \uplus h_1^F, K_1[e'_1] \wedge h_2 \uplus h_2^F, e_2 \hookrightarrow^* h'_2 \uplus h_2^F, K_2[e'_2] \wedge \\ & \quad \exists s' \sqsupseteq s. (h'_1, h'_2) \in W.H(s')(G(s')) \wedge (\tau', e'_1, e'_2) \in \mathbf{S}(\mathcal{R}(s'), G(s')) \wedge \\ & \quad \forall s'' \sqsupseteq_{\text{pub}} s'. \forall G' \geq G. (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s'')(\tau', \tau)) \end{aligned}$$

- When $n = 0$, the first case holds vacuously.
- When $n > 0$, we assume that the goal (1) holds for $n - 1$. Then we need to show that the goal (1) holds for n .
- By definition of $\mathbf{E}_W(G)(s_0, s)$, we have three cases.
- In the first two cases, the goal (1) is trivially satisfied.
- In the third case, we have

$$\begin{aligned} & \exists h'_1, h'_2, \tau', K_1, K_2, e'_1, e'_2. \\ & \quad h_1 \uplus h_1^F, e_1 \hookrightarrow^* h'_1 \uplus h_1^F, K_1[e'_1] \wedge h_2 \uplus h_2^F, e_2 \hookrightarrow^* h'_2 \uplus h_2^F, K_2[e'_2] \wedge \\ & \quad \exists s' \sqsupseteq s. (h'_1, h'_2) \in W.H(s')(G(s')) \wedge (\tau', e'_1, e'_2) \in \mathbf{S}(G(s'), G(s')) \wedge \\ & \quad \forall s'' \sqsupseteq_{\text{pub}} s'. \forall G' \geq G. (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s'')(\tau', \tau) \end{aligned}$$

- As $G(s') = W.L(s')(G(s')) \cup \mathcal{R}(s')$, by definition of \mathbf{S} , we have

$$(\tau', e'_1, e'_2) \in \mathbf{S}(G(s'), G(s')) = \mathbf{S}(W.L(s')(G(s')), G(s')) \cup \mathbf{S}(\mathcal{R}(s'), G(s')).$$

- If $(\tau', e'_1, e'_2) \in \mathbf{S}(\mathcal{R}(s'), G(s'))$, then the goal (1) is satisfied.
- If $(\tau', e'_1, e'_2) \in \mathbf{S}(W.L(s')(G(s')), G(s'))$, then by *consistent*(W), we have that $h'_1 \uplus h_1^F, K_1[e'_1] \hookrightarrow^1 h'_1 \uplus h_1^F, K_1[\text{beta}(e'_1)]$ and $h'_2 \uplus h_2^F, K_2[e'_2] \hookrightarrow^1 h'_2 \uplus h_2^F, K_2[\text{beta}(e'_2)]$ and $(\tau', \text{beta}(e'_1), \text{beta}(e'_2)) \in \mathbf{E}_W(G)(s', s')$.

- By Lemma 13, we have $(\tau, K_1[\text{beta}(e'_1)], K_2[\text{beta}(e'_2)]) \in \mathbf{E}_W(G)(s_0, s')$.
- As $(h'_1, h'_2) \in W.H(s')(G(s'))$, by induction hypothesis we have that $h'_1 \uplus h_1^F, K_1[\text{beta}(e'_1)]$ and $h'_2 \uplus h_2^F, K_2[\text{beta}(e'_2)]$ satisfy the goal (1) for $n - 1$ w.r.t. (s_0, s') .
- As $h_1 \uplus h_1^F, e_1 \hookrightarrow^+ h'_1 \uplus h_2^F, K_1[\text{beta}(e'_1)] \wedge h_2 \uplus h_2^F, e_2 \hookrightarrow^+ h'_2 \uplus h_2^F, K_2[\text{beta}(e'_2)]$ and $s' \sqsupseteq s$, we have that $h_1 \uplus h_1^F, e_1$ and $h_2 \uplus h_2^F, e_2$ satisfy the goal (1) for n w.r.t. (s_0, s) , so we are done.
- The original goal is obtained from the sub-goal (1) by pushing the quantification over n inside the first case and then observing that $\forall n. h, e \uparrow^n$ is equivalent to $h, e \uparrow$.

□

Corollary 19. If

- *consistent*(W)
- $\forall s. G(s) = W.L(s)(G(s))$
- $(\tau, e_1, e_2) \in \mathbf{E}_W(G)(s_0, s)$
- $(h_1, h_2) \in W.H(s)(G(s))$ and $h_1 \uplus h_1^F, h_2 \uplus h_2^F$ defined

then one of the following holds:

1. $h_1 \uplus h_1^F, e_1 \uparrow \wedge h_2 \uplus h_2^F, e_2 \uparrow$
2. $\exists h'_1, h'_2, v_1, v_2, s'. \frac{h_1 \uplus h_1^F, e_1 \hookrightarrow^* h'_1 \uplus h_1^F, v_1 \wedge h_2 \uplus h_2^F, e_2 \hookrightarrow^* h'_2 \uplus h_2^F, v_2 \wedge s' \sqsupseteq_{\text{pub}} [s_0, s] \wedge (h'_1, h'_2) \in W.H(s')(G(s')) \wedge (\tau, v_1, v_2) \in \overline{G(s')}}{}$

Proof. Follows from Lemma 18 for $\mathcal{R} = \lambda s. \emptyset$.

□

2.3 Compatibility

Lemma 20 (Compatibility: Var).

$$\frac{\Delta \vdash \Gamma \quad x : \sigma \in \Gamma}{\Delta; \Gamma \vdash x \sim x : \sigma}$$

Proof.

- Let $w_{\text{id}} = w_{\text{single}}(\lambda R.\emptyset, \lambda R.\{(\emptyset, \emptyset)\})$ (so $w_{\text{id}} \cdot \mathbf{N} \subseteq \mathcal{N}$ for any \mathcal{N}).
- We are done if we can show $\Delta; \Gamma \vdash x \sim_{w_{\text{id}}} x : \sigma$.
- It is obvious that $\text{stable}(w_{\text{id}})$ (the dependency is vacuous) and that $\text{consistent}(w_{\text{id}} \uparrow)$ (neither W_{ref} nor w_{id} relates any functions).
- $\text{inhabited}(w_{\text{id}} \uparrow)$ is witnessed by state $(\emptyset, *)$.
- Now suppose $G \in \text{GK}(w_{\text{id}} \uparrow)$ and $\delta \in \text{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s))$.
- We must show $(\gamma_1(x), \gamma_2(x)) \in \mathbf{E}_{w_{\text{id}} \uparrow}(G)(s, s)(\delta\sigma)$.
- From $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s))$ we know $(\gamma_1(x), \gamma_2(x)) \in \overline{G(s)}(\delta\sigma)$.
- We are done by Lemma 5.

□

Lemma 21.

1. If $(\tau, v_1, v_2) \in \overline{G(s)}$, then $(\tau', \tau \times \tau', \langle v_1, \bullet \rangle, \langle v_2, \bullet \rangle) \in \mathbf{K}_W(G)(s, s)$.
2. If $(\tau', e'_1, e'_2) \in \mathbf{E}_W(G)(s_0, s)$, then $(\tau, \tau \times \tau', \langle \bullet, e'_1 \rangle, \langle \bullet, e'_2 \rangle) \in \mathbf{K}_W(G)(s_0, s)$.

Proof.

1.
 - Suppose $(v'_1, v'_2) \in \overline{G(s)}(\tau')$.
 - We need to show $(\langle v_1, v'_1 \rangle, \langle v_2, v'_2 \rangle) \in \mathbf{E}_W(G)(s, s)(\tau \times \tau')$.
 - By Lemma 5 it suffices to show $(\langle v_1, v'_1 \rangle, \langle v_2, v'_2 \rangle) \in \overline{G(s)}(\tau \times \tau')$.
 - Hence it suffices to show $(v_1, v_2) \in \overline{G(s)}(\tau)$ and $(v'_1, v'_2) \in \overline{G(s)}(\tau')$, which we both already have.
2.
 - Suppose $(v_1, v_2) \in \overline{G(s)}(\tau)$.
 - We need to show $(\langle v_1, e'_1 \rangle, \langle v_2, e'_2 \rangle) \in \mathbf{E}_W(G)(s_0, s)(\tau \times \tau')$.
 - By Lemma 13 it suffices to show

$$(\langle v_1, \bullet \rangle, \langle v_2, \bullet \rangle) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau \times \tau')$$

for $s' \sqsupseteq [s_0, s]$ and $G' \geq G$.

- By Lemma 7 it suffices to show $(\langle v_1, \bullet \rangle, \langle v_2, \bullet \rangle) \in \mathbf{K}_W(G')(s', s')(\tau', \tau \times \tau')$.
- By part (1) it then suffices to show $(v_1, v_2) \in \overline{G'(s')}(\tau)$, which follows from $(v_1, v_2) \in \overline{G(s)}(\tau)$ by Lemma 1.

□

Lemma 22 (Compatibility: Pair).

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma \quad \Delta; \Gamma \vdash e'_1 \sim e'_2 : \sigma'}{\Delta; \Gamma \vdash \langle e_1, e'_1 \rangle \sim \langle e_2, e'_2 \rangle : \sigma \times \sigma'}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s)),$

$$\langle \langle \bullet, \gamma_1 e'_1 \rangle, \langle \bullet, \gamma_2 e'_2 \rangle \rangle \in \mathbf{K}_W(G)(s, s)(\delta\sigma, \delta\sigma \times \delta\sigma')$$

assuming $\Delta; \Gamma \vdash e'_1 \sim_W e'_2 : \sigma'$.

- By Lemma 21 it suffices to show $(\gamma_1 e'_1, \gamma_2 e'_2) \in \mathbf{E}_W(G)(s, s)(\delta\sigma')$, which follows from the assumption. □

Lemma 23 (Compatibility: Fst (Snd analogously)).

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma \times \sigma'}{\Delta; \Gamma \vdash e_1.1 \sim e_2.1 : \sigma}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s)),$

$$\langle \bullet.1, \bullet.1 \rangle \in \mathbf{K}_W(G)(s, s)(\delta\sigma \times \delta\sigma', \delta\sigma).$$

- Suppose $(v_1^\circ, v_2^\circ) \in \overline{G(s)}(\delta\sigma \times \delta\sigma')$.
- We need to show $(v_1^\circ.1, v_2^\circ.1) \in \mathbf{E}_W(G)(s, s)(\delta\sigma)$.
- Suppose $(h_1, h_2) \in W.H(s)(G(s))$ as well as $\text{defined}(h_1 \uplus h_1^F)$ and $\text{defined}(h_2 \uplus h_2^F)$.
- We know $v_1^\circ = \langle v_1, v_1' \rangle$ and $v_2^\circ = \langle v_2, v_2' \rangle$ with $(v_1, v_2) \in \overline{G(s)}(\delta\sigma)$.
- Hence $h_1 \uplus h_1^F, v_1^\circ.1 \leftrightarrow h_1 \uplus h_1^F, v_1$ and $h_2 \uplus h_2^F, v_2^\circ.1 \leftrightarrow h_2 \uplus h_2^F, v_2$.
- Since $s \sqsupseteq [s, s]$, we are done. □

Lemma 24 (Compatibility: Inl (Inr analogously)).

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma}{\Delta; \Gamma \vdash \text{inj}^1 e_1 \sim \text{inj}^1 e_2 : \sigma + \sigma'}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s)),$

$$(\text{inj}^1 \bullet, \text{inj}^1 \bullet) \in \mathbf{K}_W(G)(s, s)(\delta\sigma, \delta\sigma + \delta\sigma').$$

- Suppose $(v_1, v_2) \in \overline{G(s)}(\delta\sigma)$.
- We need to show $(\text{inj}^1 v_1, \text{inj}^1 v_2) \in \mathbf{E}_W(G)(s, s)(\delta\sigma + \delta\sigma')$.
- By Lemma 5 it suffices to show $(\text{inj}^1 v_1, \text{inj}^1 v_2) \in \overline{G(s)}(\delta\sigma + \delta\sigma')$.
- This follows from $(v_1, v_2) \in \overline{G(s)}(\delta\sigma)$. □

Lemma 25 (Compatibility: Case).

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma' + \sigma'' \quad \Delta; \Gamma, x:\sigma' \vdash e'_1 \sim e'_2 : \sigma \quad \Delta; \Gamma, x:\sigma'' \vdash e''_1 \sim e''_2 : \sigma}{\Delta; \Gamma \vdash \text{case } e_1 \text{ of inj}^1 x \Rightarrow e'_1 \mid \text{inj}^2 x \Rightarrow e''_1 \sim \text{case } e_2 \text{ of inj}^1 x \Rightarrow e'_2 \mid \text{inj}^2 x \Rightarrow e''_2 : \sigma}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s)),$
 $(\text{case } \bullet \text{ of inj}^1 x \Rightarrow \gamma_1 e'_1 \mid \text{inj}^2 x \Rightarrow \gamma_1 e''_1, \text{case } \bullet \text{ of inj}^1 x \Rightarrow \gamma_2 e'_2 \mid \text{inj}^2 x \Rightarrow \gamma_2 e''_2) \in \mathbf{K}_W(G)(s, s)(\delta\sigma' + \delta\sigma'', \delta\sigma).$
 assuming $\Delta; \Gamma, x:\sigma' \vdash e'_1 \sim_W e'_2 : \sigma$ and $\Delta; \Gamma, x:\sigma'' \vdash e''_1 \sim_W e''_2 : \sigma.$
- Thus it suffices to show that $\forall (v_1, v_2) \in \overline{G(s)}(\delta\sigma' + \delta\sigma''),$
 $(\text{case } v_1 \text{ of inj}^1 x \Rightarrow \gamma_1 e'_1 \mid \text{inj}^2 x \Rightarrow \gamma_1 e''_1, \text{case } v_2 \text{ of inj}^1 x \Rightarrow \gamma_2 e'_2 \mid \text{inj}^2 x \Rightarrow \gamma_2 e''_2) \in \mathbf{E}_W(G)(s, s)(\delta\sigma)$
- By definition of $\overline{G(s)}(\delta\sigma' + \delta\sigma''),$ we have v'_1, v'_2 such that either
 1. $v_1 = \text{inj}^1 v'_1 \wedge v_2 = \text{inj}^1 v'_2 \wedge (v'_1, v'_2) \in \overline{G(s)}(\delta\sigma');$ or
 2. $v_1 = \text{inj}^2 v'_1 \wedge v_2 = \text{inj}^2 v'_2 \wedge (v'_1, v'_2) \in \overline{G(s)}(\delta\sigma'').$
- We show the former case (the latter case can be done analogously).
- Let $\gamma'_1 := \gamma_1, x \mapsto v'_1$ and $\gamma'_2 := \gamma_2, x \mapsto v'_2.$
- Now suppose $(h_1, h_2) \in W.H(s)(G(s))$ and $h_1^F, h_2^F \in \text{Heap}$ with $h_1 \uplus h_1^F, h_2 \uplus h_2^F$ defined.
- We have

$$h_1 \uplus h_1^F, \text{case } v_1 \text{ of inj}^1 x \Rightarrow \gamma_1 e'_1 \mid \text{inj}^2 x \Rightarrow \gamma_1 e''_1 \hookrightarrow h_1 \uplus h_1^F, \gamma'_1 e'_1$$
 and

$$h_2 \uplus h_2^F, \text{case } v_2 \text{ of inj}^1 x \Rightarrow \gamma_2 e'_2 \mid \text{inj}^2 x \Rightarrow \gamma_2 e''_2 \hookrightarrow h_2 \uplus h_2^F, \gamma'_2 e'_2$$
- Thus by Lemma 4, it suffices to show

$$(\delta\sigma', (h_1, h_1^F, \gamma'_1 e'_1), (h_2, h_2^F, \gamma'_2 e'_2)) \in \mathbf{O}_W(\mathbf{E}_W)(G)(s, s).$$
- This follows from the assumption and $(\gamma'_1, \gamma'_2) \in \text{Env}(\delta(\Gamma, x : \sigma'), G(s)).$

□

Lemma 26 (Compatibility: Fix).

$$\frac{\Delta; \Gamma, f:\sigma' \rightarrow \sigma, x:\sigma' \vdash e_1 \sim e_2 : \sigma}{\Delta; \Gamma \vdash \text{fix } f(x). e_1 \sim \text{fix } f(x). e_2 : \sigma' \rightarrow \sigma}$$

Proof.

- For any $\mathcal{N},$ from the premise we have w such that $w.N \subseteq \mathcal{N}$ and $\Delta; \Gamma, f:\sigma' \rightarrow \sigma, x:\sigma' \vdash e_1 \sim_w e_2 : \sigma.$
- Let $w' = w_{\text{single}}(\lambda R. \{(\delta\sigma' \rightarrow \delta\sigma, \gamma_1 \text{fix } f(x). e_1, \gamma_2 \text{fix } f(x). e_2) \mid \delta \in \text{TyEnv}(\Delta), (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, R)\}, \lambda R. \{(\emptyset, \emptyset)\})$.
- Since $(w \otimes w').N = w.N \subseteq \mathcal{N},$ it suffices to show $\Delta; \Gamma \vdash \text{fix } f(x). e_1 \sim_{w \otimes w'} \text{fix } f(x). e_2 : \sigma' \rightarrow \sigma.$
- To do so, we first prove *inhabited* $((w \otimes w')\uparrow)$ and *consistent* $((w \otimes w')\uparrow):$

- $inhabited(w'\uparrow)$ is witnessed by state $(\emptyset, *)$, so $inhabited((w \otimes w')\uparrow)$ holds by Lemma 12.
- The part of $consistent((w \otimes w')\uparrow)$ concerning universal types follows from $consistent(w\uparrow)$ by Lemma 12, because $w'.L$ doesn't relate anything at universal types.
- Regarding the part concerning arrow types, we suppose
 1. $G \in \text{GK}((w \otimes w')\uparrow)$
 2. $(v_1, v_2) \in (w \otimes w')\uparrow.L(s_{\text{rf}}, s, s')(G(s_{\text{rf}}, s, s'))(\tilde{\sigma}' \rightarrow \tilde{\sigma})$
 3. $(v'_1, v'_2) \in \overline{G(s_{\text{rf}}, s, s')}(\tilde{\sigma}')$

and must show:

$$(beta(v_1 v'_1), beta(v_2 v'_2)) \in \mathbf{E}_{(w \otimes w')\uparrow}(G)((s_{\text{rf}}, s, s'), (s_{\text{rf}}, s, s'))(\tilde{\sigma})$$

- From (2) and the definition of \uparrow and \otimes we know:

$$\begin{aligned} (v_1, v_2) &\in w\uparrow.L(s_{\text{rf}}, s)(G(s_{\text{rf}}, s, s'))(\tilde{\sigma}' \rightarrow \tilde{\sigma}) \vee \\ (v_1, v_2) &\in w'.L(s_{\text{rf}})(s')(G(s_{\text{rf}}, s, s'))(\tilde{\sigma}' \rightarrow \tilde{\sigma}) \end{aligned}$$

- If the former is true, the claim follows from $consistent(w\uparrow)$ with the help of Lemmas 8 and 10.
- So suppose the latter.
- Then $\tilde{\sigma}' \rightarrow \tilde{\sigma} = \delta\sigma' \rightarrow \delta\sigma$ and $v_1 = \gamma_1 \text{fix } f(x).e_1$ and $v_2 = \gamma_2 \text{fix } f(x).e_2$ for $\delta \in \text{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_{\text{rf}}, s, s'))$.
- Let $\gamma'_1 = \gamma_1, f \mapsto \gamma_1 \text{fix } f(x).e_1, x \mapsto v'_1$ and $\gamma'_2 = \gamma_2, f \mapsto \gamma_2 \text{fix } f(x).e_2, x \mapsto v'_2$
- It remains to show $(\gamma'_1 e_1, \gamma'_2 e_2) \in \mathbf{E}_{(w \otimes w')\uparrow}(G)((s_{\text{rf}}, s, s'), (s_{\text{rf}}, s, s'))(\delta\sigma)$.
- By Lemmas 8 and 10 it suffices to show $(\gamma'_1 e_1, \gamma'_2 e_2) \in \mathbf{E}_{w\uparrow}(G(-, -, s'))((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\delta\sigma)$.
- This follows from the premise if we can show $(\gamma'_1, \gamma'_2) \in \text{Env}((\delta\Gamma, f:\delta\sigma' \rightarrow \delta\sigma, x:\delta\sigma'), G(s_{\text{rf}}, s, s'))$.
- This reduces to showing $(v'_1, v'_2) \in \overline{G(s_{\text{rf}}, s, s')}(\delta\sigma')$ and

$$(\gamma_1 \text{fix } f(x).e_1, \gamma_2 \text{fix } f(x).e_2) \in \overline{G(s_{\text{rf}}, s, s')}(\delta\sigma' \rightarrow \delta\sigma).$$

- The former is given as (3).
- For the latter, note that by definition of GK it suffices to show

$$(\gamma_1 \text{fix } f(x).e_1, \gamma_2 \text{fix } f(x).e_2) \in (w \otimes w')\uparrow.L(s_{\text{rf}}, s, s')(G(s_{\text{rf}}, s, s'))(\delta\sigma' \rightarrow \delta\sigma).$$

- By definition of \uparrow and \otimes it then suffices to show

$$(\gamma_1 \text{fix } f(x).e_1, \gamma_2 \text{fix } f(x).e_2) \in w'.L(s_{\text{rf}})(s')(G(s_{\text{rf}}, s, s'))(\delta\sigma' \rightarrow \delta\sigma).$$

- Since $\delta \in \text{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_{\text{rf}}, s, s'))$, this holds by construction.

- Now suppose $G \in \text{GK}((w \otimes w')\uparrow)$ and $\delta \in \text{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_{\text{rf}}, s, s'))$.
- We must show $(\gamma_1 \text{fix } f(x).e_1, \gamma_2 \text{fix } f(x).e_2) \in \mathbf{E}_{(w \otimes w')\uparrow}(G)((s_{\text{rf}}, s, s'), (s_{\text{rf}}, s, s'))(\delta\sigma' \rightarrow \delta\sigma)$.
- By Lemma 5 it suffices to show $(\gamma_1 \text{fix } f(x).e_1, \gamma_2 \text{fix } f(x).e_2) \in G(s_{\text{rf}}, s, s')(\delta\sigma' \rightarrow \delta\sigma)$.
- By definition of GK it suffices to show:

$$(\gamma_1 \text{fix } f(x).e_1, \gamma_2 \text{fix } f(x).e_2) \in (w \otimes w')\uparrow.L(s_{\text{rf}}, s, s')(G(s_{\text{rf}}, s, s'))(\delta\sigma' \rightarrow \delta\sigma)$$

- By definition of \uparrow and \otimes it suffices to show $(\gamma_1 \text{fix } f(x).e_1, \gamma_2 \text{fix } f(x).e_2) \in w'.L(s_{\text{rf}})(s')(G(s_{\text{rf}}, s, s'))(\delta\sigma' \rightarrow \delta\sigma)$.

- Since $\delta \in \text{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_{\text{rf}}, s, s'))$, this holds by construction of w' .

□

Lemma 27.

1. If $(\tau' \rightarrow \tau, v_1, v_2) \in \overline{G(s)}$, then $(\tau', \tau, v_1 \bullet, v_2 \bullet) \in \mathbf{K}_W(G)(s, s)$.
2. If $(\tau', e'_1, e'_2) \in \mathbf{E}_W(G)(s_0, s)$, then $(\tau' \rightarrow \tau, \tau, \bullet e'_1, \bullet e'_2) \in \mathbf{K}_W(G)(s_0, s)$.

Proof.

1.
 - Suppose $(v'_1, v'_2) \in \overline{G(s)}(\tau')$.
 - We need to show $(v_1 v'_1, v_2 v'_2) \in \mathbf{E}_W(G)(s, s)(\tau)$.
 - By definition of \mathbf{E}_W it suffices to show the following:
 - (a) $(v_1, v_2) \in \overline{G(s)}(\tau' \rightarrow \tau)$
 - (b) $(v'_1, v'_2) \in \overline{G(s)}(\tau')$
 - (c) $\forall s' \sqsupseteq_{\text{pub}} s. \forall G' \geq G. (\bullet, \bullet) \in \mathbf{K}_W(G')(s, s')(\tau, \tau)$
 - (a) and (b) are already given.
 - (c) follows by Lemmas 6 and 7.
2.
 - Suppose $(v_1, v_2) \in \overline{G(s)}(\tau' \rightarrow \tau)$.
 - We need to show $(v_1 e'_1, v_2 e'_2) \in \mathbf{E}_W(G)(s_0, s)(\tau)$.
 - By Lemma 13 it suffices to show

$$(v_1 \bullet, v_2 \bullet) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau)$$

for $s' \sqsupseteq [s_0, s]$ and $G' \geq G$.

- By Lemma 7 it suffices to show $(v_1 \bullet, v_2 \bullet) \in \mathbf{K}_W(G')(s', s')(\tau', \tau)$.
- By part (1) it then suffices to show $(v_1, v_2) \in \overline{G'(s')}(\tau' \rightarrow \tau)$.
- This follows from $(v_1, v_2) \in \overline{G(s)}(\tau' \rightarrow \tau)$ by Lemma 1.

□

Lemma 28 (Compatibility: App).

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma' \rightarrow \sigma \quad \Delta; \Gamma \vdash e'_1 \sim e'_2 : \sigma'}{\Delta; \Gamma \vdash e_1 e'_1 \sim e_2 e'_2 : \sigma}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s))$,

$$(\bullet \gamma_1 e'_1, \bullet \gamma_2 e'_2) \in \mathbf{K}_W(G)(s, s)(\delta\sigma' \rightarrow \delta\sigma, \delta\sigma)$$

assuming $\Delta; \Gamma \vdash e'_1 \sim_W e'_2 : \sigma'$.

- By Lemma 27 it suffices to show $(\gamma_1 e'_1, \gamma_2 e'_2) \in \mathbf{E}_W(G)(s, s)(\delta\sigma')$, which follows from the assumption.

□

Lemma 29 (Compatibility: Roll).

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma[\mu\alpha. \sigma/\alpha]}{\Delta; \Gamma \vdash \text{roll } e_1 \sim \text{roll } e_2 : \mu\alpha. \sigma}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s)),$
 $(\text{roll } \bullet, \text{roll } \bullet) \in \mathbf{K}_W(G)(s, s)(\delta\sigma[\mu\alpha. \delta\sigma/\alpha], \mu\alpha. \delta\sigma) .$
- Suppose $(v_1, v_2) \in \overline{G(s)}(\delta\sigma[\mu\alpha. \delta\sigma/\alpha]).$
- We need to show $(\text{roll } v_1, \text{roll } v_2) \in \mathbf{E}_W(G)(s, s)(\mu\alpha. \delta\sigma).$
- By Lemma 5 it suffices to show $(\text{roll } v_1, \text{roll } v_2) \in \overline{G(s)}(\mu\alpha. \delta\sigma).$
- This follows from $(v_1, v_2) \in \overline{G(s)}(\delta\sigma[\mu\alpha. \delta\sigma/\alpha]).$

□

Lemma 30 (Compatibility: Unroll).

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \mu\alpha. \sigma}{\Delta; \Gamma \vdash \text{unroll } e_1 \sim \text{unroll } e_2 : \sigma[\mu\alpha. \sigma/\alpha]}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s)),$
 $(\text{unroll } \bullet, \text{unroll } \bullet) \in \mathbf{K}_W(G)(s, s)(\mu\alpha. \delta\sigma, \delta\sigma[\mu\alpha. \delta\sigma/\alpha]) .$
- Suppose $(v_1^\circ, v_2^\circ) \in \overline{G(s)}(\mu\alpha. \delta\sigma).$
- We need to show $(\text{unroll } v_1^\circ, \text{unroll } v_2^\circ) \in \mathbf{E}_W(G)(s, s)(\delta\sigma[\mu\alpha. \delta\sigma/\alpha]).$
- Suppose $(h_1, h_2) \in W.H(s)(G(s))$ as well as $\text{defined}(h_1 \uplus h_1^F)$ and $\text{defined}(h_2 \uplus h_2^F).$
- We know $v_1^\circ = \text{roll } v_1$ and $v_2^\circ = \text{roll } v_2$ with $(v_1, v_2) \in \overline{G(s)}(\delta\sigma[\mu\alpha. \delta\sigma/\alpha]).$
- Hence $h_1 \uplus h_1^F, \text{unroll } v_1^\circ \hookrightarrow h_1 \uplus h_1^F, v_1$ and $h_2 \uplus h_2^F, \text{unroll } v_2^\circ \hookrightarrow h_2 \uplus h_2^F, v_2.$
- Since $s \sqsupseteq [s, s],$ we are done.

□

Lemma 31 (Compatibility: Ref).

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma}{\Delta; \Gamma \vdash \text{ref } e_1 \sim \text{ref } e_2 : \text{ref } \sigma}$$

Proof.

- By Lemmas 15 and 17, it suffices to show $\forall G, s_{\text{rf}}, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s)),$
 $(\text{ref } \bullet, \text{ref } \bullet) \in \mathbf{K}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\delta\sigma, \text{ref } \delta\sigma) .$
- Suppose $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s)}(\delta\sigma).$
- We need to show $(\text{ref } v_1, \text{ref } v_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\text{ref } \delta\sigma).$
- Suppose $(h_1, h_2) \in w\uparrow.H(s_{\text{rf}}, s)(G(s_{\text{rf}}, s))$ as well as $\text{defined}(h_1 \uplus h_1^F)$ and $\text{defined}(h_2 \uplus h_2^F).$
- We know $h_1 \uplus h_1^F, \text{ref } v_1 \hookrightarrow h_1 \uplus [l_1 \mapsto v_1] \uplus h_1^F, l_1$ for $l_1 \notin \text{dom}(h_1 \uplus h_1^F).$
- Similarly, $h_2 \uplus h_2^F, \text{ref } v_2 \hookrightarrow h_2 \uplus [l_2 \mapsto v_2] \uplus h_2^F, l_2$ for $l_2 \notin \text{dom}(h_2 \uplus h_2^F).$

- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $(\widetilde{s}_{\text{rf}}, \widetilde{s}) \sqsupseteq [(s_{\text{rf}}, s), (s_{\text{rf}}, s)]$ such that:
 1. $(h_1 \uplus [\ell_1 \mapsto v_1], h_2 \uplus [\ell_2 \mapsto v_2]) \in w\uparrow.\mathbf{H}(\widetilde{s}_{\text{rf}}, \widetilde{s})(G(\widetilde{s}_{\text{rf}}, \widetilde{s}))$
 2. $(\ell_1, \ell_2) \in \overline{G(\widetilde{s}_{\text{rf}}, \widetilde{s})}(\text{ref } \delta\sigma)$
- From $(h_1, h_2) \in w\uparrow.\mathbf{H}(s_{\text{rf}}, s)(G(s_{\text{rf}}, s))$ we know $h_i = h'_i \uplus h''_i$ for some h'_1, h''_1, h'_2, h''_2 with $(h'_1, h'_2) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}})(G(s_{\text{rf}}, s))$ and $(h''_1, h''_2) \in w.\mathbf{H}(s_{\text{rf}})(s)(G(s_{\text{rf}}, s))$.
- Since $\ell_1 \notin \text{dom}(h'_1)$ and $\ell_2 \notin \text{dom}(h'_2)$, we therefore know that $s_{\text{rf}} \uplus \{(\delta\sigma, \ell_1, \ell_2)\}$ is well-defined and that $s_{\text{rf}} \uplus \{(\delta\sigma, \ell_1, \ell_2)\} \in W_{\text{ref}}.\mathbf{S}$.
- We choose $\widetilde{s}_{\text{rf}} = s_{\text{rf}} \uplus \{(\delta\sigma, \ell_1, \ell_2)\}$.
- Note that $\widetilde{s}_{\text{rf}} \sqsupseteq_{\text{pub}} s_{\text{rf}}$ and that $(h'_1 \uplus [\ell_1 \mapsto v_1], h'_2 \uplus [\ell_2 \mapsto v_2]) \in W_{\text{ref}}.\mathbf{H}(\widetilde{s}_{\text{rf}})(G(s_{\text{rf}}, s))$.
- By dependent monotonicity we also get $\widetilde{s} \sqsupseteq_{\text{pub}} s$ such that $(h''_1, h''_2) \in w.\mathbf{H}(\widetilde{s}_{\text{rf}})(\widetilde{s})(G(s_{\text{rf}}, s))$.
- Together this yields $(h_1 \uplus [\ell_1 \mapsto v_1], h_2 \uplus [\ell_2 \mapsto v_2]) \in w\uparrow.\mathbf{H}(\widetilde{s}_{\text{rf}}, \widetilde{s})(G(s_{\text{rf}}, s))$ and then (1) by monotonicity.
- To show (2) it suffices, by definition of GK, to show $(\ell_1, \ell_2) \in w\uparrow.\mathbf{L}(\widetilde{s}_{\text{rf}}, \widetilde{s})(G(\widetilde{s}_{\text{rf}}, \widetilde{s}))(\text{ref } \delta\sigma)$.
- By definition of \uparrow and W_{ref} , this in turn reduces to showing $(\delta\sigma, \ell_1, \ell_2) \in \widetilde{s}_{\text{rf}}$, which holds by construction.

□

Lemma 32 (Compatibility: Deref).

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \text{ref } \sigma}{\Delta; \Gamma \vdash !e_1 \sim !e_2 : \sigma}$$

Proof.

