Refinement Types for Incremental Computational Complexity (Technical Appendix)

Ezgi Çiçek Deepak Garg Umut Acar

Extensions to the type system

This appendix considers the following additions to the main paper.

- Parametric polymorphism.
  - four new types: type variable X, universal type $\forall X \overset{\kappa}{:} K.\tau$, type operator abstraction $\lambda i :: S.\tau$ and type operator application $\tau\ I$.
  - A new kinding judgment $\Psi; \Delta \vdash T :: K$ that assigns kinds to types
  - Typing judgment $\Delta; \Phi; \Gamma \vdash e :_\kappa \tau$ changes to $\Psi; \Delta; \Phi; \Gamma \vdash e :_\kappa \tau$ in which the context Ψ binds the type variables.
  - The subtyping judgment is changed as follows: $\Psi; \Delta; \Phi \models \tau_1 \sqsubseteq \tau_2 : K$.
  - Semantics of kinds, annotated $[\![-]\!]_K$
  - Semantics of types is indexed by a type substitution environment ρ which must lie in the interpretation $\mathcal{T}[\![\Psi]\!]$. We also add corresponding type interpretations for newly added types.
- Two additional types: booleans: `bool`, and the refined singleton non-negative integer type: $\mathtt{N}[n]$. The latter is eliminated with a case construct $\mathtt{case_N}\ e\ \mathtt{of}\ \mathtt{0} \rightarrow e_1 \mid \mathtt{succ}(x) \rightarrow e_2$.
- Functions in the index domain (of the form $\underline{\lambda} t.I$) and the corresponding higher sort $S \rightarrow S$.
- Index term conditionals on constraints. These are written $C\ ?\ I_1 :\ I_2$ (if C then I_1 else I_2).

List of Figures

List of Theorems and Lemmas

Kinds	K	$::=$	$* \mid S{\to}K \mid$
Types	τ	$::=$	$\texttt{real} \mid \texttt{bool} \mid \texttt{N}[n] \mid \tau_1 \times \tau_2 \mid$
			$\texttt{list}\,[n]^{\alpha}\ \tau \mid \tau_1 \xrightarrow{\kappa} \tau_2 \mid \forall i \overset{\kappa}{::} S.\ \tau \mid \exists i{::}S.\ \tau \mid$
			$\texttt{unit} \mid C \to \tau \mid C \wedge \tau \mid (\tau)^{\mu}$
			$X \mid \forall X \overset{\kappa}{:} K.\tau \mid \lambda i :: S.\tau \mid \tau\ I$
Sorts	S	$::=$	$\mathbb{N} \mid \mathbb{R} \mid \mathbb{V} \mid S_1{\to}S_2$
Index terms	I, μ, κ	$::=$	$i \mid \mathbb{S} \mid \mathbb{C} \mid 0 \mid I+1$
			$I_1 + I_2 \mid I_1 - I_2 \mid \frac{I_1}{I_2} \mid I_1 \cdot I_2 \mid$
			$\lceil I \rceil \mid \lfloor I \rfloor \mid \texttt{log}_2(I) \mid I_1^{I_2} \mid$
			$\texttt{min}(I_1, I_2) \mid \texttt{max}(I_1, I_2) \mid$
			$\sum_{i=I_1}^{I_n} I \mid C\ ?\ I_1\ :\ I_2 \mid \underline{\lambda}t.I \mid I_1(I_2)$
Constraints	C	$::=$	$I_1 \doteq I_2 \mid I_1 < I_2 \mid \neg C \mid \bot \mid C_1 \wedge C_2 \mid C_1 \vee C_2$
Constraint env.	Φ	$::=$	$\top \mid C$
Sort env.	Δ	$::=$	$\emptyset \mid \Delta, i :: S$
Type env.	Γ	$::=$	$\emptyset \mid \Gamma, x : \tau$
Higher type env.	Ψ	$::=$	$\emptyset \mid \Psi, X : K$
Primitive env.	Υ	$::=$	$\emptyset \mid \Upsilon, \zeta : \forall \overline{t_i}, \overline{X_i}.\ \tau_1 \xrightarrow{\kappa} \tau_2$

Figure 1: Types

Values	v	$::=$	$\texttt{r} \mid \texttt{b} \mid (v_1, v_2) \mid$
			$\texttt{0} \mid \texttt{succ}\ v \mid \texttt{nil} \mid \texttt{cons}(v_1,\ v_2) \mid$
			$\texttt{fix}\ \ f(x).\,e \mid \Lambda.\,e \mid \texttt{pack}\ v \mid \nu.\,e \mid ()$
Expressions	e, f	$::=$	$x \mid \texttt{r} \mid \texttt{b} \mid (e_1, e_2) \mid \texttt{fst}\ e \mid \texttt{snd}\ e \mid$
			$\texttt{0} \mid \texttt{succ}\ e \mid \texttt{nil} \mid \texttt{cons}(e_1,\ e_2) \mid$
			$(\texttt{case}_{\texttt{N}}\ e\ \texttt{of}\ \texttt{0}\ \to\ e_1 \mid \texttt{succ}(n)\ \to\ e_2) \mid$
			$(\texttt{case}_{\texttt{L}}\ e\ \texttt{of}\ \texttt{nil}\ \to\ e_1 \mid \texttt{cons}(h, tl)\ \to\ e_2) \mid$
			$\texttt{fix}\ \ f(x).\,e \mid e_1\ e_2 \mid \zeta\ e \mid \Lambda.\,e \mid e[] \mid$
			$\texttt{pack}\ e \mid \texttt{unpack}\ e\ \texttt{as}\ x\ \texttt{in}\ e' \mid \nu.\,e \mid e[-] \mid$
			$\texttt{let}\ x\ =\ e_1\ \texttt{in}\ e_2 \mid ()$

Figure 2: Value and expression syntax

$\boxed{\Delta \vdash I :: S}$

$$\frac{}{\Delta \vdash \mathbb{S} :: \mathbb{V}}\ \mathbb{S} \qquad \frac{}{\Delta \vdash \mathbb{C} :: \mathbb{V}}\ \mathbb{C} \qquad \frac{\Delta \vdash C\ \texttt{wf} \qquad \Delta \vdash I_1 :: S \qquad \Delta \vdash I_2 :: S}{\Delta \vdash (C\ ?\ I_1\ :\ I_2) :: S}\ \textbf{cond} \qquad \frac{\Delta(t) = S}{\Delta \vdash t :: S}\ \textbf{t}$$

$$\frac{}{\Delta \vdash 0 :: \mathbb{N}}\ 0 \qquad \frac{\Delta \vdash I :: \mathbb{N}}{\Delta \vdash (I+1) :: \mathbb{N}}\ \textbf{I}$$

$$\frac{\Delta \vdash I_1 :: \mathbb{N} \qquad \Delta \vdash I_2 :: \mathbb{N} \qquad \diamond \in \{\texttt{min}, \texttt{max}, +, -, *, \div, \hat{}\}}{\Delta \vdash (I_1 \diamond I_2) :: \mathbb{N}}\ \textbf{op-bin-N}$$

$$\frac{\Delta \vdash I :: \mathbb{R} \qquad \circ \in \{\lfloor\ \rfloor, \lceil\ \rceil\}}{\Delta \vdash (\circ S) :: \mathbb{N}}\ \textbf{op-un-N}$$

$$\frac{\Delta \vdash \kappa_1 :: \mathbb{R} \qquad \Delta \vdash \kappa_2 :: \mathbb{R} \qquad \star \in \{\texttt{min}, \texttt{max}, +, -, *, /, \hat{}\}}{\Delta \vdash (\kappa_1 \star \kappa_2) :: \mathbb{R}}\ \textbf{op-bin-R}$$

$$\frac{\Delta \vdash \kappa :: \mathbb{R} \qquad \odot \in \{\texttt{log}_2()\}}{\Delta \vdash (\odot \kappa) :: \mathbb{R}}\ \textbf{op-un-R} \qquad \frac{\Delta, t :: S\ \vdash I :: S}{\Delta \vdash \underline{\lambda} t.I :: S \to S}\ \textbf{i}\lambda \qquad \frac{\Delta \vdash I_1 :: S \to S \qquad \Delta \vdash I_2 :: S}{\Delta \vdash I_1(I_2) :: S}\ \textbf{iapp}$$

$$\frac{\Delta \vdash I_1 :: \mathbb{N} \qquad \Delta \vdash I_n :: \mathbb{N} \qquad \Delta, i :: \mathbb{N} \vdash I :: S \qquad S \in \{\mathbb{N}, \mathbb{R}\}}{\Delta \vdash \sum_{i=I_1}^{I_n} I :: S}\ \textbf{isum} \qquad \frac{\Delta \vdash I :: \mathbb{N}}{\Delta \vdash I :: \mathbb{R}}\ \sqsubseteq : *$$

Figure 3: Sorting rules

$\boxed{\Psi; \Delta \vdash T :: K}$

$$\frac{\Psi(X) = K}{\Psi; \Delta \vdash X : K}\ \textbf{k-Var} \qquad \frac{\Psi; i :: S, \Delta \vdash \tau : K}{\Psi; \Delta \vdash \lambda i :: S.\tau : S \to K}\ \textbf{k-Lam} \qquad \frac{\Psi; \Delta \vdash \tau : S \to K \qquad \Delta \vdash I :: S}{\Psi; \Delta \vdash \tau\ I : K}\ \textbf{k-App}$$

$$\frac{X : K, \Psi; \Delta \vdash \tau : * \qquad \Delta \vdash \kappa :: S}{\Psi; \Delta \vdash \forall X \overset{\kappa}{::} K.\tau : *}\ \textbf{k-forall} \qquad \frac{\Psi; \Delta \vdash \tau : * \qquad \Delta \vdash \mu :: \mathbb{V}}{\Psi; \Delta \vdash (\tau)^{\mu} : *}\ \textbf{k-mu}$$

$$\frac{}{\Psi; \Delta \vdash \texttt{real} : *}\ \textbf{k-real} \qquad \frac{}{\Psi; \Delta \vdash \texttt{bool} : *}\ \textbf{k-bool} \qquad \frac{\Psi; \Delta \vdash \tau_1 : * \qquad \Psi; \Delta \vdash \tau_2 : *}{\Psi; \Delta \vdash \tau_1 \times \tau_2 : *}\ \textbf{k-pair}$$

$$\frac{\Delta \vdash n :: \mathbb{N}}{\Psi; \Delta \vdash \texttt{N}[n] : *}\ \textbf{k-nat} \qquad \frac{\Delta \vdash n :: \mathbb{N} \qquad \Delta \vdash \alpha :: \mathbb{N} \qquad \Psi; \Delta \vdash \tau : *}{\Psi; \Delta \vdash \texttt{list}\,[n]^{\alpha}\ \tau : *}\ \textbf{k-list}$$

$$\frac{\Psi; \Delta \vdash \tau_1 : * \qquad \Psi; \Delta \vdash \tau_2 : * \qquad \Delta \vdash \kappa :: \mathbb{R}}{\Psi; \Delta \vdash \tau_1 \xrightarrow{\kappa} \tau_2 : *}\ \textbf{k-fun} \qquad \frac{\Psi; i :: S, \Delta \vdash \tau : * \qquad i :: S, \Delta \vdash \kappa :: \mathbb{R}}{\Psi; \Delta \vdash \forall i \overset{\kappa}{::} S.\ \tau : *}\ \textbf{k-}\forall$$

$$\frac{\Psi; i :: S, \Delta \vdash \tau : *}{\Psi; \Delta \vdash \exists i{::}S.\ \tau : *}\ \textbf{k-}\exists \qquad \frac{}{\Psi; \Delta \vdash \texttt{unit} : *}\ \textbf{k-unit} \qquad \frac{\Delta \vdash C\ \texttt{wf} \qquad \Psi; \Delta \vdash \tau : *}{\Psi; \Delta \vdash C \to \tau : *}\ \textbf{k-C}\to$$

$$\frac{\Delta \vdash C\ \texttt{wf} \qquad \Psi; \Delta \vdash \tau : *}{\Psi; \Delta \vdash C \wedge \tau : *}\ \textbf{k-C}\wedge$$

Figure 4: Kinding rules

$\boxed{\Delta \vdash C \texttt{ wf}}$

$$\frac{\Delta \vdash I_1 :: S \qquad \Delta \vdash I_2 :: S \qquad S \in \{\mathbb{N}, \mathbb{R}\}}{\Delta \vdash I_1 < I_2 \texttt{ wf}} \textbf{ wf } < \qquad \frac{\Delta \vdash I_1 :: S \qquad \Delta \vdash I_2 :: S \qquad S \in \{\mathbb{N}, \mathbb{R}\}}{\Delta \vdash I_1 \doteq I_2 \texttt{ wf}} \textbf{ wf } \doteq$$

$$\frac{}{\Delta \vdash \top \texttt{ wf}} \textbf{ wf-}\top \qquad \frac{}{\Delta \vdash \bot \texttt{ wf}} \textbf{ wf-}\bot \qquad \frac{\Delta \vdash C \texttt{ wf}}{\Delta \vdash \neg C \texttt{ wf}} \textbf{ wf } \neg \qquad \frac{\Delta \vdash C_1 \texttt{ wf} \qquad \Delta \vdash C_2 \texttt{ wf}}{\Delta \vdash C_1 \wedge C_2 \texttt{ wf}} \textbf{ wf } \wedge$$

$$\frac{\Delta \vdash C_1 \texttt{ wf} \qquad \Delta \vdash C_2 \texttt{ wf}}{\Delta \vdash C_1 \vee C_2 \texttt{ wf}} \textbf{ wf } \vee$$

Figure 5: Constraint well-formedness

$\boxed{\Psi; \Delta; \Phi \vdash \Gamma \texttt{ wf}}$

$$\frac{\Delta \vdash \Phi \texttt{ wf}}{\Psi; \Delta; \Phi \vdash \cdot \texttt{ wf}} \textbf{ wf } \cdot \qquad \frac{\Psi; \Delta; \Phi \vdash \Gamma \texttt{ wf} \qquad \Psi; \Delta \vdash \tau : *}{\Psi; \Delta; \Phi \vdash (\Gamma, x : \tau) \texttt{ wf}} \textbf{ wf } \Gamma$$

Figure 6: Context well-formedness

$\boxed{\Psi;\Delta;\Phi \models \tau_1 \sqsubseteq \tau_2 : K}$ τ_1 is a subtype of τ_2 where τ_1 and τ_2 are kinded with K.

The converse of the conlusion in rules marked * can be proved using other rules (given their premises).

$$\frac{}{\Psi;\Delta;\Phi \models (\tau_1 \xrightarrow{\kappa} \tau_2)^{\mu} \sqsubseteq (\tau_1)^{\mu} \xrightarrow{\kappa} (\tau_2)^{\mu} : *} \to \mathbf{1}$$

$$\frac{\Psi;\Delta;\Phi \models \tau_1' \sqsubseteq \tau_1 : * \qquad \Psi;\Delta;\Phi \models \tau_2 \sqsubseteq \tau_2' : * \qquad \Delta;\Phi \models \kappa \leq \kappa'}{\Psi;\Delta;\Phi \models \tau_1 \xrightarrow{\kappa} \tau_2 \sqsubseteq \tau_1' \xrightarrow{\kappa'} \tau_2' : *} \to \mathbf{2}$$

$$\frac{}{\Psi;\Delta;\Phi \models (\tau_1 \times \tau_2)^{\mu} \equiv (\tau_1)^{\mu} \times (\tau_2)^{\mu} : *} \times \mathbf{1} \qquad \frac{\Psi;\Delta;\Phi \models \tau_1 \sqsubseteq \tau_1' : * \qquad \Psi;\Delta;\Phi \models \tau_2 \sqsubseteq \tau_2' : *}{\Psi;\Delta;\Phi \models \tau_1 \times \tau_2 \sqsubseteq \tau_1' \times \tau_2' : *} \times \mathbf{2}$$

$$\frac{}{\Psi;\Delta;\Phi \models (\mathtt{list}\,[n]^{\alpha}\ \tau)^{\mu} \equiv \mathtt{list}\,[n]^{\alpha}\ (\tau)^{\mu} : *}\ \mathbf{l1} \qquad \frac{\Delta;\Phi \models \mu \doteq \mathbb{S}}{\Psi;\Delta;\Phi \models (\mathtt{list}\,[n]^{\alpha}\ \tau)^{\mu} \equiv \mathtt{list}\,[n]^{0}\ \tau : *}\ \mathbf{l2}$$

$$\frac{\Delta;\Phi \models \alpha \doteq 0}{\Psi;\Delta;\Phi \models \mathtt{list}\,[n]^{\alpha}\ \tau \sqsubseteq \mathtt{list}\,[n]^{\alpha}\ (\tau)^{\mathbb{S}} : *}\ \mathbf{l3*}$$

$$\frac{\Delta;\Phi \models n \doteq n' \qquad \Delta;\Phi \models \alpha \leq \alpha' \qquad \Psi;\Delta;\Phi \models \tau \sqsubseteq \tau' : *}{\Psi;\Delta;\Phi \models \mathtt{list}\,[n]^{\alpha}\ \tau \sqsubseteq \mathtt{list}\,[n']^{\alpha'}\ \tau' : *}\ \mathbf{l4} \qquad \frac{\Delta;\Phi \models n \doteq n'}{\Psi;\Delta;\Phi \models \mathtt{N}[n] \sqsubseteq \mathtt{N}[n'] : *}\ \mathbf{N}$$