- By Lemmas 15 and 17, it suffices to show $\forall G, s_{\text{rf}}, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s)),$

$$(!\bullet, !\bullet) \in \mathbf{K}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\text{ref } \delta\sigma, \delta\sigma) .$$

- Suppose $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s)}(\text{ref } \delta\sigma)$.
- We need to show $(!v_1, !v_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\delta\sigma)$.
- Suppose $(h_1, h_2) \in w\uparrow.\mathbf{H}(s_{\text{rf}}, s)(G(s_{\text{rf}}, s))$ as well as defined $(h_1 \uplus h_1^{\text{F}})$ and defined $(h_2 \uplus h_2^{\text{F}})$.
- From $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s)}(\text{ref } \delta\sigma)$ we know by definition of GK and W_{ref} that $(\delta\sigma, v_1, v_2) \in s_{\text{rf}}$.
- From $(h_1, h_2) \in w\uparrow.\mathbf{H}(s_{\text{rf}}, s)(G(s_{\text{rf}}, s))$ we know $(h'_1, h'_2) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}})(G(s_{\text{rf}}, s))$ for some $h'_1 \subseteq h_1$ and $h'_2 \subseteq h_2$.
- From the definition of W_{ref} we thus get $(h'_1(v_1), h'_2(v_2)) \in \overline{G(s_{\text{rf}}, s)}(\delta\sigma)$.
- Hence we know $h_1 \uplus h_1^{\text{F}}, !v_1 \leftrightarrow h_1 \uplus h_1^{\text{F}}, h'_1(v_1)$ and $h_2 \uplus h_2^{\text{F}}, !v_2 \leftrightarrow h_2 \uplus h_2^{\text{F}}, h'_2(v_2)$.
- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $(\widetilde{s}_{\text{rf}}, \widetilde{s}) \sqsupseteq_{\text{pub}} (s_{\text{rf}}, s)$ such that:
 1. $(h_1, h_2) \in w\uparrow.\mathbf{H}(\widetilde{s}_{\text{rf}}, \widetilde{s})(G(\widetilde{s}_{\text{rf}}, \widetilde{s}))$
 2. $(h'_1(v_1), h'_2(v_2)) \in \overline{G(\widetilde{s}_{\text{rf}}, \widetilde{s})}(\delta\sigma)$
- We choose $(\widetilde{s}_{\text{rf}}, \widetilde{s}) = (s_{\text{rf}}, s)$ and are done.

□

Lemma 33.

1. If $(\text{ref } \tau, v_1, v_2) \in \overline{G(s_{\text{rf}}, s)}$,
then $(\tau, \text{unit}, v_1 := \bullet, v_2 := \bullet) \in \mathbf{K}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))$.
2. If $(\tau, e'_1, e'_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))$,
then $(\text{ref } \tau, \text{unit}, \bullet := e'_1, \bullet := e'_2) \in \mathbf{K}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))$.

Proof.

1.
 - Suppose $(v'_1, v'_2) \in \overline{G(s_{\text{rf}}, s)}(\tau)$.
 - We need to show $(v_1 := v'_1, v_2 := v'_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\text{unit})$.
 - Suppose $(h_1, h_2) \in w\uparrow.\mathbf{H}(s_{\text{rf}}, s)(G(s_{\text{rf}}, s))$ as well as defined $(h_1 \uplus h_1^{\text{F}})$ and defined $(h_2 \uplus h_2^{\text{F}})$.
 - From $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s)}(\text{ref } \tau)$ we know by definition of GK and W_{ref} that $(\tau, v_1, v_2) \in s_{\text{rf}}$.
 - From $(h_1, h_2) \in w\uparrow.\mathbf{H}(s_{\text{rf}}, s)(G(s_{\text{rf}}, s))$ we know $h_i = h'_i \uplus h''_i$ for some h'_1, h''_1, h'_2, h''_2 with $(h'_1, h'_2) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}})(G(s_{\text{rf}}, s))$ and $(h''_1, h''_2) \in w.\mathbf{H}(s_{\text{rf}})(s)(G(s_{\text{rf}}, s))$.
 - From the definition of W_{ref} we thus get $v_1 \in \text{dom}(h'_1)$ and $v_2 \in \text{dom}(h'_2)$.
 - Hence $h_1 \uplus h_1^{\text{F}}, v_1 := v'_1 \hookrightarrow h_1[v_1 \mapsto v'_1] \uplus h_1^{\text{F}}, \langle \rangle$ and $h_2 \uplus h_2^{\text{F}}, v_2 := v'_2 \hookrightarrow h_2[v_2 \mapsto v'_2] \uplus h_2^{\text{F}}, \langle \rangle$.
 - By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $(\widetilde{s}_{\text{rf}}, \widetilde{s}) \sqsupseteq_{\text{pub}} (s_{\text{rf}}, s)$ such that:
 - (a) $(h_1[v_1 \mapsto v'_1], h_2[v_2 \mapsto v'_2]) \in w\uparrow.\mathbf{H}(\widetilde{s}_{\text{rf}}, \widetilde{s})(G(\widetilde{s}_{\text{rf}}, \widetilde{s}))$
 - (b) $(\langle \rangle, \langle \rangle) \in \overline{G(\widetilde{s}_{\text{rf}}, \widetilde{s})}(\text{unit})$
 - We choose $(\widetilde{s}_{\text{rf}}, \widetilde{s}) = (s_{\text{rf}}, s)$.
 - Note that (b) is immediate.
 - Showing (a) reduces to showing $(v'_1, v'_2) \in \overline{G(\widetilde{s}_{\text{rf}}, \widetilde{s})}(\tau)$, which is given.
2.
 - Suppose $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s)}(\text{ref } \tau)$.
 - We need to show $(v_1 := e'_1, v_2 := e'_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\text{unit})$.
 - By Lemma 13 it suffices to show

$$(v_1 := \bullet, v_2 := \bullet) \in \mathbf{K}_{w\uparrow}(G')((s_{\text{rf}}, s), (\widetilde{s}_{\text{rf}}, \widetilde{s}))(\tau, \text{unit})$$

for $(\widetilde{s}_{\text{rf}}, \widetilde{s}) \sqsupseteq_{\text{pub}} (s_{\text{rf}}, s)$ and $G' \geq G$.

- By Lemma 7 it suffices to show $(v_1 := \bullet, v_2 := \bullet) \in \mathbf{K}_{w\uparrow}(G')((\widetilde{s}_{\text{rf}}, \widetilde{s}), (\widetilde{s}_{\text{rf}}, \widetilde{s}))(\tau, \text{unit})$.
- By part (1) it then suffices to show $(v_1, v_2) \in \overline{G'(\widetilde{s}_{\text{rf}}, \widetilde{s})}(\text{ref } \tau)$.
- This follows from $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s)}(\text{ref } \tau)$ by Lemma 1.

□

Lemma 34 (Compatibility: Assign).

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \text{ref } \sigma \quad \Delta; \Gamma \vdash e'_1 \sim e'_2 : \sigma}{\Delta; \Gamma \vdash e_1 := e'_1 \sim e_2 := e'_2 : \text{unit}}$$

Proof.

- By Lemmas 15 and 17, it suffices to show $\forall G, s_{\text{rf}}, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s))$,

$$(\text{ref } \delta\sigma, \text{unit}, \bullet := \gamma_1 e'_1, \bullet := \gamma_2 e'_2) \in \mathbf{K}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))$$

assuming $\Delta; \Gamma \vdash e'_1 \sim_{w\uparrow} e'_2 : \sigma$.

- By Lemma 33 it suffices to show $(\gamma_1 e'_1, \gamma_2 e'_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\delta\sigma)$, which follows from the assumption.

□

Lemma 35.

1. If $(\text{ref } \tau, v_1, v_2) \in \overline{G(s_{\text{rf}}, s)}$,
then $(\text{ref } \tau, \text{bool}, v_1 == \bullet, v_2 == \bullet) \in \mathbf{K}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))$.
2. If $(\text{ref } \tau, e'_1, e'_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))$,
then $(\text{ref } \tau, \text{bool}, \bullet == e'_1, \bullet == e'_2) \in \mathbf{K}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))$.

Proof.

1.
 - Suppose $(v'_1, v'_2) \in \overline{G(s_{\text{rf}}, s)}(\text{ref } \tau)$.
 - We need to show $(v_1 == v'_1, v_2 == v'_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\text{bool})$.
 - Suppose $(h_1, h_2) \in w\uparrow.\mathbf{H}(s_{\text{rf}}, s)(G(s_{\text{rf}}, s))$ as well as defined $(h_1 \uplus h_1^{\text{F}})$ and defined $(h_2 \uplus h_2^{\text{F}})$.
 - From $(v'_1, v'_2) \in \overline{G(s_{\text{rf}}, s)}(\text{ref } \tau)$ we know by definition of GK and W_{ref} that $(\text{ref } \tau, v'_1, v'_2) \in s_{\text{rf}}$.
 - From $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s)}(\text{ref } \tau)$ we know by definition of GK and W_{ref} that $(\text{ref } \tau, v_1, v_2) \in s_{\text{rf}}$.
 - By definition of $W_{\text{ref.S}}$ this yields $v_1 = v'_1 \iff v_2 = v'_2$.
 - Hence either $h_1 \uplus h_1^{\text{F}}, v_1 == v'_1 \hookrightarrow h_1 \uplus h_1^{\text{F}}, \text{tt}$ and $h_2 \uplus h_2^{\text{F}}, v_2 == v'_2 \hookrightarrow h_2 \uplus h_2^{\text{F}}, \text{tt}$ or $h_1 \uplus h_1^{\text{F}}, v_1 == v'_1 \hookrightarrow h_1 \uplus h_1^{\text{F}}, \text{ff}$ and $h_2 \uplus h_2^{\text{F}}, v_2 == v'_2 \hookrightarrow h_2 \uplus h_2^{\text{F}}, \text{ff}$.
 - By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $(\widetilde{s}_{\text{rf}}, \widetilde{s}) \sqsupseteq_{\text{pub}}(s_{\text{rf}}, s)$ such that:
 - (a) $(h_1, h_2) \in w\uparrow.\mathbf{H}(\widetilde{s}_{\text{rf}}, \widetilde{s})(G(\widetilde{s}_{\text{rf}}, \widetilde{s}))$
 - (b) $(\text{tt}, \text{tt}) \in \overline{G(\widetilde{s}_{\text{rf}}, \widetilde{s})}(\text{bool})$
 - (c) $(\text{ff}, \text{ff}) \in \overline{G(\widetilde{s}_{\text{rf}}, \widetilde{s})}(\text{bool})$
 - We choose $(\widetilde{s}_{\text{rf}}, \widetilde{s}) = (s_{\text{rf}}, s)$, and are done.
2.
 - Suppose $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s)}(\text{ref } \tau)$.
 - We need to show $(v_1 == e'_1, v_2 == e'_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\text{bool})$.
 - By Lemma 13 it suffices to show

$$(v_1 == \bullet, v_2 == \bullet) \in \mathbf{K}_{w\uparrow}(G')((s_{\text{rf}}, s), (\widetilde{s}_{\text{rf}}, \widetilde{s}))(\text{ref } \tau, \text{bool})$$

for $(\widetilde{s}_{\text{rf}}, \widetilde{s}) \sqsupseteq_{\text{pub}}(s_{\text{rf}}, s)$ and $G' \geq G$.

- By Lemma 7 it suffices to show $(v_1 == \bullet, v_2 == \bullet) \in \mathbf{K}_{w\uparrow}(G')((\widetilde{s}_{\text{rf}}, \widetilde{s}), (\widetilde{s}_{\text{rf}}, \widetilde{s}))(\text{ref } \tau, \text{bool})$.
- By part (1) it then suffices to show $(v_1, v_2) \in \overline{G'(\widetilde{s}_{\text{rf}}, \widetilde{s})}(\text{ref } \tau)$.
- This follows from $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s)}(\text{ref } \tau)$ by Lemma 1.

□

Lemma 36 (Compatibility: Refeq).

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \text{ref } \sigma \quad \Delta; \Gamma \vdash e'_1 \sim e'_2 : \text{ref } \sigma}{\Delta; \Gamma \vdash e_1 == e'_1 \sim e_2 == e'_2 : \text{bool}}$$

Proof.

- By Lemmas 15 and 17, it suffices to show $\forall G, s_{\text{rf}}, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s)),$

$$(\text{ref } \delta\sigma, \text{bool}, \bullet == \gamma_1 e'_1, \bullet == \gamma_2 e'_2) \in \mathbf{K}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))$$

assuming $\Delta; \Gamma \vdash e'_1 \sim_{w\uparrow} e'_2 : \text{ref } \sigma.$

- By Lemma 35 it suffices to show $(\gamma_1 e'_1, \gamma_2 e'_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\text{ref } \delta\sigma),$ which follows from the assumption.

□

Lemma 37 (Compatibility: Gen).

$$\frac{\Delta, \alpha; \Gamma \vdash e_1 \sim e_2 : \sigma}{\Delta; \Gamma \vdash \Lambda. e_1 \sim \Lambda. e_2 : \forall \alpha. \sigma}$$

Proof.

- For any \mathcal{N} , from the premise we have w such that $w.\mathbf{N} \subseteq \mathcal{N}$ and $\Delta, \alpha; \Gamma \vdash e_1 \sim_w e_2 : \sigma.$
- Let $w' = w_{\text{single}}(\lambda R. \{(\forall \alpha. \delta\sigma, \Lambda. \gamma_1 e_1, \Lambda. \gamma_2 e_2) \mid \delta \in \text{TyEnv}(\Delta), (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, R)\}, \lambda R. \{(\emptyset, \emptyset)\}).$
- Since $(w \otimes w').\mathbf{N} = w.\mathbf{N} \subseteq \mathcal{N}$, it suffices to show $\Delta; \Gamma \vdash \Lambda. e_1 \sim_{w \otimes w'} \Lambda. e_2 : \forall \alpha. \sigma.$
- To do so, we first prove *inhabited* $((w \otimes w')\uparrow)$ and *consistent* $((w \otimes w')\uparrow)$:
 - *inhabited* $(w'\uparrow)$ is witnessed by state $(\emptyset, *)$, so *inhabited* $((w \otimes w')\uparrow)$ holds by Lemma 12.
 - The part of *consistent* $((w \otimes w')\uparrow)$ concerning arrow types follows from *consistent* $(w\uparrow)$ by Lemma 12, because $w'.\mathbf{L}$ doesn't relate anything at arrow types.
 - Regarding the part concerning universal types, we suppose
 1. $G \in \text{GK}((w \otimes w')\uparrow)$
 2. $(v_1, v_2) \in (w \otimes w')\uparrow.\mathbf{L}(s_{\text{rf}}, s, s')(G(s_{\text{rf}}, s, s'))(\forall \alpha. \tilde{\sigma})$
and must show:

$$\forall \tau \in \text{CType}. (\text{beta}(v_1[]), \text{beta}(v_2[])) \in \mathbf{E}_{(w \otimes w')\uparrow}(G)((s_{\text{rf}}, s, s'), (s_{\text{rf}}, s, s'))(\tilde{\sigma}[\tau/\alpha])$$

- From (2) and the definition of \uparrow and \otimes we know:

$$(v_1, v_2) \in w\uparrow.\mathbf{L}(s_{\text{rf}}, s)(G(s_{\text{rf}}, s, s'))(\forall \alpha. \tilde{\sigma}) \vee (v_1, v_2) \in w'\uparrow.\mathbf{L}(s_{\text{rf}})(s')(G(s_{\text{rf}}, s, s'))(\forall \alpha. \tilde{\sigma})$$

- If the former is true, the claims follow from *consistent* $(w\uparrow)$ with the help of Lemmas 8 and 10.
- So suppose the latter.
- Then $\forall \alpha. \tilde{\sigma} = \forall \alpha. \delta\sigma$ and $v_1 = \Lambda. \gamma_1 e_1$ and $v_2 = \Lambda. \gamma_2 e_2$ for $\delta \in \text{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_{\text{rf}}, s, s'))).$
- Let $\delta' := \delta, \alpha \mapsto \tau.$
- It remains to show $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{(w \otimes w')\uparrow}(G)((s_{\text{rf}}, s, s'), (s_{\text{rf}}, s, s'))(\delta'\sigma)$ since $\tilde{\sigma}[\tau/\alpha] = \delta\sigma[\tau/\alpha] = \delta'\sigma.$
- By Lemmas 8 and 10 it suffices to show $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{w\uparrow}(G(-, -, s'))((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\delta'\sigma).$
- This follows from the premise since $\delta' \in \text{TyEnv}(\Delta, \alpha)$ and $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_{\text{rf}}, s, s')) = \text{Env}(\delta'\Gamma, G(s_{\text{rf}}, s, s')).$
- Now suppose $G \in \text{GK}((w \otimes w')\uparrow)$ and $\delta \in \text{TyEnv}(\Delta), (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_{\text{rf}}, s, s')).$

- We must show $(\Lambda. \gamma_1 e_1, \Lambda. \gamma_2 e_2) \in \mathbf{E}_{(w \otimes w') \uparrow}(G)((s_{\text{rf}}, s, s'), (s_{\text{rf}}, s, s'))(\forall \alpha. \delta \sigma)$.
- By Lemma 5 it suffices to show $(\Lambda. \gamma_1 e_1, \Lambda. \gamma_2 e_2) \in G(s_{\text{rf}}, s, s')(\forall \alpha. \delta \sigma)$.
- By definition of GK it suffices to show:

$$(\Lambda. \gamma_1 e_1, \Lambda. \gamma_2 e_2) \in (w \otimes w') \uparrow . \mathbf{L}(s_{\text{rf}}, s, s')(G(s_{\text{rf}}, s, s'))(\forall \alpha. \delta \sigma)$$

- By definition of \uparrow and \otimes it suffices to show $(\Lambda. \gamma_1 e_1, \Lambda. \gamma_2 e_2) \in w' . \mathbf{L}(s')(G(s_{\text{rf}}, s, s'))(\forall \alpha. \delta \sigma)$.
- Since $\delta \in \text{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \text{Env}(\delta \Gamma, G(s_{\text{rf}}, s, s'))$, this holds by construction of w' .

□

Lemma 38 (Compatibility: Inst).

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \forall \alpha. \sigma \quad \Delta \vdash \sigma'}{\Delta; \Gamma \vdash e_1 \square \sim e_2 \square : \sigma[\sigma'/\alpha]}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta \Gamma, G(s))$,

$$(\bullet \square, \bullet \square) \in \mathbf{K}_W(G)(s, s)(\forall \alpha. \delta \sigma, \delta \sigma[\delta \sigma'/\alpha]) .$$

- Suppose $(v_1^\circ, v_2^\circ) \in \overline{G(s)}(\forall \alpha. \delta \sigma)$.
- We need to show $(v_1^\circ \square, v_2^\circ \square) \in \mathbf{E}_W(G)(s, s)(\delta \sigma[\delta \sigma'/\alpha])$.
- Since $(v_1^\circ, v_2^\circ) \in \overline{G(s)}(\forall \alpha. \delta \sigma)$, by definition of \mathbf{E}_W , it suffices to show

$$\forall s' \sqsupseteq_{\text{pub}} s. \forall G' \geq G. (\bullet, \bullet) \in \mathbf{K}_W(G')(s, s')(\delta \sigma[\delta \sigma'/\alpha], \delta \sigma[\delta \sigma'/\alpha])$$

which holds by Lemma 6.

□

Lemma 39 (Compatibility: Pack).

$$\frac{\Delta \vdash \sigma' \quad \Delta; \Gamma \vdash e_1 \sim e_2 : \sigma[\sigma'/\alpha]}{\Delta; \Gamma \vdash \text{pack } e_1 \sim \text{pack } e_2 : \exists \alpha. \sigma}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta \Gamma, G(s))$,

$$(\text{pack } \bullet, \text{pack } \bullet) \in \mathbf{K}_W(G)(s, s)(\delta \sigma[\delta \sigma'/\alpha], \exists \alpha. \delta \sigma) .$$

- Suppose $(v_1, v_2) \in \overline{G(s)}(\delta \sigma[\delta \sigma'/\alpha])$.
- We need to show $(\text{pack } v_1, \text{pack } v_2) \in \mathbf{E}_W(G)(s, s)(\exists \alpha. \delta \sigma)$.
- By Lemma 5 it suffices to show $(\text{pack } v_1, \text{pack } v_2) \in \overline{G(s)}(\exists \alpha. \delta \sigma)$.
- This follows from $(v_1, v_2) \in \overline{G(s)}(\delta \sigma[\delta \sigma'/\alpha])$.

□

Lemma 40 (Compatibility: Unpack).

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \exists \alpha. \sigma \quad \Delta, \alpha; \Gamma, x : \sigma \vdash e'_1 \sim e'_2 : \sigma' \quad \Delta \vdash \sigma'}{\Delta; \Gamma \vdash \text{unpack } e_1 \text{ as } x \text{ in } e'_1 \sim \text{unpack } e_2 \text{ as } x \text{ in } e'_2 : \sigma'}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s)),$

$$(\exists \alpha. \delta\sigma, \delta\sigma', \text{unpack } \bullet \text{ as } x \text{ in } \gamma_1 e'_1, \text{unpack } \bullet \text{ as } x \text{ in } \gamma_2 e'_2) \in \mathbf{K}_W(G)(s, s)$$

assuming $\Delta, \alpha; \Gamma, x : \sigma \vdash e'_1 \sim_W e'_2 : \sigma'.$

- Thus it suffices to show that $\forall (v_1, v_2) \in \overline{G(s)}(\exists \alpha. \delta\sigma),$

$$(\delta\sigma', \text{unpack } v_1 \text{ as } x \text{ in } \gamma_1 e'_1, \text{unpack } v_2 \text{ as } x \text{ in } \gamma_2 e'_2) \in \mathbf{E}_W(G)(s, s)$$

- By definition of $\overline{G(s)}(\exists \alpha. \delta\sigma),$ we have v'_1, v'_2 and $\tau \in \text{CType}$ such that

$$v_1 = \text{pack } v'_1 \wedge v_2 = \text{pack } v'_2 \wedge (v'_1, v'_2) \in \overline{G(s)}(\delta\sigma[\tau/\alpha])$$

- Let $\delta' := \delta, \alpha \mapsto \tau$ and $\gamma'_1 := \gamma_1, x \mapsto v'_1$ and $\gamma'_2 := \gamma_2, x \mapsto v'_2.$

- Now suppose $(h_1, h_2) \in W.H(s)(G(s))$ and $h_1^F, h_2^F \in \text{Heap}$ with $h_1 \uplus h_1^F, h_2 \uplus h_2^F$ defined.

- We have $h_1 \uplus h_1^F, \text{unpack } v_1 \text{ as } x \text{ in } \gamma_1 e'_1 \hookrightarrow h_1 \uplus h_1^F, \gamma'_1 e'_1$ and $h_2 \uplus h_2^F, \text{unpack } v_2 \text{ as } x \text{ in } \gamma_2 e'_2 \hookrightarrow h_2 \uplus h_2^F, \gamma'_2 e'_2$ and thus by Lemma 4, it suffices to show

$$(\delta\sigma', (h_1, h_1^F, \gamma'_1 e'_1), (h_2, h_2^F, \gamma'_2 e'_2)) \in \mathbf{O}_W(\mathbf{E}_W)(G)(s, s) .$$

- This follows from the assumption and $\delta\sigma' = \delta'\sigma', \delta' \in \text{TyEnv}(\Delta, \alpha), (\gamma'_1, \gamma'_2) \in \text{Env}(\delta'(\Gamma, x : \tau), G(s)).$

□

2.4 Soundness

Theorem 41 (Fundamental Property). If $\Delta; \Gamma \vdash p : \sigma$, then $\Delta; \Gamma \vdash |p| \sim |p| : \sigma$.

Proof. By induction on the typing derivation, in each case using the appropriate compatibility lemma. \square

Lemma 42 (Weakening). If $\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma$ and $\Delta \subseteq \Delta' \wedge \Gamma \subseteq \Gamma'$, then $\Delta'; \Gamma' \vdash e_1 \sim e_2 : \sigma$.

Proof. One can easily see that the goal is a direct consequence of the definition from the following observation:

$$\begin{aligned} &\text{for } i = 1, 2, \forall R. \forall \delta \in \text{TyEnv}(\Delta'). \forall \gamma_i \in \text{Env}(\delta\Gamma', R). \\ &[\delta]_{\Delta} \in \text{TyEnv}(\Delta) \wedge [\gamma_i]_{\text{dom}(\Gamma)} \in \text{Env}([\delta]_{\Delta}\Gamma, R) \wedge \gamma_i e_i = [\gamma_i]_{\text{dom}(\Gamma)} e_i \end{aligned}$$

where $[f]_d$ denotes the restriction of the function f on domain d . \square

Lemma 43 (Congruence). If $\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma$ and $\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma')$, then

$$\Delta'; \Gamma' \vdash |C|[e_1] \sim |C|[e_2] : \sigma'.$$

Proof. By induction on the derivation of the context typing: in each case using the corresponding compatibility lemma. For a context containing subterms we also need Theorem 41. The rule for an empty context requires Lemma 42. \square

Lemma 44 (Adequacy). If $\cdot; \cdot \vdash e_1 \sim e_2 : \tau$, then

1. $\forall h_1, h_2$. neither h_1, e_1 nor h_2, e_2 gets stuck.
2. $\forall h_1, h_2$. $h_1, e_1 \uparrow \iff h_2, e_2 \uparrow$.

Proof.

- We know $\cdot; \cdot \vdash e_1 \sim_w e_2 : \tau$ for some w with $w.N \subseteq \text{TyNam}$.
- Hence we have *consistent*($w\uparrow$) and *inhabited*($w\uparrow$).
- Thus, using Lemma 2, there is s_0 such that $(\emptyset, \emptyset) \in w\uparrow.H(s_0)([w\uparrow](s_0))$.
- We also have $(e_1, e_2) \in \mathbf{E}_{w\uparrow}([w\uparrow])(s_0, s_0)(\tau)$.
- Since *consistent*($w\uparrow$), $(\emptyset, \emptyset) \in w\uparrow.H(s_0)([w\uparrow](s_0))$ and $\forall s$. $[w\uparrow](s) = w\uparrow.L(s)([w\uparrow](s))$, by Corollary 19 for any heaps h_1, h_2 both h_1, e_1 and h_2, e_2 diverge or both terminate without getting stuck. \square

Theorem 45 (Soundness). If $\Delta; \Gamma \vdash p_1 : \sigma$ and $\Delta; \Gamma \vdash p_2 : \sigma$, then:

$$\Delta; \Gamma \vdash |p_1| \sim |p_2| : \sigma \implies \Delta; \Gamma \vdash p_1 \sim_{\text{ctx}} p_2 : \sigma$$

Proof.

- Suppose $\Delta; \Gamma \vdash |p_1| \sim |p_2| : \sigma$ as well as $\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\cdot; \cdot; \tau)$.
- By congruence (Lemma 43), we have $\cdot; \cdot \vdash |C[|p_1|]| \sim |C[|p_2|]| : \tau$.
- By adequacy (Lemma 44), we have $h, |C[|p_1|]| \uparrow \iff h, |C[|p_2|]| \uparrow$ for any h , so we are done. \square

2.5 Symmetry

Definition 2. Given $R \in \text{VRel}$ (or VRelF), we define $R^{-1} \in \text{VRel}$ (or VRelF) as follows:

$$R^{-1} := \lambda\tau. R(\tau)^{-1}$$

Lemma 46. $(\overline{R})^{-1} = \overline{R^{-1}}$

Proof. Easy to check by induction. □

Lemma 47. $\mathbf{S}(R_f^{-1}, R_v^{-1}) = (\mathbf{S}(R_f, R_v))^{-1}$

Proof. Easy to check. □

Definition 3. Given $w \in \text{LWorld}$, we define $w^{-1} \in \text{LWorld}$ as follows:

$$\begin{aligned} w^{-1}.\mathbf{N} &:= w.\mathbf{N} \\ w^{-1}.\mathbf{S} &:= w.\mathbf{S} \\ w^{-1}.\sqsupseteq &:= w.\sqsupseteq \\ w^{-1}.\sqsupseteq_{\text{pub}} &:= w.\sqsupseteq_{\text{pub}} \\ w^{-1}.\mathbf{L}(s_{\text{rf}})(s)(R) &:= (w.\mathbf{L}(s_{\text{rf}}^{-1})(s)(R^{-1}))^{-1} \\ w^{-1}.\mathbf{H}(s_{\text{rf}})(s)(R) &:= (w.\mathbf{H}(s_{\text{rf}}^{-1})(s)(R^{-1}))^{-1} \end{aligned}$$

where $s_{\text{rf}}^{-1} := \lambda\tau. s_{\text{rf}}(\tau)^{-1}$.

Lemma 48. $w^{-1}\uparrow.\mathbf{H}(s_{\text{rf}}, s)(R) = (w\uparrow.\mathbf{H}(s_{\text{rf}}^{-1}, s)(R^{-1}))^{-1}$

Proof.

$$\begin{aligned} &w^{-1}\uparrow.\mathbf{H}(s_{\text{rf}}, s)(R) \\ = &W_{\text{ref}}.\mathbf{H}(s_{\text{rf}})(R) \otimes w^{-1}.\mathbf{H}(s_{\text{rf}})(s)(R) \\ = &\left((W_{\text{ref}}.\mathbf{H}(s_{\text{rf}})(R))^{-1} \otimes (w^{-1}.\mathbf{H}(s_{\text{rf}})(s)(R))^{-1} \right)^{-1} \\ = &(W_{\text{ref}}.\mathbf{H}(s_{\text{rf}}^{-1})(R^{-1}) \otimes w.\mathbf{H}(s_{\text{rf}}^{-1})(s)(R^{-1}))^{-1} \\ = &(w\uparrow.\mathbf{H}(s_{\text{rf}}^{-1}, s)(R^{-1}))^{-1} \end{aligned}$$

□

Lemma 49. $w^{-1}\uparrow.\mathbf{L}(s_{\text{rf}}, s)(R) = (w\uparrow.\mathbf{L}(s_{\text{rf}}^{-1}, s)(R^{-1}))^{-1}$

Proof. Analogous to Lemma 48. □

Definition 4. If $G \in \text{GK}(w^{-1}\uparrow)$, we define $G^{-1} := \lambda s_{\text{rf}}, s. G(s_{\text{rf}}^{-1}, s)^{-1}$.

Lemma 50. If $G \in \text{GK}(w^{-1}\uparrow)$, then $G^{-1} \in \text{GK}(w\uparrow)$.

Proof.

1. Monotonicity of G^{-1} follows immediately from monotonicity of G .
2. It remains to show $\forall s_{\text{rf}}, s. G^{-1}(s_{\text{rf}}, s) \geq_{\text{ref}}^{w\uparrow.\mathbf{N}} w\uparrow.\mathbf{L}(s_{\text{rf}}, s)(G^{-1}(s_{\text{rf}}, s))$:

$$\begin{aligned} &G^{-1}(s_{\text{rf}}, s) \\ = &G(s_{\text{rf}}^{-1}, s)^{-1} \\ \geq_{\text{ref}}^{w\uparrow.\mathbf{N}} &(w^{-1}\uparrow.\mathbf{L}(s_{\text{rf}}^{-1}, s)(G(s_{\text{rf}}^{-1}, s)))^{-1} \\ = &w\uparrow.\mathbf{L}(s_{\text{rf}}, s)(G(s_{\text{rf}}^{-1}, s)^{-1}) \\ = &w\uparrow.\mathbf{L}(s_{\text{rf}}, s)(G^{-1}(s_{\text{rf}}, s)) \end{aligned}$$

□

Lemma 51. If $stable(w)$, then $stable(w^{-1})$.

Proof.

- We suppose
 1. $G \in \text{GK}(w^{-1}\uparrow)$
 2. $(h_1, h_2) \in w^{-1}.\mathbf{H}(s_{\text{rf}})(s)(G(s_{\text{rf}}, s))$
 3. $s'_{\text{rf}} \sqsupseteq s_{\text{rf}}$
 4. $(h_{\text{ref}}^1, h_{\text{ref}}^2) \in W_{\text{ref}}.\mathbf{H}(s'_{\text{rf}})(G(s'_{\text{rf}}, s))$
 5. $h_{\text{ref}}^1 \uplus h_1$ defined \wedge $h_{\text{ref}}^2 \uplus h_2$ defined

and must show: $\exists s' \sqsupseteq_{\text{pub}} s. (h_1, h_2) \in w^{-1}.\mathbf{H}(s'_{\text{rf}})(s')(G(s'_{\text{rf}}, s'))$

- From (2) we know $(h_2, h_1) \in w.\mathbf{H}(s_{\text{rf}}^{-1})(s)(G(s_{\text{rf}}, s)^{-1}) = w.\mathbf{H}(s_{\text{rf}}^{-1})(s)(G^{-1}(s_{\text{rf}}^{-1}, s))$.
- From (3) we know $s'^{-1}_{\text{rf}} \sqsupseteq s_{\text{rf}}^{-1}$.
- From (4) and Lemma 46 we know $(h_{\text{ref}}^2, h_{\text{ref}}^1) \in W_{\text{ref}}.\mathbf{H}(s'^{-1}_{\text{rf}})(G(s'_{\text{rf}}, s)^{-1}) = W_{\text{ref}}.\mathbf{H}(s'^{-1}_{\text{rf}})(G^{-1}(s'^{-1}_{\text{rf}}, s))$.
- Hence, using Lemma 50, the assumption yields $s' \sqsupseteq_{\text{pub}} s$ such that

$$(h_2, h_1) \in w.\mathbf{H}(s'^{-1}_{\text{rf}})(s')(G^{-1}(s'^{-1}_{\text{rf}}, s')).$$

- This implies $(h_1, h_2) \in w^{-1}.\mathbf{H}(s'_{\text{rf}})(s')(G(s'_{\text{rf}}, s'))$.

□

Lemma 52. If $inhabited(w\uparrow)$, then $inhabited(w^{-1}\uparrow)$.

Proof.

- We suppose $G \in \text{GK}(w^{-1}\uparrow)$ and must show $\exists s_0. (\emptyset, \emptyset) \in w^{-1}\uparrow.\mathbf{H}(s_0)(G(s_0))$.
- Using the assumption and Lemma 50, we get (s_{rf}, s) such that $(\emptyset, \emptyset) \in w\uparrow.\mathbf{H}(s_{\text{rf}}, s)(G^{-1}(s_{\text{rf}}, s))$.
- Lemma 48 implies $(\emptyset, \emptyset) \in w^{-1}\uparrow.\mathbf{H}(s_{\text{rf}}^{-1}, s)(G(s_{\text{rf}}^{-1}, s))$.