$$\frac{\Psi;t :: S,\Delta;\Phi \models \tau \sqsubseteq \tau' : * \qquad \Delta;\Phi \models \kappa \leq \kappa'}{\Psi;\Delta;\Phi \models \forall t :^{\kappa}: S.\ \tau \sqsubseteq \forall t :^{\kappa'}: S.\ \tau' : *} \forall \mathbf{1} \qquad \frac{}{\Psi;\Delta;\Phi \models (\forall t :^{\kappa}: S.\ \tau)^{\mu} \equiv \forall t :^{\kappa}: S.\ (\tau)^{\mu} : *} \forall \mathbf{2}$$

$$\frac{\Psi;t :: S,\Delta;\Phi \models \tau \sqsubseteq \tau' : * \qquad t \notin FV(\Phi)}{\Psi;\Delta;\Phi \models \exists t{::}S.\ \tau \sqsubseteq \exists t{::}S.\ \tau' : *} \exists \mathbf{1} \qquad \frac{}{\Psi;\Delta;\Phi \models (\exists t{::}S.\ \tau)^{\mu} \equiv \exists t{::}S.\ (\tau)^{\mu} : *} \exists \mathbf{2}$$

$$\frac{X : K,\Psi;\Delta;\Phi \models \tau \sqsubseteq \tau' : * \qquad \Delta;\Phi \models \kappa \leq \kappa'}{\Psi;\Delta;\Phi \models \forall X :^{\kappa} K.\tau \sqsubseteq \forall X :^{\kappa} K.\tau' : *}\ \textbf{ty-}\forall\mathbf{1}$$

$$\frac{}{\Psi;\Delta;\Phi \models (\forall X :^{\kappa} K.\tau)^{\mu} \equiv \forall X :^{\kappa} K.(\tau)^{\mu} : *}\ \textbf{ty-}\forall\mathbf{2} \qquad \frac{\Psi;i :: S,\Delta;\Phi \models \tau \sqsubseteq \tau' : K}{\Psi;\Delta;\Phi \models \lambda i :: S.\tau \sqsubseteq \lambda i :: S.\tau' : S{\to}K}\ \lambda\textbf{-1}$$

$$\frac{}{\Psi;\Delta;\Phi \models (\lambda i :: S.\tau)\ I \equiv \tau[I/i] : K}\ \textbf{ty-subst} \qquad \frac{\Psi;\Delta;\Phi \models \tau \sqsubseteq \tau' : S{\to}K \qquad \Phi;\Delta \models I \doteq I'}{\Psi;\Delta;\Phi \models \tau\ I \sqsubseteq \tau'\ I' : K}\ \textbf{ty-app1}$$

$$\frac{}{\Psi;\Delta;\Phi \models (\tau)^{\mu} \sqsubseteq \tau : *}\ \mathbf{T} \qquad \frac{}{\Psi;\Delta;\Phi \models (\tau)^{\mu} \sqsubseteq ((\tau)^{\mu})^{\mu} : *}\ \mathbf{D*} \qquad \frac{}{\Psi;\Delta;\Phi \models \tau \sqsubseteq (\tau)^{\mathbb{C}} : *}\ \mathbf{I*}$$

$$\frac{\Psi;\Delta;\Phi \models \mu \doteq \mu'}{\Psi;\Delta;\Phi \models (\tau)^{\mu} \equiv (\tau)^{\mu'} : *}\ \mathbf{eq*} \qquad \frac{\Psi;\Delta;\Phi \models \tau \sqsubseteq \tau' : *}{\Psi;\Delta;\Phi \models (\tau)^{\mu} \sqsubseteq (\tau')^{\mu} : *}\ \mathbf{C} \qquad \frac{}{\Psi;\Delta;\Phi \models \tau \sqsubseteq \tau : K}\ \mathbf{refl*}$$

$$\frac{\Psi;\Delta;\Phi \models \tau_1 \sqsubseteq \tau_2 : K \qquad \Psi;\Delta;\Phi \models \tau_2 \sqsubseteq \tau_3 : K}{\Psi;\Delta;\Phi \models \tau_1 \sqsubseteq \tau_3 : K}\ \mathbf{tran} \qquad \frac{\Psi;\Delta;\Phi \wedge C \models \eta \qquad \Psi;\Delta;\Phi \wedge \neg C \models \eta}{\Psi;\Delta;\Phi \models \eta}\ \mathbf{split}$$

$$\frac{\Psi;\Delta;\Phi \wedge C' \models C \qquad \Psi;\Delta;\Phi \models \tau \sqsubseteq \tau' : *}{\Psi;\Delta;\Phi \models C \to \tau \sqsubseteq C' \to \tau' : *}\ \mathbf{c\text{-}imp} \qquad \frac{\Psi;\Delta;\Phi \wedge C \models C' \qquad \Psi;\Delta;\Phi \models \tau \sqsubseteq \tau' : *}{\Psi;\Delta;\Phi \models C \wedge \tau \sqsubseteq C' \wedge \tau' : *}\ \mathbf{c\text{-}and}$$

Figure 7: Subtyping rules

$\boxed{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \tau}$ expression e has type τ with dynamic stability κ.

The context Υ carrying types of primitive functions is omitted from all rules.

$$\frac{\Psi;\Delta \vdash \tau : *\qquad \Psi;\Delta;\Phi \vdash \Gamma\ \mathtt{wf}}{\Psi;\Delta;\Phi;\Gamma, x:\tau \vdash x :_0 \tau}\ \textbf{var} \qquad \frac{\Psi;\Delta;\Phi \vdash \Gamma\ \mathtt{wf}}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{r} :_0 (\mathtt{real})^{\mathbb{S}}}\ \textbf{real}$$

$$\frac{\Psi;\Delta;\Phi \vdash \Gamma\ \mathtt{wf}}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{b} :_0 (\mathtt{bool})^{\mathbb{S}}}\ \textbf{bool} \qquad \frac{\Psi;\Delta;\Phi;\Gamma \vdash e_1 :_{\kappa_1} \tau_1\qquad \Psi;\Delta;\Phi;\Gamma \vdash e_2 :_{\kappa_2} \tau_2}{\Psi;\Delta;\Phi;\Gamma \vdash (e_1,e_2) :_{(\kappa_1+\kappa_2)} \tau_1 \times \tau_2}\ \textbf{pair}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \tau_1 \times \tau_2}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{fst}\ e :_\kappa \tau_1}\ \textbf{fst} \qquad \frac{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \tau_1 \times \tau_2}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{snd}\ e :_\kappa \tau_2}\ \textbf{snd} \qquad \frac{\Psi;\Delta;\Phi \vdash \Gamma\ \mathtt{wf}}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{0} :_0 \mathtt{N}[0]}\ \textbf{0}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \mathtt{N}[S]}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{succ}\ e :_\kappa \mathtt{N}[S+1]}\ \textbf{succ} \qquad \frac{\Psi;\Delta \vdash \tau : *\qquad \Psi;\Delta;\Phi \vdash \Gamma\ \mathtt{wf}}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{nil} :_0 \mathtt{list}\,[0]^0\ \tau}\ \textbf{nil}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash e_1 :_{\kappa_1} (\tau)^{\mathbb{S}}\qquad \Psi;\Delta;\Phi;\Gamma \vdash e_2 :_{\kappa_2} \mathtt{list}\,[n]^\alpha\ \tau}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{cons}(e_1,\, e_2) :_{\kappa_1+\kappa_2} \mathtt{list}\,[n{+}1]^\alpha\ \tau}\ \textbf{cons1}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash e_1 :_{\kappa_1} \tau\qquad \Psi;\Delta;\Phi;\Gamma \vdash e_2 :_{\kappa_2} \mathtt{list}\,[n]^{\alpha-1}\ \tau\qquad \Delta;\Phi \models \alpha > 0}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{cons}(e_1,\, e_2) :_{\kappa_1+\kappa_2} \mathtt{list}\,[n+1]^\alpha\ \tau}\ \textbf{cons2}$$

$$\frac{\begin{array}{c}\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \mathtt{list}\,[n]^\alpha\ \tau\\ \Psi;\Delta;\Phi \wedge n \doteq 0;\Gamma \vdash e_1 :_{\kappa'} \tau'\qquad \Psi;i::\iota,\Delta;\Phi \wedge n \doteq i+1;h:(\tau)^{\mathbb{S}},tl:\mathtt{list}\,[i]^\alpha\ \tau,\Gamma \vdash e_2 :_{\kappa'} \tau'\\ \Psi;i::\iota,\beta::\iota,\Delta;\Phi \wedge n \doteq i+1 \wedge \alpha \doteq \beta+1;h:(\tau)^{\mathbb{C}},tl:\mathtt{list}\,[i]^\beta\ \tau,\Gamma \vdash e_2 :_{\kappa'} \tau'\end{array}}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{case_L}\ e\ \mathtt{of\ nil}\ \to\ e_1 \mid \mathtt{cons}(h,tl)\ \to\ e_2 :_{\kappa+\kappa'} \tau'}\ \textbf{caseL}$$

$$\frac{\begin{array}{c}\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \mathtt{N}[S]\\ \Psi;\Delta;\Phi \wedge S \doteq 0;\Gamma \vdash e_1 :_{\kappa'} \tau'\qquad \Psi;i::\iota,\Delta;\Phi \wedge S \doteq i+1;x:\mathtt{N}[i],\Gamma \vdash e_2 :_{\kappa'} \tau'\end{array}}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{case_N}\ e\ \mathtt{of}\ 0\ \to\ e_1 \mid \mathtt{succ}(x)\ \to\ e_2 :_{\kappa+\kappa'} \tau'}\ \textbf{caseN}$$

$$\frac{\Psi;\Delta;\Phi;x:\tau_1, f:\tau_1 \xrightarrow{\kappa} \tau_2,\Gamma \vdash e :_\kappa \tau_2}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{fix}\ \ f(x).\, e :_0 \tau_1 \xrightarrow{\kappa} \tau_2}\ \textbf{fix1} \qquad \frac{\Psi;\Delta;\Phi;\Gamma \vdash e_1 :_{\kappa_1} \tau_1 \xrightarrow{\kappa} \tau_2\qquad \Psi;\Delta;\Phi;\Gamma \vdash e_2 :_{\kappa_2} \tau_1}{\Psi;\Delta;\Phi;\Gamma \vdash e_1\ e_2 :_{(\kappa_1+\kappa_2+\kappa)} \tau_2}\ \textbf{app}$$

$$\frac{\Upsilon(\zeta) = \zeta : \forall \overline{t_i}, \overline{X_i}.\ \tau_1 \xrightarrow{\kappa} \tau_2\qquad \Psi;\Delta \vdash \tau_i' : *\qquad \Psi;\Delta \vdash \overline{I_i} :: S\qquad \Psi;\Delta;\Phi;\Gamma \vdash e :_{\kappa_e} \tau_1[\overline{I_i/t_i}, \overline{\tau_i'/X_i}]}{\Psi;\Delta;\Phi;\Gamma \vdash \zeta\ e :_{\kappa_e+\kappa[\overline{I_i/t_i}]} \tau_2[\overline{I_i/t_i}, \overline{\tau_i'/X_i}]}\ \textbf{primApp}$$

$$\frac{\Psi;t::S,\Delta;\Phi;\Gamma \vdash e :_\kappa \tau}{\Psi;\Delta;\Phi;\Gamma \vdash \Lambda.\, e :_0 \forall t \overset{\kappa}{::} S.\ \tau}\ \forall\mathbf{I} \qquad \frac{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \forall t \overset{\kappa'}{::} S.\ \tau\qquad \Psi;\Delta \vdash I :: S}{\Psi;\Delta;\Phi;\Gamma \vdash e[] :_{\kappa+\kappa'\{I/t\}} \tau\{I/t\}}\ \forall\mathbf{E}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \tau\{I/t\}\qquad \Psi;\Delta \vdash I :: S}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{pack}\ e :_\kappa \exists t{::}S.\ \tau}\ \exists\mathbf{I}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \exists t{::}S.\ \tau\qquad \Psi;t::S,\Delta;\Phi;x:\tau,\Gamma \vdash e' :_{\kappa'} \tau'\qquad t \notin FV(\Phi;\Gamma,\tau')}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{unpack}\ e\ \mathtt{as}\ x\ \mathtt{in}\ e' :_{\kappa+\kappa'} \tau'}\ \exists\mathbf{E}$$

Figure 8: Typing rules, part 1

$\boxed{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \tau}$ expression e has type τ with dynamic stability κ.

The context Υ carrying types of primitive functions is omitted from all rules.

$$\frac{X : K, \Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \tau}{\Psi;\Delta;\Phi;\Gamma \vdash \nu.\, e :_0 \forall X \overset{\kappa}{:} K.\tau}\ \textbf{t-forall} \qquad \frac{\Psi;\Delta;\Phi;\Gamma \vdash e :_{\kappa_e} \forall X \overset{\kappa}{:} K.\tau \qquad \Psi;\Delta \vdash \tau' : K}{\Psi;\Delta;\Phi;\Gamma \vdash e[-] :_{\kappa_e+\kappa} \tau[\tau'/X]}\ \textbf{t-app}$$

$$\frac{\Delta;\Phi \wedge C;\Gamma \vdash e :_\kappa \tau}{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa C \to \tau}\ \textbf{c-impI} \qquad \frac{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa C \to \tau \qquad \Delta;\Phi \models C}{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \tau}\ \textbf{c-impE}$$

$$\frac{\Delta;\Phi \models C \qquad \Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \tau}{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa C \wedge \tau}\ \textbf{c-andI}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash e_1 :_\kappa C \wedge \tau_1 \qquad \Delta;\Phi \wedge C;x : \tau_1,\Gamma \vdash e_2 :_\kappa \tau_2}{\Psi;\Delta;\Phi;\Gamma \vdash \texttt{let}\ x\ =\ e_1\ \texttt{in}\ e_2 :_\kappa \tau_2}\ \textbf{c-andE}$$

$$\frac{\Delta;\Phi \models \bot \qquad \Psi;\Delta;\Phi \vdash \Gamma\ \texttt{wf}}{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \tau}\ \textbf{contra}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \tau \qquad \Psi;\Delta;\Phi \models \tau \sqsubseteq \tau' : * \qquad \Delta;\Phi \models \kappa \le \kappa'}{\Psi;\Delta;\Phi;\Gamma \vdash e :_{\kappa'} \tau'}\ \sqsubseteq : *$$

$$\frac{\Delta;\Phi \wedge C;\Gamma \vdash e :_\kappa \tau \qquad \Delta;\Phi \wedge \neg C;\Gamma \vdash e :_\kappa \tau}{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \tau}\ \textbf{split}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash e :_\kappa \tau \qquad \forall y \in \Gamma.\ \ \Psi;\Delta;\Phi \models \Gamma(y) \sqsubseteq (\Gamma(y))^{\mathbb{S}} : *}{\Psi;\Delta;\Phi;\Gamma,\Gamma' \vdash e :_0 (\tau)^{\mathbb{S}}}\ \textbf{nochange}$$

$$\frac{\Psi;\Delta;\Phi;x : \tau_1, f : (\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{S}},\Gamma \vdash e :_\kappa \tau_2 \qquad \forall y \in \Gamma.\ \ \Psi;\Delta;\Phi \models \Gamma(y) \sqsubseteq (\Gamma(y))^{\mathbb{S}} : *}{\Psi;\Delta;\Phi;\Gamma,\Gamma' \vdash \texttt{fix}\ \ f(x).\, e :_0 (\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{S}}}\ \textbf{fix2}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash e_1 :_{\kappa_1} \tau_1 \qquad \Psi;\Delta;\Phi;x : \tau_1,\Gamma \vdash e_2 :_{\kappa_2} \tau_2}{\Psi;\Delta;\Phi;\Gamma \vdash \texttt{let}\ x\ =\ e_1\ \texttt{in}\ e_2 :_{\kappa_1+\kappa_2} \tau_2}\ \textbf{let} \qquad \frac{\Psi;\Delta;\Phi \vdash \Gamma\ \texttt{wf}}{\Psi;\Delta;\Phi;\Gamma \vdash () :_0 \texttt{unit}}\ \textbf{unit}$$

Figure 9: Typing rules, part 2

$\texttt{append} : (\texttt{unit} \to \forall n, m, \alpha_1, \alpha_2.\ \texttt{list}\,[n]^{\alpha_1}\ \tau \times \texttt{list}\,[m]^{\alpha_2}\ \tau \xrightarrow{0} \texttt{list}\,[n+m]^{\alpha_1+\alpha_2}\ \tau)^{\mathbb{S}}$

```
fix append(_). λ(l1, l2).
case_L l1 of
  nil  → nil
| cons(h, tl) → cons(h, append () (tl, l2))
```

$\texttt{zip} : (\texttt{unit} \to \forall n, \alpha_1, \alpha_2.\ \texttt{list}\,[n]^{\alpha_1}\ \tau_1 \times \texttt{list}\,[n]^{\alpha_2}\ \tau_2 \xrightarrow{0} \texttt{list}\,[n]^{\texttt{min}(\alpha_1+\alpha_2, n)}\ \tau_1 \times \tau_2)^{\mathbb{S}}$

```
fix zip(_). λ(l1, l2).
case_L l1 of
  nil  → nil
| cons(h1, tl1) → case_L l2 of
                    nil  → nil
                  | cons(h2, tl2) → let z = zip () (tl1, tl2) in cons((h1, h2), z)
```

$\texttt{map} : ((\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{S}} \to \forall n, \alpha.\ \texttt{list}\,[n]^{\alpha}\ \tau_1 \xrightarrow{\alpha\cdot\kappa} \texttt{list}\,[n]^{\alpha}\ \tau_2)^{\mathbb{S}}$ and
$\texttt{map} : ((\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{C}} \to \forall n, \alpha.\ \texttt{list}\,[n]^{\alpha}\ \tau_1 \xrightarrow{n\cdot\kappa} \texttt{list}\,[n]^{n}\ \tau_2)^{\mathbb{S}}$

```
fix map(f). λl.
case_L l of
  nil  → nil
| cons(h, tl) → cons(f h, map f tl)
```

Figure 10: Examples `append`, `zip`, `map`

Examples

This section describes several examples using CostIt. We list some conventions. First, in order to improve readability, we omit intro- and elim- constructors ($\Lambda.\, e$, $e[]$, $\texttt{pack}\ e$, $\texttt{unpack}\ e_1\ \texttt{as}\ x\ \texttt{in}\ e_2$) for index-variable quantifiers. Second, because our rules for typing fixpoints (**fix1** and **fix2**) apply at types $\tau_1 \xrightarrow{\kappa} \tau_2$, but not at more general types $\forall i \overset{\kappa'}{::} S.\ \tau_1 \xrightarrow{\kappa} \tau_2$, a recursive function whose type should have been $\forall i \overset{\kappa'}{::} S.\ \tau_1 \xrightarrow{\kappa} \tau_2$ may have to be given the type $\texttt{unit} \to \forall i \overset{\kappa'}{::} S.\ \tau_1 \xrightarrow{\kappa} \tau_2$. Its first argument is a dummy. When this happens, we explicitly write the `unit` type. Third, we write $\lambda x.e$ for $\texttt{fix}\ \ f(x).\, e$ when f does not appear in e. Fourth, we use pattern matching syntax for pairs, which is easily encoded, e.g., $\lambda(x, y).\, e \triangleq (\lambda z.\, \texttt{let}\ x = \texttt{fst}\ z\ \texttt{in}\ \texttt{let}\ y = \texttt{snd}\ z\ \texttt{in}\ e)$. Fifth, when the annotation κ is omitted from types $\tau_1 \xrightarrow{\kappa} \tau_2$ and $\forall i \overset{\kappa}{::} S.\ \tau$, it defaults to 0.

Instead of presenting large unreadable typing derivations for our example programs, we explain key steps of the typing derivations in text.

List append, zip and map

Figure 10 shows the standard list `append`, `zip` and `map` functions with their CostIt types. The dynamic stability of `append` and `zip` is 0 because these functions do not contain any primitive operators and they do not call any functions passed in as argument. The function `map` takes as argument a mapping function, and then invokes it. Since this mapping function may call

primitive functions, the dynamic stability of `map` is not 0. We show here how `map` is typed as it is the most difficult of the three functions.

The function `map` can be given two different types — one for mapping functions annotated $(\cdot)^{\mathbb{S}}$ and the other for mapping functions annotated $(\cdot)^{\mathbb{C}}$. Both types are shown in Figure 10. The first type of `map` is:

$$\texttt{map} : ((\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{S}} \to \forall n, \alpha.\ \texttt{list}\,[n]^{\alpha}\ \tau_1 \xrightarrow{\alpha\cdot\kappa} \texttt{list}\,[n]^{\alpha}\ \tau_2)^{\mathbb{S}}$$

To establish this type, we first show that `map` has the following type without the outer $(\cdot)^{\mathbb{S}}$ annotation, and then conclude immediately by the rule **nochange** that it also has the type above (`map` is closed, so the rule **nochange** applies trivially).

$$\texttt{map} : (\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{S}} \to \forall n, \alpha.\ \texttt{list}\,[n]^{\alpha}\ \tau_1 \xrightarrow{\alpha\cdot\kappa} \texttt{list}\,[n]^{\alpha}\ \tau_2$$

To establish this simplified type, we use the rule **fix1**.[1] In typing the body of `map`, we assume that:

$$\texttt{map} : (\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{S}} \to \forall n, \alpha.\ \texttt{list}\,[n]^{\alpha}\ \tau_1 \xrightarrow{\alpha\cdot\kappa} \texttt{list}\,[n]^{\alpha}\ \tau_2$$

$$f : (\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{S}}$$

$$l : \texttt{list}\,[n]^{\alpha}\ \tau_1$$

We want to establish a dynamic stability $\alpha \cdot \kappa$ for the body and the type $\texttt{list}\,[n]^{\alpha}\ \tau_2$ for the result. The body of `map` is a case analysis on the list l, so we use rule **caseL**. The case $l = \texttt{nil}$ succeeds easily. There, $n \doteq 0$. The output expression is `nil`, which, by rule **nil**, has dynamic stability 0, which is trivially upper-bounded by $\alpha \cdot \kappa$ (formally, we use subtyping here). The expression `nil` also has type $\texttt{list}\,[0]^{0}\ \tau_2$, which can be weakened to the type $\texttt{list}\,[n]^{\alpha}\ \tau_2$ (again, we use subtyping).

The case $l = \texttt{cons}(h, tl)$ generates two branches. In the first branch, we assume $h : (\tau_1)^{\mathbb{S}}$ and $tl : \texttt{list}\,[n-1]^{\alpha}\ \tau_1$. In the second branch, we assume $h : \tau_1$ and $tl : \texttt{list}\,[n-1]^{\alpha-1}\ \tau_1$. The second branch is easier to type, so we explain its typing first. Inductively, the expression $\texttt{map}\ f\ tl$ has type $\texttt{list}\,[n-1]^{\alpha-1}\ \tau_2$ and cost $(\alpha - 1) \cdot \kappa$. From the types of f and h, the expression $f\ h$ has type τ_2 and cost κ. Hence, by rule **cons2**, the body of the case branch, $\texttt{cons}(f\ h, \texttt{map}\ f\ tl)$, has type $\texttt{list}\,[n]^{\alpha}\ \tau_2$ and cost $(\kappa + (\alpha - 1) \cdot \kappa) = \alpha \cdot \kappa$, as required.

We type the first branch as follows. From the types of f and h, $f\ h$ has type $(\tau_2)^{\mathbb{S}}$. Further, because f and h both have types annotated $(\cdot)^{\mathbb{S}}$, we can give $f\ h$ cost 0 by rule **nochange**. Inductively, the type and cost of the expression $\texttt{map}\ f\ tl$ are $\texttt{list}\,[n-1]^{\alpha}\ \tau_2$ and $\alpha \cdot \kappa$, respectively. By rule **cons1**, the body of the case branch has type $\texttt{list}\,[n]^{\alpha}\ \tau_2$ and cost $0 + \alpha \cdot \kappa = \alpha \cdot \kappa$, as required.

The reasoning with the **nochange** rule in the previous paragraph is invalid if f has type $(\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{C}}$, which means that f may change. In this case, every element of the output list may change and, additionally, the application of f to each element may have to be recomputed. This results in the following, second type for `map`. This type is established like the type above, but

[1] We could have used **fix2** in place of **fix1** and **nochange**, but the added power provided by **fix2** is not necessary to type `map`.

the reasoning proceeds using rule **cons2** in both branches, without any use of rule **nochange**, except at the top-level.

$$\texttt{map} : ((\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{C}} \to \forall n, \alpha.\ \texttt{list}\,[n]^{\alpha}\ \tau_1 \xrightarrow{n\cdot\kappa} \texttt{list}\,[n]^{n}\ \tau_2)^{\mathbb{S}}$$

The two types of `map` can be combined into one using conditional index terms. Let $I(\mu, \alpha, n) \triangleq ((\mu \doteq \mathbb{S})\ ?\ \alpha\ :\ n)$. Then,

$$\texttt{map} : (\forall \mu{::}\mathbb{V}.\ (\tau_1 \xrightarrow{\kappa} \tau_2)^{\mu} \to \forall n, \alpha.\ \texttt{list}\,[n]^{\alpha}\ \tau_1 \xrightarrow{I(\mu,\alpha,n)\cdot\kappa} \texttt{list}\,[n]^{I(\mu,\alpha,n)}\ \tau_2)^{\mathbb{S}}$$

Alternatively, the two types of `map` can be combined using intersection types, if CostIt is extended to include them. In subsequent examples that use `map`, we use either of its types and sometimes both.

Some arithmetic properties

We prove some arithmetic properties of summations and the log function that are needed to type later examples.

Lemma 1
For $n > 1$, $\lceil \texttt{log}_2(n) \rceil = 1 + \lceil \texttt{log}_2(\lceil \frac{n}{2} \rceil) \rceil$.

Proof. We split cases on the parity of n.

Case: n even. Let $n = 2k$. Then, $k = \lceil \frac{n}{2} \rceil$ and

$$\begin{aligned} \lceil \texttt{log}_2(n) \rceil &= \lceil \texttt{log}_2(2k) \rceil \\ &= \lceil 1 + \texttt{log}_2(k) \rceil \\ &= 1 + \lceil \texttt{log}_2(k) \rceil \\ &= 1 + \lceil \texttt{log}_2(\lceil \frac{n}{2} \rceil) \rceil \end{aligned}$$

Case: n odd. Then, $\lceil \frac{n}{2} \rceil = \frac{n+1}{2}$. Let $k \geq 1$ be such that $2^{k-1} < \frac{n+1}{2} \leq 2^k$ (note that $n \geq 3$, so such a k exists). Then, $2^k - 1 < n \leq 2^{k+1} - 1$. Since n is odd, this forces $2^k + 1 \leq n \leq 2^{k+1} - 1$. Hence, $k < \texttt{log}_2(n) < k + 1$, so $\lceil \texttt{log}_2(n) \rceil = k + 1$. Clearly, $\lceil \texttt{log}_2(\frac{n+1}{2}) \rceil = k$. Hence, $\lceil \texttt{log}_2(n) \rceil = k + 1 = \lceil \texttt{log}_2(\frac{n+1}{2}) \rceil + 1 = \lceil \texttt{log}_2(\lceil \frac{n}{2} \rceil) \rceil + 1$. □

Lemma 2
Let f be a monotonic function and $n > 1$, $\alpha > 0$ and $\alpha_1 + \alpha_2 = \alpha$. Then,

$$\left\lceil \sum_{i=0}^{\lceil \texttt{log}_2(\lceil \frac{n}{2} \rceil) \rceil} f(2^i) \cdot \texttt{min}\left(\alpha_1, 2^{\lceil \texttt{log}_2(\lceil \frac{n}{2} \rceil) \rceil - i}\right) \right\rceil +$$
$$\left\lceil \sum_{i=0}^{\lceil \texttt{log}_2(\lfloor \frac{n}{2} \rfloor) \rceil} f(2^i) \cdot \texttt{min}\left(\alpha_2, 2^{\lceil \texttt{log}_2(\lfloor \frac{n}{2} \rfloor) \rceil - i}\right) \right\rceil + f(n)$$

$$\leq \sum_{i=0}^{\lceil \texttt{log}_2(n) \rceil} f(2^i) \cdot \texttt{min}\left(\alpha, 2^{\lceil \texttt{log}_2(n) \rceil - i}\right)$$

Proof. We prove the inequality through a series of transformations. In each step, we highlight the changed subexpressions in red.

$$\left[\sum_{i=0}^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil} f(2^i) \cdot \texttt{min}\left(\alpha_1, 2^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil - i}\right)\right] +$$
$$\left[\sum_{i=0}^{\lceil \log_2(\lfloor \frac{n}{2} \rfloor)\rceil} f(2^i) \cdot \texttt{min}\left(\alpha_2, 2^{\lceil \log_2(\lfloor \frac{n}{2} \rfloor)\rceil - i}\right)\right] + f(n)$$

$$\leq \left[\sum_{i=0}^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil} f(2^i) \cdot \texttt{min}\left(\alpha_1, 2^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil - i}\right)\right] +$$
$$\left[\sum_{i=0}^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil} f(2^i) \cdot \texttt{min}\left(\alpha_2, 2^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil - i}\right)\right] + f(n)$$

$$= \left[\sum_{i=0}^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil} f(2^i) \cdot \left[\texttt{min}\left(\alpha_1, 2^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil - i}\right) + \texttt{min}\left(\alpha_2, 2^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil - i}\right)\right]\right] + f(n)$$

$$\leq \left[\sum_{i=0}^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil} f(2^i) \cdot \texttt{min}\left(\alpha_1 + \alpha_2, 2 \cdot 2^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil - i}\right)\right] + f(n)$$

(Using the inequality: $\texttt{min}(a, c) + \texttt{min}(b, c) \leq \texttt{min}(a + b, 2c)$)

$$= \left[\sum_{i=0}^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil} f(2^i) \cdot \texttt{min}\left(\alpha, 2^{1 + \lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil - i}\right)\right] + f(n)$$

$$= \left[\sum_{i=0}^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil} f(2^i) \cdot \texttt{min}\left(\alpha, 2^{\lceil \log_2(n) \rceil - i}\right)\right] + f(n)$$

(by Lemma 1)

$$\leq \left[\sum_{i=0}^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil} f(2^i) \cdot \texttt{min}\left(\alpha, 2^{\lceil \log_2(n) \rceil - i}\right)\right] + f(2^{\lceil \log_2(n) \rceil})$$

($n \leq 2^{\lceil \log_2(n) \rceil}$ and f is monotone)

$$= \left[\sum_{i=0}^{\lceil \log_2(\lceil \frac{n}{2} \rceil)\rceil} f(2^i) \cdot \texttt{min}\left(\alpha, 2^{\lceil \log_2(n) \rceil - i}\right)\right] + f(2^{\lceil \log_2(n) \rceil}) \cdot \texttt{min}(\alpha, 1)$$

(because $\alpha > 0$, $\texttt{min}(\alpha, 1) = 1$)

$\texttt{bsplit} : (\texttt{unit} \to \forall n, \alpha.\ \texttt{list}\,[n]^{\alpha}\ \tau \xrightarrow{0} \exists \beta{::}S.\ (\texttt{list}\,[\lceil \frac{n}{2} \rceil]^{\beta}\ \tau \times \texttt{list}\,[\lfloor \frac{n}{2} \rfloor]^{\alpha-\beta}\ \tau))^{\mathbb{S}}$

$\texttt{fix bsplit}(\_).\ \lambda l.$
$\texttt{case}_{\texttt{L}}\ l\ \texttt{of}$
$\quad \texttt{nil} \to (\texttt{nil}, \texttt{nil})$
$\mid \texttt{cons}(h_1,\ tl_1) \to \texttt{case}_{\texttt{L}}\ tl_2\ \texttt{of}$
$\qquad \texttt{nil} \to ([h_1], \texttt{nil})$
$\qquad \mid \texttt{cons}(h_2,\ tl_2) \to \texttt{let}\ (z_1, z_2) = \texttt{bsplit}\ ()\ tl_2\ \texttt{in}\ (\texttt{cons}(h_1,\ z_1), \texttt{cons}(h_2,\ z_2))$

$\texttt{bfold} : ((\tau \times \tau \xrightarrow{\kappa} \tau)^{\mathbb{S}} \to \forall n, \alpha.\ (n > 0) \to \texttt{list}\,[n]^{\alpha}\ \tau \xrightarrow{P(n,\alpha,\kappa)} \tau)^{\mathbb{S}}$
where $P(n, \alpha, \kappa) = \sum_{i=0}^{\lceil \log_2(n) \rceil} \kappa \cdot \texttt{min}(\alpha, 2^{\lceil \log_2(n) \rceil - i}) \in O(\alpha + \alpha \cdot \log_2(n))$
$\texttt{fix bfold}(f).\ \lambda l.$
$\texttt{case}_{\texttt{L}}\ l\ \texttt{of}$
$\quad \texttt{nil} \to \ldots$
$\mid \texttt{cons}(h_1,\ tl_1) \to \texttt{case}_{\texttt{L}}\ tl_2\ \texttt{of}$
$\qquad \texttt{nil} \to ([h_1], \texttt{nil})$
$\qquad \mid \texttt{cons}(\_,\ \_) \to \texttt{let}\ (z_1, z_2) = \texttt{bsplit}\ ()\ l\ \texttt{in}\ f\ (\texttt{bfold}\ f\ z_1, \texttt{bfold}\ z_2\ f)$

Figure 11: Examples `bsplit`, `bfold`

$$= \left\lceil \sum_{i=0}^{\lceil \log_2(\lceil \frac{n}{2} \rceil) \rceil} f(2^i) \cdot \texttt{min}\left(\alpha, 2^{\lceil \log_2(n) \rceil - i}\right) \right\rceil + f(2^{\lceil \log_2(n) \rceil}) \cdot \texttt{min}\left(\alpha, 2^{(\lceil \log_2(n) \rceil - \lceil \log_2(n) \rceil)}\right)$$

$$= \sum_{i=0}^{\lceil \log_2(n) \rceil} f(2^i) \cdot \texttt{min}\left(\alpha, 2^{\lceil \log_2(n) \rceil - i}\right)$$

(by Lemma 1, $\lceil \log_2(n) \rceil = 1 + \lceil \log_2(\lceil \frac{n}{2} \rceil) \rceil$)

□

Corollary 3

Let $P(n, \alpha, \kappa) = \sum_{i=0}^{\lceil \log_2(n) \rceil} \kappa \cdot \texttt{min}(\alpha, 2^{\lceil \log_2(n) \rceil - i})$. Then, for $n > 1$, $\alpha > 0$ and $\beta \leq \alpha$,

$$\kappa + P(\left\lceil \frac{n}{2} \right\rceil, \beta, \kappa) + P(\left\lfloor \frac{n}{2} \right\rfloor, \alpha - \beta, \kappa) \leq P(n, \alpha, \kappa)$$

Proof. Immediate from Lemma 2, choosing $f(n) = \kappa$, which is trivially monotonic. □

Balanced list fold

Figure 11 shows the function `bsplit` that splits a list of length n into two lists of lengths $\lceil \frac{n}{2} \rceil$ and $\lfloor \frac{n}{2} \rfloor$, by alternating elements of the original list into the two output lists. The function's type, shown in the figure, is easily established. The only important points about `bsplit` are that (a) the number of changes allowed to the input list are distributed among the two output lists through an existential quantifier, and (b) its dynamic stability is 0.