□

Lemma 53. If $G \in \text{GK}(w^{-1}\uparrow)$, then:

$$(\mathbf{E}_{w\uparrow}(G^{-1})((s_{\text{rf}}^{-1}_0, s_0), (s_{\text{rf}}^{-1}, s)))^{-1} \subseteq \mathbf{E}_{w^{-1}\uparrow}(G)((s_{\text{rf}0}, s_0), (s_{\text{rf}}, s))$$

Proof. Let

$$\begin{aligned} \mathbf{E}'_{w^{-1}\uparrow}(G)((s_{\text{rf}0}, s_0), (s_{\text{rf}}, s))(\tau) &:= (\mathbf{E}_{w\uparrow}(G^{-1})((s_{\text{rf}}^{-1}_0, s_0), (s_{\text{rf}}^{-1}, s))(\tau))^{-1}, \\ \mathbf{K}'_{w^{-1}\uparrow}(G)((s_{\text{rf}0}, s_0), (s_{\text{rf}}, s))(\tau', \tau) &:= (\mathbf{K}_{w\uparrow}(G^{-1})((s_{\text{rf}}^{-1}_0, s_0), (s_{\text{rf}}^{-1}, s))(\tau', \tau))^{-1}. \end{aligned}$$

By coinduction, it suffices to show:

1. $\forall e_2, e_1, G, s_{\text{rf}0}, s_0, s_{\text{rf}}, s, \tau.$
 $(e_2, e_1) \in \mathbf{E}'_{w^{-1}\uparrow}(G)((s_{\text{rf}0}, s_0), (s_{\text{rf}}, s))(\tau) \implies$
 $\forall (h_2, h_1) \in w^{-1}\uparrow.\mathbf{H}(s_{\text{rf}}, s)(G(s_{\text{rf}}, s)). \forall h_2^{\text{F}}, h_1^{\text{F}}.$
 $((h_2, h_2^{\text{F}}, e_2), (h_1, h_1^{\text{F}}, e_1)) \in \mathbf{O}_{w^{-1}\uparrow}(\mathbf{K}'_{w^{-1}\uparrow}(G))((s_{\text{rf}0}, s_0), (s_{\text{rf}}, s))(\tau)$

2. $\forall K_2, K_1, G, s_{\text{rf}0}, s_0, s_{\text{rf}}, s, \tau', \tau.$
 $(K_2, K_1) \in \mathbf{K}'_{w^{-1}\uparrow}(G)((s_{\text{rf}0}, s_0), (s_{\text{rf}}, s))(\tau', \tau) \implies$
 $\forall (v_2, v_1) \in \overline{G(s_{\text{rf}}, s)}(\tau').$
 $(K_2[v_2], K_1[v_1]) \in \mathbf{E}'_{w^{-1}\uparrow}(G)((s_{\text{rf}0}, s_0), (s_{\text{rf}}, s))(\tau)$

For (1):

- By definition of $\mathbf{E}'_{w^{-1}\uparrow}$ and Lemma 48, suppose $(e_1, e_2) \in \mathbf{E}_{w\uparrow}(G^{-1})((s_{\text{rf}}^{-1}, s_0), (s_{\text{rf}}^{-1}, s))(\tau)$ and $(h_1, h_2) \in w\uparrow.H(s_{\text{rf}}^{-1}, s)(G^{-1}(s_{\text{rf}}^{-1}, s))$.
- By definition of $\mathbf{E}_{w\uparrow}$ we have $((h_1, h_1^{\text{F}}, e_1), (h_2, h_2^{\text{F}}, e_2)) \in \mathbf{O}_{w\uparrow}(\mathbf{K}_{w\uparrow})(G^{-1})((s_{\text{rf}}^{-1}, s_0), (s_{\text{rf}}^{-1}, s))(\tau)$.
- Using all the lemmas above, it is easy to check that this implies

$$((h_2, h_2^{\text{F}}, e_2), (h_1, h_1^{\text{F}}, e_1)) \in \mathbf{O}_{w^{-1}\uparrow}(\mathbf{K}'_{w^{-1}\uparrow})(G)((s_{\text{rf}0}, s_0), (s_{\text{rf}}, s))(\tau).$$

For (2):

- By definition of $\mathbf{K}'_{w^{-1}\uparrow}$ and Lemma 46, suppose $(K_1, K_2) \in \mathbf{K}_{w\uparrow}(G^{-1})((s_{\text{rf}}^{-1}, s_0), (s_{\text{rf}}^{-1}, s))(\tau', \tau)$ and $(v_1, v_2) \in \overline{G^{-1}(s_{\text{rf}}^{-1}, s)}(\tau')$.
- By definition of $\mathbf{K}_{w\uparrow}$ we have $(K_1[v_1], K_2[v_2]) \in \mathbf{E}_{w\uparrow}(G^{-1})((s_{\text{rf}}^{-1}, s_0), (s_{\text{rf}}^{-1}, s))(\tau)$.
- By definition of $\mathbf{E}'_{w^{-1}\uparrow}$, it implies that $(K_2[v_2], K_1[v_1]) \in \mathbf{E}'_{w^{-1}\uparrow}(G)((s_{\text{rf}0}, s_0), (s_{\text{rf}}, s))(\tau)$.

□

Lemma 54. If $\text{consistent}(w\uparrow)$, then $\text{consistent}(w^{-1}\uparrow)$.

Proof.

- We suppose $G \in \text{GK}(w^{-1}\uparrow)$ and $(e_1, e_2) \in \mathbf{S}(w^{-1}\uparrow.L(s_{\text{rf}}, s)(G(s_{\text{rf}}, s)), G(s_{\text{rf}}, s))(\tau)$, and must show $(\text{beta}(e_1), \text{beta}(e_2)) \in \mathbf{E}_{w^{-1}\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\tau)$.
- By Lemma 47 we know $(e_2, e_1) \in \mathbf{S}(w\uparrow.L(s_{\text{rf}}^{-1}, s)(G^{-1}(s_{\text{rf}}^{-1}, s)), G^{-1}(s_{\text{rf}}^{-1}, s))(\tau)$.
- Using the assumption and Lemma 50, we get $(\text{beta}(e_2), \text{beta}(e_1)) \in \mathbf{E}_{w\uparrow}(G^{-1})((s_{\text{rf}}^{-1}, s), (s_{\text{rf}}^{-1}, s))(\tau)$.
- We are done by Lemma 53.

□

Theorem 55. If $\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma$, then $\Delta; \Gamma \vdash e_2 \sim e_1 : \sigma$.

Proof. Suppose $\Delta; \Gamma \vdash e_1 \sim_w e_2 : \sigma$ with $\text{stable}(w)$. By Lemma 51 it suffices to show $\Delta; \Gamma \vdash e_2 \sim_{w^{-1}} e_1 : \sigma$. Using Lemmas 52 and 54, this in turn reduces to showing:

$$\forall G \in \text{GK}(w^{-1}\uparrow). \forall s_{\text{rf}}, s. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_{\text{rf}}, s)).$$

$$(\gamma_1 e_2, \gamma_2 e_1) \in \mathbf{E}_{w^{-1}\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\delta\sigma)$$

From $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_{\text{rf}}, s))$ we have $(\gamma_2, \gamma_1) \in \text{Env}(\delta\Gamma, G(s_{\text{rf}}, s)^{-1}) = \text{Env}(\delta\Gamma, G^{-1}(s_{\text{rf}}^{-1}, s))$. Lemma 50 and the assumption thus yield $(\gamma_2 e_1, \gamma_1 e_2) \in \mathbf{E}_{w\uparrow}(G^{-1})((s_{\text{rf}}^{-1}, s), (s_{\text{rf}}^{-1}, s))(\delta\sigma)$. We are done by Lemma 53. □

3 Examples

3.1 World Generator

$$\text{NLWorld} := \{ \mathcal{W} \in \text{Names} \rightarrow \text{LWorld} \mid \forall \mathcal{N}. \mathcal{W}(\mathcal{N}).\mathbf{N} \subseteq \mathcal{N} \}$$

Definition 5. We define $\mathbf{G} : \text{NLWorld} \rightarrow \text{NLWorld}$ as follows.

$$\begin{aligned} \mathbf{G}(\mathcal{W})(\mathcal{N}).\mathbf{N} &:= \mathcal{N} \\ \mathbf{G}(\mathcal{W})(\mathcal{N}).\mathbf{S} &:= \{ (s_1, \dots, s_n) \mid n \in \mathbb{N} \wedge \forall i \in \{1 \dots n\}. s_i \in \mathcal{W}(\mathcal{N}_i).\mathbf{S} \} \\ \mathbf{G}(\mathcal{W})(\mathcal{N}).\mathbf{L}(s_{\text{rf}})(s_1, \dots, s_n)(R) &:= \bigcup_{i \in \{1 \dots n\}} \mathcal{W}(\mathcal{N}_i).\mathbf{L}(s_{\text{rf}})(s_i)(R) \\ \mathbf{G}(\mathcal{W})(\mathcal{N}).\mathbf{H}(s_{\text{rf}})(s_1, \dots, s_n)(R) &:= \otimes_{i \in \{1 \dots n\}} \mathcal{W}(\mathcal{N}_i).\mathbf{H}(s_{\text{rf}})(s_i)(R) \end{aligned}$$

where $\{\mathcal{N}_i\}$ is a countably infinite splitting of \mathcal{N} *i.e.*, $\mathcal{N} = \mathcal{N}_1 \uplus \mathcal{N}_2 \uplus \mathcal{N}_3 \uplus \dots$

The transition on $\mathbf{G}(\mathcal{W})(\mathcal{N})$ is generated by the following rule.

$$\begin{aligned} (s_1, \dots, s_k, s_{k+1}) \sqsupseteq_{\text{pub}} (s_1, \dots, s_k) \\ (s'_1, \dots, s'_k) \sqsupseteq_{\text{pub}} (s_1, \dots, s_k) &\text{ if } s'_1 \sqsupseteq_{\text{pub}} s_1 \wedge \dots \wedge s'_k \sqsupseteq_{\text{pub}} s_k \\ (s'_1, \dots, s'_k) \sqsupseteq (s_1, \dots, s_k) &\text{ if } s'_1 \sqsupseteq s_1 \wedge \dots \wedge s'_k \sqsupseteq s_k \\ (s'_1, \dots, s'_j) \sqsupseteq (s_1, \dots, s_k) &\text{ if } (s'_1, \dots, s'_j) \sqsupseteq_{\text{pub}} (s_1, \dots, s_k) \end{aligned}$$

We define the following notation.

$$\begin{aligned} \{n \setminus i\} &:= \{1, \dots, i-1, i+1, \dots, n\} \\ G(\{s_k\}_{k \in \{n \setminus i\}}) &:= G(-, s_1, \dots, s_{i-1}, -, s_{i+1}, \dots, s_n) \end{aligned}$$

Lemma 56.

$$\forall G \in \text{GK}(\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow). \forall s_1 \dots s_{i-1}, s_{i+1} \dots s_n. G(\{s_k\}_{k \in \{n \setminus i\}}) \in \text{GK}(\mathcal{W}(\mathcal{N}_i)\uparrow)$$

Proof.

- We need to show $G(\{s_k\}_{k \in \{n \setminus i\}})$ is monotone w.r.t. \sqsubseteq , which follows directly from the definition of \sqsubseteq and monotonicity of G .
- We have

$$\begin{aligned} &G(\{s_k\}_{k \in \{n \setminus i\}})(s_{\text{rf}}, s_i) \\ &= G(s_{\text{rf}}, s_1 \dots s_n) \\ &\stackrel{\geq_{\text{ref}}}{\geq} \mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow.\mathbf{L}(s_{\text{rf}}, s_1 \dots s_n)(G(s_{\text{rf}}, s_1 \dots s_n)) \\ &\geq \mathcal{W}(\mathcal{N}_i)\uparrow.\mathbf{L}(s_{\text{rf}}, s_i)(G(s_{\text{rf}}, s_1, \dots, s_n)) \\ &= \mathcal{W}(\mathcal{N}_i)\uparrow.\mathbf{L}(s_{\text{rf}}, s_i)(G(\{s_k\}_{k \in \{n \setminus i\}})(s_{\text{rf}}, s_i)) . \end{aligned}$$

- Now it suffices to show that the latter inequality is contained in $\stackrel{\geq_{\text{ref}}}{\geq} \mathcal{N}_i$, which follows from $\forall i. \mathcal{W}(\mathcal{N}_i) \in \text{LWorld}$ and the fact that $\mathcal{N}_1, \dots, \mathcal{N}_n$ are disjoint. □

Lemma 57. If $W = \mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow$ and $\forall \mathcal{N}'. \text{stable}(\mathcal{W}(\mathcal{N}'))$ and $G \in \text{GK}(W)$, then:

1. $\mathbf{E}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \setminus i\}}))((s_{\text{rf}}^0, s_i^0), (s_{\text{rf}}, s_i)) \leq \mathbf{E}_W(G)((s_{\text{rf}}^0, s_1 \dots s_{i-1}, s_i^0, s_{i+1} \dots s_n), (s_{\text{rf}}, s_1 \dots s_n))$
2. $\mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \setminus i\}}))((s_{\text{rf}}^0, s_i^0), (s_{\text{rf}}, s_i)) \leq \mathbf{K}_W(G)((s_{\text{rf}}^0, s_1 \dots s_{i-1}, s_i^0, s_{i+1} \dots s_n), (s_{\text{rf}}, s_1 \dots s_n))$

Proof. We define \mathbf{E}'_W and \mathbf{K}'_W as follows:

$$\begin{aligned} \mathbf{E}'_W(G)((s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0), (s_{\text{rf}}, s_1 \dots s_n)) &= \{ (\tau, e_1, e_2) \mid \\ &(\forall k \in \{n_0 \setminus i\}. s_k \sqsupseteq_{\text{pub}} s_k^0) \wedge (\tau, e_1, e_2) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \setminus i\}}))((s_{\text{rf}}^0, s_i^0), (s_{\text{rf}}, s_i)) \} \\ \mathbf{K}'_W(G)((s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0), (s_{\text{rf}}, s_1 \dots s_n)) &= \{ (\tau', \tau, K_1, K_2) \mid \\ &(\forall k \in \{n_0 \setminus i\}. s_k \sqsupseteq_{\text{pub}} s_k^0) \wedge (\tau', \tau, K_1, K_2) \in \mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \setminus i\}}))((s_{\text{rf}}^0, s_i^0), (s_{\text{rf}}, s_i)) \} \end{aligned}$$

Then it suffices to show $\mathbf{E}'_W \leq \mathbf{E}_W$ and $\mathbf{K}'_W \leq \mathbf{K}_W$ by coinduction. Concretely, we have to show:

1. $\forall e_1, e_2, G, s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0, s_{\text{rf}}, s_1 \dots s_n, \tau.$
 $(e_1, e_2) \in \mathbf{E}'_W(G)((s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0), (s_{\text{rf}}, s_1 \dots s_n))(\tau) \implies$
 $\forall (h_1, h_2) \in W.\mathbf{H}(s_{\text{rf}}, s_1 \dots s_n)(G(s_{\text{rf}}, s_1 \dots s_n)). \forall h_1^F, h_2^F.$
 $((h_1, h_1^F, e_1), (h_2, h_2^F, e_2)) \in \mathbf{O}_W(\mathbf{K}'_W(G)((s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0), (s_{\text{rf}}, s_1 \dots s_n))(\tau))$
2. $\forall K_1, K_2, G, s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0, s_{\text{rf}}, s_1 \dots s_n, \tau', \tau.$
 $(K_1, K_2) \in \mathbf{K}'_W(G)((s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0), (s_{\text{rf}}, s_1 \dots s_n))(\tau', \tau) \implies$
 $\forall (v_1, v_2) \in \overline{G}(s_{\text{rf}}, s_1 \dots s_n)(\tau'). (K_1[v_1], K_2[v_2]) \in \mathbf{E}'_W(G)((s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0), (s_{\text{rf}}, s_1 \dots s_n))(\tau)$

For (1):

- Suppose $(e_1, e_2) \in \mathbf{E}'_W(G)((s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0), (s_{\text{rf}}, s_1 \dots s_n))(\tau)$ and $(h_1, h_2) \in W.\mathbf{H}(s_{\text{rf}}, s_1 \dots s_n)(G(s_{\text{rf}}, s_1 \dots s_n))$.
- By definition of \mathbf{E}'_W we have $(\forall k \in \{n_0 \setminus i\}). s_k \sqsupseteq_{\text{pub}} s_k^0$ and

$$(\tau, e_1, e_2) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \setminus i\}}))((s_{\text{rf}}^0, s_i^0), (s_{\text{rf}}, s_i)) .$$

- We must show $((h_1, h_1^F, e_1), (h_2, h_2^F, e_2)) \in \mathbf{O}_W(\mathbf{K}'_W(G)((s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0), (s_{\text{rf}}, s_1 \dots s_n))(\tau))$.
- So suppose defined $(h_1 \uplus h_1^F)$ and defined $(h_2 \uplus h_2^F)$.
- From $(h_1, h_2) \in W.\mathbf{H}(s_{\text{rf}}, s_1 \dots s_n)(G(s_{\text{rf}}, s_1 \dots s_n))$, we have $h_1 = h_1' \uplus h_1''$ and $h_2 = h_2' \uplus h_2''$ with $(h_1', h_2') \in \mathcal{W}(\mathcal{N}_i)\uparrow.\mathbf{H}(s_{\text{rf}}, s_i)(G(s_{\text{rf}}, s_1 \dots s_n))$ and $(h_1'', h_2'') \in \otimes_{k \in \{n \setminus i\}} \mathcal{W}(\mathcal{N}_k).\mathbf{H}(s_{\text{rf}})(s_k)(G(s_{\text{rf}}, s_1 \dots s_n))$.
- Hence $((h_1', h_1'' \uplus h_1^F, e_1), (h_2', h_2'' \uplus h_2^F, e_2)) \in \mathbf{O}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(\mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow})(G(\{s_k\}_{k \in \{n \setminus i\}}))((s_{\text{rf}}^0, s_i^0), (s_{\text{rf}}, s_i))(\tau)$.
- Consequently at least one of the following three properties holds:

A) $h_1 \uplus h_1^F, e_1 \uparrow$ and $h_2 \uplus h_2^F, e_2 \uparrow$

B) (a) $h_1 \uplus h_1^F, e_1 \hookrightarrow^* \widetilde{h}_1' \uplus h_1'' \uplus h_1^F, v_1$ and $h_2 \uplus h_2^F, e_2 \hookrightarrow^* \widetilde{h}_2' \uplus h_2'' \uplus h_2^F, v_2$

(b) $(\widetilde{s}_{\text{rf}}, \widetilde{s}_i) \sqsupseteq [(s_{\text{rf}}^0, s_i^0), (s_{\text{rf}}, s_i)]$

(c) $(\widetilde{h}_1', \widetilde{h}_2') \in \mathcal{W}(\mathcal{N}_i)\uparrow.\mathbf{H}(\widetilde{s}_{\text{rf}}, \widetilde{s}_i)(G(\widetilde{s}_{\text{rf}}, s_1 \dots s_{i-1}, \widetilde{s}_i, s_{i+1} \dots s_n))$

(d) $(v_1, v_2) \in \overline{G}(\widetilde{s}_{\text{rf}}, s_1 \dots s_{i-1}, \widetilde{s}_i, s_{i+1} \dots s_n)(\tau)$

C) (a) $h_1 \uplus h_1^F, e_1 \hookrightarrow^* \widetilde{h}_1' \uplus h_1'' \uplus h_1^F, v_1$ and $h_2 \uplus h_2^F, e_2 \hookrightarrow^* \widetilde{h}_2' \uplus h_2'' \uplus h_2^F, v_2$

(b) $(\widetilde{s}_{\text{rf}}, \widetilde{s}_i) \sqsupseteq (s_{\text{rf}}, s_i)$

(c) $(\widetilde{h}_1', \widetilde{h}_2') \in \mathcal{W}(\mathcal{N}_i)\uparrow.\mathbf{H}(\widetilde{s}_{\text{rf}}, \widetilde{s}_i)(G(\widetilde{s}_{\text{rf}}, s_1 \dots s_{i-1}, \widetilde{s}_i, s_{i+1} \dots s_n))$

(d) $(e_1', e_2') \in \mathbf{S}(G(\widetilde{s}_{\text{rf}}, s_1 \dots s_{i-1}, \widetilde{s}_i, s_{i+1} \dots s_n), G(\widetilde{s}_{\text{rf}}, s_1 \dots s_{i-1}, \widetilde{s}_i, s_{i+1} \dots s_n))(\widetilde{\tau})$

(e) $\forall (\widetilde{s}_{\text{rf}}, \widetilde{s}_i) \sqsupseteq_{\text{pub}} (s_{\text{rf}}, s_i). \forall G' \geq G(\{s_k\}_{k \in \{n \setminus i\}}). (K_1, K_2) \in \mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G')((s_{\text{rf}}^0, s_i^0), (\widetilde{s}_{\text{rf}}, \widetilde{s}_i))(\widetilde{\tau}, \tau)$

- If (A) holds, then we are done.

- If (B) holds:

- For all $k \in \{n \setminus i\}$, iteratively applying $\text{stable}(\mathcal{W}(\mathcal{N}_k))$ and using monotonicity gets us $\widetilde{s}_k \sqsupseteq_{\text{pub}} s_k$ such that:

$$(h_1'', h_2'') \in \otimes_{k \in \{n \setminus i\}} \mathcal{W}(\mathcal{N}_k).\mathbf{H}(\widetilde{s}_{\text{rf}})(\widetilde{s}_k)(G(\widetilde{s}_{\text{rf}}, \widetilde{s}_1 \dots \widetilde{s}_n))$$

- Thus from (Bc), monotonicity, and the definition of W we get

$$(\widetilde{h}_1' \uplus h_1'', \widetilde{h}_2' \uplus h_2'') \in W.\mathbf{H}(\widetilde{s}_{\text{rf}}, \widetilde{s}_1 \dots \widetilde{s}_n)(G(\widetilde{s}_{\text{rf}}, \widetilde{s}_1 \dots \widetilde{s}_n))$$

- From (Bb) we get $(\widetilde{s}_{\text{rf}}, \widetilde{s}_1 \dots \widetilde{s}_n) \sqsupseteq [(s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0), (s_{\text{rf}}, s_1 \dots s_n)]$.

- Together with (Ba), (Bd), and monotonicity we are done.

- If (C) holds:

- For all $k \in \{n \setminus i\}$, iteratively applying $stable(\mathcal{W}(\mathcal{N}_k))$ and using monotonicity gets us $\tilde{s}_k \sqsupseteq_{\text{pub}} s_k$ such that:

$$(h_1'', h_2'') \in \otimes_{k \in \{n \setminus i\}} \mathcal{W}(\mathcal{N}_k) \cdot \mathbf{H}(\widetilde{s_{\text{rf}}})(\widetilde{s}_k)(G(\widetilde{s_{\text{rf}}}, \widetilde{s}_1 \dots \widetilde{s}_n))$$

- Thus from (Cc), monotonicity, and the definition of W we get

$$(\widetilde{h}_1' \uplus h_1'', \widetilde{h}_2' \uplus h_2'') \in W \cdot \mathbf{H}(\widetilde{s_{\text{rf}}}, \widetilde{s}_1 \dots \widetilde{s}_n)(G(\widetilde{s_{\text{rf}}}, \widetilde{s}_1 \dots \widetilde{s}_n))$$

- From (Cb) we get $(\widetilde{s_{\text{rf}}}, \widetilde{s}_1 \dots \widetilde{s}_n) \sqsupseteq [(s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0), (s_{\text{rf}}, s_1 \dots s_n)]$.

- After applying monotonicity to (Cd), it remains to show:

$$\begin{aligned} & \forall (\widehat{s_{\text{rf}}}, \widehat{s}_1 \dots \widehat{s}_m) \sqsupseteq_{\text{pub}} (\widetilde{s_{\text{rf}}}, \widetilde{s}_1 \dots \widetilde{s}_n) \cdot \forall G' \geq G. \\ & (K_1, K_2) \in \mathbf{K}'_W(G')((s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0), (\widehat{s_{\text{rf}}}, \widehat{s}_1 \dots \widehat{s}_m))(\widetilde{\tau}, \tau) \end{aligned}$$

- So suppose $(\widehat{s_{\text{rf}}}, \widehat{s}_1 \dots \widehat{s}_m) \sqsupseteq_{\text{pub}} (\widetilde{s_{\text{rf}}}, \widetilde{s}_1 \dots \widetilde{s}_n)$ and $G' \geq G$.

- By monotonicity we have $G'(\{\widehat{s}_k\}_{k \in \{m \setminus i\}}) \geq G(\{s_k\}_{k \in \{n \setminus i\}})$.

- From (Ce) we therefore get $(K_1, K_2) \in \mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G'(\{\widehat{s}_k\}_{k \in \{m \setminus i\}}))((s_{\text{rf}}^0, s_i^0), (\widehat{s_{\text{rf}}}, \widehat{s}_i))(\widetilde{\tau}, \tau)$.

- By definition of \mathbf{K}'_W this implies $(K_1, K_2) \in \mathbf{K}'_W(G')((s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0), (\widehat{s_{\text{rf}}}, \widehat{s}_1 \dots \widehat{s}_m))(\widetilde{\tau}, \tau)$.

For (2):

- Suppose $(K_1, K_2) \in \mathbf{K}'_W(G)((s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0), (s_{\text{rf}}, s_1 \dots s_n))(\tau', \tau)$ and $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s_1 \dots s_n)}(\tau')$.

- By definition of \mathbf{K}'_W we have $(\forall k \in \{n_0 \setminus i\}. s_k \sqsupseteq_{\text{pub}} s_k^0)$ and

$$(\tau', \tau, K_1, K_2) \in \mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \setminus i\}}))((s_{\text{rf}}^0, s_i^0), (s_{\text{rf}}, s_i)) \cdot p$$

- We must show $(\tau, K_1[v_1], K_2[v_2]) \in \mathbf{E}'_W(G)((s_{\text{rf}}^0, s_1^0 \dots s_{n_0}^0), (s_{\text{rf}}, s_1 \dots s_n))$.

- By definition of \mathbf{E}'_W it suffices to show

$$(\tau, K_1[v_1], K_2[v_2]) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \setminus i\}}))((s_{\text{rf}}^0, s_i^0), (s_{\text{rf}}, s_i)) \cdot$$

- Since $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s_1 \dots s_n)}(\tau')$, we are done. □

Lemma 58. Suppose $\forall \mathcal{N}. stable(\mathcal{W}(\mathcal{N}))$.

1. $\forall \mathcal{N}. stable(\mathbf{G}(\mathcal{W})(\mathcal{N}))$

2. If $\forall \mathcal{N}. consistent(\mathcal{W}(\mathcal{N})\uparrow)$, then $\forall \mathcal{N}. consistent(\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow)$.

Proof.

- We suppose

(a) $G \in \mathbf{GK}(\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow)$

(b) $(\tau, e_1, e_2) \in \mathbf{S}(\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow) \cdot \mathbf{L}(s_{\text{rf}}, s_1 \dots s_n)(G(s_{\text{rf}}, s_1 \dots s_n), G(s_{\text{rf}}, s_1 \dots s_n))$

and must show $(\tau, beta(e_1), beta(e_2)) \in \mathbf{E}_{\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow}(G)((s_{\text{rf}}, s_1 \dots s_n), (s_{\text{rf}}, s_1 \dots s_n))$.

- From (b) and the definition of \mathbf{S} we know: for some i ,

$$(\tau, e_1, e_2) \in \mathbf{S}(\mathcal{W}(\mathcal{N}_i)\uparrow) \cdot \mathbf{L}(s_{\text{rf}}, s_i)(G(s_{\text{rf}}, s_1 \dots s_n), G(s_{\text{rf}}, s_1 \dots s_n))$$

- The claim follows from $consistent(\mathcal{W}(\mathcal{N}_i)\uparrow)$ with the help of Lemmas 56 and 57. □

Lemma 59. $inhabited(\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow)$

Proof. It is easy to check that $(\emptyset, \emptyset) \in \mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow \cdot \mathbf{H}(\emptyset, ())(R)$ for any R . □

3.2 Substitutivity

Theorem 60.

$$\frac{\Delta; \Gamma, x:\sigma' \vdash e_1 \sim e_2 : \sigma \quad \Delta; \Gamma \vdash v_1 \sim v_2 : \sigma'}{\Delta; \Gamma \vdash e_1[v_1/x] \sim e_2[v_2/x] : \sigma}$$

Proof. By Lemma 16 it suffices to show:

$$\frac{\Delta; \Gamma, x:\sigma' \vdash e_1 \sim_W e_2 : \sigma \quad \Delta; \Gamma \vdash v_1 \sim_W v_2 : \sigma'}{\Delta; \Gamma \vdash e_1[v_1/x] \sim_W e_2[v_2/x] : \sigma}$$

This boils down to showing

$$(\delta\sigma, \gamma_1(e_1[v_1/x]), \gamma_2(e_2[v_2/x])) \in \mathbf{E}_W(G)(s, s)$$

for $\delta \in \text{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s))$.

- So suppose $(h_1, h_2) \in W.H(s)(G(s))$ and $h_1^F, h_2^F \in \text{Heap}$.
- We must show $(\delta\sigma, (h_1, h_1^F, \gamma_1(e_1[v_1/x])), (h_2, h_2^F, \gamma_2(e_2[v_2/x]))) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s, s)$.
- From the second premise we get $(\delta\sigma', \gamma_1 v_1, \gamma_2 v_2) \in \mathbf{E}_W(G)(s, s)$.
- As a consequence of this, there is $s' \sqsupseteq_{\text{pub}} s$ such that:
 1. $(\delta\sigma', \gamma_1 v_1, \gamma_2 v_2) \in \overline{G(s')}$
 2. $(h_1, h_2) \in W.H(s')(G(s'))$
- Let $\gamma'_1 := \gamma_1, x \mapsto \gamma_1 v_1$ and $\gamma'_2 := \gamma_2, x \mapsto \gamma_2 v_2$.
- By monotonicity and (1) we have $\gamma' \in \text{Env}(\delta(\Gamma, x:\sigma'), G(s'))$.
- The first premise then yields $(\delta\sigma, \gamma'_1 e_1, \gamma'_2 e_2) \in \mathbf{E}_W(G)(s', s')$.
- By Lemma 7 we get $(\delta\sigma, \gamma'_1 e_1, \gamma'_2 e_2) \in \mathbf{E}_W(G)(s, s')$.
- This implies $(\delta\sigma, (h_1, h_1^F, \gamma_1(e_1[v_1/x])), (h_2, h_2^F, \gamma_2(e_2[v_2/x]))) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s, s')$.
- We are done by Lemma 4 and (2).

□

3.3 Expansion

Theorem 61.

$$\frac{\Delta; \Gamma \vdash e'_1 \sim e'_2 : \sigma \quad \forall h, \gamma. h, \gamma e_1 \hookrightarrow^* h, \gamma e'_1 \quad \forall h, \gamma. h, \gamma e_2 \hookrightarrow^* h, \gamma e'_2}{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma}$$

Proof. By Lemma 16 it suffices to show:

$$\frac{\Delta; \Gamma \vdash e'_1 \sim_W e'_2 : \sigma \quad \forall h, \gamma. h, \gamma e_1 \hookrightarrow^* h, \gamma e'_1 \quad \forall h, \gamma. h, \gamma e_2 \hookrightarrow^* h, \gamma e'_2}{\Delta; \Gamma \vdash e_1 \sim_W e_2 : \sigma}$$

This boils down to showing

$$(\delta\sigma, (h_1, h_1^F, \gamma_1 e_1), (h_2, h_2^F, \gamma_2 e_2)) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s, s)$$

in a context where the premise provides

$$(\delta\sigma, (h_1, h_1^F, \gamma_1 e'_1), (h_2, h_2^F, \gamma_2 e'_2)) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s, s).$$

Using the side condition, we are done by Lemma 4.

□

3.4 Beta Law

Theorem 62.

$$\frac{\Delta; \Gamma, x:\sigma' \vdash e_1 \sim e_2 : \sigma \quad \Delta; \Gamma \vdash v_1 \sim v_2 : \sigma'}{\Delta; \Gamma \vdash (\lambda x. e_1) v_1 \sim e_2[v_2/x] : \sigma}$$

Proof. From the premises and Theorem 60 we know $\Delta; \Gamma \vdash e_1[v_1/x] \sim e_2[v_2/x] : \sigma$. Thus the conclusion holds by Theorem 61. \square

3.5 Awkward Example

$$\begin{aligned} \tau &:= (\text{unit} \rightarrow \text{unit}) \rightarrow \text{int} \\ v_1 &:= \lambda f. f \langle \rangle; 1 \\ e_2 &:= \text{let } x = \text{ref } 0 \text{ in} \\ &\quad \lambda f. x := 1; f \langle \rangle; !x \end{aligned}$$

We show $\cdot; \cdot \vdash v_1 \sim e_2 : \tau$. So let \mathcal{N} be given. The proof splits conceptually into three parts:

1. Constructing a local world \hat{w} with $\hat{w}.\mathbf{N} \subseteq \mathcal{N}$, $\text{stable}(\hat{w})$, and $\text{inhabited}(\hat{w}\uparrow)$.
2. Showing $\text{consistent}(\hat{w}\uparrow)$. This is the meat of the proof.
3. Showing that v_1 and e_2 are related by $\mathbf{E}_{\hat{w}\uparrow}$.

Constructing the world. First, we define $w \in \text{LWorld}$ as follows:

$$\begin{aligned} w.\mathbf{N} &:= \emptyset \\ w.\mathbf{S} &:= \text{Loc} \times \{0, 1\} \\ w.\sqsupseteq &:= w.\sqsupseteq_{\text{pub}} \\ w.\sqsupseteq_{\text{pub}} &:= \{((\ell, 1), (\ell, 0)) \mid \ell \in \text{Loc}\}^* \\ w.\mathbf{L} &:= \lambda_{s_{\text{rf}}, (\ell, n), R}. \{((\text{unit} \rightarrow \text{unit}) \rightarrow \text{int}, v_1, (\lambda f. \ell := 1; f \langle \rangle; !\ell))\} \\ w.\mathbf{H} &:= \lambda_{s_{\text{rf}}, (\ell, n), R}. \{\emptyset, [\ell \mapsto n]\} \end{aligned}$$

Now let $\hat{w} = \mathbf{G}(\lambda \mathcal{N}. w)(\mathcal{N})$. By definition of \mathbf{G} we have $\hat{w}.\mathbf{N} \subseteq \mathcal{N}$. Furthermore, by Lemmas 58 and 59 we know $\text{stable}(\hat{w})$ and $\text{inhabited}(\hat{w}\uparrow)$.