Using `bsplit`, we define the balanced fold function, `bfold`, that applies an associative folding function to a list using a balanced divide-and-conquer technique. Its type is:

$$\texttt{bfold} : ((\tau \times \tau \xrightarrow{\kappa} \tau)^{\mathbb{S}} \to \forall n, \alpha.\ (n > 0) \to \texttt{list}\,[n]^{\alpha}\ \tau \xrightarrow{P(n,\alpha,\kappa)} \tau)^{\mathbb{S}}$$

where $P(n, \alpha, \kappa) = \sum_{i=0}^{\lceil \texttt{log}_2(n) \rceil} \kappa \cdot \texttt{min}(\alpha, 2^{\lceil \texttt{log}_2(n) \rceil - i})$

We now explain how the type of `bfold` is established. We use rule **fix2**. In typing the body of `bfold`, we assume that:

$\texttt{bfold} : ((\tau \times \tau \xrightarrow{\kappa} \tau)^{\mathbb{S}} \to \forall n, \alpha.\ (n > 0) \to \texttt{list}\,[n]^{\alpha}\ \tau \xrightarrow{P(n,\alpha,\kappa)} \tau)^{\mathbb{S}}$

$f : (\tau \times \tau \xrightarrow{\kappa} \tau)^{\mathbb{S}}$

$l : \texttt{list}\,[n]^{\alpha}\ \tau$

$n > 0$

We have to show that the body of `bfold` has type τ and cost at most $P(n, \alpha, \kappa)$. The former is trivially checked, so we focus only on the latter. The body of `bfold` has two nested case analyses. The `nil` case of the outer one is irrelevant, because we assume that the list's length $n > 0$. Technically, this case succeeds by typing rule **contra**. The `nil` case of the inner case analysis is also straightforward. The body of this case analysis is a value $([h_1], \texttt{nil})$, which has cost 0 (the typing rules ensure that every value has cost 0). Trivially, this cost is no more than $P(n, \alpha, \kappa)$.

To type the body of the `cons` case of the inner case analysis, we further split the following two cases using the typing rule **split**: $\alpha > 0$ and $\alpha \doteq 0$.

Case: $\alpha > 0$**.** From the typing of `bsplit`, we know that for some β:

$z_1 : \texttt{list}\,\left[\lceil \frac{n}{2} \rceil\right]^{\beta}\ \tau$

$z_2 : \texttt{list}\,\left[\lfloor \frac{n}{2} \rfloor\right]^{\alpha-\beta}\ \tau$

Inductively, from the types of `bfold` and f, we derive that:

$(\texttt{bfold}\ f\ z_1)$ has cost $P(\lceil \frac{n}{2} \rceil, \beta, \kappa)$

$(\texttt{bfold}\ f\ z_2)$ has cost $P(\lfloor \frac{n}{2} \rfloor, \alpha - \beta, \kappa)$

Hence, the body of the case, $(f\ (\texttt{bfold}\ f\ z_1, \texttt{bfold}\ f\ z_2))$, has cost

$$\kappa + P(\left\lceil \frac{n}{2} \right\rceil, \beta, \kappa) + P(\left\lfloor \frac{n}{2} \right\rfloor, \alpha - \beta, \kappa)$$

Here, the additional κ cost accounts for the application of f. Note that in this case branch, $n > 1$ and we assumed that $\alpha > 0$. Hence, by Corollary 3, the expression above is upper-bounded by $P(n, \alpha, \kappa)$, as needed.

Case: $\alpha \doteq 0$**.** We show that the body of the case analysis has cost 0. As for $\alpha > 0$, we derive that

$z_1 : \texttt{list}\,\left[\lceil \frac{n}{2} \rceil\right]^{\beta}\ \tau$

$z_2 : \texttt{list}\,\left[\lfloor \frac{n}{2} \rfloor\right]^{\alpha-\beta}\ \tau$

However, because $\alpha \doteq 0$ (and, hence, $\beta \doteq 0$), by subtyping rules **l4** and **l2**, we can show that

$$\texttt{list}\ [\lceil \tfrac{n}{2} \rceil]^{\beta}\ \tau \sqsubseteq (\texttt{list}\ [\lceil \tfrac{n}{2} \rceil]^{\beta}\ \tau)^{\mathbb{S}} : *$$

$$\texttt{list}\ [\lfloor \tfrac{n}{2} \rfloor]^{\alpha-\beta}\ \tau \sqsubseteq (\texttt{list}\ [\lfloor \tfrac{n}{2} \rfloor]^{\alpha-\beta}\ \tau)^{\mathbb{S}} : *$$

The types of `bfold` and f already have annotations $(\cdot)^{\mathbb{S}}$. It follows by the typing rule **nochange** that the body of the case, $(f\ (\texttt{bfold}\ f\ z_1, \texttt{bfold}\ f\ z_2))$, has cost 0. This completes the typing of `bfold`.

We show that `bfold`'s stability $P(n,\alpha,\kappa) = \sum_{i=0}^{\lceil \log_2(n) \rceil} \kappa \cdot \texttt{min}(\alpha, 2^{\lceil \log_2(n) \rceil - i})$ lies in $O(\kappa \cdot (\alpha + \alpha \cdot \log_2(n/\alpha)))$, which is in $O(\kappa \cdot \log_2(n))$ for $\alpha \in O(1)$ and in $O(\kappa \cdot n)$ for $\alpha \in O(n)$.

Lemma 4
$P(n,\alpha,\kappa) \in O(\kappa \cdot (\alpha + \alpha \cdot \log_2(n/\alpha)))$. Specifically, for constant κ, $P(n,\alpha,\kappa) \in O(\alpha + \alpha \cdot \log_2(n/\alpha))$.

Proof. We proceed by splitting cases on i in the summation in $P(n,\alpha,\kappa)$. Consider the case $i > \lceil \log_2(n) \rceil - \lceil \log_2(\alpha) \rceil$. Then, $\lceil \log_2(n) \rceil - i < \lceil \log_2(\alpha) \rceil$ and, hence, $\lceil \log_2(n) \rceil - i \leq \lfloor \log_2(\alpha) \rfloor \leq \log_2(\alpha)$. So, $2^{\lceil \log_2(n) \rceil - i} \leq \alpha$. And, $\texttt{min}(\alpha, 2^{\lceil \log_2(n) \rceil - i}) = 2^{\lceil \log_2(n) \rceil - i}$.

In the case $i \leq \lceil \log_2(n) \rceil - \lceil \log_2(\alpha) \rceil$, $\lceil \log_2(n) \rceil - i \geq \lceil \log_2(\alpha) \rceil$ and $2^{\lceil \log_2(n) \rceil - i} \geq \alpha$, so $\texttt{min}(\alpha, 2^{\lceil \log_2(n) \rceil - i}) = \alpha$.

It follows that

$$\begin{aligned}
P(n,\alpha,\kappa) &= \sum_{i=0}^{\lceil \log_2(n) \rceil} \kappa \cdot \texttt{min}(\alpha, 2^{\lceil \log_2(n) \rceil - i}) \\
&= \sum_{i=0}^{\lceil \log_2(n) \rceil - \lceil \log_2(\alpha) \rceil} \kappa \cdot \texttt{min}(\alpha, 2^{\lceil \log_2(n) \rceil - i}) + \sum_{i=\lceil \log_2(n) \rceil - \lceil \log_2(\alpha) \rceil + 1}^{\lceil \log_2(n) \rceil} \kappa \cdot \texttt{min}(\alpha, 2^{\lceil \log_2(n) \rceil - i}) \\
&= \kappa \cdot \alpha \cdot (\lceil \log_2(n) \rceil - \lceil \log_2(\alpha) \rceil + 1) + \kappa \cdot (2^{\lceil \log_2(\alpha) \rceil - 1} + \ldots + 2^0) \\
&= \kappa \cdot \alpha \cdot (\lceil \log_2(n) \rceil - \lceil \log_2(\alpha) \rceil + 1) + \kappa \cdot (2^{\lceil \log_2(\alpha) \rceil} - 1) \\
&\in O(\kappa \cdot \alpha \cdot \log_2(n/\alpha)) + O(\kappa \cdot \alpha) \\
&= O(\kappa \cdot (\alpha + \alpha \cdot \log_2(n/\alpha)))
\end{aligned}$$

□

Divide-and-conquer and merge sort

Figure 12 shows a generic higher-order, divide-and-conquer function for list-valued algorithms on lists and a specific application of it, merge sort (the paper shows only the merge sort instance of the generic function). The generic function, `divConqList`, takes as its first argument a "conquer" function (called `conq`) that combines the two sublists obtained from recursive calls into a single output list. Overall, `divConqList` functions exactly like `bfold`: It partitions the input list using `bsplit`, recurs on the sublists and then combines the results using `conq`. The difference is that (a) Here, the result is a list of the same length as the original list and (b) The cost of the function `conq` can be an arbitrary monotonic function g of the list length n, i.e.,

$$\texttt{divConqList} : (\forall g{::}S \xrightarrow{\text{mon}} S.\ (\forall n, \alpha, \beta.\ \texttt{list}\,\left[\lceil \tfrac{n}{2} \rceil\right]^{\alpha}\ \tau \times \texttt{list}\,\left[\lfloor \tfrac{n}{2} \rfloor\right]^{\beta}\ \tau \xrightarrow{g(n)} \texttt{list}\,[n]^{n}\ \tau)^{\mathbb{S}}$$
$$\rightarrow \forall n, \alpha.\ \texttt{list}\,[n]^{\alpha}\ \tau \xrightarrow{R(g,n,\alpha)} \texttt{list}\,[n]^{n}\ \tau)^{\mathbb{S}}$$

$$\text{where } R(g,n,\alpha) = \sum_{i=0}^{\lceil \texttt{log}_2(n) \rceil} g(2^i) \cdot \texttt{min}(\alpha, 2^{\lceil \texttt{log}_2(n) \rceil - i})$$

```
fix divConqList(conq). λl.
caseL l of
  nil  → nil
| cons(h1, tl1)  →  caseL tl1 of
                      nil  → cons(h1, nil)
                    | cons(_, _)  →  let (z1, z2) = bsplit () l in
                                     conq (divConqList conq z1, divConqList conq z2)
```

$$\texttt{merge}_{\texttt{prim}} : (\forall n_1, n_2, \alpha_1, \alpha_2.\ (\texttt{list}\,[n_1]^{\alpha_1}\ \texttt{real} \times \texttt{list}\,[n_2]^{\alpha_2}\ \texttt{real}) \xrightarrow{n_1+n_2} \texttt{list}\,[n_1+n_2]^{n_1+n_2}\ \texttt{real})^{\mathbb{S}}$$

$$\texttt{mergeSort} : (\forall n, \alpha.\ \texttt{list}\,[n]^{\alpha}\ \tau \xrightarrow{Q(n,\alpha)} \texttt{list}\,[n]^{n}\ \tau)^{\mathbb{S}}$$
$$\text{where } Q(n,\alpha) = \sum_{i=0}^{\lceil \texttt{log}_2(n) \rceil} 2^i \cdot \texttt{min}(\alpha, 2^{\lceil \texttt{log}_2(n) \rceil - i}) \in O(n \cdot (1 + \texttt{log}_2(\alpha)))$$
$$\texttt{mergesort} = \lambda l.\, \texttt{divConqList}\ (\texttt{merge}_{\texttt{prim}})\ l$$

Figure 12: Examples `divConqList`, `mergeSort`

the cost of `conq` can depend on the length of the list. This flexibility is necessary to correctly analyze some algorithms like mergesort.

The dynamic stability of the function is $R(g,n,\alpha) = \sum_{i=0}^{\lceil \mathtt{log}_2(n)\rceil} g(2^i)\cdot \mathtt{min}(\alpha, 2^{\lceil \mathtt{log}_2(n)\rceil - i})$. The function is typed exactly like `bfold`. The difference is that in the case $\alpha > 0$, the inequality we obtain is:

$$g(n) + R(g, \left\lceil \frac{n}{2} \right\rceil, \beta) + R(g, \left\lfloor \frac{n}{2} \right\rfloor, \alpha - \beta) \leq R(g,n,\alpha)$$

After expanding the definition of R, this inequality reduces to Lemma 2.

The merge sort function, `mergeSort`, uses the `divConqList` function by passing to it a standard "merge" function (called $\mathtt{merge}_{\mathtt{prim}}$ here) that merges two sorted lists in linear time. Note that even if there a single element change in any one merged list, then every element of the output of the merge can change. This justifies the annotation $n_1 + n_2$ in the output type ($\mathtt{list}\,[\_]^{n_1+n_2}\ \_$) of $\mathtt{merge}_{\mathtt{prim}}$ in Figure 12. Also, the control flow of the merge function typically depends on the contents of the merged lists. Hence, such a function cannot be typed within CostIt. Instead, its linear dynamic stability must be established by other means (this is actually trivial, because the merge function's worst-case execution time is linear and there are existing results in self-adjusting computation which show that change propagation is asymptotically no costlier than evaluation from scratch).

There are other algorithms whose structure is exactly like merge sort, but whose "conquer" functions do not have data-dependent control flow. An example is the $O(n \cdot \mathtt{log}_2(n))$ subalgorithm of the fast Fourier transform, that evaluates a degree n polynomial on the n complex nth roots of -1. Such a function can be typed entirely within CostIt.

The dynamic stability of merge sort is $Q(n,\alpha) = R(\lambda x.x, n, \alpha) = \sum_{i=0}^{\lceil \mathtt{log}_2(n)\rceil} 2^i \cdot \mathtt{min}(\alpha, 2^{\lceil \mathtt{log}_2(n)\rceil - i})$. We show that this quantity lies in $O(n \cdot (1 + \mathtt{log}_2(\alpha)))$.

Lemma 5
$Q(n,\alpha) \in O(n \cdot (1 + \mathtt{log}_2(\alpha)))$.

Proof. We proceed by splitting cases on i in the summation in $Q(n,\alpha)$. Consider the case $i > \lceil \mathtt{log}_2(n)\rceil - \lceil \mathtt{log}_2(\alpha)\rceil$. Then, $\lceil \mathtt{log}_2(n)\rceil - i < \lceil \mathtt{log}_2(\alpha)\rceil$ and, hence, $\lceil \mathtt{log}_2(n)\rceil - i \leq \lfloor \mathtt{log}_2(\alpha)\rfloor \leq \mathtt{log}_2(\alpha)$. So, $2^{\lceil \mathtt{log}_2(n)\rceil - i} \leq \alpha$. And, $\mathtt{min}(\alpha, 2^{\lceil \mathtt{log}_2(n)\rceil - i}) = 2^{\lceil \mathtt{log}_2(n)\rceil - i}$.

In the case $i \leq \lceil \mathtt{log}_2(n)\rceil - \lceil \mathtt{log}_2(\alpha)\rceil$, $\lceil \mathtt{log}_2(n)\rceil - i \geq \lceil \mathtt{log}_2(\alpha)\rceil$ and $2^{\lceil \mathtt{log}_2(n)\rceil - i} \geq \alpha$, so $\mathtt{min}(\alpha, 2^{\lceil \mathtt{log}_2(n)\rceil - i}) = \alpha$.