Showing consistency. In order to show $\text{consistent}(\hat{w}\uparrow)$, it suffices by Lemma 58 to just show $\text{consistent}(w\uparrow)$.

- So suppose $(s_{\text{rf}}, (\ell, n)) \in w\uparrow.\mathbf{S}$ and $(v'_1, v'_2) \in \overline{G(s_{\text{rf}}, (\ell, n))}(\text{unit} \rightarrow \text{unit})$.
- We need to show:

$$((v'_1 \langle \rangle; 1), (\ell := 1; v'_2 \langle \rangle; !\ell)) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{rf}}, (\ell, n)), (s_{\text{rf}}, (\ell, n)))(\text{int})$$

- So suppose $\text{defined}(h_1 \uplus h_1^{\text{F}})$ and $\text{defined}(h_2 \uplus h_2^{\text{F}})$ as well as

$$(h_1, h_2) \in w\uparrow.\mathbf{H}(s_{\text{rf}}, (\ell, n))(G(s_{\text{rf}}, (\ell, n))).$$

- Then there are $(h_1^{\text{ref}}, h_2^{\text{ref}}) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}})(G(s_{\text{rf}}, (\ell, n)))$ such that $h_1 = h_1^{\text{ref}}$ and $h_2 = h_2^{\text{ref}} \uplus [\ell \mapsto n]$.
- Therefore we know:

$$h_2 \uplus h_2^{\text{F}}, (\ell := 1; v'_2 \langle \rangle; !\ell) \hookrightarrow h_2^{\text{ref}} \uplus [\ell \mapsto 1] \uplus h_2^{\text{F}}, (v'_2 \langle \rangle; !\ell)$$

- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $s' \sqsupseteq (\ell, n)$ such that:

1. $(h_1^{\text{ref}}, h_2^{\text{ref}} \uplus [\ell \mapsto 1]) \in w\uparrow.\mathbf{H}(s_{\text{rf}}, s')(G(s_{\text{rf}}, s'))$
2. $(v'_1, v'_2) \in \overline{G(s_{\text{rf}}, s')}(\mathbf{unit} \rightarrow \mathbf{unit})$
3. $(\langle \rangle, \langle \rangle) \in \overline{G(s_{\text{rf}}, s')}(\mathbf{unit})$
4. $\forall (s'_{\text{rf}}, s'') \sqsupseteq_{\text{pub}} (s_{\text{rf}}, s'). \forall G' \geq G. ((\bullet; 1), (\bullet; !\ell)) \in \mathbf{K}_{w\uparrow}(G')((s_{\text{rf}}, (\ell, n)), (s'_{\text{rf}}, s''))(\mathbf{unit}, \mathbf{int})$

- We pick $s' = (\ell, 1) \sqsupseteq (\ell, n)$.
- (1) follows from monotonicity and $(\emptyset, [\ell \mapsto 1]) \in w.\mathbf{H}(s')(G(s'))$, which holds by construction.
- As (2) holds by monotonicity, and (3) is immediate, it remains to show (4).
- So suppose $(s'_{\text{rf}}, s'') \sqsupseteq_{\text{pub}} (s_{\text{rf}}, s')$ and $G' \geq G$.
- Then necessarily $s'' = s'$.
- We must show $((\langle \rangle; 1), (\langle \rangle; !\ell)) \in \mathbf{E}_{w\uparrow}(G')((s_{\text{rf}}, (\ell, n)), (s'_{\text{rf}}, s''))(\mathbf{int})$.
- So suppose defined $(h'_1 \uplus h_1^{\text{F}'})$ and defined $(h'_2 \uplus h_2^{\text{F}'})$ as well as $(h'_1, h'_2) \in w\uparrow.\mathbf{H}(s'_{\text{rf}}, s'')(G'(s'_{\text{rf}}, s''))$.
- Then there are $h_1^{\text{ref}}, h_2^{\text{ref}}$ such that $h'_1 = h_1^{\text{ref}}$ and $h'_2 = h_2^{\text{ref}} \uplus [\ell \mapsto 1]$.
- Therefore we know:

$$h'_2 \uplus h_2^{\text{F}'}, (\langle \rangle; !\ell) \hookrightarrow^* h'_2 \uplus h_2^{\text{F}'}, 1$$

- Of course we also know:

$$h'_1 \uplus h_1^{\text{F}'}, (\langle \rangle; 1) \hookrightarrow^* h'_1 \uplus h_1^{\text{F}'}, 1$$

- Since $(s'_{\text{rf}}, s'') \sqsupseteq_{\text{pub}} (s_{\text{rf}}, (\ell, n))$, it suffices by definition of $\mathbf{E}_{w\uparrow}$ to show $(1, 1) \in \overline{G'(s'_{\text{rf}}, s'')}(\mathbf{int})$, which is immediate.

Proving the programs related. It remains to show $(v_1, e_2) \in \mathbf{E}_{\widehat{w}\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\tau)$ for any G, s_{rf}, s .

- So suppose $(h_1, h_2) \in \widehat{w}\uparrow.\mathbf{H}(s_{\text{rf}}, s)(G(s_{\text{rf}}, s))$ as well as defined $(h_1 \uplus h_1^{\text{F}})$ and defined $(h_2 \uplus h_2^{\text{F}})$.
- Then there are

$$(h_1^{\text{ref}}, h_2^{\text{ref}}) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}})(G(s_{\text{rf}}, s)) \text{ and } (\widehat{h}_1, \widehat{h}_2) \in \widehat{w}.\mathbf{H}(s_{\text{rf}})(s)(G(s_{\text{rf}}, s))$$

with $h_1 = h_1^{\text{ref}} \uplus \widehat{h}_1$ and $h_2 = h_2^{\text{ref}} \uplus \widehat{h}_2$.

- Hence we have $h_2 \uplus h_2^{\text{F}}, e_2 \hookrightarrow h_2^{\text{ref}} \uplus \widehat{h}_2 \uplus [\ell \mapsto 0] \uplus h_2^{\text{F}}, v_2$, where $v_2 = \lambda f. \ell := 1; f \langle \rangle; !\ell$ and ℓ is fresh.
- We are done if we can find $s' \sqsupseteq_{\text{pub}} s$ such that:

1. $(h_1^{\text{ref}} \uplus \widehat{h}_1, h_2^{\text{ref}} \uplus \widehat{h}_2 \uplus [\ell \mapsto 0]) \in \widehat{w}\uparrow.\mathbf{H}(s_{\text{rf}}, s')(G(s_{\text{rf}}, s'))$
2. $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s')}(\tau)$

- We pick $s' = (s, (\ell, 0)) \sqsupseteq_{\text{pub}} s$.
- To show (1), it suffices by monotonicity to show $(\widehat{h}_1, \widehat{h}_2 \uplus [\ell \mapsto 0]) \in \widehat{w}.\mathbf{H}(s_{\text{rf}})(s')(G(s_{\text{rf}}, s'))$.
- By monotonicity and construction of \widehat{w} it then suffices to show $(\emptyset, [\ell \mapsto 0]) \in w.\mathbf{H}(s_{\text{rf}})(\ell, 0)(G(s_{\text{rf}}, s'))$, which holds by construction of w .
- To show (2) it suffices by definition of GK to show $(v_1, v_2) \in \widehat{w}\uparrow.\mathbf{L}(s_{\text{rf}}, s')(G(s_{\text{rf}}, s'))(\tau)$.
- By construction of \widehat{w} it then suffices to show $(v_1, v_2) \in w.\mathbf{L}(\ell, 0)(G(s_{\text{rf}}, s'))(\tau)$, which also holds by construction of w .

3.6 Well-Bracketed State Change

$$\begin{aligned}
\tau &:= (\text{unit} \rightarrow \text{unit}) \rightarrow \text{int} \\
v_1 &:= \lambda f. f \langle \rangle; f \langle \rangle; 1 \\
e_2 &:= \text{let } x = \text{ref } 0 \text{ in} \\
&\quad \lambda f. x := 0; f \langle \rangle; x := 1; f \langle \rangle; !x
\end{aligned}$$

We show $\cdot; \cdot \vdash v_1 \sim e_2 : \tau$. So let \mathcal{N} be given. The proof splits conceptually into three parts:

1. Constructing a local world \widehat{w} with $\widehat{w}.\mathbf{N} \subseteq \mathcal{N}$, $\text{stable}(\widehat{w})$, and $\text{inhabited}(\widehat{w}\uparrow)$.
2. Showing $\text{consistent}(\widehat{w}\uparrow)$. This is the meat of the proof.
3. Showing that v_1 and e_2 are related by $\mathbf{E}_{\widehat{w}\uparrow}$.

Constructing the world. First, we define $w \in \text{LWorld}$ as follows:

$$\begin{aligned}
w.\mathbf{N} &:= \emptyset \\
w.\mathbf{S} &:= \text{Loc} \times \{0, 1\} \\
w.\sqsupseteq &:= w.\sqsupseteq_{\text{pub}} \cup \{((\ell, 0), (\ell, 1)) \mid \ell \in \text{Loc}\} \\
w.\sqsupseteq_{\text{pub}} &:= \{((\ell, 1), (\ell, 0)) \mid \ell \in \text{Loc}\}^* \\
w.\mathbf{L} &:= \lambda s_{\text{rf}}, (\ell, n), R. \{((\text{unit} \rightarrow \text{unit}) \rightarrow \text{int}, v_1, (\lambda f. \ell := 0; f \langle \rangle; \ell := 1; f \langle \rangle; !\ell))\} \\
w.\mathbf{H} &:= \lambda s_{\text{rf}}, (\ell, n), R. \{\emptyset, [\ell \mapsto n]\}
\end{aligned}$$

Now let $\widehat{w} = \mathbf{G}(\lambda \mathcal{N}. w)(\mathcal{N})$. By definition of \mathbf{G} we have $\widehat{w}.\mathbf{N} \subseteq \mathcal{N}$. Furthermore, by Lemmas 58 and 59 we know $\text{stable}(\widehat{w})$ and $\text{inhabited}(\widehat{w}\uparrow)$.

Showing consistency. In order to show $\text{consistent}(\widehat{w}\uparrow)$, it suffices by Lemma 58 to just show $\text{consistent}(w\uparrow)$.

- So suppose $(s_{\text{rf}}, (\ell, n)) \in w\uparrow.\mathbf{S}$ and $(v'_1, v'_2) \in \overline{G(s_{\text{rf}}, (\ell, n))}(\text{unit} \rightarrow \text{unit})$.
- We need to show:

$$((v'_1 \langle \rangle; v'_1 \langle \rangle; 1), (\ell := 0; v'_2 \langle \rangle; \ell := 1; v'_2 \langle \rangle; !\ell)) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{rf}}, (\ell, n)), (s_{\text{rf}}, (\ell, n)))(\text{int})$$

- So suppose defined($h_1 \uplus h_1^{\text{F}}$) and defined($h_2 \uplus h_2^{\text{F}}$) as well as

$$(h_1, h_2) \in w\uparrow.\mathbf{H}(s_{\text{rf}}, (\ell, n))(G(s_{\text{rf}}, (\ell, n))).$$

- Then there are $(h_1^{\text{ref}}, h_2^{\text{ref}}) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}})(G(s_{\text{rf}}, (\ell, n)))$ such that $h_1 = h_1^{\text{ref}}$ and $h_2 = h_2^{\text{ref}} \uplus [\ell \mapsto n]$.
- Therefore we know:

$$h_2 \uplus h_2^{\text{F}}, (\ell := 0; v'_2 \langle \rangle; \ell := 1; v'_2 \langle \rangle; !\ell) \hookrightarrow h_2^{\text{ref}} \uplus [\ell \mapsto 0] \uplus h_2^{\text{F}}, (v'_2 \langle \rangle; \ell := 1; v'_2 \langle \rangle; !\ell)$$

- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $s' \sqsupseteq (\ell, n)$ such that:

1. $(h_1^{\text{ref}}, h_2^{\text{ref}} \uplus [\ell \mapsto 0]) \in w\uparrow.\mathbf{H}(s_{\text{rf}}, s')(G(s_{\text{rf}}, s'))$
2. $(v'_1, v'_2) \in \overline{G(s_{\text{rf}}, s')}(\text{unit} \rightarrow \text{unit})$
3. $(\langle \rangle, \langle \rangle) \in \overline{G(s_{\text{rf}}, s')}(\text{unit})$
4. $\forall (s'_{\text{rf}}, \tilde{s}') \sqsupseteq_{\text{pub}} (s_{\text{rf}}, s'). \forall G' \geq G. ((\bullet; v'_1 \langle \rangle; 1), (\bullet; \ell := 1; v'_2 \langle \rangle; !\ell)) \in \mathbf{K}_{w\uparrow}(G')((s_{\text{rf}}, (\ell, n)), (s'_{\text{rf}}, \tilde{s}'))(\text{unit}, \text{int})$

- We pick $s' = (\ell, 0) \sqsupseteq (\ell, n)$.

- (1) follows from monotonicity and $(\emptyset, [\ell \mapsto 1]) \in w.\mathbf{H}(s_{\text{rf}})(s')(G(s_{\text{rf}}, s'))$, which holds by construction.
- As (2) holds by monotonicity, and (3) is immediate, it remains to show (4).
- So suppose $(s'_{\text{rf}}, \tilde{s}') \sqsupseteq_{\text{pub}} (s_{\text{rf}}, s')$ and $G' \geq G$.
- We need to show:

$$((\langle \rangle; v'_1 \langle \rangle; 1), (\langle \rangle; \ell := 1; v'_2 \langle \rangle; !\ell)) \in \mathbf{E}_{w\uparrow}(G')((s_{\text{rf}}, (\ell, n)), (s'_{\text{rf}}, \tilde{s}'))(\text{int})$$

- So suppose defined $(h'_1 \uplus h_1^{F'})$ and defined $(h'_2 \uplus h_2^{F'})$ as well as

$$(h'_1, h'_2) \in w\uparrow.\mathbf{H}(s'_{\text{rf}}, \tilde{s}')(G'(s'_{\text{rf}}, \tilde{s}')).$$

- Then there are $(h_1^{\text{ref}}, h_2^{\text{ref}}) \in W_{\text{ref}}.\mathbf{H}(s'_{\text{rf}})(G'(s'_{\text{rf}}, \tilde{s}'))$ such that $h'_1 = h_1^{\text{ref}}$ and $h'_2 = h_2^{\text{ref}} \uplus [\ell \mapsto n']$.
- Therefore we know:

$$\begin{aligned} h'_1 \uplus h_1^{F'}, (\langle \rangle; v'_1 \langle \rangle; 1) &\hookrightarrow h_1^{\text{ref}} \uplus h_1^{F'}, (v'_1 \langle \rangle; 1) \\ h'_2 \uplus h_2^{F'}, (\langle \rangle; \ell := 1; v'_2 \langle \rangle; !\ell) &\hookrightarrow h_2^{\text{ref}} \uplus [\ell \mapsto 1] \uplus h_2^{F'}, (v'_2 \langle \rangle; !\ell) \end{aligned}$$

- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $s'' \sqsupseteq \tilde{s}'$ such that:

1. $(h_1^{\text{ref}}, h_2^{\text{ref}} \uplus [\ell \mapsto 1]) \in w\uparrow.\mathbf{H}(s'_{\text{rf}}, s'')(G'(s'_{\text{rf}}, s''))$
2. $(v'_1, v'_2) \in \overline{G'(s'_{\text{rf}}, s'')(\text{unit} \rightarrow \text{unit})}$
3. $(\langle \rangle, \langle \rangle) \in \overline{G'(s'_{\text{rf}}, s'')(\text{unit})}$
4. $\forall (s''_{\text{rf}}, \tilde{s}'') \sqsupseteq_{\text{pub}} (s'_{\text{rf}}, s''). \forall G'' \geq G'. ((\bullet; 1), (\bullet; !\ell)) \in \mathbf{K}_{w\uparrow}(G'')((s_{\text{rf}}, (\ell, n)), (s''_{\text{rf}}, \tilde{s}''))(\text{unit}, \text{int})$

- We pick $s'' = (\ell, 1) \sqsupseteq \tilde{s}'$.
- (1) follows from monotonicity and $(\emptyset, [\ell \mapsto 1]) \in w.\mathbf{H}(s_{\text{rf}})(s')(G'(s'))$, which holds by construction.
- As (2) holds by monotonicity, and (3) is immediate, it remains to show (4).
- So suppose $(s''_{\text{rf}}, \tilde{s}'') \sqsupseteq_{\text{pub}} (s'_{\text{rf}}, s'')$ and $G'' \geq G'$.

- Then necessarily $\tilde{s}'' = s''$.
- We must show $((\langle \rangle; 1), (\langle \rangle; !\ell)) \in \mathbf{E}_{w\uparrow}(G'')((s_{\text{rf}}, (\ell, n)), (s''_{\text{rf}}, s''))(\text{int})$.
- So suppose defined $(h''_1 \uplus h_1^{F''})$ and defined $(h''_2 \uplus h_2^{F''})$ as well as $(h''_1, h''_2) \in w\uparrow.\mathbf{H}(s''_{\text{rf}}, s'')(G''(s''_{\text{rf}}, s''))$.
- Then there are $h_1^{\text{ref}}, h_2^{\text{ref}}$ such that $h''_1 = h_1^{\text{ref}}$ and $h''_2 = h_2^{\text{ref}} \uplus [\ell \mapsto 1]$.

- Therefore we know:

$$h''_2 \uplus h_2^{F''}, (\langle \rangle; !\ell) \hookrightarrow^* h_2^{\text{ref}} \uplus h_2^{F''}, 1$$

- Of course we also know:

$$h''_1 \uplus h_1^{F''}, (\langle \rangle; 1) \hookrightarrow^* h_1^{\text{ref}} \uplus h_1^{F''}, 1$$

- Since $(s''_{\text{rf}}, s'') \sqsupseteq_{\text{pub}} (s_{\text{rf}}, (\ell, n))$, it suffices by definition of $\mathbf{E}_{w\uparrow}$ to show $(1, 1) \in \overline{G''(s''_{\text{rf}}, s'')(\text{int})}$, which is immediate.

Proving the programs related. It remains to show $(v_1, e_2) \in \mathbf{E}_{\widehat{w}\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\tau)$ for any G, s_{rf}, s .

- So suppose $(h_1, h_2) \in \widehat{w}\uparrow.\mathbf{H}(s_{\text{rf}}, s)(G(s_{\text{rf}}, s))$ as well as $\text{defined}(h_1 \uplus h_1^{\text{F}})$ and $\text{defined}(h_2 \uplus h_2^{\text{F}})$.
- Then there are

$$(h_1^{\text{ref}}, h_2^{\text{ref}}) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}})(G(s_{\text{rf}}, s)) \text{ and } (\widehat{h}_1, \widehat{h}_2) \in \widehat{w}.\mathbf{H}(s_{\text{rf}})(s)(G(s_{\text{rf}}, s))$$

with $h_1 = h_1^{\text{ref}} \uplus \widehat{h}_1$ and $h_2 = h_2^{\text{ref}} \uplus \widehat{h}_2$.

- Hence we have $h_2 \uplus h_2^{\text{F}}, e_2 \hookrightarrow h_2^{\text{ref}} \uplus \widehat{h}_2 \uplus [\ell \mapsto 0] \uplus h_2^{\text{F}}, v_2$, where $v_2 = \lambda f. \ell := 0; f \langle \rangle; \ell := 1; f \langle \rangle; !\ell$ and ℓ is fresh.
- We are done if we can find $s' \sqsupseteq_{\text{pub}} s$ such that:

1. $(h_1^{\text{ref}} \uplus \widehat{h}_1, h_2^{\text{ref}} \uplus \widehat{h}_2 \uplus [\ell \mapsto 0]) \in \widehat{w}\uparrow.\mathbf{H}(s_{\text{rf}}, s')(G(s_{\text{rf}}, s'))$
2. $(v_1, v_2) \in \overline{G}(s_{\text{rf}}, s')(\tau)$

- We pick $s' = (s, (\ell, 0)) \sqsupseteq_{\text{pub}} s$.
- To show (1), it suffices by monotonicity to show $(\widehat{h}_1, \widehat{h}_2 \uplus [\ell \mapsto 0]) \in \widehat{w}.\mathbf{H}(s_{\text{rf}})(s')(G(s_{\text{rf}}, s'))$.
- By monotonicity and construction of \widehat{w} it then suffices to show $(\emptyset, [\ell \mapsto 0]) \in w.\mathbf{H}(s_{\text{rf}})(\ell, 0)(G(s_{\text{rf}}, s'))$, which holds by construction of w .
- To show (2) it suffices by definition of GK to show $(v_1, v_2) \in \widehat{w}\uparrow.\mathbf{L}(s_{\text{rf}}, s')(G(s_{\text{rf}}, s'))(\tau)$.
- By construction of \widehat{w} it then suffices to show $(v_1, v_2) \in w.\mathbf{L}(s_{\text{rf}})(\ell, 0)(G(s_{\text{rf}}, s'))(\tau)$, which also holds by construction of w .

3.7 Twin Abstraction

$$\begin{aligned} \tau &:= \exists \alpha. \exists \beta. (\text{unit} \rightarrow \alpha) \times (\text{unit} \rightarrow \beta) \times (\alpha \times \beta \rightarrow \text{bool}) \\ e_1 &:= \text{let } x = \text{ref } 0 \text{ in pack } \langle \text{int}, \text{pack } \langle \text{int}, \lambda_. x := !x + 1; !x, \\ &\quad \lambda_. x := !x + 1; !x, \\ &\quad \lambda p. p.1 = p.2 \rangle \rangle \\ e_2 &:= \text{let } x = \text{ref } 0 \text{ in pack } \langle \text{int}, \text{pack } \langle \text{int}, \lambda_. x := !x + 1; !x, \\ &\quad \lambda_. x := !x + 1; !x, \\ &\quad \lambda p. \text{ff} \rangle \rangle \end{aligned}$$

We show $;\cdot \vdash e_1 \sim e_2 : \tau$. So let \mathcal{N} be given. The proof splits conceptually into three parts:

1. Constructing a world w with $w.\mathbf{N} \subseteq \mathcal{N}$, $\text{stable}(w)$, and $\text{inhabited}(w\uparrow)$.
2. Showing $\text{consistent}(w\uparrow)$. This is the meat of the proof.
3. Showing that e_1 and e_2 are related by $\mathbf{E}_{w\uparrow}$.

Constructing the world. First, we define $\mathcal{W} \in \text{NLWorld}$ as follows:

$$\begin{aligned} \mathcal{W}(\mathcal{N}').\mathbf{N} &:= \{\mathcal{N}'(1), \mathcal{N}'(2)\} \\ \mathcal{W}(\mathcal{N}').\mathbf{S} &:= \{(\ell_1, \ell_2, S_1, S_2) \in \text{Loc} \times \text{Loc} \times \mathbb{P}(\mathbb{N}_{>0}) \times \mathbb{P}(\mathbb{N}_{>0}) \mid S_1 \cap S_2 = \emptyset\} \\ \mathcal{W}(\mathcal{N}').\sqsupseteq &:= \mathcal{W}(\mathcal{N}').\sqsupseteq_{\text{pub}} \\ \mathcal{W}(\mathcal{N}').\sqsupseteq_{\text{pub}} &:= \{((\ell'_1, \ell'_2, S'_1, S'_2), (\ell_1, \ell_2, S_1, S_2)) \mid \ell_1 = \ell'_1 \wedge \ell_2 = \ell'_2 \wedge S_1 \subseteq S'_1 \wedge S_2 \subseteq S'_2\} \\ \mathcal{W}(\mathcal{N}').\mathbf{L} &:= \lambda(\ell_1, \ell_2, S_1, S_2), R. \{(\mathcal{N}'(1), n, n) \mid n \in S_1\} \uplus \{(\mathcal{N}'(2), n, n) \mid n \in S_2\} \uplus \\ &\quad \{((\text{unit} \rightarrow \mathcal{N}'(1)), (\lambda_. \ell_1 := !\ell_1 + 1; !\ell_1), (\lambda_. \ell_1 := !\ell_1 + 1; !\ell_1))\} \uplus \\ &\quad \{((\text{unit} \rightarrow \mathcal{N}'(2)), (\lambda_. \ell_2 := !\ell_2 + 1; !\ell_2), (\lambda_. \ell_2 := !\ell_2 + 1; !\ell_2))\} \uplus \\ &\quad \{((\mathcal{N}'(1) \times \mathcal{N}'(2) \rightarrow \text{bool}), (\lambda p. p.1 = p.2), (\lambda p. \text{ff}))\} \\ \mathcal{W}(\mathcal{N}').\mathbf{H} &:= \lambda(\ell_1, \ell_2, S_1, S_2), R. \{([\ell_1 \mapsto n], [\ell_2 \mapsto n]) \mid n = \max(\{0\} \uplus S_1 \uplus S_2)\} \end{aligned}$$

where $\mathcal{N}'(1)$ and $\mathcal{N}'(2)$ denote two distinct elements of \mathcal{N}' .

Now let $w = \mathbf{G}(\mathcal{W})(\mathcal{N})$. By definition of \mathbf{G} we have $w.N \subseteq \mathcal{N}$. Furthermore, by Lemmas 58 and 59 we know $\text{stable}(w)$ and $\text{inhabited}(w\uparrow)$.

Showing consistency. In order to show $\text{consistent}(w\uparrow)$, it suffices by Lemma 58 to just show $\text{consistent}(\mathcal{W}(\mathcal{N}')\uparrow)$ for any \mathcal{N}' . This decomposes into the following subgoals (for any $G, s_{\text{rf}}, s = (\ell_1, \ell_2, S_1, S_2)$):

1. $((\ell_1 := !\ell_1 + 1; !\ell_1), (\ell_1 := !\ell_1 + 1; !\ell_1)) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}')\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\mathcal{N}'(1))$
2. $((\ell_2 := !\ell_2 + 1; !\ell_2), (\ell_2 := !\ell_2 + 1; !\ell_2)) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}')\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\mathcal{N}'(2))$
3. $\forall (v'_1, v'_2) \in \overline{G(s_{\text{rf}}, s)}(\mathcal{N}'(1) \times \mathcal{N}'(2)). (v'_1.1 = v'_1.2, \text{ff}) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}')\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\text{bool})$

For (1) (part (2) is analogously):

- Suppose $(h_1, h_2) \in \mathcal{W}(\mathcal{N}')\uparrow.H(s_{\text{rf}}, s)(G(s_{\text{rf}}, s))$ as well as $\text{defined}(h_1 \uplus h_1^{\text{F}})$ and $\text{defined}(h_2 \uplus h_2^{\text{F}})$.
- Then there are

$$(h_1^{\text{ref}}, h_2^{\text{ref}}) \in W_{\text{ref}}.H(s_{\text{rf}})(G(s_{\text{rf}}, s)) \text{ and } (h_1^{\circ}, h_2^{\circ}) \in \mathcal{W}(\mathcal{N}').H(s_{\text{rf}})(s)(G(s_{\text{rf}}, s))$$

with $h_1 = h_1^{\text{ref}} \uplus h_1^{\circ}$ and $h_2 = h_2^{\text{ref}} \uplus h_2^{\circ}$.

- By construction of $\mathcal{W}(\mathcal{N}')$ we know $h_1^{\circ} = [\ell_1 \mapsto n]$ and $h_2^{\circ} = [\ell_2 \mapsto n]$ where $n = \max(\{0\} \uplus S_1 \uplus S_2)$.

- Hence $h_1 \uplus h_1^{\text{F}}, (\ell_1 := !\ell_1 + 1; !\ell_1) \hookrightarrow^* h_1^{\text{ref}} \uplus [\ell_1 \mapsto n + 1] \uplus h_1^{\text{F}}, n + 1$
and $h_2 \uplus h_2^{\text{F}}, (\ell_2 := !\ell_2 + 1; !\ell_2) \hookrightarrow^* h_2^{\text{ref}} \uplus [\ell_2 \mapsto n + 1] \uplus h_2^{\text{F}}, n + 1$.

- By definition of $\mathbf{E}_{\mathcal{W}(\mathcal{N}')\uparrow}$ it suffices to find $s' \sqsupseteq_{\text{pub}} s$ such that:

- a) $(h_1^{\text{ref}} \uplus [\ell_1 \mapsto n + 1], h_1^{\text{ref}} \uplus [\ell_2 \mapsto n + 1]) \in \mathcal{W}(\mathcal{N}')\uparrow.H(s_{\text{rf}}, s')(G(s_{\text{rf}}, s'))$
- b) $(n + 1, n + 1) \in \overline{G(s_{\text{rf}}, s')}(\mathcal{N}'(1))$

- We pick $s' = (\ell_1, \ell_2, S_1 \uplus \{n + 1\}, S_2)$.

- Note that $n + 1 \notin S_1 \cup S_2$ and thus $(S_1 \uplus \{n + 1\}) \cap S_2 = \emptyset$, so s' is well-formed.

- Since $n + 1 = \max(\{0\} \uplus S_1 \uplus \{n + 1\} \uplus S_2)$, (a) follows from $([\ell_1 \mapsto n + 1], [\ell_2 \mapsto n + 1]) \in \mathcal{W}(\mathcal{N}').H(s_{\text{rf}})(s')(G(s_{\text{rf}}, s'))$ by construction of $\mathcal{W}(\mathcal{N}')$.

- To show (b) it suffices, by definition of GK, to show

$$(n + 1, n + 1) \in \mathcal{W}(\mathcal{N}')\uparrow.L(s_{\text{rf}}, s')(G(s_{\text{rf}}, s'))(\mathcal{N}'(1)).$$

- This follows from

$$(n + 1, n + 1) \in \mathcal{W}(\mathcal{N}').L(s_{\text{rf}})(s')(G(s_{\text{rf}}, s'))(\mathcal{N}'(1)),$$

which in turns holds by construction of $\mathcal{W}(\mathcal{N}')$.

For (3):

- Suppose $(v'_1, v'_2) \in \overline{G(s_{\text{rf}}, s)}(\mathcal{N}'(1) \times \mathcal{N}'(2))$.
- Then $v'_1 = \langle \widehat{v}_1, \widetilde{v}_1 \rangle$ and $v'_2 = \langle \widehat{v}_2, \widetilde{v}_2 \rangle$ with $(\widehat{v}_1, \widehat{v}_2) \in \overline{G(s_{\text{rf}}, s)}(\mathcal{N}'(1))$ and $(\widetilde{v}_1, \widetilde{v}_2) \in \overline{G(s_{\text{rf}}, s)}(\mathcal{N}'(2))$.
- By definition of GK and construction of $\mathcal{W}(\mathcal{N}')$ we know $\widehat{v}_1 = \widehat{v}_2 \in S_1$ and $\widetilde{v}_1 = \widetilde{v}_2 \in S_2$.
- Now suppose $(h_1, h_2) \in \mathcal{W}(\mathcal{N}')\uparrow.H(s_{\text{rf}}, s)(G(s_{\text{rf}}, s))$ as well as $\text{defined}(h_1 \uplus h_1^{\text{F}})$ and $\text{defined}(h_2 \uplus h_2^{\text{F}})$.
- Since $S_1 \cap S_2 = \emptyset$, we get $h_1 \uplus h_1^{\text{F}}, v'_1.1 = v'_1.2 \hookrightarrow^* h_1 \uplus h_1^{\text{F}}, \text{ff}$ and $h_2 \uplus h_2^{\text{F}}, \text{ff} \hookrightarrow^* h_2 \uplus h_2^{\text{F}}, \text{ff}$.
- Since $(\text{ff}, \text{ff}) \in \overline{G(s_{\text{rf}}, s)}(\text{bool})$, we are done.

Proving the programs related. It remains to show $(e_1, e_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{rf}}, s), (s_{\text{rf}}, s))(\tau)$ for any G, s_{rf}, s .

- So suppose $(h_1, h_2) \in w\uparrow.\mathbf{H}(s_{\text{rf}}, s)(G(s_{\text{rf}}, s))$ as well as defined $(h_1 \uplus h_1^{\text{F}})$ and defined $(h_2 \uplus h_2^{\text{F}})$.
- Then there are

$$(h_1^{\text{ref}}, h_2^{\text{ref}}) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}})(G(s_{\text{rf}}, s)) \text{ and } (\widehat{h}_1, \widehat{h}_2) \in w.\mathbf{H}(s_{\text{rf}})(s)(G(s_{\text{rf}}, s))$$

with $h_1 = h_1^{\text{ref}} \uplus \widehat{h}_1$ and $h_2 = h_2^{\text{ref}} \uplus \widehat{h}_2$.

- Hence we have

$$h_1 \uplus h_1^{\text{F}}, e_1 \hookrightarrow h_1^{\text{ref}} \uplus \widehat{h}_1 \uplus [\ell_1 \mapsto 0] \uplus h_1^{\text{F}}, \text{pack pack } v_1 \text{ and } h_2 \uplus h_2^{\text{F}}, e_2 \hookrightarrow h_2^{\text{ref}} \uplus \widehat{h}_2 \uplus [\ell_2 \mapsto 0] \uplus h_2^{\text{F}}, \text{pack pack } v_2$$

where ℓ_1 and ℓ_2 are fresh and v_1, v_2 are what you think they are.

- We are done if we can find $s' \sqsupseteq_{\text{pub}} s$ such that:

1. $(h_1^{\text{ref}} \uplus \widehat{h}_1 \uplus [\ell_1 \mapsto 0], h_2^{\text{ref}} \uplus \widehat{h}_2 \uplus [\ell_2 \mapsto 0]) \in w\uparrow.\mathbf{H}(s_{\text{rf}}, s')(G(s_{\text{rf}}, s'))$
2. $(v_1, v_2) \in \overline{G(s_{\text{rf}}, s')}(\tau)$

- We pick $s' = (s, (\ell_1, \ell_2, \emptyset, \emptyset)) \sqsupseteq_{\text{pub}} s$.

- To show (1), it suffices by monotonicity to show $(\widehat{h}_1 \uplus [\ell_1 \mapsto 0], \widehat{h}_2 \uplus [\ell_2 \mapsto 0]) \in w.\mathbf{H}(s_{\text{rf}})(s')(G(s_{\text{rf}}, s'))$.

- By monotonicity and construction of w it then suffices to show $([\ell_1 \mapsto 0], [\ell_2 \mapsto 0]) \in \mathcal{W}(\mathcal{N}').\mathbf{H}(s_{\text{rf}})(\ell_1, \ell_2, \emptyset, \emptyset)(G(s_{\text{rf}}, s'))$ (for any \mathcal{N}'), which holds by construction of \mathcal{W} .