It follows that

$$\begin{aligned}
Q(n,\alpha) &= \sum_{i=0}^{\lceil \mathtt{log}_2(n)\rceil} 2^i \cdot \mathtt{min}(\alpha, 2^{\lceil \mathtt{log}_2(n)\rceil - i}) \\
&= \sum_{i=0}^{\lceil \mathtt{log}_2(n)\rceil - \lceil \mathtt{log}_2(\alpha)\rceil} 2^i \cdot \mathtt{min}(\alpha, 2^{\lceil \mathtt{log}_2(n)\rceil - i}) + \sum_{i=\lceil \mathtt{log}_2(n)\rceil - \lceil \mathtt{log}_2(\alpha)\rceil + 1}^{\lceil \mathtt{log}_2(n)\rceil} 2^i \cdot \mathtt{min}(\alpha, 2^{\lceil \mathtt{log}_2(n)\rceil - i}) \\
&= \sum_{i=0}^{\lceil \mathtt{log}_2(n)\rceil - \lceil \mathtt{log}_2(\alpha)\rceil} 2^i \cdot \alpha + \sum_{i=\lceil \mathtt{log}_2(n)\rceil - \lceil \mathtt{log}_2(\alpha)\rceil + 1}^{\lceil \mathtt{log}_2(n)\rceil} 2^i \cdot 2^{\lceil \mathtt{log}_2(n)\rceil - i}
\end{aligned}$$

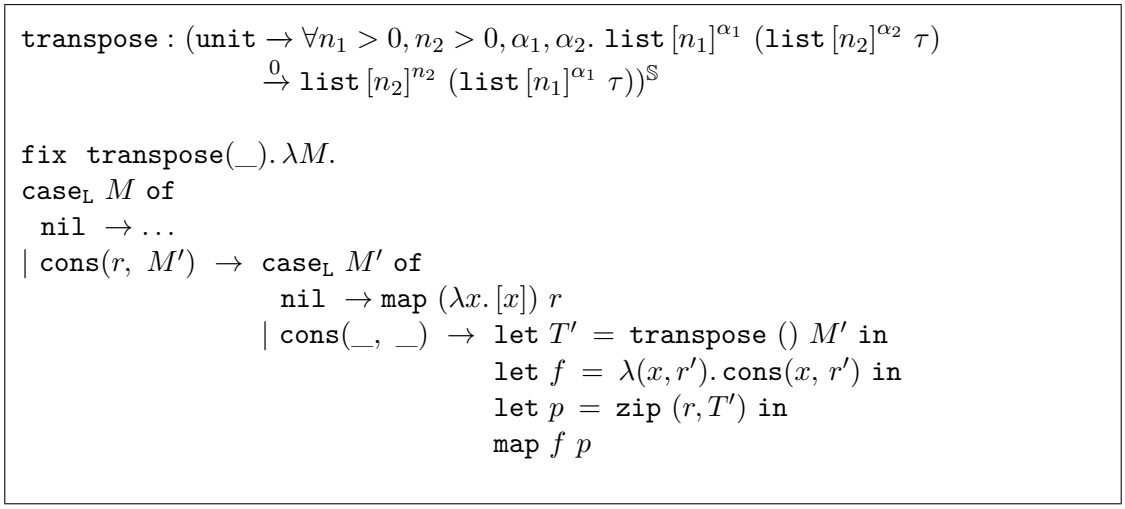

Figure 13: Example `transpose`

$$
\begin{aligned}
&= \alpha \cdot (2^0 + \ldots + 2^{\lceil \log_2(n) \rceil - \lceil \log_2(\alpha) \rceil}) + 2^{\lceil \log_2(n) \rceil} \cdot \lceil \log_2(\alpha) \rceil \\
&= \alpha \cdot (2^{\lceil \log_2(n) \rceil - \lceil \log_2(\alpha) \rceil + 1} - 1) + 2^{\lceil \log_2(n) \rceil} \cdot \lceil \log_2(\alpha) \rceil \\
&\in O(n) + O(n \cdot \log_2(\alpha)) \\
&= O(n \cdot (1 + \log_2(\alpha)))
\end{aligned}
$$

□

Matrix transpose

Figure 13 shows a standard matrix transpose function. The dynamic stability of this function is 0 because the function invokes no primitive functions. The function takes as input a matrix represented in row-major form as a list of lists of type $\texttt{list}\,[n_1]^{\alpha_1}\ \texttt{list}\,[n_2]^{\alpha_2}\ \tau$. This type means that the matrix has size $n_1 \times n_2$ and that, of the n_1 rows, α_1 are allowed to change and in each changed row, up to α_2 column elements may change. It is easy to see that the result of the transpose may *not* have the obvious type $\texttt{list}\,[n_2]^{\alpha_2}\ \texttt{list}\,[n_1]^{\alpha_1}\ \tau$; instead, its type is $\texttt{list}\,[n_2]^{n_2}\ \texttt{list}\,[n_1]^{\alpha_1}\ \tau$. That is, every row in the result may change. Consider, for instance, the following matrix in which x denotes an element that may change.

$$\begin{bmatrix} x & x & x & 2 \\ 3 & x & x & x \end{bmatrix}$$

This matrix has type $\texttt{list}\,[2]^2\ \texttt{list}\,[4]^3\ \texttt{real}$ but its transpose, shown below, does not have type $\texttt{list}\,[4]^3\ \texttt{list}\,[2]^2\ \texttt{real}$. Instead, it has the type $\texttt{list}\,[4]^4\ \texttt{list}\,[2]^2\ \texttt{real}$.

$$\begin{bmatrix} x & 3 \\ x & x \\ x & x \\ 2 & x \end{bmatrix}$$

We show here how the type of `transpose` is established. The dynamic stability is trivially counted to be 0 in every step, so we omit its description everywhere. Instead, we focus on the refinements to the `list` type. We start with the rule **nochange**, reducing our typing goal to:

$\texttt{transpose} : \texttt{unit} \to \forall n_1 > 0, n_2 > 0, \alpha_1, \alpha_2.\, \texttt{list}\,[n_1]^{\alpha_1}\ (\texttt{list}\,[n_2]^{\alpha_2}\ \tau) \xrightarrow{0} \texttt{list}\,[n_2]^{n_2}\ (\texttt{list}\,[n_1]^{\alpha_1}\ \tau)$

Next, we use the rule **fix1**. In typing the body of `transpose`, we assume that `transpose` has the type above and that:

$M : \texttt{list}\,[n_1]^{\alpha_1}\ \texttt{list}\,[n_2]^{\alpha_2}\ \tau$

$n_1, n_2 > 0$

We split cases $\alpha_1 > 0$ and $\alpha_1 \doteq 0$.

Case: $\alpha_1 > 0$**.** The body of `transpose` is a case analysis, so we use rule **caseL**. The **nil** case is irrelevant because $n_1 > 0$. For the `cons` case, there are two branches, as usual.

Subcase: In the first branch we assume:

$r : (\texttt{list}\,[n_2]^{\alpha_2}\ \tau)^{\mathbb{S}}$

$M' : \texttt{list}\,[n_1 - 1]^{\alpha_1}\ \texttt{list}\,[n_2]^{\alpha_2}\ \tau$

Next, the function case analyzes M'. If $M' = \texttt{nil}$, it returns $\texttt{map}\ (\lambda x.\,[x])\ r$. We need to show that this expression has the type $\texttt{list}\,[n_2]^{n_2}\ \texttt{list}\,[1]^{\alpha_1}\ \tau$ (note $n_1 \doteq 1$ here). This is straightforward: $\lambda x.\,[x]$ has type $\tau \xrightarrow{0} \texttt{list}\,[1]^1\ \tau$ by rule **cons2**. So, either type of map from Section yields $(\texttt{map}\ (\lambda x.\,[x])\ r) : \texttt{list}\,[n_2]^{n_2}\ \texttt{list}\,[1]^1\ \tau$. Since $\alpha_1 > 0$, subtyping yields $(\texttt{map}\ (\lambda x.\,[x])\ r) : \texttt{list}\,[n_2]^{n_2}\ \texttt{list}\,[1]^{\alpha_1}\ \tau$.

For $M' \neq \texttt{nil}$, we show below the types of various variables in the body of `transpose`.

$T' = (\texttt{transpose}\ ()\ M') : \texttt{list}\,[n_2]^{n_2}\ \texttt{list}\,[n_1 - 1]^{\alpha_1}\ \tau$ (inductively)

$f = (\lambda(x, r').\,\texttt{cons}(x,\, r')) : ((\tau)^{\mathbb{S}} \times \texttt{list}\,[n_1 - 1]^{\alpha_1}\ \tau) \to \texttt{list}\,[n_1]^{\alpha_1}\ \tau$ (rule **cons1**)

$r : (\texttt{list}\,[n_2]^{\alpha_2}\ \tau)^{\mathbb{S}} \sqsubseteq : *\texttt{list}\,[n_2]^{n_2}\ (\tau)^{\mathbb{S}}$ (subtyping rules **l1, l2, l3** and **l4**)

$p = (\texttt{zip}\ (r, T')) : \texttt{list}\,[n_2]^{n_2}\ ((\tau)^{\mathbb{S}} \times \texttt{list}\,[n_1 - 1]^{\alpha_1}\ \tau)$ (type of `zip`, Section)

Using either type of `map`, we derive that the output $(\texttt{map}\ f\ p)$ has type $\texttt{list}\,[n_2]^{n_2}\ \texttt{list}\,[n_1]^{\alpha_1}\ \tau$, as needed.

Subcase: In the second branch we assume:

$r : \texttt{list}\,[n_2]^{\alpha_2}\ \tau$

$M' : \texttt{list}\,[n_1 - 1]^{\alpha_1 - 1}\ \texttt{list}\,[n_2]^{\alpha_2}\ \tau$

The case $M' = \texttt{nil}$ is typed as in the previous subcase. For $M' \neq \texttt{nil}$, we show below the types of various variables in the body of `transpose`.

$T' = (\texttt{transpose}\ ()\ M') : \texttt{list}\,[n_2]^{n_2}\ \texttt{list}\,[n_1 - 1]^{\alpha_1 - 1}\ \tau$ (inductively)

$f = (\lambda(x, r').\,\texttt{cons}(x,\, r')) : (\tau \times \texttt{list}\,[n_1 - 1]^{\alpha_1 - 1}\ \tau) \to \texttt{list}\,[n_1]^{\alpha_1}\ \tau$ (rule **cons2**)

$p = (\texttt{zip}\ (r, T')) : \texttt{list}\,[n_2]^{n_2}\ (\tau \times \texttt{list}\,[n_1 - 1]^{\alpha_1 - 1}\ \tau)$ (type of `zip`, Section)

$\texttt{dotProd} : (\forall n, \alpha_1, \alpha_2.\ (\texttt{list}\,[n]^{\alpha_1}\ \texttt{real} \times \texttt{list}\,[n]^{\alpha_2}\ \texttt{real}) \xrightarrow{P_d(n,\alpha_1,\alpha_2)} \texttt{real})^{\mathbb{S}}$
where $P_d(n, \alpha_1, \alpha_2) = \sum_{i=0}^{\lceil \log_2(n) \rceil} \texttt{min}(\texttt{min}(\alpha_1+\alpha_2, n), 2^{\lceil \log_2(n) \rceil - i})$

$\texttt{dotProd} \ = \ \lambda(l_1, l_2).\texttt{bfold}\ (+)\ (\texttt{map}\ (*)\ (\texttt{zip}\ ()\ (l_1, l_2)))$

$\texttt{matrixMult} : (\texttt{unit} \to \forall n, m, k, \alpha_1, \alpha_2, \beta_1, \beta_2.\ (\texttt{list}\,[n]^{\alpha_1}\ \texttt{list}\,[m]^{\alpha_2}\ \texttt{real} \times \texttt{list}\,[k]^{\beta_1}\ \texttt{list}\,[m]^{\beta_2}\ \texttt{real})$
$\xrightarrow{P_r} \texttt{list}\,[n]^{n}\ \texttt{list}\,[k]^{k}\ \texttt{real})^{\mathbb{S}}$
where $P_r = (\alpha_1 \cdot k + \beta_1 \cdot n - \alpha_1 \cdot \beta_1) \cdot P_d(m, \alpha_2, \beta_2)$

```
fix matrixMult(_). λ(M1, M2).
caseL M1 of
 nil  → nil
| cons(r1, M1') → let R' = matrixMult () (M1', M2) in
                  let f = λc2. (dotProd (r1, c2)) in
                  let r' = map f M2 in
                  cons(r', R')
```

Figure 14: Examples `dotProd`, `matrixMult`

Using either type of `map`, we derive that the output (`map` f p) has type $\texttt{list}\,[n_2]^{n_2}\ \texttt{list}\,[n_1]^{\alpha_1}\ \tau$, as needed.

Case: $\alpha_1 \doteq 0$**.** The two branches for $M' \neq \texttt{nil}$ are typed exactly as above (those typing sub-derivations are parametric in α_1). The interesting case is $M' = \texttt{nil}$ where the function returns `map` $(\lambda x.\,[x])\ r$. We need to show that this expression has type $\texttt{list}\,[n_2]^{n_2}\ \texttt{list}\,[1]^{0}\ \tau$ (note $n_1 \doteq 1$ and $\alpha_1 \doteq 0$). Since M has type $\texttt{list}\,[n_1]^{\alpha_1}\ \texttt{list}\,[n_2]^{\alpha_2}\ \tau$ and $\alpha_1 \doteq 0$, by subtyping rules **l2** and **l3**, M also has type $\texttt{list}\,[n_1]^{0}\ \texttt{list}\,[n_2]^{n_2}\ (\tau)^{\mathbb{S}}$. Hence, r has type $\texttt{list}\,[n_2]^{n_2}\ (\tau)^{\mathbb{S}}$. Further, we can give $\lambda x.\,[x]$ the type $((\tau)^{\mathbb{S}} \to \texttt{list}\,[1]^{0}\ \tau)$ using rule **cons1**. So, from either type of `map`, (`map` $(\lambda x.\,[x])\ r) : \texttt{list}\,[n_2]^{n_2}\ \texttt{list}\,[1]^{0}\ \tau$.

Vector dot product and matrix multiplication

Figure 14 shows a standard vector dot product function, `dotProd`, obtained by composing `map` and `bfold`. The type of the function follows immediately from the types of `map` and `bfold`. If the two input vectors have length n each and are allowed α_1 and α_2 changes, then the dynamic stability of `dotProd` is $P_d(n, \alpha_1, \alpha_2) = \sum_{i=0}^{\lceil \log_2(n) \rceil} \texttt{min}(\texttt{min}(\alpha_1+\alpha_2, n), 2^{\lceil \log_2(n) \rceil - i})$. For $\beta = \texttt{min}(\alpha_1 + \alpha_2, n)$, this stability is in $O(\beta + \beta \cdot \texttt{log}_2(n/\beta))$ by Lemma 4. When $\alpha_1, \alpha_2 \in O(1)$, $\beta \in O(1)$ and this stability reduces to $O(\texttt{log}_2(n))$. When $\alpha_1, \alpha_2 \in O(n)$, $\beta \in O(n)$ and this stability reduces to $O(n)$. Both of these are as expected.

Figure 14 also shows a standard matrix multiplication funtion, `matrixMult`, that multiplies two matrices of sizes $n \times m$ and $m \times k$. The function assumes that the first matrix is represented

row-major, while the second matrix is represented column-major. The function iterates over the rows of the first matrix; for each row, it iterates over the columns of the second matrix; for each row and column, it computes a dot product. The interesting aspect of this function's type is its dynamic stability. If α_1 rows of the first matrix and β_1 columns of the second matrix can change, then at most $(\alpha_1 \cdot k + \beta_1 \cdot n - \alpha_1 \cdot \beta_1)$ elements of the result can change. So, at most these many dot products must be recomputed. If each row of the first matrix can have α_2 element changes and each column of the second matrix can have β_2 changes, then from the type of `dotProd`, the cost of recomputing each dot product is $P_d(m, \alpha_2, \beta_2)$. Hence, the dynamic stability is $P_r = (\alpha_1 \cdot k + \beta_1 \cdot n - \alpha_1 \cdot \beta_1) \cdot P_d(m, \alpha_2, \beta_2)$.

This dynamic stability may look complex, but it is not. Consider the special case of square matrices with $m = k = n$. Then, for $\alpha_1, \alpha_2, \beta_1, \beta_2 \in O(1)$ (fixed number of changes), $P_r \in O(n \cdot \texttt{log}_2(n))$. For $\alpha_1, \alpha_2, \beta_1, \beta_2 \in O(n)$ (arbitrary number of changes), $P_r \in O(n^3)$.

We explain how `matrixMult` is typed. First, we use the rule **nochange** to reduce the type of `matrixMult` to:

$$\texttt{matrixMult}: \ \texttt{unit} \to \forall n, m, k, \alpha_1, \alpha_2, \beta_1, \beta_2.\ (\texttt{list}\,[n]^{\alpha_1}\ \texttt{list}\,[m]^{\alpha_2}\ \texttt{real} \times \texttt{list}\,[k]^{\beta_1}\ \texttt{list}\,[m]^{\beta_2}\ \texttt{real}) \xrightarrow{P_r} \texttt{list}\,[n]^{n}\ \texttt{list}\,[k]^{k}\ \texttt{real}$$

In typing the body of `matrixMult`, we assume the following types for arguments:

$M_1 : \texttt{list}\,[n]^{\alpha_1}\ \texttt{list}\,[m]^{\alpha_2}\ \texttt{real}$

$M_2 : \texttt{list}\,[k]^{\beta_1}\ \texttt{list}\,[m]^{\beta_2}\ \texttt{real}$

The body of `matrixMult` is a case analysis on M_1, so we use the rule **caseL**. The case $M_1 = \texttt{nil}$ is trivially discharged: The output in this case is `nil`, which has cost 0 by rule **nil**.

The case $M_1 = \texttt{cons}(r_1, M_1')$ results in two branches. We define $Q = P_d(m, \alpha_2, \beta_2)$ for brevity.

Subcase: In one branch, we assume that

$r_1 : (\texttt{list}\,[m]^{\alpha_2}\ \texttt{real})^{\mathbb{S}}$

$M_1' : \texttt{list}\,[n-1]^{\alpha_1}\ \texttt{list}\,[m]^{\alpha_2}\ \texttt{real}$

We list below the change propagation costs of various subexpressions and their types.

- $R' = \texttt{matrixMult}\ ()\ (M_1', M_2)$
  Type: $\texttt{list}\,[n-1]^{n-1}\ \texttt{list}\,[k]^{k}\ \texttt{real}$
  Cost: $(\alpha_1 \cdot k + \beta_1 \cdot (n-1) - \alpha_1 \cdot \beta_1) \cdot Q$ (inductively)

- $f = \lambda c_2.\,(\texttt{dotProd}\ (r_1, c_2))$
  Type: $(\texttt{list}\,[m]^{\beta_2}\ \texttt{real} \xrightarrow{Q} \texttt{real})^{\mathbb{S}}$
  Cost: 0 (type of `dotProd`; rule **nochange**)

- $r' = \texttt{map}\ f\ M_2$
  Type: $\texttt{list}\,[k]^{\beta_1}\ \texttt{real} \sqsubseteq : *\texttt{list}\,[k]^{k}\ \texttt{real}$
  Cost: $\beta_1 \cdot Q$ (first type of `map`; $f : (\cdot)^{\mathbb{S}}$)

- Output = $\texttt{cons}(r', R')$
  Type: $\texttt{list}\,[n]^{n}\ \texttt{list}\,[k]^{k}\ \texttt{real}$
  Cost: 0 (rule **cons2**)

The total cost is $(\alpha_1 \cdot k + \beta_1 \cdot (n-1) - \alpha_1 \cdot \beta_1) \cdot Q + 0 + \beta_1 \cdot Q + 0 = (\alpha_1 \cdot k + \beta_1 \cdot n - \alpha_1 \cdot \beta_1) \cdot Q$, as required.

Subcase: In the second branch, we assume that

$r_1 : \texttt{list}\,[m]^{\alpha_2}\ \texttt{real}$

$M_1' : \texttt{list}\,[n-1]^{\alpha_1 - 1}\ \texttt{list}\,[m]^{\alpha_2}\ \texttt{real}$

We list below the change propagation costs of various subexpressions and their types.

- $R' = \texttt{matrixMult}\ ()\ (M_1', M_2)$
  Type: $\texttt{list}\,[n-1]^{n-1}\ \texttt{list}\,[k]^{k}\ \texttt{real}$
  Cost: $((\alpha_1 - 1) \cdot k + \beta_1 \cdot (n-1) - (\alpha_1 - 1) \cdot \beta_1) \cdot Q = ((\alpha_1 - 1) \cdot k + \beta_1 \cdot n - \alpha_1 \cdot \beta_1) \cdot Q$ (inductively)

- $f = \lambda c_2.\,(\texttt{dotProd}\ (r_1, c_2))$
  Type: $\texttt{list}\,[m]^{\beta_2}\ \texttt{real} \xrightarrow{Q} \texttt{real}$
  Cost: 0 (type of `dotProd`)

- $r' = \texttt{map}\ f\ M_2$
  Type: $\texttt{list}\,[k]^{k}\ \texttt{real}$
  Cost: $k \cdot Q$ (second type of `map`)

- Output = $\texttt{cons}(r', R')$
  Type: $\texttt{list}\,[n]^{n}\ \texttt{list}\,[k]^{k}\ \texttt{real}$
  Cost: 0 (rule **cons2**)

The total cost is $((\alpha_1 - 1) \cdot k + \beta_1 \cdot n - \alpha_1 \cdot \beta_1) \cdot Q + 0 + k \cdot Q + 0 = (\alpha_1 \cdot k + \beta_1 \cdot n - \alpha_1 \cdot \beta_1) \cdot Q$, as required.

$$
\begin{array}{rrl}
\text{Traces} & T & ::= \quad \mathtt{r} \mid \mathtt{b} \mid (T_1, T_2) \mid \mathtt{fst}\ T \mid \mathtt{snd}\ T \mid \\
& & \quad \mathtt{0} \mid \mathtt{succ}\ T \mid \mathtt{case_0}(T, T') \mid \mathtt{case_s}(T, T') \mid \\
& & \quad \mathtt{nil} \mid \mathtt{cons}(T_1, T_2) \mid \mathtt{case_{nil}}(T, T') \mid \mathtt{case_{cons}}(T, T') \mid \\
& & \quad \mathtt{fix} f(x).e \mid \mathtt{app}(T_1, T_2, T_r) \mid \mathtt{primApp}(T, v_r, \zeta) \mid \\
& & \quad \Lambda.e \mid \mathtt{iApp}(T, T_r) \mid \mathtt{pack}\ T \mid \mathtt{unpack}\ T\ \mathtt{as}\ x\ \mathtt{in}\ T' \mid \\
& & \quad \mathtt{let}\ x\ =\ T_1\ \mathtt{in}\ T_2 \mid ()
\end{array}
$$

Figure 15: Traces

$\boxed{e \Downarrow v, T}$ Expression e evaluates to value v with trace T

$$\frac{}{\mathtt{r} \Downarrow \mathtt{r}, \mathtt{r}}\ \mathbf{r} \qquad \frac{}{\mathtt{b} \Downarrow \mathtt{b}, \mathtt{b}}\ \mathbf{b} \qquad \frac{e_1 \Downarrow v_1, T_1 \qquad e_2 \Downarrow v_2, T_2}{(e_1, e_2) \Downarrow (v_1, v_2), (T_1, T_2)}\ \mathbf{pair} \qquad \frac{e \Downarrow v, T}{\mathtt{fst}\ e \Downarrow \mathtt{fst}\ v, \mathtt{fst}\ T}\ \mathbf{fst}$$

$$\frac{e \Downarrow v, T}{\mathtt{snd}\ e \Downarrow \mathtt{snd}\ v, \mathtt{snd}\ T}\ \mathbf{snd} \qquad \frac{}{\mathtt{0} \Downarrow \mathtt{0}, \mathtt{0}}\ \mathbf{0} \qquad \frac{e \Downarrow v, T}{\mathtt{succ}\ e \Downarrow \mathtt{succ}\ v, \mathtt{succ}\ T}\ \mathbf{Succ}$$

$$\frac{e \Downarrow \mathtt{0}, T \qquad e_1 \Downarrow v_1, T_1}{\mathtt{case_N}\ e\ \mathtt{of}\ \mathtt{0}\ \rightarrow\ e_1 \mid \mathtt{succ}(x)\ \rightarrow\ e_2 \Downarrow v_1, \mathtt{case_0}(T, T_1)}\ \mathbf{case\text{-}z}$$

$$\frac{e \Downarrow \mathtt{succ}\ v, T \qquad e_2[v/x] \Downarrow v_2, T_2}{\mathtt{case_N}\ e\ \mathtt{of}\ \mathtt{0}\ \rightarrow\ e_1 \mid \mathtt{succ}(x)\ \rightarrow\ e_2 \Downarrow v_1, \mathtt{case_s}(T, T_2)}\ \mathbf{case\text{-}s} \qquad \frac{}{\mathtt{nil} \Downarrow \mathtt{nil}, \mathtt{nil}}\ \mathbf{nil}$$

$$\frac{e_1 \Downarrow v_1, T_1 \qquad e_2 \Downarrow v_2, T_2}{\mathtt{cons}(e_1,\ e_2) \Downarrow \mathtt{cons}(v_1,\ v_2), \mathtt{cons}(T_1, T_2)}\ \mathbf{cons}$$

$$\frac{e \Downarrow \mathtt{nil}, T \qquad e_1 \Downarrow v_1, T_1}{\mathtt{case_L}\ e\ \mathtt{of}\ \mathtt{nil}\ \rightarrow\ e_1 \mid \mathtt{cons}(h, tl)\ \rightarrow\ e_2 \Downarrow v_1, \mathtt{case_{nil}}(T, T_1)}\ \mathbf{case\text{-}nil}$$

$$\frac{e \Downarrow \mathtt{cons}(v_h,\ v_{tl}), T \qquad e_2[v_h/h, v_{tl}/tl] \Downarrow v_2, T_2}{\mathtt{case_L}\ e\ \mathtt{of}\ \mathtt{nil}\ \rightarrow\ e_1 \mid \mathtt{cons}(h, tl)\ \rightarrow\ e_2 \Downarrow v_2, \mathtt{case_{cons}}(T, T_2)}\ \mathbf{case\text{-}cons}$$

$$\frac{}{\mathtt{fix}\ \ f(x).\, e \Downarrow \mathtt{fix}\ \ f(x).\, e, \mathtt{fix} f(x).e}\ \mathbf{fix}$$

$$\frac{e_1 \Downarrow \mathtt{fix}\ \ f(x).\, e, T_1 \qquad e_2 \Downarrow v_2, T_2 \qquad e[v_2/x, (\mathtt{fix}\ \ f(x).\, e)/f] \Downarrow v_r, T_r}{e_1\ e_2 \Downarrow v_r, \mathtt{app}(T_1, T_2, T_r)}\ \mathbf{app}$$

$$\frac{e \Downarrow v, T \qquad \widehat{\zeta}(v) = (\_, v_r)}{\zeta\ e \Downarrow v_r, \mathtt{primApp}(T, v_r, \zeta)}\ \mathbf{primapp} \qquad \frac{}{\Lambda.\, e \Downarrow \Lambda.\, e, \Lambda.e}\ \mathbf{Lam} \qquad \frac{e \Downarrow \Lambda.\, e', T \qquad e' \Downarrow v_r, T_r}{e[] \Downarrow v_r, \mathtt{iApp}(T, T_r)}\ \mathbf{App}$$

$$\frac{e \Downarrow v, T}{\mathtt{pack}\ e \Downarrow \mathtt{pack}\ v, \mathtt{pack}\ T}\ \mathbf{pack} \qquad \frac{e \Downarrow \mathtt{pack}\ v, T \qquad e[v/x] \Downarrow v_r, T_r}{\mathtt{unpack}\ e\ \mathtt{as}\ x\ \mathtt{in}\ e' \Downarrow v_r, \mathtt{unpack}\ T\ \mathtt{as}\ x\ \mathtt{in}\ T_r}\ \mathbf{unpack}$$

$$\frac{}{\nu.\, e \Downarrow \nu.\, e, \nu.e}\ \mathbf{tyLam} \qquad \frac{e \Downarrow \nu.\, e', T \qquad e' \Downarrow v_r, T_r}{e[-] \Downarrow v_r, \mathtt{tApp}(T, T_r)}\ \mathbf{tyApp}$$

$$\frac{e \Downarrow v, T \qquad e'[v/x] \Downarrow v_r, T_r}{\mathtt{let}\ x\ =\ e\ \mathtt{in}\ e' \Downarrow v_r, \mathtt{let}\ x\ =\ T\ \mathtt{in}\ T_r}\ \mathbf{let} \qquad \frac{}{() \Downarrow (), ()}\ \mathbf{unit}$$

Figure 16: Evaluation semantics

$$
\begin{array}{lll}
\text{Bi-values} & w ::= & \texttt{keep(r)} \mid \texttt{repl(r, r')} \mid \texttt{keep(b)} \mid \texttt{repl(b, b')} \mid \\
& & (w_1, w_2) \mid \texttt{0} \mid \texttt{succ}\ w \mid \texttt{nil} \mid \texttt{cons}(w_1, w_2) \mid \\
& & \texttt{fix}\ f(x).\text{æ} \mid \Lambda.\text{æ} \mid \texttt{pack}\ w \mid \nu.\text{æ} \mid () \\
\text{Bi-expressions} & \text{æ} ::= & x \mid \texttt{keep(r)} \mid \texttt{repl(r, r')} \mid \texttt{keep(b)} \mid \texttt{repl(b, b')} \mid \\
& & (\text{æ}_1, \text{æ}_2) \mid \texttt{fst}\ \text{æ} \mid \texttt{snd}\ \text{æ} \mid \\
& & \texttt{0} \mid \texttt{succ}\ \text{æ} \mid \texttt{nil} \mid \texttt{cons}(\text{æ}_1, \text{æ}_2) \mid \\
& & (\texttt{case}_{\texttt{N}}\ \text{æ}\ \texttt{of 0} \rightarrow \text{æ}_1 \mid \texttt{succ}\ x \rightarrow \text{æ}_2) \mid \\
& & (\texttt{case}_{\texttt{L}}\ \text{æ}\ \texttt{of nil} \rightarrow \text{æ}_1 \mid \texttt{cons}(h, tl) \rightarrow \text{æ}_2) \mid \\
& & \texttt{fix}\ f(x).\text{æ} \mid \text{æ}_1\ \text{æ}_2 \mid \zeta\ \text{æ} \mid \Lambda.\text{æ} \mid \text{æ}[] \mid \\
& & \texttt{pack}\ \text{æ} \mid \texttt{unpack}\ \text{æ}\ \texttt{as}\ x\ \texttt{in}\ \text{æ}' \mid \\
& & \nu.\text{æ} \mid \text{æ}[-] \mid \texttt{let}\ x = \text{æ}_1\ \texttt{in}\ \text{æ}_2 \mid ()
\end{array}
$$

$$\boxed{\texttt{stable}(w) \triangleq \texttt{replace} \notin w \text{ and } \texttt{stable}(\text{æ}) \triangleq \texttt{replace} \notin \text{æ}}$$

Figure 17: Syntax of bi-values and bi-expression

$$
\begin{array}{rcl||rcl}
\mathrm{L}(\texttt{keep(r)}) & = & \texttt{r} & \mathrm{R}(\texttt{keep(r)}) & = & \texttt{r} \\
\mathrm{L}(\texttt{repl(r, r')}) & = & \texttt{r} & \mathrm{R}(\texttt{repl(r, r')}) & = & \texttt{r'} \\
\mathrm{L}(\texttt{keep(b)}) & = & \texttt{b} & \mathrm{R}(\texttt{keep(b)}) & = & \texttt{b} \\
\mathrm{L}(\texttt{repl(b, b')}) & = & \texttt{b} & \mathrm{R}(\texttt{repl(b, b')}) & = & \texttt{b'} \\
\mathrm{L}(\texttt{0}) & = & \texttt{0} & \mathrm{R}(\texttt{0}) & = & \texttt{0} \\
\mathrm{L}(\texttt{succ}\ \text{æ}) & = & \texttt{succ}\ \mathrm{L}(\text{æ}) & \mathrm{R}(\texttt{succ}\ \text{æ}) & = & \texttt{succ}\ \mathrm{R}(\text{æ}) \\
& & \vdots & & & \vdots
\end{array}
$$

Homomorphic in all other syntactic constructs

$$\boxed{\text{If } \mathrm{L}(\text{æ}) = e \text{ and } \mathrm{R}(\text{æ}) = e', \text{ then define } \texttt{merge}(e, e') = \text{æ}.}$$

Figure 18: $\mathrm{L}(\text{æ})$: Left or original expression. $\mathrm{R}(\text{æ})$: Right or modified expression.

$\boxed{\Psi;\Delta;\Phi;\Gamma \vdash w \gg \tau \text{ and } \Psi;\Delta;\Phi;\Gamma \vdash \mathfrak{e} \gg_\kappa \tau}$ Bi-value and bi-expression typing

$$\frac{}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{keep(r)} \gg (\mathtt{real})^{\mathbb{S}}}\ \textbf{keep-r} \qquad \frac{}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{keep(b)} \gg (\mathtt{bool})^{\mathbb{S}}}\ \textbf{keep-b}$$

$$\frac{}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{repl(r,r')} \gg (\mathtt{real})^{\mathbb{C}}}\ \textbf{repl-r} \qquad \frac{}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{repl(b,b')} \gg (\mathtt{bool})^{\mathbb{C}}}\ \textbf{repl-b}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash w_1 \gg \tau_1 \qquad \Psi;\Delta;\Phi;\Gamma \vdash w_2 \gg \tau_2}{\Psi;\Delta;\Phi;\Gamma \vdash (w_1,w_2) \gg \tau_1 \times \tau_2}\ \textbf{pair} \qquad \frac{}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{0} \gg \mathtt{N}[0]}\ \mathtt{0}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash w \gg \mathtt{N}[n]}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{succ}\ w \gg \mathtt{N}[n{+}1]}\ \textbf{Succ} \qquad \frac{}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{nil} \gg \mathtt{list}\,[0]^0\ \tau}\ \textbf{nil}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash w_1 \gg (\tau)^{\mathbb{S}} \qquad \Psi;\Delta;\Phi;\Gamma \vdash w_2 \gg \mathtt{list}\,[n]^\alpha\ \tau}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{cons}(w_1,w_2) \gg \mathtt{list}\,[n{+}1]^\alpha\ \tau}\ \textbf{cons1}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash w_1 \gg \tau \qquad \Psi;\Delta;\Phi;\Gamma \vdash w_2 \gg \mathtt{list}\,[n]^{\alpha-1}\ \tau \qquad \Delta;\Phi \models \alpha > 0}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{cons}(w_1,w_2) \gg \mathtt{list}\,[n{+}1]^\alpha\ \tau}\ \textbf{cons2}$$

$$\frac{\Psi;t :: S,\Delta;\Phi;\Gamma \vdash \mathfrak{e} \gg_\kappa \tau \qquad t \notin FV(\Phi;\Gamma)}{\Psi;\Delta;\Phi;\Gamma \vdash \Lambda.\mathfrak{e} \gg \forall t \overset{\kappa}{::} S.\ \tau}\ \textbf{Lam} \qquad \frac{\Psi;\Delta;\Phi;\Gamma \vdash w \gg \tau\{I/t\} \qquad \Delta \vdash I :: \mathtt{\kappa}}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{pack}\ w \gg \exists t{::}S.\ \tau}\ \textbf{pack}$$

$$\frac{X : K,\Psi;\Delta;\Phi;\Gamma \vdash \mathfrak{e} \gg_\kappa \tau}{\Psi;\Delta;\Phi;\Gamma \vdash \nu.\mathfrak{e} \gg \forall X \overset{\kappa}{:} K.\tau}\ \textbf{tylam} \qquad \frac{\Psi;\Delta;\Phi;x : \tau_1, f : \tau_1 \xrightarrow{\kappa} \tau_2,\Gamma \vdash \mathfrak{e} \gg_\kappa \tau_2}{\Psi;\Delta;\Phi;\Gamma \vdash \mathtt{fix}\ \ f(x).\,\mathfrak{e} \gg \tau_1 \xrightarrow{\kappa} \tau_2}\ \textbf{fix1}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash w \gg \tau \qquad \forall z \in \Gamma.\ \ \Psi;\Delta;\Phi \models \Gamma(z) \sqsubseteq (\Gamma(z))^{\mathbb{S}} : * \qquad \mathtt{stable}(w)}{\Psi;\Delta;\Phi;\Gamma,\Gamma' \vdash w \gg (\tau)^{\mathbb{S}}}\ \textbf{nochange}$$

$$\frac{\Psi;\Delta;\Phi;x : \tau_1, f : (\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{S}},\Gamma \vdash \mathfrak{e} \gg_\kappa \tau_2 \qquad \forall z \in \Gamma.\ \ \Psi;\Delta;\Phi \models \Gamma(z) \sqsubseteq (\Gamma(z))^{\mathbb{S}} : * \qquad \mathtt{stable}(\mathfrak{e})}{\Psi;\Delta;\Phi;\Gamma,\Gamma' \vdash \mathtt{fix}\ \ f(x).\,\mathfrak{e} \gg (\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{S}}}\ \textbf{fix2}$$

$$\frac{\Psi;\Delta;\Phi \wedge C;\Gamma \vdash w \gg \tau}{\Psi;\Delta;\Phi;\Gamma \vdash w \gg C \to \tau}\ \textbf{c-imp} \qquad \frac{\Delta;\Phi \models C \qquad \Psi;\Delta;\Phi;\Gamma \vdash w \gg \tau}{\Delta;\Phi \vdash w \gg C \wedge \tau}\ \textbf{c-and}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash w \gg \tau \qquad \Delta;\Phi \models \tau \sqsubseteq \tau' : *}{\Psi;\Delta;\Phi;\Gamma \vdash w \gg \tau'}\ \sqsubseteq : * \qquad \frac{}{\Psi;\Delta;\Phi;\Gamma \vdash () \gg \mathtt{unit}}\ \textbf{unit}$$

$$\frac{\Psi;\Delta;\Phi;\Gamma \vdash w_i \gg \tau_i \qquad \Psi;\Delta;\Phi;\overline{x_i : \tau_i},\Gamma \vdash e :_\kappa \tau}{\Psi;\Delta;\Phi;\Gamma \vdash \ulcorner e \urcorner[\overline{w_i/x_i}] \gg_\kappa \tau}\ \textbf{exp}$$