- To show (2), we pick the witness types $\mathcal{N}_n(1)$ and $\mathcal{N}_n(2)$, where $n := |s'|$.

- It thus suffices to show:

$$(v_1, v_2) \in \overline{G(s_{\text{rf}}, s')}((\text{unit} \rightarrow \mathcal{N}_n(1)) \times (\text{unit} \rightarrow \mathcal{N}_n(2)) \times (\mathcal{N}_n(1) \times \mathcal{N}_n(2) \rightarrow \text{bool}))$$

- This in turn reduces to showing the following:

- $((\text{unit} \rightarrow \mathcal{N}_n(1)), (\lambda_. \ell_1 := !\ell_1 + 1; !\ell_1), (\lambda_. \ell_1 := !\ell_1 + 1; !\ell_1)) \in \overline{G(s_{\text{rf}}, s')}$
- $((\text{unit} \rightarrow \mathcal{N}_n(2)), (\lambda_. \ell_2 := !\ell_2 + 1; !\ell_2), (\lambda_. \ell_2 := !\ell_2 + 1; !\ell_2)) \in \overline{G(s_{\text{rf}}, s')}$
- $(\mathcal{N}_n(1) \times \mathcal{N}_n(2) \rightarrow \text{bool}), (\lambda p. p.1 = p.2), (\lambda p. \text{ff})) \in \overline{G(s_{\text{rf}}, s')}$

- By definition of GK and construction of w , it suffices to show that these triples are in $\mathcal{W}(\mathcal{N}_n).\mathbf{L}(\ell_1, \ell_2, \emptyset, \emptyset)(G(s_{\text{rf}}, s'))$.

- This is true by construction of \mathcal{W} .

4 Weak Isomorphism Theorem

4.1 Weak Isomorphisms

Definition 6. Assuming $W_1, W_2 \in \text{World}$, then a function $\phi \in W_1.\mathcal{S} \rightarrow \mathbb{P}(W_2.\mathcal{S})$ is a *weak morphism* from W_1 to W_2 , written $\phi : W_1 \rightarrow W_2$, if:

1. $W_1.\mathcal{N} = W_2.\mathcal{N}$
2. $\forall s_1, s'_1. s_1 \sqsubseteq s'_1 \implies \forall s_2 \in \phi(s_1), s'_2 \in \phi(s'_1). s_2 \sqsubseteq s'_2$
3. $\forall s_1, s'_1. s_1 \sqsubseteq_{\text{pub}} s'_1 \implies \forall s_2 \in \phi(s_1), s'_2 \in \phi(s'_1). s_2 \sqsubseteq_{\text{pub}} s'_2$
4. $\forall s_1. \forall s_2 \in \phi(s_1). W_1.\mathcal{L}(s_1) = W_2.\mathcal{L}(s_2)$
5. $\forall s_1. \forall G \in \text{GK}(W_1). W_1.\mathcal{H}(s_1)(G(s_1)) \leq \bigcup_{s_2 \in \phi(s_1)} W_2.\mathcal{H}(s_2)(G(s_1))$

Definition 7. The identity weak morphism id_W on W is defined as $\text{id}_W(s) = \{s\}$. It is obvious that id_W forms a weak morphism.

Definition 8. The composition of weak morphisms $\psi \circ \phi$ is defined as $(\psi \circ \phi)(s) = \bigcup_{s' \in \phi(s)} \psi(s')$. We will show that $\psi \circ \phi$ forms a weak morphism in Lemma 69.

Definition 9. Between two weak morphisms $\phi_1, \phi_2 : W_1 \rightarrow W_2$, we define the following preorders \sqsubseteq and \sqsubseteq_{pub} :

$$\begin{aligned} \phi_1 \sqsupseteq \phi_2 & \quad \text{iff} \quad \forall s. \forall s_1 \in \phi_1(s). \forall s_2 \in \phi_2(s). s_1 \sqsupseteq s_2 \\ \phi_1 \sqsupseteq_{\text{pub}} \phi_2 & \quad \text{iff} \quad \forall s. \forall s_1 \in \phi_1(s). \forall s_2 \in \phi_2(s). s_1 \sqsupseteq_{\text{pub}} s_2 \end{aligned}$$

Definition 10. A pair of weak morphisms $\phi : W_1 \rightarrow W_2, \psi : W_2 \rightarrow W_1$ is a weak isomorphism, written $\phi : W_1 \cong W_2 : \psi$, if $\psi \circ \phi \sqsupseteq_{\text{pub}} \text{id}$ and $\phi \circ \psi \sqsupseteq_{\text{pub}} \text{id}$.

4.2 Global Knowledge Constructions

Recall that for a monotone function $F \in \text{VRelF} \rightarrow \text{VRelF}$ and $R \in \text{VRelF}$, we write $[F]_R^*$ for the least fixpoint of the monotone function $F(-) \cup R$.

Definition 11. Given $\phi : W_1 \rightarrow W_2$ and $G \in \text{GK}(W_2)$, we define $\overleftarrow{G}_\phi \in W_1.\mathcal{S} \rightarrow \text{VRelF}$ as follows.

$$\overleftarrow{G}_\phi(s_1) = [W_1.\mathcal{L}(s_1)]^*_{(\bigcup_{s'_1 \sqsubseteq s_1 \wedge s'_2 \in \phi(s'_1)} G(s'_2))}$$

Definition 12. Given $\phi : W_1 \rightarrow W_2$ and $G \in \text{GK}(W_1)$, we define $\overrightarrow{G}_\phi^{s'_1} \in W_2.\mathcal{S} \rightarrow \text{VRelF}$ for $s_1 \in W_1.\mathcal{S}$ as follows.

$$\overrightarrow{G}_\phi^{s'_1}(s_2) = [W_2.\mathcal{L}(s_2)]^*_{(\bigcup_{s'_1 \sqsubseteq s_1 \wedge s'_2 \sqsubseteq s_2 \wedge s'_2 \in \phi(s'_1)} G(s'_1))}$$

Lemma 63. Given $\phi : W_1 \rightarrow W_2$ and $G \in \text{GK}(W_2)$, we have $\forall s_2 \in \phi(s_1). \overleftarrow{G}_\phi(s_1) = G(s_2)$.

Proof.

- Suppose $s_2 \in \phi(s_1)$.
- We first show $G(s_2) = \bigcup_{s'_1 \sqsubseteq s_1 \wedge s'_2 \in \phi(s'_1)} G(s'_2)$:
 - $G(s_2) \leq \bigcup_{s'_1 \sqsubseteq s_1 \wedge s'_2 \in \phi(s'_1)} G(s'_2)$ is obvious.
 - To see the other inclusion, note that whenever $s'_2 \in \phi(s'_1)$ and $s'_1 \sqsubseteq s_1$, then $s'_2 \sqsubseteq s_2$ and thus $G(s'_2) \leq G(s_2)$.

- Consequently we know $\overleftarrow{G}_\phi(s_1) = [W_1.L(s_1)]_{G(s_2)}^* = W_1.L(s_1)([W_1.L(s_1)]_{G(s_2)}^*) \cup G(s_2) \geq G(s_2)$.
- To show $[W_1.L(s_1)]_{G(s_2)}^* \leq G(s_2)$, it suffices by induction to show $W_1.L(s_1)(G(s_2)) \cup G(s_2) \leq G(s_2)$.
- This follows from $W_1.L(s_1)(G(s_2)) = W_2.L(s_2)(G(s_2)) \leq G(s_2)$.

□

Lemma 64. If $\phi : W_1 \rightarrow W_2$ and $G \in \text{GK}(W_2)$, then $\overleftarrow{G}_\phi \in \text{GK}(W_1)$.

Proof.

- \overleftarrow{G}_ϕ is monotone by definition because $[W_1.L(s_1)]_{(-)}^*$ is monotone.
- We have $\overleftarrow{G}_\phi(s_1) = W_1.L(s_1)(\overleftarrow{G}_\phi(s_1)) \cup \bigcup_{s'_1 \sqsubseteq s_1 \wedge s'_2 \in \phi(s'_1)} G(s'_2) \geq W_1.L(s_1)(\overleftarrow{G}_\phi(s_1))$.
- Moreover, for any $\tau \in \text{CType}$ we have $\overleftarrow{G}_\phi(s_1)(\text{ref } \tau) = W_1.L(s_1)(\overleftarrow{G}_\phi(s_1))(\text{ref } \tau)$ because:

$$\begin{aligned}
& \bigcup_{s'_1 \sqsubseteq s_1 \wedge s'_2 \in \phi(s'_1)} G(s'_2)(\text{ref } \tau) \\
&= \bigcup_{s'_1 \sqsubseteq s_1 \wedge s'_2 \in \phi(s'_1)} W_2.L(s'_2)(G(s'_2))(\text{ref } \tau) \quad (G \in \text{GK}(W_2)) \\
&= \bigcup_{s'_1 \sqsubseteq s_1 \wedge s'_2 \in \phi(s'_1)} W_1.L(s'_1)(G(s'_2))(\text{ref } \tau) \quad (\phi : W_1 \rightarrow W_2) \\
&= \bigcup_{s'_1 \sqsubseteq s_1 \wedge s'_2 \in \phi(s'_1)} W_1.L(s'_1)(\overleftarrow{G}_\phi(s'_1))(\text{ref } \tau) \quad (\text{Lemma 63}) \\
&\subseteq \bigcup_{s'_1 \sqsubseteq s_1 \wedge s'_2 \in \phi(s'_1)} W_1.L(s_1)(\overleftarrow{G}_\phi(s_1))(\text{ref } \tau) \\
&= W_1.L(s_1)(\overleftarrow{G}_\phi(s_1))(\text{ref } \tau)
\end{aligned}$$

- Using an analogous argument, for any $\mathbf{n} \in W_1.N = W_2.N$, we have $\overleftarrow{G}_\phi(s_1)(\mathbf{n}) = W_1.L(s_1)(\overleftarrow{G}_\phi(s_1))(\mathbf{n})$.

□

Lemma 65. Given $\phi : W_1 \rightarrow W_2$ and $G \in \text{GK}(W_1)$, we have $\forall s_2 \in \phi(s_1). \overrightarrow{G}_\phi^{s_1}(s_2) = G(s_1)$.

Proof.

- Suppose $s_2 \in \phi(s_1)$.
- We first show $G(s_1) = \bigcup_{s'_1 \sqsubseteq s_1 \wedge s'_2 \sqsubseteq s_2 \wedge s'_2 \in \phi(s'_1)} G(s'_1)$:
 - $G(s_1) \leq \bigcup_{s'_1 \sqsubseteq s_1 \wedge s'_2 \sqsubseteq s_2 \wedge s'_2 \in \phi(s'_1)} G(s'_1)$ is obvious.
 - To see the other inclusion, note that whenever $s'_1 \sqsubseteq s_1$, then $G(s'_1) \leq G(s_1)$.
- Consequently we know $\overrightarrow{G}_\phi^{s_1}(s_2) = [W_2.L(s_2)]_{G(s_1)}^* = W_2.L(s_2)([W_2.L(s_2)]_{G(s_1)}^*) \cup G(s_1) \geq G(s_1)$.
- To show $[W_2.L(s_2)]_{G(s_1)}^* \leq G(s_1)$, it suffices by induction to show $W_2.L(s_2)(G(s_1)) \cup G(s_1) \leq G(s_1)$.
- This follows from $W_2.L(s_2)(G(s_1)) = W_1.L(s_1)(G(s_1)) \leq G(s_1)$.

□

Lemma 66. If $\phi : W_1 \rightarrow W_2$ and $G \in \text{GK}(W_1)$, then $\overrightarrow{G}_\phi^{s_1} \in \text{GK}(W_2)$ for any $s_1 \in W_1.S$.

Proof.

- We have the following monotonicity by definition because $[W_2.L(s_2)]_{(-)}^*$ is monotone:

$$\forall \tilde{s}_1 \sqsupseteq \hat{s}_1. \forall \tilde{s}_2 \sqsupseteq \hat{s}_2. \overrightarrow{G}_\phi^{s_1}(\tilde{s}_2) \geq \overrightarrow{G}_\phi^{s_1}(\hat{s}_2)$$

- We have $\overrightarrow{G}_\phi^{s_1^1}(s_2) = W_2.\mathbf{L}(s_2)(\overrightarrow{G}_\phi^{s_1^1}(s_2)) \cup \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} G(s_1') \geq W_2.\mathbf{L}(s_2)(\overrightarrow{G}_\phi^{s_1^1}(s_2))$.
- Moreover, for any $\tau \in \text{CType}$ we have $\overrightarrow{G}_\phi^{s_1^1}(s_2)(\text{ref } \tau) = W_2.\mathbf{L}(s_2)(\overrightarrow{G}_\phi^{s_1^1}(s_2))(\text{ref } \tau)$ because:

$$\begin{aligned}
& \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} G(s_1')(\text{ref } \tau) \\
&= \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} W_1.\mathbf{L}(s_1')(G(s_1'))(\text{ref } \tau) \quad (G \in \text{GK}(W_1)) \\
&= \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} W_2.\mathbf{L}(s_2')(G(s_1'))(\text{ref } \tau) \quad (\phi : W_1 \rightarrow W_2) \\
&= \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} W_2.\mathbf{L}(s_2')(\overrightarrow{G}_\phi^{s_1^1}(s_2'))(\text{ref } \tau) \quad (\text{Lemma 65}) \\
&\subseteq \bigcup_{s_1' \sqsubseteq s_1 \wedge s_2' \sqsubseteq s_2 \wedge s_2' \in \phi(s_1')} W_2.\mathbf{L}(s_2)(\overrightarrow{G}_\phi^{s_1^1}(s_2))(\text{ref } \tau) \quad (\text{Monotonicity}) \\
&= W_2.\mathbf{L}(s_2)(\overrightarrow{G}_\phi^{s_1^1}(s_2))(\text{ref } \tau)
\end{aligned}$$

- Using an analogous argument, for any $\mathbf{n} \in W_2.\mathbf{N} = W_1.\mathbf{N}$, we have $\overrightarrow{G}_\phi^{s_1^1}(s_2)(\mathbf{n}) = W_2.\mathbf{L}(s_2)(\overrightarrow{G}_\phi^{s_1^1}(s_2))(\mathbf{n})$. □

4.3 Category of Worlds

Lemma 67. If $\phi : W_1 \rightarrow W_2$, then $\phi \circ \text{id}_{W_1} = \phi = \text{id}_{W_2} \circ \phi$.

Proof. Obvious. □

Lemma 68. If $\phi : W_1 \rightarrow W_2$, $\psi : W_2 \rightarrow W_3$, $\chi : W_3 \rightarrow W_4$, then $\chi \circ (\psi \circ \phi) = (\chi \circ \psi) \circ \phi$.

Proof.

$$\begin{aligned}
& s_4 \in (\chi \circ (\psi \circ \phi))(s_1) \\
&\iff \exists s_3. s_4 \in \chi(s_3) \wedge s_3 \in (\psi \circ \phi)(s_1) \\
&\iff \exists s_3, s_2. s_4 \in \chi(s_3) \wedge s_3 \in \psi(s_2) \wedge s_2 \in \phi(s_1) \\
&\iff \exists s_2. s_4 \in (\chi \circ \psi)(s_2) \wedge s_2 \in \phi(s_1) \\
&\iff s_4 \in ((\chi \circ \psi) \circ \phi)(s_1)
\end{aligned}$$
□

Lemma 69. If $\phi : W_1 \rightarrow W_2$ and $\psi : W_2 \rightarrow W_3$, then $\psi \circ \phi$ forms a weak morphism.

Proof. Conditions (1) through (4) hold vacuously. Condition (5) follows from Lemmas 65 and 66. □

Proposition 70. Worlds with weak morphisms form a category.

Proof. It follows from Lemmas 67, 68 and 69. □

4.4 Isomorphism Theorem

Definition 13. Given $\phi : W_1 \rightarrow W_2$, we define $|-|_\phi \in \mathbb{P}(W_1.\mathbf{S}) \rightarrow \mathbb{P}(W_2.\mathbf{S})$ as follows:

$$|S|_\phi = \{s_1 \in S \mid \phi(s_1) \neq \emptyset\}$$

When ϕ is clear from context, we often just write $|S|$.

Lemma 71. If $\phi : W_1 \cong W_2 : \psi$ and $G \in \text{GK}(W_2)$, then:

$$\begin{aligned}
& \bigcup_{s_1^0 \in |\psi(s_2^0)|} \bigcap_{s_1 \in |\psi(s_2)|} \mathbf{E}_{W_1}(\overleftarrow{G}_\phi)(s_1^0, s_1) \leq \mathbf{E}_{W_2}(G)(s_2^0, s_2) \\
& \bigcup_{s_1^0 \in |\psi(s_2^0)|} \bigcap_{s_1 \in |\psi(s_2)|} \mathbf{K}_{W_1}(\overleftarrow{G}_\phi)(s_1^0, s_1) \leq \mathbf{K}_{W_2}(G)(s_2^0, s_2)
\end{aligned}$$

Proof. We define:

$$\begin{aligned}\mathbf{E}'_{W_2}(G)(s_2^0, s_2) &= \bigcup_{s_1^0 \in |\psi(s_2^0)|} \bigcap_{s_1 \in |\psi(s_2)|} \mathbf{E}_{W_1}(\overleftarrow{G}_\phi)(s_1^0, s_1) \\ \mathbf{K}'_{W_2}(G)(s_2^0, s_2) &= \bigcup_{s_1^0 \in |\psi(s_2^0)|} \bigcap_{s_1 \in |\psi(s_2)|} \mathbf{K}_{W_1}(\overleftarrow{G}_\phi)(s_1^0, s_1)\end{aligned}$$

We prove $\mathbf{E}'_{W_2} \leq \mathbf{E}_{W_2}$ and $\mathbf{K}'_{W_2} \leq \mathbf{K}_{W_2}$ by coinduction. Concretely, we have to show:

1. $\forall e_1, e_2, G, s_2^0, s_2, \tau.$
 $(e_1, e_2) \in \mathbf{E}'_{W_2}(G)(s_2^0, s_2)(\tau) \implies$
 $\forall (h_1, h_2) \in W_2.H(s_2)(G(s_2)). \forall h_1^F, h_2^F.$
 $((h_1, h_1^F, e_1), (h_2, h_2^F, e_2)) \in \mathbf{O}_{W_2}(\mathbf{K}'_{W_2})(G)(s_2^0, s_2)(\tau)$
2. $\forall K_1, K_2, G, s_2^0, s_2, \tau', \tau.$
 $(K_1, K_2) \in \mathbf{K}'_{W_2}(G)(s_2^0, s_2)(\tau', \tau) \implies$
 $\forall (v_1, v_2) \in \overleftarrow{G}(s_2)(\tau'). (K_1[v_1], K_2[v_2]) \in \mathbf{E}'_{W_2}(G)(s_2^0, s_2)(\tau)$

Part (1):

- Suppose $(e_1, e_2) \in \mathbf{E}'_{W_2}(G)(s_2^0, s_2)(\tau)$, and thus $(e_1, e_2) \in \bigcap_{s_1 \in |\psi(s_2)|} \mathbf{E}_{W_1}(\overleftarrow{G}_\phi)(s_1^0, s_1)(\tau)$ for some $s_1^0 \in |\psi(s_2^0)|$.
- Further suppose $(h_1, h_2) \in W_2.H(s_2)(G(s_2))$, and thus $(h_1, h_2) \in \bigcup_{s_1 \in \psi(s_2)} W_1.H(s_1)(G(s_2))$.
- Thus there exists $s_1 \in \psi(s_2)$ such that $(h_1, h_2) \in W_1.H(s_1)(G(s_2))$.
- By Lemma 65 we know $G(s_2) = \overrightarrow{G}_\psi^{s_2^0}(s_1)$ and thus $W_1.H(s_1)(\overrightarrow{G}_\psi^{s_2^0}(s_1)) \neq \emptyset$.
- Since $W_1.H(s_1)(\overrightarrow{G}_\psi^{s_2^0}(s_1)) \subseteq \bigcup_{s_2' \in \phi(s_1)} W_2.H(s_2')(\overrightarrow{G}_\psi^{s_2^0}(s_1))$, there also exists $s_2' \in \phi(s_1)$.
- Since $s_2' \in (\phi \circ \psi)(s_2)$ and $\phi \circ \psi \sqsupseteq_{\text{pub}} \text{id}$, we have that $s_2' \sqsupseteq_{\text{pub}} s_2$.
- Hence $(h_1, h_2) \in W_1.H(s_1)(G(s_2'))$, which means $(h_1, h_2) \in W_1.H(s_1)(\overleftarrow{G}_\phi(s_1))$ by Lemma 63.
- For h_1^F and h_2^F with defined $(h_1 \uplus h_1^F)$ and defined $(h_2 \uplus h_2^F)$ we then get three cases from $(e_1, e_2) \in \mathbf{E}_{W_1}(\overleftarrow{G}_\phi)(s_1^0, s_1)(\tau)$:
 - a) $h_1 \uplus h_1^F, e_1 \uparrow \wedge h_2 \uplus h_2^F, e_2 \uparrow$
We are done.
 - b) $h_1 \uplus h_1^F, e_1 \hookrightarrow^* h_1' \uplus h_1^F, v_1 \wedge h_2 \uplus h_2^F, e_2 \hookrightarrow^* h_2' \uplus h_2^F, v_2$
with $s_1' \sqsupseteq [s_1^0, s_1] \wedge (h_1', h_2') \in W_1.H(s_1')(\overleftarrow{G}_\phi(s_1')) \wedge (v_1, v_2) \in \overleftarrow{G}_\phi(s_1')(\tau)$
 - Since $W_1.H(s_1')(\overleftarrow{G}_\phi(s_1')) \subseteq \bigcup_{s_2'' \in \phi(s_1')} W_2.H(s_2'')(\overleftarrow{G}_\phi(s_1'))$, there exists $s_2'' \in \phi(s_1')$ such that $(h_1', h_2') \in W_2.H(s_2'')(G(s_2''))$ by Lemma 63.
 - Also by Lemma 63 we have $(v_1, v_2) \in \overleftarrow{G}(s_2'')(\tau)$.
 - It remains to show $s_2'' \sqsupseteq [s_2^0, s_2]$.
 - From $s_2'' \in \phi(s_1')$ and $s_2' \in \phi(s_1)$ we get $s_2'' \sqsupseteq s_2' \sqsupseteq s_2$.
 - From $s_1^0 \in |\psi(s_2^0)|$ we know there is $s_2^0 \in \phi(s_1^0)$.
 - From $s_2'' \in \phi(s_1')$ and $s_2^0 \in \phi(s_1^0)$ we get $s_2'' \sqsupseteq_{\text{pub}} s_2^0$.
 - Since $s_2^0 \in (\phi \circ \psi)(s_2)$ we also get $s_2^0 \sqsupseteq_{\text{pub}} s_2$ and thus $s_2'' \sqsupseteq_{\text{pub}} s_2$.
 - c) $h_1 \uplus h_1^F, e_1 \hookrightarrow^* h_1' \uplus h_1^F, K_1[e_1'] \wedge h_2 \uplus h_2^F, e_2 \hookrightarrow^n h_2' \uplus h_2^F, K_2[e_2']$
with $s_1' \sqsupseteq s_1 \wedge (h_1', h_2') \in W_1.H(s_1')(\overleftarrow{G}_\phi(s_1')) \wedge (e_1', e_2') \in \mathbf{S}(\overleftarrow{G}_\phi(s_1'), \overleftarrow{G}_\phi(s_1'))(\tau')$ and
 $\forall s_1'' \sqsupseteq_{\text{pub}} s_1'. \forall G' \geq \overleftarrow{G}_\phi. (K_1, K_2) \in \mathbf{K}_{W_1}(G')(s_1^0, s_1'')(\tau', \tau)$

- Since $W_1.H(s'_1)(\overleftarrow{G}_\phi(s'_1)) \subseteq \bigcup_{s'_2 \in \phi(s'_1)} W_2.H(s'_2)(\overleftarrow{G}_\phi(s'_1))$, there exists $s'_2 \in \phi(s'_1)$ such that $(h'_1, h'_2) \in W_2.H(s'_2)(G(s'_2))$ by Lemma 63.
- Also by Lemma 63 we have $(e'_1, e'_2) \in \mathbf{S}(G(s'_2), G(s'_2))(\tau')$.
- From $s'_2 \in \phi(s'_1)$ and $s'_2 \in \phi(s_1)$ we get $s'_2 \supseteq s'_2 \supseteq s_2$.
- It remains to show: $\forall s'_2 \supseteq_{\text{pub}} s'_2. \forall G' \geq G. (K_1, K_2) \in \mathbf{K}'_{W_2}(G')(s'_2, s'_2)(\tau', \tau)$
- So suppose $s'_2 \supseteq_{\text{pub}} s'_2$ and $G' \geq G$.
- By definition of \mathbf{K}'_{W_2} it suffices to show $(K_1, K_2) \in \mathbf{K}_{W_1}(G')(s'_1, s'_1)(\tau', \tau)$ for any $s'_1 \in |\psi(s'_2)|$.
- Since $(h'_1, h'_2) \in W_2.H(s'_2)(G(s'_2)) \subseteq \bigcup_{s'_1 \in \psi(s'_2)} W_1.H(s'_1)(G(s'_2))$, there exists $s'_1 \in \psi(s'_2)$.
- First, note that $\overleftarrow{G}'_\phi \geq \overleftarrow{G}_\phi$.
- Second, from $s'_1 \in |\psi(s'_2)|$ and $s'_2 \supseteq_{\text{pub}} s'_2$ and $s'_1 \in \psi(s'_2)$ we get $s'_1 \supseteq_{\text{pub}} s'_1$, which in turn yields $s'_1 \supseteq_{\text{pub}} s'_1$ because $s'_1 \in (\psi \circ \phi)(s'_1)$.
- The claim then follows from $\forall s'_1 \supseteq_{\text{pub}} s'_1. \forall G' \geq \overleftarrow{G}'_\phi. (K_1, K_2) \in \mathbf{K}_{W_1}(G')(s'_1, s'_1)(\tau', \tau)$.

Part (2):

- Suppose $(K_1, K_2) \in \mathbf{K}'_{W_2}(G)(s'_2, s_2)(\tau', \tau)$, i.e., $(K_1, K_2) \in \bigcap_{s_1 \in |\psi(s_2)|} \mathbf{K}_{W_1}(\overleftarrow{G}_\phi)(s'_1, s_1)(\tau', \tau)$ for some $s'_1 \in |\psi(s'_2)|$.
- Further suppose $(v_1, v_2) \in \overline{G(s_2)}(\tau')$.
- By definition of \mathbf{E}'_{W_2} it suffices to show $(K_1[v_1], K_2[v_2]) \in \mathbf{E}_{W_1}(\overleftarrow{G}_\phi)(s'_1, s_1)(\tau)$ for any $s_1 \in |\psi(s_2)|$.
- Pick $s'_2 \in \phi(s_1)$, so $s'_2 \in (\phi \circ \psi)(s_2)$ and thus $s'_2 \supseteq_{\text{pub}} s_2$.
- Hence $(v_1, v_2) \in \overline{G(s_2)}(\tau') \subseteq \overline{G(s'_2)}(\tau') = \overline{\overleftarrow{G}_\phi(s_1)}(\tau')$ by Lemma 63.
- The claim then follows from $(K_1, K_2) \in \mathbf{K}_{W_1}(\overleftarrow{G}_\phi)(s'_1, s_1)(\tau', \tau)$.

□

Corollary 72. If $\phi : W_1 \cong W_2 : \psi$ and $G \in \text{GK}(W_2)$, then:

$$\forall s_2. (\forall s_1 \in |\psi(s_2)|. (\tau, e_1, e_2) \in \mathbf{E}_{W_1}(\overleftarrow{G}_\phi)(s_1, s_1)) \implies (\tau, e_1, e_2) \in \mathbf{E}_{W_2}(G)(s_2, s_2)$$

Proof.

- Suppose $\forall s_1 \in |\psi(s_2)|. (\tau, e_1, e_2) \in \mathbf{E}_{W_1}(\overleftarrow{G}_\phi)(s_1, s_1)$.
- We need to show $(\tau, e_1, e_2) \in \mathbf{E}_{W_2}(G)(s_2, s_2)$.
- Now suppose $W_2.H(s_2)(G(s_2)) \neq \emptyset$ (otherwise there is nothing to show).
- From $W_2.H(s_2)(G(s_2)) \leq \bigcup_{s_1 \in \psi(s_2)} W_1.H(s_1)(G(s_2))$ we get $s_1^0 \in \psi(s_2)$ with $W_1.H(s_1^0)(G(s_2)) \neq \emptyset$.
- By Lemma 65 we know $G(s_2) = \overrightarrow{G}_\psi^{s_2}(s_1^0)$ and thus $W_1.H(s_1^0)(\overrightarrow{G}_\psi^{s_2}(s_1^0)) \neq \emptyset$.
- Since also $W_1.H(s_1^0)(\overrightarrow{G}_\psi^{s_2}(s_1^0)) \leq \bigcup_{s'_2 \in \phi(s_1^0)} W_2.H(s'_2)(\overrightarrow{G}_\psi^{s_2}(s_1^0))$, we have $\phi(s_1^0) \neq \emptyset$ and thus $s_1^0 \in |\psi(s_2)|$.
- By Lemma 71, it suffices to show $(\tau, e_1, e_2) \in \mathbf{E}_{W_1}(\overleftarrow{G}_\phi)(s_1^0, s_1^0)$ for any $s_1 \in |\psi(s_2)|$.
- Since $s_1, s_1^0 \in \psi(s_2)$ and thus $s_1 \supseteq_{\text{pub}} s_1^0$, this follows from the assumption by Lemma 7.

□

Theorem 73 (Weak isomorphisms preserve equivalence). If $\phi : W_1 \cong W_2 : \psi$, then: $\forall \Delta, \Gamma, \tau, e_1, e_2$.

$$\Delta; \Gamma \vdash e_1 \sim_{W_1} e_2 : \tau \iff \Delta; \Gamma \vdash e_1 \sim_{W_2} e_2 : \tau$$

Proof. By symmetry, it is enough to show $\Delta; \Gamma \vdash e_1 \sim_{W_1} e_2 : \tau \implies \Delta; \Gamma \vdash e_1 \sim_{W_2} e_2 : \tau$. From the premise we know:

1. *inhabited*(W_1)
2. *consistent*(W_1)
3. $\forall G \in \text{GK}(W_1). \forall s_1. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_1)). (\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{W_1}(G)(s_1, s_1)(\delta\tau)$

a) We prove *inhabited*(W_2).

- Suppose $G \in \text{GK}(W_2)$.
- From (1) we know there is s_1 such that $(\emptyset, \emptyset) \in W_1.H(s_1)(\overleftarrow{G}_\phi(s_1))$.
- From $W_1.H(s_1)(\overleftarrow{G}_\phi(s_1)) \leq \bigcup_{s_2 \in \phi(s_1)} W_2.H(s_2)(\overleftarrow{G}_\phi(s_1))$ we get $s_2 \in \phi(s_1)$ with $(\emptyset, \emptyset) \in W_2.H(s_2)(\overleftarrow{G}_\phi(s_1))$.
- By Lemma 63 we have $(\emptyset, \emptyset) \in W_2.H(s_2)(G(s_2))$.

b) We prove *consistent*(W_2).

- Let $G \in \text{GK}(W_2)$ and $(e'_1, e'_2) \in \mathbf{S}(W_2.L(s_2)(G(s_2)), G(s_2))(\tau')$.
- We need to show $(\text{beta}(e'_1), \text{beta}(e'_2)) \in \mathbf{E}_{W_2}(G)(s_2, s_2)(\tau')$.
- By Corollary 72, it suffices to show $(\text{beta}(e'_1), \text{beta}(e'_2)) \in \mathbf{E}_{W_1}(\overleftarrow{G}_\phi)(s_1, s_1)(\tau')$ for any $s_1 \in |\psi(s_2)|$.
- Since $\phi(s_1) \neq \emptyset$, we have $s'_2 \in \phi(s_1)$ and thus $\overleftarrow{G}_\phi(s_1) = G(s'_2)$ by Lemma 63.
- Since $s'_2 \in (\phi \circ \psi)(s_2)$, we have $s'_2 \sqsupseteq_{\text{pub}} s_2$ and thus $\overleftarrow{G}_\phi(s_1) \geq G(s_2)$.
- Thus we have $\mathbf{S}(W_2.L(s_2)(G(s_2)), G(s_2)) \leq \mathbf{S}(W_2.L(s_2)(\overleftarrow{G}_\phi(s_1)), \overleftarrow{G}_\phi(s_1)) \leq \mathbf{S}(W_1.L(s_1)(\overleftarrow{G}_\phi(s_1)), \overleftarrow{G}_\phi(s_1))$.
- Consequently, the claim follows from (2).

c) We prove $\forall G \in \text{GK}(W_2). \forall s_2. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_2)). (\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{W_2}(G)(s_2, s_2)(\delta\tau)$.

- Let $G \in \text{GK}(W_2)$, $\delta \in \text{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_2))$.
- By Corollary 72, it suffices to show $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{W_1}(\overleftarrow{G}_\phi)(s_1, s_1)(\delta\tau)$ for any $s_1 \in |\psi(s_2)|$.
- Since $\phi(s_1) \neq \emptyset$, we have $s'_2 \in \phi(s_1)$ and thus $\overleftarrow{G}_\phi(s_1) = G(s'_2)$ by Lemma 63.
- Since $s'_2 \in (\phi \circ \psi)(s_2)$, we have $s'_2 \sqsupseteq_{\text{pub}} s_2$ and thus $\overleftarrow{G}_\phi(s_1) \geq G(s_2)$.
- Thus we have $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_2)) \leq \text{Env}(\delta\Gamma, \overleftarrow{G}_\phi(s_1))$.
- Consequently, the claim follows from (3).

□

4.5 Examples

Erased World. For $W \in \text{World}$, we define its erasure $|W| \in \text{World}$ as follows.

$$\begin{aligned} |W|.N &:= W.N \\ |W|.S &:= \{s \in W.S \mid \exists G \in \text{GK}(W). W.H(s)(G(s)) \neq \emptyset\} \\ |W|. \sqsupseteq &:= W. \sqsupseteq \\ |W|. \sqsupseteq_{\text{pub}} &:= W. \sqsupseteq_{\text{pub}} \\ |W|.L &:= W.L \\ |W|.H &:= W.H \end{aligned}$$

Note that erasing preserves inhabitation and consistency.