Figure 19: Typing rules for bi-values and bi-expressions

$\boxed{\langle T, \mathscr{e} \rangle \curvearrowright w', T', c'}$ Change propagation with cost-counting

$$\frac{}{\langle \mathtt{n}, \mathtt{keep}(\_) \rangle \curvearrowright \mathtt{keep}(\mathtt{r}), \mathtt{n}, 0} \textbf{ r-keep} \qquad \frac{}{\langle \mathtt{n}, \mathtt{repl}(\_, \mathtt{r}') \rangle \curvearrowright \mathtt{repl}(\mathtt{r}, \mathtt{r}'), \mathtt{n}', 0} \textbf{ r-repl}$$

$$\frac{\langle T_1, \mathscr{e}_1 \rangle \curvearrowright w_1', T_1', c_1' \qquad \langle T_2, \mathscr{e}_2 \rangle \curvearrowright w_2', T_2', c_2'}{\langle (T_1, T_2), (\mathscr{e}_1, \mathscr{e}_2) \rangle \curvearrowright (w_1', w_2'), (T_1', T_2'), c_1' + c_2'} \textbf{ r-pair} \qquad \frac{\langle T, \mathscr{e} \rangle \curvearrowright (w_1, w_2), T', c'}{\langle \mathtt{fst}\ T, \mathtt{fst}\ \mathscr{e} \rangle \curvearrowright w_1, \mathtt{fst}\ T', c'} \textbf{ r-fst}$$

$$\frac{\langle T, \mathscr{e} \rangle \curvearrowright (w_1, w_2), T', c'}{\langle \mathtt{snd}\ T, \mathtt{snd}\ \mathscr{e} \rangle \curvearrowright w_2, \mathtt{snd}\ T', c'} \textbf{ r-snd} \qquad \frac{}{\langle \mathtt{0}, \mathtt{0} \rangle \curvearrowright \mathtt{0}, \mathtt{0}, 0} \textbf{ r-0}$$

$$\frac{\langle T, \mathscr{e} \rangle \curvearrowright w', T', c'}{\langle \mathtt{succ}\ T, \mathtt{succ}\ \mathscr{e} \rangle \curvearrowright \mathtt{succ}\ w', \mathtt{succ}\ T', c'} \textbf{ r-succ} \qquad \frac{}{\langle \mathtt{nil}, \mathtt{nil} \rangle \curvearrowright \mathtt{nil}, \mathtt{nil}, 0} \textbf{ r-nil}$$

$$\frac{\langle T, p \rangle \curvearrowright \mathtt{0}, T', c' \qquad \langle T_1, p_1 \rangle \curvearrowright p_1', T_1', c_1'}{\langle \mathtt{case_0}(T, T_1), \mathtt{case_N}\ \mathscr{e}\ \mathtt{of\ 0}\ \rightarrow\ \mathscr{e}_1 \mid \mathtt{succ}\ x\ \rightarrow\ \mathscr{e}_2 \rangle \curvearrowright w_1', \mathtt{case_0}(T', T_1'), c' + c_1'} \textbf{ r-case-z}$$

$$\frac{\langle T, \mathscr{e} \rangle \curvearrowright \mathtt{succ}\ w, T', c' \qquad \langle T_2, \mathscr{e}_2[w/x] \rangle \curvearrowright w_2', T_2', c_2'}{\langle \mathtt{case_s}(T, T_1), \mathtt{case_N}\ \mathscr{e}\ \mathtt{of\ 0}\ \rightarrow\ \mathscr{e}_1 \mid \mathtt{succ}\ x\ \rightarrow\ \mathscr{e}_2 \rangle \curvearrowright w_2', \mathtt{case_s}(T', T_2'), c' + c_2'} \textbf{ r-case-s}$$

$$\frac{\langle T_1, \mathscr{e}_1 \rangle \curvearrowright w_1', T_1', c_1' \qquad \langle T_2, \mathscr{e}_2 \rangle \curvearrowright w_2', T_2', c_2'}{\langle \mathtt{cons}(T_1, T_2), \mathtt{cons}(\mathscr{e}_1, \mathscr{e}_2) \rangle \curvearrowright \mathtt{cons}(w_1', w_2'), \mathtt{cons}(T_1', T_2'), c_1' + c_2'} \textbf{ r-cons}$$

$$\frac{\langle T, \mathscr{e} \rangle \curvearrowright \mathtt{nil}, T', c' \qquad \langle T_1, \mathscr{e}_1 \rangle \curvearrowright w_1', T_1', c_1'}{\langle \mathtt{case_{nil}}(T, T_1), \mathtt{case_L}\ \mathscr{e}\ \mathtt{of\ nil}\ \rightarrow\ \mathscr{e}_1 \mid \mathtt{cons}(h, tl)\ \rightarrow\ \mathscr{e}_2 \rangle \curvearrowright w_1', \mathtt{case_{nil}}(T', T_1'), c' + c_1'} \textbf{ r-case-nil}$$

$$\frac{\langle T, \mathscr{e} \rangle \curvearrowright \mathtt{cons}(w_h, w_{tl}), T', c' \qquad \langle T_2, \mathscr{e}_2[w_h/h, w_{tl}/tl] \rangle \curvearrowright w_2', T_2', c_2'}{\langle \mathtt{case_{cons}}(T, T_1), \mathtt{case_L}\ \mathscr{e}\ \mathtt{of\ nil}\ \rightarrow\ \mathscr{e}_1 \mid \mathtt{cons}(h, tl)\ \rightarrow\ \mathscr{e}_2 \rangle \curvearrowright w_2', \mathtt{case_{cons}}(T', T_2'), c' + c_2'} \textbf{ r-case-cons}$$

$$\frac{}{\langle \mathtt{fix}\ \ f(x).\, e', \mathtt{fix}\ f(x).\mathscr{e} \rangle \curvearrowright \mathtt{fix}\ f(x).\mathtt{merge}(e', \mathrm{R}(\mathscr{e})), \mathtt{fix} f(x).\mathrm{R}(\mathscr{e}), 0} \textbf{ r-fix}$$

$$\frac{\langle T_1, \mathscr{e}_1 \rangle \curvearrowright \mathtt{fix}\ f(x).\mathscr{e}, T_1', c_1' \qquad \langle T_2, \mathscr{e}_2 \rangle \curvearrowright w_2', T_2', c_2' \qquad \langle T_r, \mathscr{e}[w_2'/x, (\mathtt{fix}\ f(x).\mathscr{e})/f] \rangle \curvearrowright w_r', T_r', c_r'}{\langle \mathtt{app}(T_1, T_2, T_r), \mathscr{e}_1\ \mathscr{e}_2 \rangle \curvearrowright w_r', \mathtt{app}(T_1', T_2', T_r'), c_1' + c_2' + c_r'} \textbf{ r-app}$$

$$\frac{\mathtt{stable}(\mathscr{e})}{\langle \mathtt{primApp}(T, v_r, \zeta), \zeta\ \mathscr{e} \rangle \curvearrowright \ulcorner v_r \urcorner, \mathtt{primApp}(T, v_r, \zeta), 0} \textbf{ r-prim-s}$$

$$\frac{\neg \mathtt{stable}(\mathscr{e}) \qquad \langle T, \mathscr{e} \rangle \curvearrowright w', T', c' \qquad (c_r', v_r') = \widehat{\zeta}(\mathrm{R}(w'))}{\langle \mathtt{primApp}(T, v_r, \zeta), \zeta\ \mathscr{e} \rangle \curvearrowright \mathtt{merge}(v_r, v_r'),\ \mathtt{primApp}(T', v_r', \zeta),\ c' + c_r'} \textbf{ r-prim}$$

$$\frac{}{\langle \Lambda.e', \Lambda.\mathscr{e} \rangle \curvearrowright \Lambda.\mathtt{merge}(e', \mathrm{R}(\mathscr{e})), \Lambda.\mathrm{R}(\mathscr{e}), 0} \textbf{ r-Lam}$$

$$\frac{\langle T, \mathscr{e} \rangle \curvearrowright \Lambda.\mathscr{e}', T', c' \qquad \langle T_r, \mathscr{e}' \rangle \curvearrowright w_r', T_r', c_r'}{\langle \mathtt{iApp}(T, T_r), \mathscr{e}[] \rangle \curvearrowright w_r', \mathtt{iApp}(T', T_r'), c' + c_r'} \textbf{ r-App}$$

$$\frac{\langle T, \mathscr{e} \rangle \curvearrowright w', T', c'}{\langle \mathtt{pack}\ T, \mathtt{pack}\ \mathscr{e} \rangle \curvearrowright \mathtt{pack}\ w', \mathtt{pack}\ T', c'} \textbf{ r-pack}$$

$$\frac{\langle T, \mathscr{e} \rangle \curvearrowright \mathtt{pack}\ w', T', c' \qquad \langle T_r, \mathscr{e}'[w'/x] \rangle \curvearrowright w_r', T_r', c_r'}{\langle \mathtt{unpack}\ T\ \mathtt{as}\ x\ \mathtt{in}\ T_r, \mathtt{unpack}\ \mathscr{e}\ \mathtt{as}\ x\ \mathtt{in}\ \mathscr{e}' \rangle \curvearrowright w_r', \mathtt{unpack}\ T'\ \mathtt{as}\ x\ \mathtt{in}\ T_r', c' + c_r'} \textbf{ r-unpack}$$

$$\frac{}{\langle \nu.e', \nu.\mathscr{e} \rangle \curvearrowright \nu.\mathtt{merge}(e', \mathrm{R}(\mathscr{e})), \nu.\mathrm{R}(\mathscr{e}), 0} \textbf{ r-tyLam}$$

$$\frac{\langle T, \mathscr{e} \rangle \curvearrowright \nu.\mathscr{e}', T', c' \qquad \langle T_r, \mathscr{e}' \rangle \curvearrowright w_r', T_r', c_r'}{\langle \mathtt{tApp}(T, T_r), \mathscr{e}[-] \rangle \curvearrowright w_r', \mathtt{tApp}(T', T_r'), c' + c_r'} \textbf{ r-tyApp} \qquad \frac{}{\langle (), () \rangle \curvearrowright (), (), 0} \textbf{ r-unit}$$

$$\frac{\langle T_1, \mathscr{e}_1 \rangle \curvearrowright w_1', T_1', c_1' \qquad \langle T_2, \mathscr{e}_2[w_1'/x] \rangle \curvearrowright w_2', T_2', c_2'}{\langle \mathtt{let}\ x\ =\ T_1\ \mathtt{in}\ T_2, \mathtt{let}\ x\ =\ \mathscr{e}_1\ \mathtt{in}\ \mathscr{e}_2 \rangle \curvearrowright w_2', \mathtt{let}\ x\ =\ T_1'\ \mathtt{in}\ T_2', c_1' + c_2'} \textbf{ r-let}$$

Figure 20: Change propagation rules

$$
\begin{array}{l}
|\mathtt{v}| = 0 \quad \text{where} \quad \mathtt{v} = \mathtt{b}, \mathtt{r}, \mathtt{nil}, \mathtt{0}, \mathtt{fix} f(x).e, \Lambda.e, \nu.e, () \\
|\mathtt{succ}\ T| = |T| \\
|(T_1, T_2)| = |T_1| + |T_2| \\
|\mathtt{cons}(T_1, T_2)| = |T_1| + |T_2| \\
|\mathtt{pack}\ T| = |T| \\
|\mathtt{fst}\ T| = |T| + 1 \\
|\mathtt{snd}\ T| = |T| + 1 \\
|\mathtt{unpack}\ T\ \mathtt{as}\ x\ \mathtt{in}\ T_r| = |T| + |T_r| + 1 \\
|\mathtt{app}(T_1, T_2, T_r)| = |T_1| + |T_2| + |T_r| + 1 \\
|\mathtt{iApp}(T, T_r)| = |T| + |T_r| + 1 \\
|\mathtt{case}_{\mathtt{0}}(T, T')| = |T| + |T'| + 1 \\
|\mathtt{case}_{\mathtt{s}}(T, T')| = |T| + |T'| + 1 \\
|\mathtt{case}_{\mathtt{nil}}(T, T')| = |T| + |T'| + 1 \\
|\mathtt{case}_{\mathtt{cons}}(T, T')| = |T| + |T'| + 1 \\
|\mathtt{tApp}(T, T_r)| = |T| + |T_r| + 1 \\
|\mathtt{let}\ x\ =\ T\ \mathtt{in}\ T_r| = |T| + |T_r| + 1 \\
|\mathtt{primApp}(T, v_r, \zeta)| = |T| + 1
\end{array}
$$

Figure 21: Trace size

$$
\begin{array}{lcl}
[\![-]\!]_K & : & S \times S \times \cdots \times S \to (\text{Step index} \times \text{Bi-value}) \\
[\![*]\!]_K & = & \{R \subseteq \mathcal{P}(\text{Step index} \times \text{Bi-value}) \mid \forall j, m, \boldsymbol{w}.\ (m, \boldsymbol{w}) \in R \wedge j < m \Rightarrow (j, \boldsymbol{w}) \in R\} \\
[\![S{\to}K]\!]_K & = & S \to [\![K]\!]_K
\end{array}
$$

Figure 22: Semantics of Kinds

$[\![\tau]\!]^{\rho}_{v} \subseteq S \times S \times \cdots \times S \to (\text{Step index} \times \text{Bi-value})$ $\quad m$ denotes a step-index