Theorem 74. $\exists \phi, \psi. \phi : W \cong |W| : \psi$

Proof. We define ϕ, ψ as follows:

$$\begin{aligned}\phi(s) &:= \{s\} \cap |W|.S \\ \psi(s) &:= \{s\}\end{aligned}$$

It is easy to check all the properties of a weak isomorphism. □

Flattened World. For $W \in \text{World}$, we define its flattening $\text{Flat}(W) \in \text{World}$ as follows.

$$\begin{aligned}\text{Flat}(W).S &:= W.S \times \text{Heap} \times \text{Heap} \\ \text{Flat}(W).\sqsupseteq &:= \{((s', h'_1, h'_2), (s, h_1, h_2)) \mid s' \sqsupseteq s\} \\ \text{Flat}(W).\sqsupseteq_{\text{pub}} &:= \{((s', h'_1, h'_2), (s, h_1, h_2)) \mid s' \sqsupseteq_{\text{pub}} s\} \\ \text{Flat}(W).L(s, h_1, h_2) &:= W.L(s) \\ \text{Flat}(W).H(s, h_1, h_2)(R) &:= \{(h_1, h_2)\} \cap W.H(s)(R)\end{aligned}$$

Note that flattening preserves inhabitation and consistency.

Theorem 75. $\exists \phi, \psi. \phi : W \cong \text{Flat}(W) : \psi$

Proof. We define ϕ, ψ as follows:

$$\begin{aligned}\phi(s) &:= \{(s, h_1, h_2) \mid h_1, h_2 \in \text{Heap}\} \\ \psi(s, h_1, h_2) &:= \{s\}\end{aligned}$$

It is easy to check all the properties of a weak isomorphism. □

5 Transitivity

Suppose $\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma$ and $\Delta; \Gamma \vdash e_2 \sim e_3 : \sigma$. The goal of this section is to prove $\Delta; \Gamma \vdash e_1 \sim e_3 : \sigma$. To this end, suppose we are given \mathcal{N} . We may assume $\mathcal{N} = \mathcal{N}_1 \uplus \mathcal{N}_2 \uplus \mathcal{N}_\exists$ with $\text{names}(\Gamma, \sigma) \cap \mathcal{N}_\exists = \emptyset$. Then there are W_1, w_1, W_2, w_2 such that:

- $W_i = w_i \uparrow$
- $\text{stable}(w_i)$
- $w_i.\mathbf{N} \subseteq \mathcal{N}_i$
- $\Gamma \vdash e_1 \sim_{W_1} e_2 : \sigma$ and $\Gamma \vdash e_2 \sim_{W_2} e_3 : \sigma$

5.1 Constructing a Full World That Relates e_1 and e_3

5.1.1 Type Decomposition

Definition 14. We mutually inductively define $\sigma_1 \approx \sigma_2$ and $\sigma_1 \sim \sigma_2$ for $\sigma_1, \sigma_2 \in \text{Type}$ as follows:

$$\begin{array}{ll}
 \mathbf{n} \approx \mathbf{n} & \text{if } \mathbf{n} \notin \mathcal{N}_\exists \\
 \alpha \approx \alpha & \\
 \tau_{\text{base}} \approx \tau_{\text{base}} & \\
 \sigma_1 \times \sigma'_1 \approx \sigma_2 \times \sigma'_2 & \text{if } \sigma_1 \sim \sigma_2 \wedge \sigma'_1 \sim \sigma'_2 \\
 \sigma_1 + \sigma'_1 \approx \sigma_2 + \sigma'_2 & \text{if } \sigma_1 \sim \sigma_2 \wedge \sigma'_1 \sim \sigma'_2 \\
 \sigma_1 \rightarrow \sigma'_1 \approx \sigma_2 \rightarrow \sigma'_2 & \text{if } \sigma_1 \sim \sigma_2 \wedge \sigma'_1 \sim \sigma'_2 \\
 \mu\alpha. \sigma_1 \approx \mu\alpha. \sigma_2 & \text{if } \sigma_1 \sim \sigma_2 \\
 \forall\alpha. \sigma_1 \approx \forall\alpha. \sigma_2 & \text{if } \sigma_1 \sim \sigma_2 \\
 \exists\alpha. \sigma_1 \approx \exists\alpha. \sigma_2 & \text{if } \sigma_1 \sim \sigma_2 \\
 \text{ref } \sigma_1 \approx \text{ref } \sigma_2 & \text{if } \sigma_1 \sim \sigma_2 \\
 \text{with} & \\
 \sigma_1 \sim \sigma_2 & \text{if } \sigma_1, \sigma_2 \in \text{CType} \vee \sigma_1 \approx \sigma_2
 \end{array}$$

Definition 15. Since CType and \mathcal{N}_\exists are countably infinite sets, there exists a bijective function

$$\mathbf{A} \in \{ (\tau_1, \tau_2) \in \text{CType} \times \text{CType} \mid \tau_1 \not\approx \tau_2 \} \rightarrow \mathcal{N}_\exists .$$

Definition 16. Given $\sigma \in \text{Type}$, we define $\sigma_{(1)}, \sigma_{(2)} \in \text{Type}$ recursively as follows:

$$\begin{array}{ll}
 \mathbf{n}_{(i)} & := \begin{cases} \tau_i & \text{if } \mathbf{n} = \mathbf{A}(\tau_1, \tau_2) \text{ for some } \tau_1, \tau_2 \\ \mathbf{n} & \text{otherwise, i.e., } \mathbf{n} \notin \mathcal{N}_\exists \end{cases} \\
 \alpha_{(i)} & := \alpha \\
 \tau_{\text{base}(i)} & := \tau_{\text{base}} \\
 (\sigma \times \sigma')_{(i)} & := \sigma_{(i)} \times \sigma'_{(i)} \\
 (\sigma + \sigma')_{(i)} & := \sigma_{(i)} + \sigma'_{(i)} \\
 (\sigma \rightarrow \sigma')_{(i)} & := \sigma_{(i)} \rightarrow \sigma'_{(i)} \\
 (\forall\alpha. \sigma)_{(i)} & := \forall\alpha. \sigma_{(i)} \\
 (\exists\alpha. \sigma)_{(i)} & := \exists\alpha. \sigma_{(i)} \\
 (\mu\alpha. \sigma)_{(i)} & := \mu\alpha. \sigma_{(i)} \\
 (\text{ref } \sigma)_{(i)} & := \text{ref } \sigma_{(i)}
 \end{array}$$

Lemma 76. For $\sigma \in \text{Type}$,

$$\sigma_{(1)} \in \text{CType} \wedge \sigma_{(2)} \in \text{CType} \iff \sigma \in \text{CType}$$

Proof. By straightforward induction on σ . □

Lemma 77. For $\sigma \in \text{Type}$,

$$\sigma_{(1)} \sim \sigma_{(2)}$$

Proof. By straightforward induction on σ . □

Lemma 78. For $\sigma \in \text{Type}$,

$$\sigma_{(1)} \approx \sigma_{(2)} \iff \sigma \notin \mathcal{N}_{\exists}$$

Proof. Straightforward to show by case analysis on σ using Lemma 77. □

Lemma 79 (Injectivity of Type Decomposition). For $\sigma_1, \sigma_2 \in \text{Type}$,

$$\sigma_{1(1)} = \sigma_{2(1)} \wedge \sigma_{1(2)} = \sigma_{2(2)} \implies \sigma_1 = \sigma_2$$

Proof. Easy to show by induction on σ_1 . We just show the following representative cases.

- when $\sigma_1 = \mathbf{A}(\tau_1, \tau_2) \in \mathcal{N}_{\exists}$:
 - We have $\sigma_2 \in \mathcal{N}_{\exists}$ by Lemma 78.
 - Thus we have $\sigma_1 = \mathbf{A}(\tau_1, \tau_2) = \sigma_2$ since \mathbf{A} is bijective.
- when $\sigma_1 = \mathbf{n} \notin \mathcal{N}_{\exists}$:
 - By case analysis on σ_2 , we have $\sigma_2 \in \text{TyNam}$.
 - By Lemma 78, we have $\sigma_2 \notin \mathcal{N}_{\exists}$.
 - Thus we have $\sigma_2 = \mathbf{n} = \sigma_1$.
- when $\sigma_1 = \sigma'_1 \rightarrow \sigma''_1$:
 - By Lemmas 77 and 78, we have $\sigma_2 \notin \mathcal{N}_{\exists}$.
 - By case analysis on σ_2 , we have $\sigma_2 = \sigma'_2 \rightarrow \sigma''_2$ for some $\sigma'_2, \sigma''_2 \in \text{Type}$.
 - Then we have $\sigma'_{1(i)} = \sigma'_{2(i)}$ and $\sigma''_{1(i)} = \sigma''_{2(i)}$ for $i = 1, 2$.
 - Thus by induction hypothesis we have $\sigma'_1 = \sigma'_2 \wedge \sigma''_1 = \sigma''_2$, which yields $\sigma_1 = \sigma_2$.
- when $\sigma_1 = \exists \alpha. \sigma'_1$:
 - By Lemmas 77 and 78, we have $\sigma_2 \notin \mathcal{N}_{\exists}$.
 - By case analysis on σ_2 , we have $\sigma_2 = \exists \alpha. \sigma'_2$ for some $\sigma'_2 \in \text{Type}$.
 - Then we have $\sigma'_{1(i)} = \sigma'_{2(i)}$ for $i = 1, 2$.
 - Thus by induction hypothesis we have $\sigma'_1 = \sigma'_2$, which yields $\sigma_1 = \sigma_2$.

□

Lemma 80. For $\sigma_1, \sigma_2 \in \text{Type}$,

$$\sigma_1 \sim \sigma_2 \implies \exists \sigma. \sigma_{(1)} = \sigma_1 \wedge \sigma_{(2)} = \sigma_2$$

Proof. Easy to show by induction on σ_1 . We just show the following representative cases.

If $\sigma_1 \not\approx \sigma_2$, then $\sigma_1, \sigma_2 \in \text{CType}$ and we are done for $\sigma = \mathbf{A}(\sigma_1, \sigma_2)$. Otherwise we proceed as follows:

- when $\sigma_1 = \mathbf{n} \in \text{TyNam}$:
 - From $\sigma_1 \approx \sigma_2$, we have $\sigma_2 = \mathbf{n} \notin \mathcal{N}_{\exists}$.

- Thus we are done by letting $\sigma = \mathbf{n}$.
- when $\sigma_1 = \sigma'_1 \rightarrow \sigma''_1$:
 - From $\sigma_1 \approx \sigma_2$, we have $\sigma_2 = \sigma'_2 \rightarrow \sigma''_2$ such that $\sigma'_1 \sim \sigma'_2$ and $\sigma''_1 \sim \sigma''_2$.
 - By induction hypothesis, we have σ' and σ'' such that $\sigma'_{(i)} = \sigma'_i$ and $\sigma''_{(i)} = \sigma''_i$ for $i = 1, 2$.
 - Thus we are done by letting $\sigma = \sigma' \rightarrow \sigma''$.
- when $\sigma_1 = \exists\alpha. \sigma'_1$:
 - From $\sigma_1 \approx \sigma_2$, we have $\sigma_2 = \exists\alpha. \sigma'_2$ such that $\sigma'_1 \sim \sigma'_2$.
 - By induction hypothesis, we have σ' such that $\sigma'_{(i)} = \sigma'_i$ for $i = 1, 2$.
 - Thus we are done by letting $\sigma = \exists\alpha. \sigma'$.

□

Corollary 81 (Surjectivity of Type Decomposition). For $\tau_1, \tau_2 \in \text{CType}$, we have $\tau \in \text{CType}$ such that $\tau_{(1)} = \tau_1 \wedge \tau_{(2)} = \tau_2$.

Proof. Since $\tau_1 \sim \tau_2$ by definition, we have $\sigma \in \text{Type}$ such that $\sigma_{(1)} = \tau_1 \wedge \sigma_{(2)} = \tau_2$ by Lemma 80. Hence $\sigma \in \text{CType}$ by Lemma 76. □

5.1.2 World Construction

Definition 17. Since CType and CVal are countable sets, there exists an injective function

$$\mathbf{I} \in \text{CType} \times \text{CVal} \times \text{CVal} \rightarrow \mathbb{N}.$$

Definition 18. Given $R \in \text{VRelF}$, we define $R_{\{1\}}, R_{\{2\}} \in \text{VRelF}$ as follows:

$$\begin{aligned} R_{\{1\}} &:= \{ (\tau_{(1)}, v_1, \mathbf{I}(\tau, v_1, v_3)) \mid \tau \in \text{CTypeF} \setminus (\mathcal{N} \cup \{\text{ref } \tau' \in \text{CType}\}) \wedge (\tau, v_1, v_3) \in R \} \\ R_{\{2\}} &:= \{ (\tau_{(2)}, \mathbf{I}(\tau, v_1, v_3), v_3) \mid \tau \in \text{CTypeF} \setminus (\mathcal{N} \cup \{\text{ref } \tau' \in \text{CType}\}) \wedge (\tau, v_1, v_3) \in R \} \end{aligned}$$

Definition 19. For $X_1, X_2 \in \text{VRel}$, we define $X_1 \bullet X_2 \in \text{VRel}$ as follows:

$$(X_1 \bullet X_2)(\tau) := X_1(\tau_{(1)}) \circ X_2(\tau_{(2)})$$

Note that this is well-defined due to Lemma 76.

Recall that for a monotone function $F \in \text{VRelF} \rightarrow \text{VRelF}$ and $R \in \text{VRelF}$, we write $[F]_R^*$ for the least fixpoint of the monotone function $F(-) \cup R$.

Definition 20. We define $W \in \text{World}$ as follows:

$$\begin{aligned} W.N &:= \mathcal{N} \\ W.S &:= W_1.S \times W_2.S \\ W.\sqsubseteq &:= \{ (p, p') \mid p.1 \sqsubseteq p'.1 \wedge p.2 \sqsubseteq p'.2 \} \\ W.\sqsubseteq_{\text{pub}} &:= \{ (p, p') \mid p.1 \sqsubseteq_{\text{pub}} p'.1 \wedge p.2 \sqsubseteq_{\text{pub}} p'.2 \} \\ W.L(s_1, s_2)(R) &:= \{ (\tau, v_1, v_3) \in \overline{W_1.L(s_1)([W_1.L(s_1)]_{R_{\{1\}}}^*)} \bullet \overline{W_2.L(s_2)([W_2.L(s_2)]_{R_{\{2\}}}^*)} \mid \tau \in \text{CTypeF} \setminus \mathcal{N}_{\exists} \} \uplus \\ &\quad \{ (\mathbf{n}, v_1, v_3) \in \overline{[W_1.L(s_1)]_{R_{\{1\}}}^*} \bullet \overline{[W_2.L(s_2)]_{R_{\{2\}}}^*} \mid \mathbf{n} \in \mathcal{N}_{\exists} \} \\ W.H(s_1, s_2)(R) &:= W_1.H(s_1)([W_1.L(s_1)]_{R_{\{1\}}}^*) \circ W_2.H(s_2)([W_2.L(s_2)]_{R_{\{2\}}}^*) \end{aligned}$$

It is easy to check that W is well-defined.

5.1.3 Transitivity of Value Equivalence

Definition 21. Given $G \in \text{GK}(W)$ and $(s_1, s_2) \in W.S = W_1.S \times W_2.S$, we define $G_{(1)}^{s_2} \in W_1.S \rightarrow \text{VRelF}$ and $G_{(2)}^{s_1} \in W_2.S \rightarrow \text{VRelF}$ as follows:

$$\begin{aligned} G_{(1)}^{s_2}(s) &:= [W_1.L(s)]_{G(s, s_2)_{\{1\}}}^* \\ G_{(2)}^{s_1}(s) &:= [W_2.L(s)]_{G(s_1, s)_{\{2\}}}^* \end{aligned}$$

Lemma 82.

1. $\forall G \in \text{GK}(W). \forall s_2 \in W_2.S. G_{(1)}^{s_2} \in \text{GK}(W_1)$
2. $\forall G \in \text{GK}(W). \forall s_1 \in W_1.S. G_{(2)}^{s_1} \in \text{GK}(W_2)$

Proof. We only show part (1) since part (2) is analogous. Monotonicity of $G_{(1)}^{s_2}$ is easy to show by induction, using that G and $(-)_{\{1\}}$ and $W_1.L$ are monotone.

It remains to show $G_{(1)}^{s_2}(s_1) \geq_{\text{ref}}^{W_1.N} W_1.L(s_1)(G_{(1)}^{s_2}(s_1))$ for any s_1 . For $\tau \in \text{CTypeF}$ we know:

$$\begin{aligned} &G_{(1)}^{s_2}(s_1)(\tau) \\ &= [W_1.L(s)]_{G(s_1, s_2)_{\{1\}}}^*(\tau) \\ &= W_1.L(s_1)([W_1.L]_{G(s_1, s_2)_{\{1\}}}^*(\tau) \cup G(s_1, s_2)_{\{1\}}(\tau)) \\ &= W_1.L(s_1)(G_{(1)}^{s_2}(s_1)(\tau) \cup G(s_1, s_2)_{\{1\}}(\tau)) \end{aligned}$$

The claim follows from this and the fact that by construction $G(s_1, s_2)_{\{1\}}(\mathbf{n}) = \emptyset = G(s_1, s_2)_{\{1\}}(\text{ref } \tau')$ for any $\mathbf{n} \in W_1.N \subseteq \mathcal{N}$ and τ' . \square

Lemma 83. $\forall R \in \text{VRelF}. \forall \tau \in \text{CTypeF} \setminus (\mathcal{N} \cup \{\text{ref } \tau' \in \text{CType}\})$.

$$\begin{aligned} \forall s_1, R_1. W_1.L(s_1)(R_1)(\tau_{(1)}) \circ R_{\{2\}}(\tau_{(2)}) &= \emptyset \wedge \\ \forall s_2, R_2. R_{\{1\}}(\tau_{(1)}) \circ W_2.L(s_2)(R_2)(\tau_{(2)}) &= \emptyset \end{aligned}$$

Proof. We only show the former part since the other part holds analogously.

- When $\tau \in \text{TyNam} \setminus \mathcal{N}$: holds vacuously since $W_i.L(s_i)(R_i)(\tau_{(i)}) = \emptyset$.
- When $\tau = \tau' \rightarrow \tau''$: holds vacuously since $v_2 \in \text{FunVal}$ for any $(v_1, v_2) \in W_1.L(s_1)(R_1)(\tau_{(1)})$ but $\mathbf{I}(\tau, v_1, v_3) \notin \text{FunVal}$ for any τ, v_1, v_3 .
- When $\tau = \forall \alpha. \sigma$: holds vacuously since $v_2 \in \text{TyFunVal}$ for any $(v_1, v_2) \in W_1.L(s_1)(R_1)(\tau_{(1)})$ but $\mathbf{I}(\tau, v_1, v_3) \notin \text{TyFunVal}$ for any τ, v_1, v_3 .

\square

Lemma 84. $\forall R \in \text{VRelF}. \forall \tau \in \text{CTypeF} \setminus (\mathcal{N} \cup \{\text{ref } \tau' \in \text{CType}\})$.

$$R_{\{1\}}(\tau_{(1)}) \circ R_{\{2\}}(\tau_{(2)}) = R(\tau)$$

Proof. By construction of $R_{\{1\}}$ and $R_{\{2\}}$, the injectivity of \mathbf{I} , and Lemma 79. \square

Lemma 85.

$$\forall \tau \in \text{CTypeF}. \forall G \in \text{GK}(W). \forall (s_1, s_2) \in W.S. \left(\overline{G_{(1)}^{s_2}(s_1)} \bullet \overline{G_{(2)}^{s_1}(s_2)} \right) (\tau) = G(s_1, s_2)(\tau)$$

Proof. By case analysis on τ .

- when $\tau = \mathbf{n} \in \mathcal{N}_\exists$:

$$\begin{aligned}
& \overline{G_{(1)}^{s_2}(s_1)}(\mathbf{n}_{(1)}) \circ \overline{G_{(2)}^{s_1}(s_2)}(\mathbf{n}_{(2)}) \\
&= W.L(s_1, s_2)(G(s_1, s_2))(\mathbf{n}) && \text{(construction of } W.L) \\
&= G(s_1, s_2)(\mathbf{n}) && (G \in \text{GK}(W))
\end{aligned}$$

- when $\tau = \text{ref } \tau'$ or $\tau \in \mathcal{N}_1 \uplus \mathcal{N}_2$:

$$\begin{aligned}
& \overline{G_{(1)}^{s_2}(s_1)}(\tau_{(1)}) \circ \overline{G_{(2)}^{s_1}(s_2)}(\tau_{(2)}) \\
&= G_{(1)}^{s_2}(s_1)(\tau_{(1)}) \circ G_{(2)}^{s_1}(s_2)(\tau_{(2)}) \\
&= (W_1.L(s_1)(G_{(1)}^{s_2}(s_1))(\tau_{(1)}) \cup G(s_1, s_2)_{\{1\}}(\tau_{(1)})) \circ (W_2.L(s_2)(G_{(2)}^{s_1}(s_2))(\tau_{(2)}) \cup G(s_1, s_2)_{\{2\}}(\tau_{(2)})) \\
& && \text{(fixpoint)} \\
&= W_1.L(s_1)(G_{(1)}^{s_2}(s_1))(\tau_{(1)}) \circ W_2.L(s_2)(G_{(2)}^{s_1}(s_2))(\tau_{(2)}) && \text{(construction of } (-)_{\{i\}}) \\
&= W.L(s_1, s_2)(G(s_1, s_2))(\tau) && \text{(construction of } W.L(s_1, s_2)) \\
&= G(s_1, s_2)(\tau) && (G \in \text{GK}(W))
\end{aligned}$$

- when $\tau \in \text{CTypeF} \setminus (\mathcal{N} \cup \{\text{ref } \tau' \in \text{CType}\})$:

$$\begin{aligned}
& \overline{G_{(1)}^{s_2}(s_1)}(\tau_{(1)}) \circ \overline{G_{(2)}^{s_1}(s_2)}(\tau_{(2)}) \\
&= G_{(1)}^{s_2}(s_1)(\tau_{(1)}) \circ G_{(2)}^{s_1}(s_2)(\tau_{(2)}) \\
&= (W_1.L(s_1)(G_{(1)}^{s_2}(s_1))(\tau_{(1)}) \cup G(s_1, s_2)_{\{1\}}(\tau_{(1)})) \circ (W_2.L(s_2)(G_{(2)}^{s_1}(s_2))(\tau_{(2)}) \cup G(s_1, s_2)_{\{2\}}(\tau_{(2)})) \\
& && \text{(fixpoint)} \\
&= (W_1.L(s_1)(G_{(1)}^{s_2}(s_1))(\tau_{(1)}) \circ W_2.L(s_2)(G_{(2)}^{s_1}(s_2))(\tau_{(2)})) \cup (G(s_1, s_2)_{\{1\}}(\tau_{(1)}) \circ G(s_1, s_2)_{\{2\}}(\tau_{(2)})) \\
& && \text{(Lemma 83)} \\
&= W.L(s_1, s_2)(G(s_1, s_2))(\tau) \cup (G(s_1, s_2)_{\{1\}}(\tau_{(1)}) \circ G(s_1, s_2)_{\{2\}}(\tau_{(2)})) && \text{(construction of } W.L(s_1, s_2)) \\
&= W.L(s_1, s_2)(G(s_1, s_2))(\tau) \cup G(s_1, s_2)(\tau) && \text{(Lemma 84)} \\
&= G(s_1, s_2)(\tau) && (G \in \text{GK}(W))
\end{aligned}$$

□

Recall that \overline{R} is the least fixpoint of the monotone function $F_R : \text{VRel} \rightarrow \text{VRel}$ given as follows:

$$\begin{aligned}
F_R(X)(\tau_{\text{base}}) &:= \text{ID}_{\tau_{\text{base}}} \\
F_R(X)(\tau_1 \times \tau_2) &:= \{ ((v_1, v'_1), (v_2, v'_2)) \mid (v_1, v_2) \in X(\tau_1) \wedge (v'_1, v'_2) \in X(\tau_2) \} \\
F_R(X)(\tau_1 + \tau_2) &:= \{ (\text{inj}^1 v_1, \text{inj}^1 v_2) \mid (v_1, v_2) \in X(\tau_1) \} \cup \{ (\text{inj}^2 v_1, \text{inj}^2 v_2) \mid (v_1, v_2) \in X(\tau_2) \} \\
F_R(X)(\exists \alpha. \sigma) &:= \{ (\text{pack } v_1, \text{pack } v_2) \mid \exists \tau' \in \text{CType}. (v_1, v_2) \in X(\sigma[\tau'/\alpha]) \} \\
F_R(X)(\mu \alpha. \sigma) &:= \{ (\text{roll } v_1, \text{roll } v_2) \mid (v_1, v_2) \in X(\sigma[\mu \alpha. \sigma/\alpha]) \} \\
F_R(X)(\tau_1 \rightarrow \tau_2) &:= R(\tau_1 \rightarrow \tau_2) \\
F_R(X)(\forall \alpha. \sigma) &:= R(\forall \alpha. \sigma) \\
F_R(X)(\mathbf{n}) &:= R(\mathbf{n}) \\
F_R(X)(\text{ref } \tau) &:= R(\text{ref } \tau)
\end{aligned}$$

Lemma 86.

$$\forall \tau \in \text{CType} \setminus \text{CTypeF}. (F_{R_1}(X_1) \bullet F_{R_2}(X_2))(\tau) = F_R(X_1 \bullet X_2)(\tau)$$

Proof. Easy to check by case analysis of τ . We show the only interesting case, $\tau = \exists\alpha. \sigma$:

$$\begin{aligned}
& (v_1, v_3) \in (F_{R_1}(X_1) \bullet F_{R_2}(X_2))(\exists\alpha. \sigma) \\
\iff & \exists v'_1, v'_2, v'_3. v_1 = \text{pack } v'_1 \wedge v_3 = \text{pack } v'_3 \wedge (\text{pack } v'_1, \text{pack } v'_2) \in F_{R_1}(X_1)(\exists\alpha. \sigma_{(1)}) \wedge \\
& \quad (\text{pack } v'_2, \text{pack } v'_3) \in F_{R_2}(X_2)(\exists\alpha. \sigma_{(2)}) \\
\iff & \exists v'_1, v'_2, v'_3. \exists \tau'_1, \tau'_2 \in \text{CType}. v_1 = \text{pack } v'_1 \wedge v_3 = \text{pack } v'_3 \wedge (v'_1, v'_2) \in X_1(\sigma_{(1)}[\tau'_1/\alpha]) \wedge \\
& \quad (v'_2, v'_3) \in X_2(\sigma_{(2)}[\tau'_2/\alpha]) \\
\iff & \exists v'_1, v'_2, v'_3. \exists \tau' \in \text{CType}. v_1 = \text{pack } v'_1 \wedge v_3 = \text{pack } v'_3 \wedge (v'_1, v'_2) \in X_1(\sigma_{(1)}[\tau'_{(1)}/\alpha]) \wedge \\
& \quad (v'_2, v'_3) \in X_2(\sigma_{(2)}[\tau'_{(2)}/\alpha]) \quad (\text{Corollary 81}) \\
\iff & \exists v'_1, v'_2, v'_3. \exists \tau' \in \text{CType}. v_1 = \text{pack } v'_1 \wedge v_3 = \text{pack } v'_3 \wedge (v'_1, v'_2) \in X_1(\sigma[\tau'/\alpha]_{(1)}) \wedge \\
& \quad (v'_2, v'_3) \in X_2(\sigma[\tau'/\alpha]_{(2)}) \\
\iff & \exists v'_1, v'_2, v'_3. \exists \tau' \in \text{CType}. v_1 = \text{pack } v'_1 \wedge v_3 = \text{pack } v'_3 \wedge (v'_1, v'_3) \in (X_1 \bullet X_2)(\sigma[\tau'/\alpha]) \\
\iff & (v_1, v_3) \in F_R(X_1 \bullet X_2)(\exists\alpha. \sigma)
\end{aligned}$$

□

Lemma 87 (Generalized Fixed-Point Induction). For a monotone function $F \in \text{VRelF} \rightarrow \text{VRelF}$ and $R \in \text{VRelF}$,

$$F(R \cap [F]_{\emptyset}^*) \subseteq R \implies [F]_{\emptyset}^* \subseteq R$$

Proof. Suppose $F(R \cap [F]_{\emptyset}^*) \subseteq R$. By monotonicity of F , we have $F(R \cap [F]_{\emptyset}^*) \subseteq F([F]_{\emptyset}^*) = [F]_{\emptyset}^*$. Thus we have $F(R \cap [F]_{\emptyset}^*) \subseteq (R \cap [F]_{\emptyset}^*)$, i.e., $R \cap [F]_{\emptyset}^*$ is a prefixpoint of F . Thus we have $[F]_{\emptyset}^* \subseteq (R \cap [F]_{\emptyset}^*) \subseteq R$. □

Lemma 88 (Transitivity of Value Equivalence).

$$\forall G \in \text{GK}(W). \forall (s_1, s_2) \in W. \text{S. } \overline{G_{(1)}^{s_2}(s_1)} \bullet \overline{G_{(2)}^{s_1}(s_2)} = \overline{G(s_1, s_2)}$$

Proof. First part (\subseteq): It suffices to show $\overline{G_{(1)}^{s_2}(s_1)} \subseteq S$, where:

$$S = \{ (\tau, v_1, v_2) \mid \forall \tau', v'_3. \tau = \tau'_{(1)} \wedge (\tau'_{(2)}, v_2, v'_3) \in \overline{G_{(2)}^{s_1}(s_2)} \implies (\tau', v_1, v'_3) \in \overline{G(s_1, s_2)} \}$$

We prove it using Lemma 87, i.e., it suffices to show $F_{G_{(1)}^{s_2}(s_1)}(S') \subseteq S$ for $S' = S \cap \overline{G_{(1)}^{s_2}(s_1)}$, which is equivalent to show $F_{G_{(1)}^{s_2}(s_1)}(S') \bullet \overline{G_{(2)}^{s_1}(s_2)} \subseteq \overline{G(s_1, s_2)}$ by definition of S .

• $\tau \notin \text{CTypeF}$:

$$\begin{aligned}
& (F_{G_{(1)}^{s_2}(s_1)}(S') \bullet \overline{G_{(2)}^{s_1}(s_2)})(\tau) \\
&= (F_{G_{(1)}^{s_2}(s_1)}(S') \bullet F_{G_{(2)}^{s_1}(s_2)}(\overline{G_{(2)}^{s_1}(s_2)}))(\tau) \\
&= F_{G(s_1, s_2)}(S' \bullet \overline{G_{(2)}^{s_1}(s_2)})(\tau) \quad (\text{Lemma 86}) \\
&\subseteq F_{G(s_1, s_2)}(\overline{G(s_1, s_2)})(\tau) \\
&= \overline{G(s_1, s_2)}(\tau)
\end{aligned}$$

• $\tau \in \text{CTypeF}$:

$$(F_{G_{(1)}^{s_2}(s_1)}(S') \bullet \overline{G_{(2)}^{s_1}(s_2)})(\tau) \subseteq (\overline{G_{(1)}^{s_2}(s_1)} \bullet \overline{G_{(2)}^{s_1}(s_2)})(\tau) = G(s_1, s_2)(\tau) = \overline{G(s_1, s_2)}(\tau) \quad (\text{Lemma 85})$$

Second part (\supseteq): By induction it suffices to show $F_{G(s_1, s_2)}(\overline{G_{(1)}^{s_2}(s_1)} \bullet \overline{G_{(2)}^{s_1}(s_2)}) \subseteq \overline{G_{(1)}^{s_2}(s_1)} \bullet \overline{G_{(2)}^{s_1}(s_2)}$.

• $\tau \notin \text{CTypeF}$:

$$\begin{aligned}
& F_{G(s_1, s_2)}(\overline{G_{(1)}^{s_2}(s_1)} \bullet \overline{G_{(2)}^{s_1}(s_2)})(\tau) \\
&= (F_{G_{(1)}^{s_2}(s_1)}(\overline{G_{(1)}^{s_2}(s_1)}) \bullet F_{G_{(2)}^{s_1}(s_2)}(\overline{G_{(2)}^{s_1}(s_2)}))(\tau) \quad (\text{Lemma 86}) \\
&= (\overline{G_{(1)}^{s_2}(s_1)} \bullet \overline{G_{(2)}^{s_1}(s_2)})(\tau)
\end{aligned}$$

- $\tau \in \text{CTypeF}$:

$$\begin{aligned}
& F_{G(s_1, s_2)}(\overline{G_{(1)}^{s_2}(s_1)} \bullet \overline{G_{(2)}^{s_1}(s_2)})(\tau) \\
&= \overline{G(s_1, s_2)}(\tau) \\
&= \overline{(G_{(1)}^{s_2}(s_1) \bullet G_{(2)}^{s_1}(s_2))}(\tau) \quad (\text{Lemma 85})
\end{aligned}$$

□

5.1.4 Transitivity of Term Equivalence

Lemma 89 (Transitivity of Term Equivalence). If $G \in \text{GK}(W)$ and $(s_1^0, s_2^0), (s_1, s_2) \in W.S$, then:

1. $\mathbf{E}_{W_1}(G_{(1)}^{s_2})(s_1^0, s_1)(\tau_{(1)}) \circ \mathbf{E}_{W_2}(G_{(2)}^{s_1})(s_2^0, s_2)(\tau_{(2)}) \subseteq \mathbf{E}_W(G)((s_1^0, s_2^0), (s_1, s_2))(\tau)$
2. $\mathbf{K}_{W_1}(G_{(1)}^{s_2})(s_1^0, s_1)(\tau_{(1)}, \pi_{(1)}) \circ \mathbf{K}_{W_2}(G_{(2)}^{s_1})(s_2^0, s_2)(\tau_{(2)}, \pi_{(2)}) \subseteq \mathbf{K}_W(G)((s_1^0, s_2^0), (s_1, s_2))(\tau, \pi)$

Proof. Let

$$\begin{aligned}
\mathbf{E}'_W(G)((s_1^0, s_2^0), (s_1, s_2))(\tau) &= \mathbf{E}_{W_1}(G_{(1)}^{s_2})(s_1^0, s_1)(\tau_{(1)}) \circ \mathbf{E}_{W_2}(G_{(2)}^{s_1})(s_2^0, s_2)(\tau_{(2)}) \\
\mathbf{K}'_W(G)((s_1^0, s_2^0), (s_1, s_2))(\tau, \pi) &= \mathbf{K}_{W_1}(G_{(1)}^{s_2})(s_1^0, s_1)(\tau_{(1)}, \pi_{(1)}) \circ \mathbf{K}_{W_2}(G_{(2)}^{s_1})(s_2^0, s_2)(\tau_{(2)}, \pi_{(2)})
\end{aligned}$$

Now it suffices to show that $\mathbf{E}'_W, \mathbf{K}'_W$ forms a post-fixpoint.

We first consider \mathbf{K}'_W . We suppose

- $(\tau_{(1)}, \pi_{(1)}, K_1, K_2) \in \mathbf{K}_{W_1}(G_{(1)}^{s_2})(s_1^0, s_1)$
- $(\tau_{(2)}, \pi_{(2)}, K_2, K_3) \in \mathbf{K}_{W_2}(G_{(2)}^{s_1})(s_2^0, s_2)$
- $(\tau, v_1, v_3) \in \overline{G(s_1, s_2)}$

and must show $(\pi, K_1[v_1], K_3[v_3]) \in \mathbf{E}'_W(G)((s_1^0, s_2^0), (s_1, s_2))$. By Lemma 88 there is v_2 such that $(\tau_{(1)}, v_1, v_2) \in \overline{G_{(1)}^{s_2}(s_1)}$ and $(\tau_{(2)}, v_2, v_3) \in \overline{G_{(2)}^{s_1}(s_2)}$. Hence we get:

- $(\pi_{(1)}, K_1[v_1], K_2[v_2]) \in \mathbf{E}_{W_1}(G_{(1)}^{s_2})(s_1^0, s_1)$
- $(\pi_{(2)}, K_2[v_2], K_3[v_3]) \in \mathbf{E}_{W_2}(G_{(2)}^{s_1})(s_2^0, s_2)$

By definition of \mathbf{E}'_W we are done.

We now consider \mathbf{E}'_W . Suppose $(\tau_{(1)}, e_1, e_2) \in \mathbf{E}_{W_1}(G_{(1)}^{s_2})(s_1^0, s_1)$ and $(\tau_{(2)}, e_2, e_3) \in \mathbf{E}_{W_2}(G_{(2)}^{s_1})(s_2^0, s_2)$. Further suppose $(h_1, h_3) \in W.H(s_1, s_2)(G(s_1, s_2))$ and $h_1^F, h_3^F \in \text{Heap}$ such that $h_1 \uplus h_1^F, h_3 \uplus h_3^F$ defined. By construction of $W.H$, we have h_2 such that $(h_1, h_2) \in W_1.H(s_1)(G_{(1)}^{s_2})$ and $(h_2, h_3) \in W_2.H(s_2)(G_{(2)}^{s_1})$. By Lemma 18, from *consistent*(W_1), $(\tau_{(1)}, e_1, e_2) \in \mathbf{E}_{W_1}(G_{(1)}^{s_2})(s_1^0, s_1)$ and $G_{(1)}^{s_2} = W_1.L(G_{(1)}^{s_2}) \cup G(s_1, s_2)_{\{1\}}$, we get three cases by letting $h_2^F = \emptyset$. For each of these, again by Lemma 18 and letting $h_2^F = \emptyset$, we get another three subcases from *consistent*(W_2) and $(\tau_{(2)}, e_2, e_3) \in \mathbf{E}_{W_2}(G_{(2)}^{s_1})(s_2^0, s_2)$. So there are nine cases in total.

1. (1) $h_1 \uplus h_1^F, e_1 \uparrow \wedge h_2, e_2 \uparrow$
(1) $h_2, e_2 \uparrow \wedge h_3 \uplus h_3^F, e_3 \uparrow$

We are done because $h_1 \uplus h_1^F, e_1 \uparrow \wedge h_3 \uplus h_3^F, e_3 \uparrow$.

2. (1) $h_1 \uplus h_1^F, e_1 \uparrow \wedge h_2, e_2 \uparrow$
(2) $h_2, e_2 \hookrightarrow^* h_2', v_2 \wedge h_3 \uplus h_3^F, e_3 \hookrightarrow^* h_3', v_3$

This is a contradiction by determinacy.

3. (1) $h_1 \uplus h_1^F, e_1 \uparrow \wedge h_2, e_2 \uparrow$
(3) $h_2, e_2 \hookrightarrow^* h'_2, K_2[e'_2] \wedge h_3 \uplus h_3^F, e_3 \hookrightarrow^* h'_3, K_3[e'_3]$ with $(\tau', e'_2, e'_3) \in \mathbf{S}(G(s_1, s'_2)_{\{2\}}, G^{s_1}_{(2)}(s'_2))$

Since $e'_2 = \mathbf{I}(\tilde{\tau}, f_1, f_3) v_2$ or $e'_2 = \mathbf{I}(\tilde{\tau}, f_1, f_3) \llbracket$ for some $\tilde{\tau}, f_1, f_3, v_2$, we know by determinacy that e_2 eventually gets stuck. This is a contradiction.

4. (2) $h_1 \uplus h_1^F, e_1 \hookrightarrow^* h'_1 \uplus h_1^F, v_1 \wedge h_2, e_2 \hookrightarrow^* h'_2, v_2$ with $s'_1 \sqsupseteq [s_1^0, s_1]$ and $(h'_1, h'_2) \in W_1.H(s'_1)(G^{s_2}_{(1)}(s'_1))$
and $(\tau_{(1)}, v_1, v_2) \in \overline{G^{s_2}_{(1)}(s'_1)}$
(2) $h_2, e_2 \hookrightarrow^* h''_2, v'_2 \wedge h_3 \uplus h_3^F, e_3 \hookrightarrow^* h'_3 \uplus h_3^F, v_3$ with $s'_2 \sqsupseteq [s_2^0, s_2]$ and $(h''_2, h'_3) \in W_2.H(s'_2)(G^{s_1}_{(2)}(s'_2))$
and $(\tau_{(2)}, v'_2, v_3) \in \overline{G^{s_1}_{(2)}(s'_2)}$

By determinacy we have $h'_2 = h''_2$ and $v_2 = v'_2$. Since $G^{s_2}_{(1)}(s'_1) \leq G^{s'_2}_{(1)}(s'_1)$ and $G^{s_1}_{(2)}(s'_2) \leq G^{s'_1}_{(2)}(s'_2)$, we have $(\tau, v_1, v_3) \in \overline{G(s'_1, s'_2)}$ by Lemma 88. Similarly, $(h'_1, h'_3) \in W.H(s'_1, s'_2)(G(s'_1, s'_2))$ by construction of $W.H$. Since $(s'_1, s'_2) \sqsupseteq [(s_1^0, s_2^0), (s_1, s_2)]$, we are done.

5. (2) $h_1 \uplus h_1^F, e_1 \hookrightarrow^* h'_1 \uplus h_1^F, v_1 \wedge h_2, e_2 \hookrightarrow^* h'_2, v_2$
(3) $h_2, e_2 \hookrightarrow^* h''_2, K_2[e'_2] \wedge h_3 \uplus h_3^F, e_3 \hookrightarrow^* h'_3 \uplus h_3^F, K_3[e'_3]$ with $(\tau', e'_2, e'_3) \in \mathbf{S}(G(s_1, s'_2)_{\{2\}}, G^{s_1}_{(2)}(s'_2))$

Since $e'_2 = \mathbf{I}(\tilde{\tau}, f_1, f_3) v_2$ or $e'_2 = \mathbf{I}(\tilde{\tau}, f_1, f_3) \llbracket$ for some $\tilde{\tau}, f_1, f_3, v_2$, we know by determinacy that e_2 eventually gets stuck. This is a contradiction.

6. (3) $h_1 \uplus h_1^F, e_1 \hookrightarrow^* h'_1 \uplus h_1^F, K_1[e'_1] \wedge h_2, e_2 \hookrightarrow^* h'_2, K_2[e'_2]$ with $s'_1 \sqsupseteq s_1$ and $(h'_1, h'_2) \in W_1.H(s'_1)(G^{s_2}_{(1)}(s'_1))$
and $(\tau', e'_1, e'_2) \in \mathbf{S}(G(s'_1, s_2)_{\{1\}}, G^{s_2}_{(1)}(s'_1))$ and $\forall s''_1 \sqsupseteq_{\text{pub}} s'_1. \forall G' \geq G^{s_2}_{(1)}. (\tau', \tau_{(1)}, K_1, K_2) \in \mathbf{K}_{W_1}(G')(s_1^0, s''_1)$
(3) $h_2, e_2 \hookrightarrow^* h''_2, K_2[e'_2] \wedge h_3 \uplus h_3^F, e_3 \hookrightarrow^* h'_3 \uplus h_3^F, K_3[e'_3]$ with $s'_2 \sqsupseteq s_2$ and $(h''_2, h'_3) \in W_2.H(s'_2)(G^{s_1}_{(2)}(s'_2))$
and $(\tau'', e''_2, e'_3) \in \mathbf{S}(G(s_1, s'_2)_{\{2\}}, G^{s_1}_{(2)}(s'_2))$ and $\forall s''_2 \sqsupseteq_{\text{pub}} s'_2. \forall G' \geq G^{s_1}_{(2)}. (\tau'', \tau_{(2)}, K_2, K_3) \in \mathbf{K}_{W_2}(G')(s_2^0, s''_2)$

By definition of \mathbf{S} , $G(s'_1, s_2)_{\{1\}}$ and $G(s_1, s'_2)_{\{2\}}$, there are four possibilities.

(a) We have for some $\tilde{\tau}, \hat{\tau}, f_1, f_3, v_1, v_2$,

- $e'_1 = f_1 v_1$ and $e'_2 = \mathbf{I}(\tilde{\tau} \rightarrow \hat{\tau}, f_1, f_3) v_2$ and $\tau' = \hat{\tau}_{(1)}$
- $(\tilde{\tau} \rightarrow \hat{\tau}, f_1, f_3) \in G(s'_1, s_2) \subseteq G(s'_1, s'_2)$ and $(\tilde{\tau}_{(1)}, v_1, v_2) \in \overline{G^{s_2}_{(1)}(s'_1)} \subseteq \overline{G^{s'_2}_{(1)}(s'_1)}$

and for some $\tilde{\tau}', \hat{\tau}', f'_1, f'_3, v'_2, v_3$,

- $e''_2 = \mathbf{I}(\tilde{\tau}' \rightarrow \hat{\tau}', f'_1, f'_3) v'_2$ and $e'_3 = f'_3 v_3$ and $\tau'' = \hat{\tau}'_{(2)}$
- $(\tilde{\tau}' \rightarrow \hat{\tau}', f'_1, f'_3) \in G(s_1, s'_2) \subseteq G(s'_1, s'_2)$ and $(\tilde{\tau}'_{(2)}, v'_2, v_3) \in \overline{G^{s_1}_{(2)}(s'_2)} \subseteq \overline{G^{s'_1}_{(2)}(s'_2)}$

Since both e'_2 and e''_2 are stuck, we know by determinacy:

- $h'_2 = h''_2$ and $K_2 = K'_2$ and $\mathbf{I}(\tilde{\tau} \rightarrow \hat{\tau}, f_1, f_3) = \mathbf{I}(\tilde{\tau}' \rightarrow \hat{\tau}', f'_1, f'_3)$ and $v_2 = v'_2$

Since \mathbf{I} is injective, we also have:

- $\tilde{\tau} = \tilde{\tau}'$ and $\hat{\tau} = \hat{\tau}'$ and $f_1 = f'_1$ and $f_3 = f'_3$.

Since $e'_3 = f_3 v_3 \wedge (f_1, f_3) \in G(s'_1, s'_2)(\tilde{\tau} \rightarrow \hat{\tau}) \wedge (v_1, v_3) \in \overline{G(s'_1, s'_2)}(\tilde{\tau})$ by Lemma 88, we have

- $(\hat{\tau}, e'_1, e'_3) \in \mathbf{S}(G(s'_1, s'_2), G(s'_1, s'_2))$.

Since $(h'_1, h'_2) \in W_1.H(s'_1)(G^{s_2}_{(1)}(s'_1)) \subseteq W_1.H(s'_1)(G^{s'_2}_{(1)}(s'_1))$ and $(h'_2, h'_3) \in W_2.H(s'_2)(G^{s_1}_{(2)}(s'_2)) \subseteq W_2.H(s'_2)(G^{s'_1}_{(2)}(s'_2))$, we have

- $(s'_1, s'_2) \sqsupseteq (s_1, s_2)$ and $(h'_1, h'_3) \in W.H(s'_1, s'_2)(G(s'_1, s'_2))$ by construction of $W.H$.

It remains to show that $\forall (s''_1, s''_2) \sqsupseteq_{\text{pub}} (s'_1, s'_2). \forall G' \geq G. (\hat{\tau}, \tau, K_1, K_3) \in \mathbf{K}'_W(G)((s_1^0, s_2^0), (s''_1, s''_2))$.

Since $G^{s'_2}_{(1)} \geq G^{s_2}_{(1)}$ and $G^{s'_1}_{(2)} \geq G^{s_1}_{(2)}$, we have

$$(\tau', \tau_{(1)}, K_1, K_2) \in \mathbf{K}_{W_1}(G^{s'_2}_{(1)})(s_1^0, s''_1) \wedge (\tau'', \tau_{(2)}, K_2, K_3) \in \mathbf{K}_{W_2}(G^{s'_1}_{(2)})(s_2^0, s''_2)$$

Note that $\tau' = \widehat{\tau}_{(1)}$ and $\tau'' = \widehat{\tau}_{(2)}$.

Thus, by definition of \mathbf{K}'_W , we have $(\widehat{\tau}, \tau, K_1, K_3) \in \mathbf{K}'_W(G')((s_1^0, s_2^0), (s_1'', s_2''))$.

(b) We have for some $\sigma, \widehat{\tau}_1, f_1, f_3$,

- $e'_1 = f_1 \llbracket$ and $e'_2 = \mathbf{I}(\forall \alpha. \sigma, f_1, f_3) \llbracket$ and $\tau' = \sigma_{(1)}[\widehat{\tau}_1/\alpha]$
- $(\forall \alpha. \sigma, f_1, f_3) \in G(s'_1, s_2) \subseteq G(s'_1, s'_2)$

and for some $\sigma', \widehat{\tau}_2, f'_1, f'_3$,

- $e''_2 = \mathbf{I}(\forall \alpha. \sigma', f'_1, f'_3) \llbracket$ and $e'_3 = f'_3 \llbracket$ and $\tau'' = \sigma'_{(2)}[\widehat{\tau}_2/\alpha]$
- $(\forall \alpha. \sigma', f'_1, f'_3) \in G(s_1, s'_2) \subseteq G(s'_1, s'_2)$

Since both e'_2 and e''_2 are stuck, we know by determinacy:

- $h'_2 = h''_2$ and $K_2 = K'_2$ and $\mathbf{I}(\forall \alpha. \sigma, f_1, f_3) = \mathbf{I}(\forall \alpha. \sigma', f'_1, f'_3)$.

Since \mathbf{I} is injective, we also have:

- $\sigma = \sigma'$ and $f_1 = f'_1$ and $f_3 = f'_3$.

Since $e'_3 = f_3 \llbracket \wedge (f_1, f_3) \in G(s'_1, s'_2)(\forall \alpha. \sigma)$, we have

- $(\sigma[\widehat{\tau}/\alpha], e'_1, e'_3) \in \mathbf{S}(G(s'_1, s'_2), G(s'_1, s'_2))$ for some $\widehat{\tau}$ with $\widehat{\tau}_{(1)} = \widehat{\tau}_1 \wedge \widehat{\tau}_{(2)} = \widehat{\tau}_2$ by Corollary 81.

Since $(h'_1, h'_2) \in W_1.H(s'_1)(G^{s_2}_{(1)}(s'_1)) \subseteq W_1.H(s'_1)(G^{s'_2}_{(1)}(s'_1))$ and $(h'_2, h'_3) \in W_2.H(s'_2)(G^{s_1}_{(2)}(s'_2)) \subseteq W_2.H(s'_2)(G^{s'_1}_{(2)}(s'_2))$, we have

- $(s'_1, s'_2) \sqsupseteq (s_1, s_2)$ and $(h'_1, h'_3) \in W.H(s'_1, s'_2)(G(s'_1, s'_2))$ by construction of $W.H$.

It remains to show that $\forall (s_1'', s_2'') \sqsupseteq_{\text{pub}} (s'_1, s'_2). \forall G' \geq G. (\sigma[\widehat{\tau}/\alpha], \tau, K_1, K_3) \in \mathbf{K}'_W(G')((s_1^0, s_2^0), (s_1'', s_2''))$.

Since $G^{s_2''}_{(1)} \geq G^{s_2}_{(1)}$ and $G^{s_1''}_{(2)} \geq G^{s_1}_{(2)}$, we have

$$(\tau', \tau_{(1)}, K_1, K_2) \in \mathbf{K}_{W_1}(G^{s_2''}_{(1)})(s_1^0, s_1'') \wedge (\tau'', \tau_{(2)}, K_2, K_3) \in \mathbf{K}_{W_2}(G^{s_1''}_{(2)})(s_2^0, s_2'')$$

Note that $\tau' = \sigma_{(1)}[\widehat{\tau}_1/\alpha] = \sigma[\widehat{\tau}/\alpha]_{(1)}$ and $\tau'' = \sigma_{(2)}[\widehat{\tau}_2/\alpha] = \sigma[\widehat{\tau}/\alpha]_{(2)}$.

Thus, by definition of \mathbf{K}'_W , we have $(\sigma[\widehat{\tau}/\alpha], \tau, K_1, K_3) \in \mathbf{K}'_W(G')((s_1^0, s_2^0), (s_1'', s_2''))$.

(c) Proceeding as in the previous two cases, we get $e'_2 = \mathbf{I}(\widetilde{\tau} \rightarrow \widehat{\tau}, f_1, f_3) v_2$ and $e''_2 = \mathbf{I}(\forall \alpha. \widetilde{\tau}', f'_1, f'_3) \llbracket$ and later then $e'_2 = e''_2$, which is a contradiction.

(d) Similar to the previous case.

7. The remaining three cases (2)(1), (3)(1) and (3)(2) are symmetric to (1)(2), (1)(3) and (2)(3), respectively.

□

5.1.5 Transitivity w.r.t. the Full World

Lemma 90.

$$\Delta; \Gamma \vdash e_1 \sim_W e_3 : \sigma$$

Proof.

We show *inhabited*(W).

- By Lemma 2 we have $[W_i] \in \text{GK}(W_i)$ for $i = 1, 2$.
- From *inhabited*(W_i) for $i = 1, 2$, we have s_i^0 such that $(\emptyset, \emptyset) \in W_i.H(s_i^0)([W_i](s_i^0))$.

- Thus, for any $G \in \text{GK}(W)$, we have

$$\begin{aligned}
(\emptyset, \emptyset) &\in W_1.\mathbf{H}(s_1^0)([W_1](s_1^0)) \circ W_2.\mathbf{H}(s_2^0)([W_2](s_2^0)) \\
&\subseteq W_1.\mathbf{H}(s_1^0)(G_{(1)}^{s_1^0}(s_1^0)) \circ W_2.\mathbf{H}(s_2^0)(G_{(2)}^{s_2^0}(s_2^0)) \quad (\text{Lemmas 82 and 2}) \\
&= W.\mathbf{H}(s_1^0, s_2^0)(G(s_1^0, s_2^0)) \quad (\text{construction of } W.\mathbf{H})
\end{aligned}$$

We show *consistent*(W).

- Suppose $G \in \text{GK}(W)$ and $(e'_1, e'_3) \in \mathbf{S}(W.\mathbf{L}(s_1, s_2)(G(s_1, s_2)), G(s_1, s_2))(\tau')$.
- We need to show $(\text{beta}(e'_1), \text{beta}(e'_3)) \in \mathbf{E}_W(G)((s_1, s_2), (s_1, s_2))(\tau')$.
- By definition of \mathbf{S} and $W.\mathbf{L}$, and by Lemma 88, there is e'_2 such that $(e'_1, e'_2) \in \mathbf{S}(W_1.\mathbf{L}(s_1)(G_{(1)}^{s_2^0}(s_1)), G_{(1)}^{s_2^0}(s_1))(\tau'_{(1)})$ and $(e'_2, e'_3) \in \mathbf{S}(W_2.\mathbf{L}(s_2)(G_{(2)}^{s_1^0}(s_2)), G_{(2)}^{s_1^0}(s_2))(\tau'_{(2)})$.
- From *consistent*(W_1) and *consistent*(W_2), we get

$$(\tau'_{(1)}, \text{beta}(e'_1), \text{beta}(e'_2)) \in \mathbf{E}_{W_1}(G_{(1)}^{s_2^0})(s_1, s_1) \wedge (\tau'_{(2)}, \text{beta}(e'_2), \text{beta}(e'_3)) \in \mathbf{E}_{W_2}(G_{(2)}^{s_1^0})(s_2, s_2) .$$

- By Lemma 89 we are done.

We show $\forall G \in \text{GK}(W). \forall s_1, s_2. \forall \delta \in \text{TyEnv}(\Delta). \forall (\gamma_1, \gamma_3) \in \text{Env}(\delta\Gamma, G(s_1, s_2))$.

$$(\delta\sigma, \gamma_1 e_1, \gamma_3 e_3) \in \mathbf{E}_W(G)((s_1, s_2), (s_1, s_2)) .$$

- By Lemma 88 there exists γ_2 such that

$$(\gamma_1, \gamma_2) \in \text{Env}((\delta\Gamma)_{(1)}, G_{(1)}^{s_2^0}(s_1)) \wedge (\gamma_2, \gamma_3) \in \text{Env}((\delta\Gamma)_{(2)}, G_{(2)}^{s_1^0}(s_2)) .$$

- Since $\text{names}(\Gamma) \cap \mathcal{N}_\exists = \emptyset$, we have $(\delta\Gamma)_{(i)} = \delta_{(i)}\Gamma$.
- From $\Delta; \Gamma \vdash e_1 \sim_{W_1} e_2 : \sigma$ and $\Delta; \Gamma \vdash e_2 \sim_{W_2} e_3 : \sigma$ we thus get:

$$(\delta_{(1)}\sigma, \gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{W_1}(G_{(1)}^{s_2^0})(s_1, s_1) \wedge (\delta_{(2)}\sigma, \gamma_2 e_2, \gamma_3 e_3) \in \mathbf{E}_{W_2}(G_{(2)}^{s_1^0})(s_2, s_2)$$

- Since $\text{names}(\sigma) \cap \mathcal{N}_\exists = \emptyset$, we have $\delta_{(i)}\sigma = (\delta\sigma)_{(i)}$.
- Thus, by Lemma 89, we have $(\delta\sigma, \gamma_1 e_1, \gamma_3 e_3) \in \mathbf{E}_W(G)((s_1, s_2), (s_1, s_2))$.

□

5.2 Constructing an Isomorphic Lifted World

We now come to the second part of the proof. Recall that the goal is to show $\Delta; \Gamma \vdash e_1 \sim_{e_3} : \sigma$ and that, to this end, we already assumed a set of names \mathcal{N} to be given. Hence we must find $w \in \text{LWorld}$ such that:

1. $w.\mathbf{N} \subseteq \mathcal{N}$
2. *stable*(w)
3. $\Delta; \Gamma \vdash e_1 \sim_{w\uparrow} e_3 : \tau$

We will now construct such a w . However, instead of showing (3) directly, we will rely on Theorem 73 and Lemma 90 and just show that $w\uparrow$ is isomorphic to W .

Definition 22. For $s_{\text{rf}}, s'_{\text{rf}} \in W_{\text{ref}}.\mathbf{S}$, we define $s_{\text{rf}} \setminus_{[1]} s'_{\text{rf}}, s_{\text{rf}} \setminus_{[2]} s'_{\text{rf}} \in W_{\text{ref}}.\mathbf{S}$ as follows:

$$\begin{aligned} s_{\text{rf}} \setminus_{[1]} s'_{\text{rf}} &:= \{ (\tau, \ell_1, \ell_2) \in s_{\text{rf}} \mid \forall \tau', \ell'. (\tau', \ell_1, \ell') \notin s'_{\text{rf}} \} \\ s_{\text{rf}} \setminus_{[2]} s'_{\text{rf}} &:= \{ (\tau, \ell_1, \ell_2) \in s_{\text{rf}} \mid \forall \tau', \ell'. (\tau', \ell', \ell_2) \notin s'_{\text{rf}} \} \end{aligned}$$

Definition 23. We construct $w \in \text{LWorld}$ as follows (recall that $W_i = w_i \uparrow$).

$$\begin{aligned} w.\mathbf{N} &:= W.\mathbf{N} \\ w.\mathbf{S} &:= W.\mathbf{S} \\ w.\sqsupseteq &:= W.\sqsupseteq \\ w.\sqsupseteq_{\text{pub}} &:= W.\sqsupseteq_{\text{pub}} \\ w.\mathbf{L}(s_{\text{rf}})(s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)(R) &:= \{ (\tau, v_1, v_3) \in W.\mathbf{L}(s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)(R) \mid \forall \tau'. \tau \neq \text{ref } \tau' \} \\ w.\mathbf{H}(s_{\text{rf}})(s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)(R) &:= \{ (h_1, h_3) \mid s_{\text{rf}} = s_{\text{rf}}^1 \bullet s_{\text{rf}}^2 \wedge \exists h_1^\circ, h_1^\bullet, h_{2a}^\circ, h_{2a}^\bullet, h_{2b}^\circ, h_{2b}^\bullet, h_3^\circ, h_3^\bullet. \\ &\quad h_1 = h_1^\circ \uplus h_1^{\text{lc}} \wedge h_{2a}^\circ \uplus h_{2a}^{\text{lc}} = h_{2b}^\circ \uplus h_{2b}^{\text{lc}} \wedge h_3 = h_3^\circ \uplus h_3^{\text{lc}} \wedge \\ &\quad \text{dom}(h_{2a}^{\text{lc}}) \cap \text{dom}_{[2]}(s_{\text{rf}}^1) = \emptyset \wedge \text{dom}(h_{2b}^{\text{lc}}) \cap \text{dom}_{[1]}(s_{\text{rf}}^2) = \emptyset \wedge \\ &\quad (h_1^\circ, h_{2a}^\circ) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}}^1 \setminus_{[1]} s_{\text{rf}}^2)([W_1.\mathbf{L}(s_{\text{rf}}^1, s_{\text{lc}}^1)]_{R_{\{1\}}^*}) \wedge \\ &\quad (h_1^{\text{lc}}, h_{2a}^{\text{lc}}) \in w_1.\mathbf{H}(s_{\text{rf}}^1)(s_{\text{lc}}^1)([W_1.\mathbf{L}(s_{\text{rf}}^1, s_{\text{lc}}^1)]_{R_{\{1\}}^*}) \wedge \\ &\quad (h_{2b}^\circ, h_3^\circ) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}}^2 \setminus_{[2]} s_{\text{rf}}^2)([W_2.\mathbf{L}(s_{\text{rf}}^2, s_{\text{lc}}^2)]_{R_{\{2\}}^*}) \wedge \\ &\quad (h_{2b}^{\text{lc}}, h_3^{\text{lc}}) \in w_2.\mathbf{H}(s_{\text{rf}}^2)(s_{\text{lc}}^2)([W_2.\mathbf{L}(s_{\text{rf}}^2, s_{\text{lc}}^2)]_{R_{\{2\}}^*}) \} \end{aligned}$$

Definition 24. For $G \in \text{GK}(w \uparrow)$, we define $\overleftarrow{G} \in W.\mathbf{S} \rightarrow \text{VRelF}$ as follows:

$$\overleftarrow{G}(s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2) := G(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2, s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2) .$$

Lemma 91.

$$s_{\text{rf}}^1, s_{\text{rf}}^2 \in W_{\text{ref}}.\mathbf{S} \implies s_{\text{rf}}^1 \bullet s_{\text{rf}}^2 \in W_{\text{ref}}.\mathbf{S}$$

Proof.

- Since s_{rf}^1 and s_{rf}^2 are finite by assumption, $s_{\text{rf}}^1 \bullet s_{\text{rf}}^2$ is finite, too.
- Now suppose $(\tau, \ell_1, \ell_3), (\tau', \ell'_1, \ell'_3) \in s_{\text{rf}}^1 \bullet s_{\text{rf}}^2$.
- Then there is ℓ_2 such that $(\tau_{(1)}, \ell_1, \ell_2) \in s_{\text{rf}}^1$ and $(\tau_{(2)}, \ell_2, \ell_3) \in s_{\text{rf}}^2$.
- Also there is ℓ'_2 such that $(\tau'_{(1)}, \ell'_1, \ell'_2) \in s_{\text{rf}}^1$ and $(\tau'_{(2)}, \ell'_2, \ell'_3) \in s_{\text{rf}}^2$.
- Now further suppose $\ell_1 = \ell'_1$ (the reasoning for $\ell_3 = \ell'_3$ is analogous).
- From the assumption we get $\tau_{(1)} = \tau'_{(1)}$ and $\ell_2 = \ell'_2$.
- From the latter and the assumption we get $\tau_{(2)} = \tau'_{(2)}$ and $\ell_3 = \ell'_3$.
- It thus remains to show $\tau = \tau'$, which follows by Lemma 79.

□

Lemma 92.

1. If $\hat{s}_{\text{rf}}^1 \sqsupseteq s_{\text{rf}}^1$ and $\hat{s}_{\text{rf}}^2 \sqsupseteq s_{\text{rf}}^2$, then $\hat{s}_{\text{rf}}^1 \bullet \hat{s}_{\text{rf}}^2 \sqsupseteq s_{\text{rf}}^1 \bullet s_{\text{rf}}^2$.
2. If $\hat{s}_{\text{rf}}^1 \sqsupseteq_{\text{pub}} s_{\text{rf}}^1$ and $\hat{s}_{\text{rf}}^2 \sqsupseteq_{\text{pub}} s_{\text{rf}}^2$, then $\hat{s}_{\text{rf}}^1 \bullet \hat{s}_{\text{rf}}^2 \sqsupseteq_{\text{pub}} s_{\text{rf}}^1 \bullet s_{\text{rf}}^2$.

Proof. Easy to check.

□

Lemma 93. For $G \in \text{GK}(w \uparrow)$, we have $\overleftarrow{G} \in \text{GK}(W)$.

Proof. We know from Lemma 92 and $G \in \text{GK}(w\uparrow)$ that \overleftarrow{G} is monotone. It thus remains to show $\forall s. \overleftarrow{G}(s) \geq_{\text{ref}}^{w.N} W.L(s)(\overleftarrow{G}(s))$:

- Suppose $s = (s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)$ and τ are given.
- From $G \in \text{GK}(w\uparrow)$ we know $\overleftarrow{G}(s)(\tau) \geq_{\text{ref}}^{w.N} w\uparrow.L(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2, s)(\overleftarrow{G}(s))(\tau)$.
- Note that $w.N = W.N$.
- If τ is not of the form $\text{ref } \tau'$, then we have:

$$\begin{aligned} & w\uparrow.L(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2, s)(\overleftarrow{G}(s))(\tau) \\ &= w.L(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2, s)(\overleftarrow{G}(s))(\tau) \\ &= W.L(s)(\overleftarrow{G}(s))(\tau) \end{aligned}$$

- If $\tau = \text{ref } \tau'$, then we have:

$$\begin{aligned} & w\uparrow.L(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2, s)(\overleftarrow{G}(s))(\tau) \\ &= W_{\text{ref}}.L(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2)(\overleftarrow{G}(s))(\tau) \\ &= (s_{\text{rf}}^1 \bullet s_{\text{rf}}^2)(\tau') \\ &= s_{\text{rf}}^1(\tau'_{(1)}) \circ s_{\text{rf}}^2(\tau'_{(2)}) \\ &= W_{\text{ref}}.L(s_{\text{rf}}^1)([W_1.L(s_{\text{rf}}^1, s_{\text{lc}}^1)]_{\overleftarrow{G}(s)\{1\}}^*)(\tau_{(1)}) \circ W_{\text{ref}}.L(s_{\text{rf}}^2)([W_2.L(s_{\text{rf}}^2, s_{\text{lc}}^2)]_{\overleftarrow{G}(s)\{2\}}^*)(\tau_{(2)}) \\ &= W_1.L(s_{\text{rf}}^1, s_{\text{lc}}^1)([W_1.L(s_{\text{rf}}^1, s_{\text{lc}}^1)]_{\overleftarrow{G}(s)\{1\}}^*)(\tau_{(1)}) \circ W_2.L(s_{\text{rf}}^2, s_{\text{lc}}^2)([W_2.L(s_{\text{rf}}^2, s_{\text{lc}}^2)]_{\overleftarrow{G}(s)\{2\}}^*)(\tau_{(2)}) \\ &= (W_1.L(s_{\text{rf}}^1, s_{\text{lc}}^1)([W_1.L(s_{\text{rf}}^1, s_{\text{lc}}^1)]_{\overleftarrow{G}(s)\{1\}}^*)) \bullet (W_2.L(s_{\text{rf}}^2, s_{\text{lc}}^2)([W_2.L(s_{\text{rf}}^2, s_{\text{lc}}^2)]_{\overleftarrow{G}(s)\{2\}}^*))(\tau) \\ &= W.L(s)(\overleftarrow{G}(s))(\tau) \end{aligned}$$

□

Lemma 94. $w.N \subseteq \mathcal{N}$

Proof. By construction. □

5.2.1 Stability

Definition 25. Lemma 88 gives rise to a choice function *mediate* that, given $G \in \text{GK}(W)$ and $(\tau, v_1, v_3) \in \overline{G}(s_1, s_2)$, returns a value $v_2 = \text{mediate}(G, s_1, s_2, \tau, v_1, v_3)$ such that $(\tau_{(1)}, v_1, v_2) \in \overline{G}_{(1)}^{s_2}(s_1)$ and $(\tau_{(2)}, v_2, v_3) \in \overline{G}_{(2)}^{s_1}(s_2)$. We usually leave out some arguments of *mediate* that are clear from context.

Lemma 95 (Stability of w). *stable*(w)

Proof.

- Suppose $G \in \text{GK}(w\uparrow)$, $s = (s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)$, $(h_1, h_3) \in w.H(s_{\text{rf}})(s)(G(s_{\text{rf}}, s))$ and $\hat{s}_{\text{rf}} \sqsupseteq s_{\text{rf}}$.
- Further suppose $(\hat{h}_1^\bullet, \hat{h}_3^\bullet) \in W_{\text{ref}}.H(\hat{s}_{\text{rf}})(G(\hat{s}_{\text{rf}}, s))$ and defined($h_1 \uplus \hat{h}_1^\bullet$) and defined($h_3 \uplus \hat{h}_3^\bullet$).
- We must find $\hat{s} = (\hat{s}_{\text{rf}}^1, \hat{s}_{\text{lc}}^1, \hat{s}_{\text{rf}}^2, \hat{s}_{\text{lc}}^2) \sqsupseteq_{\text{pub}} s$ such that $(h_1, h_3) \in w.H(\hat{s}_{\text{rf}})(\hat{s})(G(\hat{s}_{\text{rf}}, \hat{s}))$.

- From $(h_1, h_3) \in w.H(s_{\text{rf}})(s)(G(s_{\text{rf}}, s))$ we know that there are $h_1^\circ, h_1^{\text{lc}}, h_{2a}^\circ, h_{2a}^{\text{lc}}, h_{2b}^\circ, h_{2b}^{\text{lc}}, h_3^\circ, h_3^{\text{lc}}$ such that:

1. $h_1 = h_1^\circ \uplus h_1^{\text{lc}} \wedge h_{2a}^\circ \uplus h_{2a}^{\text{lc}} = h_{2b}^\circ \uplus h_{2b}^{\text{lc}} \wedge h_3 = h_3^\circ \uplus h_3^{\text{lc}}$
2. $\text{dom}(h_{2a}^{\text{lc}}) \cap \text{dom}_{[2]}(s_{\text{rf}}^1) = \emptyset \wedge \text{dom}(h_{2b}^{\text{lc}}) \cap \text{dom}_{[1]}(s_{\text{rf}}^2) = \emptyset$
3. $(h_1^\circ, h_{2a}^\circ) \in W_{\text{ref}}.H(s_{\text{rf}}^1 \setminus_{[1]} s_{\text{rf}})(G_1)$
4. $(h_1^{\text{lc}}, h_{2a}^{\text{lc}}) \in w_1.H(s_{\text{rf}}^1)(s_{1c}^1)(G_1)$
5. $(h_{2b}^\circ, h_3^\circ) \in W_{\text{ref}}.H(s_{\text{rf}}^2 \setminus_{[2]} s_{\text{rf}})(G_2)$
6. $(h_{2b}^{\text{lc}}, h_3^{\text{lc}}) \in w_2.H(s_{\text{rf}}^2)(s_{1c}^2)(G_2)$

where G_i is short for $[W_i.L(s_{\text{rf}}^i, s_{1c}^i)]_{G(s_{\text{rf}}, s)_{\{i\}}}^*$.

- We know $\hat{s}_{\text{rf}} = s_{\text{rf}} \uplus s^+$ for some s^+ .
- For each $(\tau, \ell_1, \ell_3) \in s^+$ we pick a fresh location $\ell_{(\tau, \ell_1, \ell_3)}$.
- Now let $\hat{s}_{\text{rf}}^1 = s_{\text{rf}}^1 \uplus \{(\tau_{(1)}, \ell_1, \ell_{(\tau, \ell_1, \ell_3)}) \mid (\tau, \ell_1, \ell_3) \in s^+\}$.
- And let $\hat{s}_{\text{rf}}^2 = s_{\text{rf}}^2 \uplus \{(\tau_{(2)}, \ell_{(\tau, \ell_1, \ell_3)}, \ell_3) \mid (\tau, \ell_1, \ell_3) \in s^+\}$.
- Using $s_{\text{rf}}, s_{\text{rf}}^1, s_{\text{rf}}^2, \hat{s}_{\text{rf}} \in W_{\text{ref}}.S$ and $s_{\text{rf}} = s_{\text{rf}}^\bullet \bullet s_{\text{rf}}^2$, it is easy to see that $\hat{s}_{\text{rf}}^1 \bullet \hat{s}_{\text{rf}}^2 = \hat{s}_{\text{rf}}$.
- We show $\hat{s}_{\text{rf}}^1, \hat{s}_{\text{rf}}^2 \in W_{\text{ref}}.S$:
 - We do only one part, the other is symmetric.
 - Suppose $(\tau', \ell_1, \ell_2) \in s_{\text{rf}}^1$ and $(\tau, \ell_1, \ell_3) \in s^+$, *i.e.*, $(\tau, \ell_1, \ell_3) \in \hat{s}_{\text{rf}} \setminus s_{\text{rf}}$.
 - We derive a contradiction.
 - Since $\ell_1 \in \text{dom}(\hat{h}_1^\bullet)$ and $\text{defined}(h_1 \uplus \hat{h}_1^\bullet)$, we get $\ell_1 \notin \text{dom}(h_1) \supseteq \text{dom}(h_1^\circ)$.
 - From (3) we learn $\ell_1 \notin \text{dom}_{[1]}(s_{\text{rf}}^1 \setminus_{[1]} s_{\text{rf}})$, and hence $\ell_1 \in \text{dom}_{[1]}(s_{\text{rf}})$.
 - Consequently there is τ'', ℓ_3'' such that $(\tau'', \ell_1, \ell_3'') \in s_{\text{rf}} \subseteq \hat{s}_{\text{rf}}$.
 - Since $(\tau, \ell_1, \ell_3) \in s^+ \subseteq \hat{s}_{\text{rf}}$, we learn $\tau = \tau''$ and $\ell_3 = \ell_3''$.
 - This contradicts $(\tau, \ell_1, \ell_3) \notin s_{\text{rf}}$.
- $\hat{s}_{\text{rf}}^i \supseteq s_{\text{rf}}^i$ holds by construction.
- From $(\hat{h}_1^\bullet, \hat{h}_3^\bullet) \in W_{\text{ref}}.H(\hat{s}_{\text{rf}})(G(\hat{s}_{\text{rf}}, s_{\text{rf}}^1, s_{1c}^1, s_{\text{rf}}^2, s_{1c}^2))$ we know by monotonicity that $(\hat{h}_1^\bullet, \hat{h}_3^\bullet) \in W_{\text{ref}}.H(\hat{s}_{\text{rf}})(\overleftarrow{G}(\hat{s}_{\text{rf}}^1, s_{1c}^1, \hat{s}_{\text{rf}}^2, s_{1c}^2))$.
- Note that $\overleftarrow{G} \in \text{GK}(W)$ by Lemma 93.
- We define:
 7. $h_1^{\text{rf}} = \hat{h}_1^\bullet \uplus h_1^\circ$
 8. $\hat{h}_2^\bullet = \{ \ell_2 \mapsto \text{mediate}(\overleftarrow{G}, \tau, \hat{h}_1^\bullet(\ell_1), \hat{h}_3^\bullet(\ell_3)) \mid (\tau_{(1)}, \ell_1, \ell_2) \in \hat{s}_{\text{rf}}^1 \wedge (\tau_{(2)}, \ell_2, \ell_3) \in \hat{s}_{\text{rf}}^2 \}$
 9. $h_{2a}^{\text{rf}} = \hat{h}_2^\bullet \uplus h_{2a}^\circ$
 10. $h_{2b}^{\text{rf}} = \hat{h}_2^\bullet \uplus h_{2b}^\circ$
 11. $h_3^{\text{rf}} = \hat{h}_3^\bullet \uplus h_3^\circ$
- It is easy to check that:
 - $\text{dom}(h_1^{\text{rf}}) = \text{dom}_{[1]}(\hat{s}_{\text{rf}}^1) \wedge \text{dom}(h_{2a}^{\text{rf}}) = \text{dom}_{[2]}(\hat{s}_{\text{rf}}^2)$
 - $\text{dom}(h_{2b}^{\text{rf}}) = \text{dom}_{[1]}(\hat{s}_{\text{rf}}^2) \wedge \text{dom}(h_3^{\text{rf}}) = \text{dom}_{[2]}(\hat{s}_{\text{rf}}^2)$

- Since $G(s_{\text{rf}}, s) = \overleftarrow{G}(s)$ we know from (3–6) by monotonicity:
 12. $(h_{1^\circ}, h_{2a^\circ}) \in W_{\text{ref}} \cdot \mathbf{H}(s_{\text{rf}}^1 \setminus_{[1]} s_{\text{rf}})(\overleftarrow{G}_{(1)}^{(s_{\text{rf}}^2, s_{\text{ic}}^2)}(\hat{s}_{\text{rf}}^1, s_{\text{ic}}^1))$
 13. $(h_{1^{\text{lc}}}, h_{2a^{\text{lc}}}) \in w_1 \cdot \mathbf{H}(s_{\text{rf}}^1)(s_{\text{ic}}^1)(\overleftarrow{G}_{(1)}^{(s_{\text{rf}}^2, s_{\text{ic}}^2)}(s_{\text{rf}}^1, s_{\text{ic}}^1))$
 14. $(h_{2b^\circ}, h_3^\circ) \in W_{\text{ref}} \cdot \mathbf{H}(s_{\text{rf}}^2 \setminus_{[2]} s_{\text{rf}})(\overleftarrow{G}_{(2)}^{(s_{\text{rf}}^1, s_{\text{ic}}^1)}(\hat{s}_{\text{rf}}^2, s_{\text{ic}}^2))$
 15. $(h_{2b^{\text{lc}}}, h_3^{\text{lc}}) \in w_2 \cdot \mathbf{H}(s_{\text{rf}}^2)(s_{\text{ic}}^2)(\overleftarrow{G}_{(2)}^{(s_{\text{rf}}^1, s_{\text{ic}}^1)}(s_{\text{rf}}^2, s_{\text{ic}}^2))$
- Using (6–11), (13), and $(\hat{h}_1^\bullet, \hat{h}_3^\bullet) \in W_{\text{ref}} \cdot \mathbf{H}(\hat{s}_{\text{rf}})(\overleftarrow{G}(\hat{s}_{\text{rf}}^1, s_{\text{ic}}^1, \hat{s}_{\text{rf}}^2, s_{\text{ic}}^2))$, it is easy to check that:
 - $\forall (\tau_1, \ell_1, \ell_2) \in \hat{s}_{\text{rf}}^1. (\tau_1, h_{1^\circ}^{\text{rf}}(\ell_1), h_{2a^\circ}^{\text{rf}}(\ell_2)) \in \overleftarrow{G}_{(1)}^{(s_{\text{rf}}^2, s_{\text{ic}}^2)}(\hat{s}_{\text{rf}}^1, s_{\text{ic}}^1)$
 - $\forall (\tau_2, \ell_2, \ell_3) \in \hat{s}_{\text{rf}}^2. (\tau_2, h_{2b^\circ}^{\text{rf}}(\ell_2), h_3^\circ(\ell_3)) \in \overleftarrow{G}_{(2)}^{(s_{\text{rf}}^1, s_{\text{ic}}^1)}(\hat{s}_{\text{rf}}^2, s_{\text{ic}}^2)$
- Consequently we have:
 16. $(h_{1^{\text{rf}}}, h_{2a^{\text{rf}}}) \in W_{\text{ref}} \cdot \mathbf{H}(\hat{s}_{\text{rf}}^1)(\overleftarrow{G}_{(1)}^{(s_{\text{rf}}^2, s_{\text{ic}}^2)}(\hat{s}_{\text{rf}}^1, s_{\text{ic}}^1))$
 17. $(h_{2b^{\text{rf}}}, h_3^{\text{rf}}) \in W_{\text{ref}} \cdot \mathbf{H}(\hat{s}_{\text{rf}}^2)(\overleftarrow{G}_{(2)}^{(s_{\text{rf}}^1, s_{\text{ic}}^1)}(\hat{s}_{\text{rf}}^2, s_{\text{ic}}^2))$
- From (1–2), (7–11), (16–17), defined $(h_1 \uplus \hat{h}_1^\bullet)$ and defined $(h_3 \uplus \hat{h}_3^\bullet)$ it is easy to see that:
 18. $\text{defined}(h_{1^{\text{lc}}} \uplus h_{1^{\text{rf}}}) \wedge \text{defined}(h_{2a^{\text{lc}}} \uplus h_{2a^{\text{rf}}})$
 19. $\text{defined}(h_{2b^{\text{lc}}} \uplus h_{2b^{\text{rf}}}) \wedge \text{defined}(h_3^{\text{lc}} \uplus h_3^{\text{rf}})$
- From (13), (16), (18), and $\text{stable}(w_1)$ we get $\hat{s}_{\text{ic}}^1 \sqsupseteq_{\text{pub}} s_{\text{ic}}^1$ such that $(h_{1^{\text{lc}}}, h_{2a^{\text{lc}}}) \in w_1 \cdot \mathbf{H}(\hat{s}_{\text{rf}}^1)(\hat{s}_{\text{ic}}^1)(\overleftarrow{G}_{(1)}^{(s_{\text{rf}}^2, s_{\text{ic}}^2)}(\hat{s}_{\text{rf}}^1, \hat{s}_{\text{ic}}^1))$.
- From (15), (17), (19), and $\text{stable}(w_2)$ we get $\hat{s}_{\text{ic}}^2 \sqsupseteq_{\text{pub}} s_{\text{ic}}^2$ such that $(h_{2b^{\text{lc}}}, h_3^{\text{lc}}) \in w_2 \cdot \mathbf{H}(\hat{s}_{\text{rf}}^2)(\hat{s}_{\text{ic}}^2)(\overleftarrow{G}_{(2)}^{(s_{\text{rf}}^1, s_{\text{ic}}^1)}(\hat{s}_{\text{rf}}^2, \hat{s}_{\text{ic}}^2))$.
- Thus by monotonicity we get $(h_{1^{\text{lc}}}, h_{2a^{\text{lc}}}) \in w_1 \cdot \mathbf{H}(\hat{s}_{\text{rf}}^1)(\hat{s}_{\text{ic}}^1)(\overleftarrow{G}_{(1)}^{(s_{\text{rf}}^2, s_{\text{ic}}^2)}(\hat{s}_{\text{rf}}^1, \hat{s}_{\text{ic}}^1))$ and $(h_{2b^{\text{lc}}}, h_3^{\text{lc}}) \in w_2 \cdot \mathbf{H}(\hat{s}_{\text{rf}}^2)(\hat{s}_{\text{ic}}^2)(\overleftarrow{G}_{(2)}^{(s_{\text{rf}}^1, s_{\text{ic}}^1)}(\hat{s}_{\text{rf}}^2, \hat{s}_{\text{ic}}^2))$.
- From (12) we get by monotonicity $(h_{1^\circ}, h_{2a^\circ}) \in W_{\text{ref}} \cdot \mathbf{H}(\hat{s}_{\text{rf}}^1 \setminus_{[1]} \hat{s}_{\text{rf}})(\overleftarrow{G}_{(1)}^{(s_{\text{rf}}^2, s_{\text{ic}}^2)}(\hat{s}_{\text{rf}}^1, \hat{s}_{\text{ic}}^1))$ because $\hat{s}_{\text{rf}}^1 \setminus_{[1]} \hat{s}_{\text{rf}} = s_{\text{rf}}^1 \setminus_{[1]} s_{\text{rf}}$.
- From (14) we get by monotonicity $(h_{2b^\circ}, h_3^\circ) \in W_{\text{ref}} \cdot \mathbf{H}(\hat{s}_{\text{rf}}^2 \setminus_{[2]} \hat{s}_{\text{rf}})(\overleftarrow{G}_{(2)}^{(s_{\text{rf}}^1, s_{\text{ic}}^1)}(\hat{s}_{\text{rf}}^2, \hat{s}_{\text{ic}}^2))$ because $\hat{s}_{\text{rf}}^2 \setminus_{[2]} \hat{s}_{\text{rf}} = s_{\text{rf}}^2 \setminus_{[2]} s_{\text{rf}}$.
- Hence $(h_1, h_3) \in w \cdot \mathbf{H}(\hat{s}_{\text{rf}})(\hat{s}_{\text{rf}}^1, \hat{s}_{\text{ic}}^1, \hat{s}_{\text{rf}}^2, \hat{s}_{\text{ic}}^2)(G(\hat{s}_{\text{rf}}^1, \hat{s}_{\text{rf}}^1, \hat{s}_{\text{ic}}^1, \hat{s}_{\text{rf}}^2, \hat{s}_{\text{ic}}^2))$ by construction of w .

□

5.2.2 Isomorphism

Lemma 96 (Isomorphism between W and $w\uparrow$). $\exists \phi, \psi. \phi : W \cong w\uparrow : \psi$

Proof. We define $\phi \in W.S \rightarrow \mathbb{P}(w\uparrow.S)$ and $\psi \in w\uparrow.S \rightarrow \mathbb{P}(W.S)$ as follows.

$$\begin{aligned} \phi(s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2) &:= \{ (s_{\text{rf}}^1 \bullet s_{\text{rf}}^2, s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2) \} \\ \psi(s_{\text{rf}}, s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2) &:= \begin{cases} \{ (s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2) \} & \text{if } s_{\text{rf}} = s_{\text{rf}}^1 \bullet s_{\text{rf}}^2 \\ \emptyset & \text{otherwise} \end{cases} \end{aligned}$$

It is easy to see that $\phi \circ \psi \sqsupseteq_{\text{pub}} \text{id}$ and $\psi \circ \phi \sqsupseteq_{\text{pub}} \text{id}$. So it remains to show that ϕ and ψ are world morphisms:

1. To show: $\phi : W \rightarrow w\uparrow$

(a) To show: $W.N = w\uparrow.N$

- $w\uparrow.N = W_{\text{ref}}.N \uplus w.N = w.N = W.N$.

(b) To show: $\forall s_1, s'_1. s_1 \sqsubseteq s'_1 \implies \forall s_2 \in \phi(s_1), s'_2 \in \phi(s'_1). s_2 \sqsubseteq s'_2$

- This boils down to the fact that $s_{\text{rf}}^1 \bullet s_{\text{rf}}^2 \sqsubseteq \hat{s}_{\text{rf}}^1 \bullet \hat{s}_{\text{rf}}^2$ if $s_{\text{rf}}^1 \sqsubseteq \hat{s}_{\text{rf}}^1$ and $s_{\text{rf}}^2 \sqsubseteq \hat{s}_{\text{rf}}^2$.

(c) To show: $\forall s_1, s'_1. s_1 \sqsubseteq_{\text{pub}} s'_1 \implies \forall s_2 \in \phi(s_1), s'_2 \in \phi(s'_1). s_2 \sqsubseteq_{\text{pub}} s'_2$

- See (1b).

(d) $\forall s_1, \forall s_2 \in \phi(s_1). W.L(s_1) = w\uparrow.L(s_2)$

- In fact, we show $\forall s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2. W.L(s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2) = w\uparrow.L(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2, s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)$.
For non-reference types this is immediate:

$$\begin{aligned} &W.L(s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)(R)(\tau) \\ &= w.L(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2, s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)(R)(\tau) && \text{(construction of } w) \\ &= w\uparrow.L(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2, s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)(R)(\tau) && \text{(construction of } W_{\text{ref}}) \end{aligned}$$

For reference types we have:

$$\begin{aligned} &W.L(s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)(R)(\text{ref } \tau) \\ &= W_1.L(s_{\text{rf}}^1, s_{\text{lc}}^1)(R_1)(\text{ref } \tau_{(1)}) \circ W_2.L(s_{\text{rf}}^2, s_{\text{lc}}^2)(R_2)(\text{ref } \tau_{(2)}) && \text{(construction of } W) \\ &= W_{\text{ref}}.L(s_{\text{rf}}^1)(R_1)(\text{ref } \tau_{(1)}) \circ W_{\text{ref}}.L(s_{\text{rf}}^2)(R_2)(\text{ref } \tau_{(2)}) && (W_i = w_i\uparrow) \\ &= s_{\text{rf}}^1(\tau_{(1)}) \circ s_{\text{rf}}^2(\tau_{(2)}) && \text{(construction of } W_{\text{ref}}) \\ &= (s_{\text{rf}}^1 \bullet s_{\text{rf}}^2)(\tau) \\ &= W_{\text{ref}}.L(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2)(R)(\text{ref } \tau) && \text{(construction of } W_{\text{ref}}) \\ &= w\uparrow.L(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2, s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)(R)(\text{ref } \tau) \end{aligned}$$

where R_i is short for $[W_i.L(s_{\text{rf}}^i, s_{\text{lc}}^i)]_{R_{\{i\}}}^*$.

(e) $\forall s, \forall G \in \text{GK}(W). W.H(s)(G(s)) \leq \bigcup_{s' \in \phi(s)} w\uparrow.H(s')(G(s))$

- Let $s = (s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)$ and G be given and suppose $(h_1, h_3) \in W.H(s)(G(s))$.
- Let $s' = (s_{\text{rf}}^1 \bullet s_{\text{rf}}^2, s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)$, so $s' \in \phi(s)$.
- We will show $(h_1, h_3) \in w\uparrow.H(s')(G(s))$.
- We know by construction of W that there is h_2 such that $(h_1, h_2) \in W_1.H(s_{\text{rf}}^1, s_{\text{lc}}^1)(G_1)$ and $(h_2, h_3) \in W_2.H(s_{\text{rf}}^2, s_{\text{lc}}^2)(G_2)$, where G_i is short for $[W_i.L(s_{\text{rf}}^i, s_{\text{lc}}^i)]_{G(s)_{\{i\}}}^*$.
- Hence there are $h_1^{\text{rf}}, h_1^{\text{lc}}, h_{2a}^{\text{rf}}, h_{2a}^{\text{lc}}, h_{2b}^{\text{rf}}, h_{2b}^{\text{lc}}, h_3^{\text{rf}}, h_3^{\text{lc}}$ such that:
 - i. $h_1 = h_1^{\text{rf}} \uplus h_1^{\text{lc}}$
 - ii. $h_2 = h_{2a}^{\text{rf}} \uplus h_{2a}^{\text{lc}}$

- iii. $h_2 = h_{2b}^{\text{rf}} \uplus h_{2b}^{\text{lc}}$
- iv. $h_3 = h_3^{\text{rf}} \uplus h_3^{\text{lc}}$
- v. $(h_1^{\text{rf}}, h_{2a}^{\text{rf}}) \in W_{\text{ref}} \cdot \mathbf{H}(s_{\text{rf}}^1)(G_1)$
- vi. $(h_1^{\text{lc}}, h_{2a}^{\text{lc}}) \in w_1 \cdot \mathbf{H}(s_{\text{rf}}^1)(s_{\text{lc}}^1)(G_1)$
- vii. $(h_{2b}^{\text{rf}}, h_3^{\text{rf}}) \in W_{\text{ref}} \cdot \mathbf{H}(s_{\text{rf}}^2)(G_2)$
- viii. $(h_{2b}^{\text{lc}}, h_3^{\text{lc}}) \in w_2 \cdot \mathbf{H}(s_{\text{rf}}^2)(s_{\text{lc}}^2)(G_2)$
- Let $s_i^\circ = s_{\text{rf}}^i \setminus [i] (s_{\text{rf}}^1 \bullet s_{\text{rf}}^2)$.
- Let $s_i^\bullet = s_{\text{rf}}^i \setminus s_i^\circ$.
- Note that $s_{\text{rf}}^i = s_i^\bullet \uplus s_i^\circ$.
- Hence by (v), (vii) and construction of W_{ref} there are $h_1^\bullet, h_1^\circ, h_{2a}^\bullet, h_{2a}^\circ, h_{2b}^\bullet, h_{2b}^\circ, h_3^\bullet, h_3^\circ$ such that:
 - ix. $h_1^{\text{rf}} = h_1^\bullet \uplus h_1^\circ$
 - x. $h_{2a}^{\text{rf}} = h_{2a}^\bullet \uplus h_{2a}^\circ$
 - xi. $h_{2b}^{\text{rf}} = h_{2b}^\bullet \uplus h_{2b}^\circ$
 - xii. $h_3^{\text{rf}} = h_3^\bullet \uplus h_3^\circ$
 - xiii. $(h_1^\bullet, h_{2a}^\bullet) \in W_{\text{ref}} \cdot \mathbf{H}(s_1^\bullet)(G_1)$
 - xiv. $(h_1^\circ, h_{2a}^\circ) \in W_{\text{ref}} \cdot \mathbf{H}(s_1^\circ)(G_1)$
 - xv. $(h_{2b}^\bullet, h_3^\bullet) \in W_{\text{ref}} \cdot \mathbf{H}(s_2^\bullet)(G_2)$
 - xvi. $(h_{2b}^\circ, h_3^\circ) \in W_{\text{ref}} \cdot \mathbf{H}(s_2^\circ)(G_2)$
- Also, from (ii-iii), (v), (vii) we know $\text{dom}(h_{2a}^{\text{lc}}) \cap \text{dom}_{[2]}(s_{\text{rf}}^1) = \emptyset \wedge \text{dom}(h_{2b}^{\text{lc}}) \cap \text{dom}_{[1]}(s_{\text{rf}}^2) = \emptyset$.
- We show $(h_1^\bullet, h_3^\bullet) \in W_{\text{ref}} \cdot \mathbf{H}(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2)(G(s))$:
 - Suppose $(\tau, \ell_1, \ell_3) \in s_{\text{rf}}^1 \bullet s_{\text{rf}}^2$.
 - We must show $(\tau, h_1^\bullet(\ell_1), h_3^\bullet(\ell_3)) \in \overline{G(s)}$.
 - Observe that $s_1^\bullet \bullet s_2^\bullet = s_{\text{rf}}^1 \bullet s_{\text{rf}}^2$.
 - So there is ℓ_2 such that $(\tau_{(1)}, \ell_1, \ell_2) \in s_1^\bullet$ and $(\tau_{(2)}, \ell_2, \ell_3) \in s_2^\bullet$.
 - From (xiii) we know $(\tau_{(1)}, h_1^\bullet(\ell_1), h_{2a}^\bullet(\ell_2)) \in \overline{G_1}$.
 - From (xv) we know $(\tau_{(2)}, h_{2b}^\bullet(\ell_2), h_3^\bullet(\ell_3)) \in \overline{G_2}$.
 - Since $h_{2a}^\bullet, h_{2b}^\bullet \subseteq h_2$, we have $h_{2a}^\bullet(\ell_2) = h_{2b}^\bullet(\ell_2)$ and thus $(\tau, h_1^\bullet(\ell_1), h_3^\bullet(\ell_3)) \in \overline{G(s)}$ by Lemma 88.
- Since $h_1 \setminus h_1^\bullet = h_1^\circ \uplus h_1^{\text{lc}}$ and $h_3 \setminus h_3^\bullet = h_3^\circ \uplus h_3^{\text{lc}}$, we know by construction of w that $(h_1 \setminus h_1^\bullet, h_3 \setminus h_3^\bullet) \in w \cdot \mathbf{H}(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2)(s)(G(s))$.
- Hence $(h_1, h_3) \in w \uparrow \cdot \mathbf{H}(s')(G(s))$.

2. To show: $\psi : w \uparrow \rightarrow W$

- (a) To show: $w \uparrow \cdot \mathbf{N} = W \cdot \mathbf{N}$
 - See (1a).
- (b) To show: $\forall s_1, s'_1. s_1 \sqsubseteq s'_1 \implies \forall s_2 \in \psi(s_1), s'_2 \in \psi(s'_1). s_2 \sqsubseteq s'_2$
 - Easy to see.
- (c) To show: $\forall s_1, s'_1. s_1 \sqsubseteq_{\text{pub}} s'_1 \implies \forall s_2 \in \psi(s_1), s'_2 \in \psi(s'_1). s_2 \sqsubseteq_{\text{pub}} s'_2$
 - See (2b).
- (d) $\forall s_1. \forall s_2 \in \psi(s_1). w \uparrow \cdot \mathbf{L}(s_1) = W \cdot \mathbf{L}(s_2)$
 - See (1c).
- (e) $\forall s. \forall G \in \text{GK}(w \uparrow). w \uparrow \cdot \mathbf{H}(s)(G(s)) \leq \bigcup_{s' \in \psi(s)} W \cdot \mathbf{H}(s')(G(s))$

- Let $s = (s_{\text{rf}}, s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)$ and G be given and suppose $(h_1, h_3) \in w\uparrow.\mathbf{H}(s)(G(s))$.
- This implies $s_{\text{rf}} = s_{\text{rf}}^1 \bullet s_{\text{rf}}^2$ and $s' \in \psi(s)$ for $s' = (s_{\text{rf}}^1, s_{\text{lc}}^1, s_{\text{rf}}^2, s_{\text{lc}}^2)$.
- We will show $(h_1, h_3) \in W.\mathbf{H}(s')(G(s))$.
- We know there are $h_1^\bullet, h_1', h_3^\bullet, h_3'$ such that:
 - $h_1 = h_1^\bullet \uplus h_1'$
 - $h_3 = h_3^\bullet \uplus h_3'$
 - $(h_1^\bullet, h_3^\bullet) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2)(G(s))$
 - $(h_1', h_3') \in w.\mathbf{H}(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2)(s')(G(s))$.
- From (iv) we further know there are $h_1^\circ, h_1^{\text{lc}}, h_{2a}^\circ, h_{2a}^{\text{lc}}, h_{2b}^\circ, h_{2b}^{\text{lc}}, h_3^\circ, h_3^{\text{lc}}$ such that:
 - $h_1' = h_1^\circ \uplus h_1^{\text{lc}}$
 - $h_{2a}^\circ \uplus h_{2a}^{\text{lc}} = h_{2b}^\circ \uplus h_{2b}^{\text{lc}}$
 - $h_3' = h_3^\circ \uplus h_3^{\text{lc}}$
 - viii. $\text{dom}(h_{2a}^{\text{lc}}) \cap \text{dom}_{[2]}(s_{\text{rf}}^1) = \emptyset \wedge \text{dom}(h_{2b}^{\text{lc}}) \cap \text{dom}_{[1]}(s_{\text{rf}}^2) = \emptyset$
 - ix. $(h_1^\circ, h_{2a}^\circ) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}}^1 \setminus_{[1]}(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2))(G_1)$
 - x. $(h_1^{\text{lc}}, h_{2a}^{\text{lc}}) \in w_1.\mathbf{H}(s_{\text{rf}}^1)(s_{\text{lc}}^1)(G_1)$
 - xi. $(h_{2b}^\circ, h_3^\circ) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}}^2 \setminus_{[2]}(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2))(G_2)$
 - xii. $(h_{2b}^{\text{lc}}, h_3^{\text{lc}}) \in w_2.\mathbf{H}(s_{\text{rf}}^2)(s_{\text{lc}}^2)(G_2)$
 where G_i is short for $[W_i.\mathbf{L}(s_{\text{rf}}^i, s_{\text{lc}}^i)]_{G(s)_{\{i\}}}^*$.
- We have $\overleftarrow{G}(s') = G(s)$. Thus by Lemmas 93 and 88, we have $\overline{G_1} \bullet \overline{G_2} = \overline{G(s)}$.
- Thus, for each $(\tau, \ell_1, \ell_3) \in s_{\text{rf}}^1 \bullet s_{\text{rf}}^2$, we know from (iii) that there is $v_{(\tau, \ell_1, \ell_3)}$ such that $(\tau_{(1)}, h_1^\bullet(\ell_1), v_{(\tau, \ell_1, \ell_3)}) \in \overline{G_1}$ and $(\tau_{(2)}, v_{(\tau, \ell_1, \ell_3)}, h_3^\bullet(\ell_3)) \in \overline{G_2}$.
- Let $h_2^\bullet := \{\ell \mapsto v_{(\tau, \ell_1, \ell_3)} \mid (\tau_{(1)}, \ell_1, \ell) \in s_{\text{rf}}^1 \wedge (\tau_{(2)}, \ell, \ell_3) \in s_{\text{rf}}^2\}$.
- Let $s_i^\circ = s_{\text{rf}}^i \setminus_{[i]}(s_{\text{rf}}^1 \bullet s_{\text{rf}}^2)$.
- Let $s_i^\bullet = s_{\text{rf}}^i \setminus s_i^\circ$.
- Then we have $(h_1^\bullet, h_2^\bullet) \in W_{\text{ref}}.\mathbf{H}(s_1^\bullet)(G_1)$ and $(h_2^\bullet, h_3^\bullet) \in W_{\text{ref}}.\mathbf{H}(s_2^\bullet)(G_2)$.
- Observe that $s_i^\circ \uplus s_i^\bullet = s_{\text{rf}}^i$.
- Consequently, $(h_1^\circ \uplus h_1^\bullet, h_{2a}^\circ \uplus h_2^\bullet) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}}^1)(G_1)$ and $(h_{2b}^\circ \uplus h_2^\bullet, h_3^\circ \uplus h_3^\bullet) \in W_{\text{ref}}.\mathbf{H}(s_{\text{rf}}^2)(G_2)$.
- From (viii), (x) and (xii) we get $(h_1^\circ \uplus h_1^\bullet \uplus h_1^{\text{lc}}, h_{2a}^\circ \uplus h_2^\bullet \uplus h_{2a}^{\text{lc}}) \in W_1.\mathbf{H}(s_{\text{rf}}^1, s_{\text{lc}}^1)(G_1)$ and $(h_{2b}^\circ \uplus h_2^\bullet \uplus h_{2b}^{\text{lc}}, h_3^\circ \uplus h_3^\bullet \uplus h_3^{\text{lc}}) \in W_2.\mathbf{H}(s_{\text{rf}}^2, s_{\text{lc}}^2)(G_2)$.
- By construction of W , this means $(h_1, h_3) = (h_1^\circ \uplus h_1^\bullet \uplus h_1^{\text{lc}}, h_3^\circ \uplus h_3^\bullet \uplus h_3^{\text{lc}}) \in W.\mathbf{H}(s')(G(s))$. □

5.2.3 Transitivity

Theorem 97 (Transitivity). $\Delta; \Gamma \vdash e_1 \sim e_3 : \sigma$

Proof. We have $\Delta; \Gamma \vdash e_1 \sim_{w\uparrow} e_3 : \tau$ by Lemmas 90 and 96 and Theorem 73. The result then follows from Lemma 95. □