$[\![\tau]\!]^{\rho,\kappa}_{\varepsilon} \subseteq \text{Step index} \times \text{Bi-expression}$

$$
\begin{array}{ll}
[\![(\tau)^{\mathbb{S}}]\!]^{\rho}_{v} & = \{(m, \boldsymbol{w}) \mid (m, \boldsymbol{w}) \in [\![\tau]\!]^{\rho}_{v} \wedge \mathtt{stable}(\boldsymbol{w})\} \\
[\![(\tau)^{\mathbb{C}}]\!]^{\rho}_{v} & = [\![\tau]\!]^{\rho}_{v} \\
[\![\mathtt{real}]\!]^{\rho}_{v} & = \{(m, \mathtt{keep}(\mathtt{r})) \mid \top\} \ \cup \ \{(m, \mathtt{repl}(\mathtt{r}, \mathtt{r}')) \mid \top\} \\
[\![\mathtt{list}\,[0]^{\alpha}\ \tau]\!]^{\rho}_{v} & = \{(m, \mathtt{nil}) \mid \top\} \\
[\![\mathtt{list}\,[n{+}1]^{\alpha}\,\tau]\!]^{\rho}_{v} & = \{(m, \mathtt{cons}(\boldsymbol{w}_1, \boldsymbol{w}_2)) \mid \\
 & \quad ((m, \boldsymbol{w}_1) \in [\![(\tau)^{\mathbb{S}}]\!]^{\rho}_{v} \wedge (m, \boldsymbol{w}_2) \in [\![\mathtt{list}\,[n]^{\alpha}\,\tau]\!]^{\rho}_{v}) \vee \\
 & \quad ((m, \boldsymbol{w}_1) \in [\![\tau]\!]^{\rho}_{v} \ \wedge \ (m, \boldsymbol{w}_2) \in [\![\mathtt{list}\,[n]^{\alpha-1}\ \tau]\!]^{\rho}_{v} \wedge \alpha > 0)\} \\
[\![\tau_1 \xrightarrow{\kappa} \tau_2]\!]^{\rho}_{v} & = \{(m, \mathtt{fix}\ f(x).\mathfrak{e}) \mid \ \forall j < m, \ \forall \boldsymbol{w}\ (j, \boldsymbol{w}) \in [\![\tau_1]\!]^{\rho}_{v} \\
 & \quad \Rightarrow (j, \mathfrak{e}[\mathtt{fix}\ f(x).\mathfrak{e}/f][\boldsymbol{w}/x]) \in [\![\tau_2]\!]^{\rho,\kappa}_{\varepsilon}\} \\
[\![\forall t :^{\kappa}: S.\ \tau]\!]^{\rho}_{v} & = \{(m, \Lambda.\mathfrak{e}) \mid \forall I. \ \vdash I :: S \ \ (m, \mathfrak{e}) \in [\![\tau[I/t]]\!]^{\rho,\kappa[I/t]}_{\varepsilon}\} \\
[\![\exists t{::}S.\ \tau]\!]^{\rho}_{v} & = \{(m, \mathtt{pack}\ \boldsymbol{w}) \mid \exists I. \vdash I :: S \ \wedge (m, \boldsymbol{w}) \in [\![\tau[I/t]]\!]^{\rho}_{v}\} \\
[\![\tau_1 \times \tau_2]\!]^{\rho}_{v} & = \{(m, (\boldsymbol{w}_1, \boldsymbol{w}_2)) \mid (m, \boldsymbol{w}_1) \in [\![\tau_1]\!]^{\rho}_{v} \wedge (m, \boldsymbol{w}_2) \in [\![\tau_2]\!]^{\rho}_{v}\} \\
[\![C \to \tau]\!]^{\rho}_{v} & = \{(m, \boldsymbol{w}) \mid \ \not\models C \ \vee \ (m, \boldsymbol{w}) \in \ [\![\tau]\!]^{\rho}_{v}\} \\
[\![C \wedge \tau]\!]^{\rho}_{v} & = \{(m, \boldsymbol{w}) \mid \ \models C \ \wedge \ (m, \boldsymbol{w}) \in \ [\![\tau]\!]^{\rho}_{v}\} \\
[\![\mathtt{unit}]\!]^{\rho}_{v} & = \{(m, ()) \mid \top\} \\
[\![X]\!]^{\rho}_{v} & = \rho(X) \\
[\![\forall X :^{\kappa}: K.\tau]\!]^{\rho}_{v} & = \{(m, \lambda\,\mathfrak{e}) \mid \forall R \in [\![K]\!]_K, \ (m, \mathfrak{e}) \in [\![\tau]\!]^{\kappa,(\rho, X \mapsto R)}_{\varepsilon}\} \\
[\![\lambda i :: S.\tau]\!]^{\rho}_{v} & = \lambda i :: S.\, [\![\tau]\!]^{\rho}_{v} \\
[\![\tau\ I]\!]^{\rho}_{v} & = [\![\tau]\!]^{\rho}_{v}\ I
\end{array}
$$

$$
\begin{array}{ll}
[\![\tau]\!]^{\rho,\kappa}_{\varepsilon} & = \{(m, \mathfrak{e}) \mid \forall j < m.\ \mathrm{L}(\mathfrak{e}) \Downarrow v, T \ \wedge \ j = |T| \\
 & \quad \Rightarrow \exists\ v', T', \boldsymbol{w}', c' \ \text{ such that} \\
 & \qquad 1.\ \langle T, \mathfrak{e}\rangle \curvearrowright \boldsymbol{w}', T', c' \\
 & \qquad 2.\ \mathrm{R}(\mathfrak{e}) \Downarrow v', T' \\
 & \qquad 3.\ v' = \mathrm{R}(\boldsymbol{w}') \ \wedge \ v = \mathrm{L}(\boldsymbol{w}') \\
 & \qquad 4.\ c' \leq \kappa \\
 & \qquad 5.\ (m - j, \boldsymbol{w}') \in [\![\tau]\!]^{\rho}_{v} \\
 & \quad \} \\
\mathcal{T}[\![\cdot]\!] & = \{\emptyset\} \\
\mathcal{T}[\![\Psi, X : K]\!] & = \{\rho, X \mapsto R \mid \rho \in \mathcal{T}[\![\Psi]\!] \wedge R \in [\![K]\!]_K\}
\end{array}
$$

$$
\begin{array}{ll}
\mathcal{D}[\![\cdot]\!] & = \{\emptyset\} \\
\mathcal{D}[\![\Delta, t :: S]\!] & = \{\sigma[t \mapsto I] \mid \sigma \in \mathcal{D}[\![\Delta]\!] \ \wedge \ \vdash I :: S\}
\end{array}
$$

$$
\begin{array}{ll}
\mathcal{G}[\![\cdot]\!]^{\rho} & = \{\emptyset\} \\
\mathcal{G}[\![\Gamma, x : \tau]\!]^{\rho} & = \{(m, \theta[x \mapsto \boldsymbol{w}]) \mid (m, \theta) \in \mathcal{G}[\![\Gamma]\!]^{\rho} \ \wedge (m, \boldsymbol{w}) \in \ [\![\tau]\!]^{\rho}_{v}\}
\end{array}
$$

Figure 23: Step-indexed interpretation of types

$$
\begin{aligned}
[\![\subseteq]\!]_{-} &: (S \times S \times \cdots \times S \to (\text{Step index} \times \text{Bi-value})) \\
[\![\subseteq]\!]_{*} &= \subseteq \\
[\![\subseteq]\!]_{S \to K} &= \{(R_1, R_2) \mid \forall \vdash I :: S,\ \ (R_1\ I, R_2\ I) \in [\![\subseteq]\!]_K\}
\end{aligned}
$$

Figure 24: Semantics of Subtyping

Theorems and Lemmas

We use some abbreviations throughout. STS stands for "suffices to show" or "it suffices to show". TS stands for "to show" or "remains to show".

We assume that the constraint judgment $\Delta; \Phi \models C$ satisfies some standard properties.

Assumption 6 (Constraint conditions)
The following hold.

1. [Subst1] If $\Delta, i :: S; \Phi \models C$ and $\Delta \vdash I :: S$, then $\Delta; \Phi[I/i] \models C[I/i]$.
2. [Subst2] If $\Delta; \Phi \models C$ and $\Delta; \Phi \wedge C \models C'$, then $\Delta; \Phi \models C'$.
3. [Neg] $\Delta; \Phi \models \neg C$ iff $\Delta; \Phi \not\models C$.
4. [Corr1] If $\models n_1 \leq n_2$, then $n_1 \leq n_2$.
5. [Corr2] If $\models I \doteq I'$, then $I = I'$.

Lemma 7 (Sort/Kind environment substitution)
The following hold.

1. If $\Delta \vdash I :: S$ and $\Delta, i :: S \vdash I' :: S'$, then $\Delta \vdash I'[I/i] :: S'$.
2. If $\Delta \vdash I :: S$ and $\Delta, i :: S \vdash C$ `wf`, then $\Delta \vdash C[I/i]$ `wf`.
3. If $\Delta \vdash I :: S$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$, then $\vdash \sigma I :: S$.
4. If $\Psi; \Delta \vdash \tau : K$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$, then $\Psi; \cdot \vdash \sigma\tau : K$

Proof. (1) and (2) are established by simultaneous induction on the second given derivations. (3) follows from (1). (4) is by induction on the kinding judgement. □

Lemma 8 (Downward closure for context Γ)
If $\Psi; \Delta; \Phi \vdash \Gamma$ `wf` and $\rho \in \mathcal{T}[\![\Psi]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $k \leq m$, then $(k, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$

Proof. Since $\Psi; \Delta; \Phi \vdash \Gamma$ `wf`, forall $x_i : \tau_i \in \Gamma$, we have $\vdash \sigma\tau_i : *$. By Lemma 9, $[\![\sigma\tau_i]\!]^\rho_v \in [\![*]\!]_K$(†). Since $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$, forall $(m, \theta(x_i)) \in [\![\sigma\tau_i]\!]^\rho_v$. By unrolling the statement (†) using $(m, \theta(x_i)) \in [\![\sigma\tau_i]\!]^\rho_v$ and $k \leq m$, we get $(k, \theta(x_i)) \in [\![\sigma\tau_i]\!]^\rho_v$. Therefore $(k, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$.

□

Lemma 9 (Kinding Soundness)
If $\Psi; \Delta \vdash \tau : K$ and $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$, then $[\![\sigma\tau]\!]^\rho_v \in [\![K]\!]_K$

Proof. By induction on the kinding judgment. We show some representative cases below.

Case $\dfrac{\Psi(X) = K}{\Psi; \Delta \vdash X : K}$ **k-Var**
TS: $[\![\sigma X]\!]^\rho_v \in [\![K]\!]_K$
STS: $\rho(X) \in [\![K]\!]_K$ which follows by the definition of $\rho \in \mathcal{T}[\![\Psi]\!]$ since $\Psi(X) = K$.

Case $\dfrac{\Psi; i :: S, \Delta \vdash \tau : K}{\Psi; \Delta \vdash \lambda i :: S.\tau : S{\to}K}$ **k-Lam**
TS: $[\![\lambda i :: S.\sigma\tau]\!]^\rho_v \in [\![S{\to}K]\!]_K$
STS: $[\![\lambda i :: S.\sigma\tau]\!]^\rho_v \in S{\to}[\![K]\!]_K$
By unrolling the definition of $[\![\cdot]\!]^\rho_v$, STS: $\lambda i :: S.[\![\sigma\tau]\!]^\rho_v \in S{\to}[\![K]\!]_K$
Assume that $\vdash I :: S(\star)$, then STS: $(\lambda i :: S.[\![\sigma\tau]\!]^\rho_v)\ I \in [\![K]\!]_K$
By IH using $(\star)$, we get $[\![\sigma[I/i]\tau]\!]^\rho_v \in [\![K]\!]_K$ which is semantically equivalent to $(\lambda i :: S.[\![\sigma\tau]\!]^\rho_v)\ I \in [\![K]\!]_K$.

Case $\dfrac{\Psi; \Delta \vdash \tau : S{\to}K \qquad \Delta \vdash I :: S}{\Psi; \Delta \vdash \tau\ I : K}$ **k-App**
TS: $[\![\sigma\tau\ \sigma I]\!]^\rho_v \in [\![K]\!]_K$.
STS: $[\![\sigma\tau]\!]^\rho_v\ \sigma I \in [\![K]\!]_K$.
By Assumption 6 on $\Delta \vdash I :: S$ using σ, we get $\vdash \sigma I :: S$.
By IH, we get $[\![\sigma\tau]\!]^\rho_v \in [\![S{\to}K]\!]_K = S{\to}[\![K]\!]_K$.
By semantic application with σI, we get $[\![\sigma\tau]\!]^\rho_v\ \sigma I \in [\![K]\!]_K$. □

Lemma 10 (Constraint Well-formedness)
If $\Psi; \Delta; \Phi \vdash \Gamma$ `wf` then $\Delta \vdash \Phi$ `wf`

Proof. By induction on constraint well-formedness judgement. □

Lemma 11 (Well-formedness)
If $\Psi; \Delta; \Phi; \Gamma \vdash e :_\kappa \tau$ then

1. $\Delta \vdash \Phi$ `wf`
2. $\Psi; \Delta; \Phi \vdash \Gamma$ `wf`
3. $\Psi; \Delta \vdash \tau : *$

Proof. The first statement follows from instantiating Lemma 10 on second statement.
Proof of the second and third statements are by induction on the typing derivation. □

Lemma 12 (No input change)
If $\mathrm{L}(\text{æ}) \Downarrow v, T$ and $\langle T, \text{æ}\rangle \curvearrowright w', T', c'$ and `stable`(æ) then `stable`(w') and $c' = 0$.

Proof. By induction on the given derivation of $\curvearrowright$. □

Lemma 13 (Bi-value propagation)
$\langle \mathrm{L}(w), w\rangle \curvearrowright w, \mathrm{R}(w), 0$.

Proof. By induction on w. We show some representative cases.

Case $w =$ `keep(r)`
$\mathrm{L}($`keep(r)`$) =$ `r`. Immediate from rule **r-keep**.

Case $w =$ `repl(r,r')`
$\mathrm{L}($`repl(r,r')`$) =$ `r` and $\mathrm{R}($`repl(r,r')`$) =$ `r'`. Immediate from rule **r-repl**.

Case $w =$ `0`
Immediate from rule **r-0**.

Case $w =$ `succ` w
By IH on w, $\langle \mathrm{L}(w), w\rangle \curvearrowright w, \mathrm{R}(w), 0$. Applying rule **r-succ** yields the desired result.

Case $w = \texttt{fix}\ f(x).\text{æ}$

Immediate from rule **r-fix**, noting that $\texttt{merge}(\mathrm{L}(\text{æ}), \mathrm{R}(\text{æ})) = \text{æ}$.

□

Lemma 14 (Value interpretation containment)
If $(m, w) \in [\![\tau]\!]^{\rho}_{v}$ then $(m, w) \in [\![\tau]\!]^{\rho,0}_{\varepsilon}$.

Proof. Following the definition of $[\![\tau]\!]^{\rho,0}_{\varepsilon}$, assume that $\mathrm{L}(w) \Downarrow v, T$ and $j = |T| < m$.
We have to show that there exist v', w', T', c' such that:

1. $\langle T, w\rangle \curvearrowright w', T', c'$
2. $\mathrm{R}(w') \Downarrow v', T'$
3. $v = \mathrm{L}(w') \ \wedge\ v' = \mathrm{R}(w')$
4. $c' = 0$
5. $(m - j, w') \in [\![\sigma\tau]\!]^{\rho}_{v}$

Since w is a bi-value, $\mathrm{L}(w)$ and $\mathrm{R}(w)$ are values and, hence, $\mathrm{L}(w) \Downarrow \mathrm{L}(w), \mathrm{L}(w)$ and $\mathrm{R}(w) \Downarrow \mathrm{R}(w), \mathrm{R}(w)$. This forces $v = \mathrm{L}(w)$, $v' = \mathrm{R}(w)$, $T = \mathrm{L}(w)$, $T' = \mathrm{R}(w)$ and $j = 0$. We choose $w' = w$. This trivially yields (2), (3) and (5). Next, from Lemma 13, $\langle \mathrm{L}(w), w\rangle \curvearrowright w, \mathrm{R}(w), 0$. This yields (1) and (4).

□

Lemma 15 (Characterization of $\mathbb{C}$ for bi-expressions)
If $(m, \text{æ}) \in [\![\tau]\!]^{\rho,\kappa}_{\varepsilon}$ then $(m, \text{æ}) \in [\![(\tau)^{\mathbb{C}}]\!]^{\rho,\kappa}_{\varepsilon}$.

Proof. We unroll the definitions of $[\![\tau]\!]^{\rho,\kappa}_{\varepsilon}$ and $[\![(\tau)^{\mathbb{C}}]\!]^{\rho,\kappa}_{\varepsilon}$. (1)–(4) in the latter follow from (1)–(4) in the former. (5) in the latter follows from (5) in the former and the definition $[\![(\tau)^{\mathbb{C}}]\!]^{\rho}_{v} = [\![\tau]\!]^{\rho}_{v}$. □

Lemma 16 (Characterization of $\mathbb{S}$ for bi-expressions)
If $(m, \text{æ}) \in [\![\tau]\!]^{\rho,\kappa}_{\varepsilon}$ and $\texttt{stable}(\text{æ})$ then $(m, \text{æ}) \in [\![(\tau)^{\mathbb{S}}]\!]^{\rho,\kappa}_{\varepsilon}$.

Proof. Assume $(m, \text{æ}) \in [\![\tau]\!]^{\rho,\kappa}_{\varepsilon}$ and $\texttt{stable}(\text{æ})$. Following the definition of $(m, \text{æ}) \in [\![(\tau)^{\mathbb{S}}]\!]^{\rho,\kappa}_{\varepsilon}$, assume that $\mathrm{L}(\text{æ}) \Downarrow v, T$ and $j = |T| < m$. We must show that there exist v', T', w', c' such that:

1. $\langle T, \text{æ}\rangle \curvearrowright w', T', c'$
2. $\mathrm{R}(\text{æ}) \Downarrow v', T'$
3. $v = \mathrm{L}(w') \ \wedge\ v' = \mathrm{R}(w')$
4. $c' \leq \kappa$
5. $(m - j, w') \in [\![(\tau)^{\mathbb{S}}]\!]^{\rho}_{v}$

To prove these, we unroll the definition of $(m, \text{æ}) \in [\![\tau]\!]^{\rho,\kappa}_{\varepsilon}$. (1)–(4) above follow from (1)–(4) in that definition. (5) in that definition yields $(m - j, w') \in [\![\tau]\!]^{\rho}_{v}$. Thus, to prove (5) above, we only need to show that $\texttt{stable}(w')$. That follows from Lemma 12 applied to (1) above and the assumption $\texttt{stable}(\text{æ})$. □

Lemma 17 (Bi-value subtyping soundness)
If $\Psi;\Delta;\Phi \models \tau \sqsubseteq \tau' : K$ and $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$, then $[\![\sigma\tau]\!]^\rho_v$ and $[\![\sigma\tau']\!]^\rho_v$ exist such that $([\![\sigma\tau]\!]^\rho_v, [\![\sigma\tau']\!]^\rho_v) \in [\![\sqsubseteq]\!]_K$.

Proof. By instantiating the Lemma 18, we get $\Psi;\Delta \vdash \tau : K$ and $\Psi;\Delta \vdash \tau' : K$. Then, by instantiating Lemma 9, we get $[\![\sigma\tau]\!]^\rho_v \in [\![K]\!]_K$ and $[\![\sigma\tau']\!]^\rho_v \in [\![K]\!]_K$ i.e. $[\![\sigma\tau]\!]^\rho_v$ and $[\![\sigma\tau']\!]^\rho_v$ exist.
We show that $([\![\sigma\tau]\!]^\rho_v, [\![\sigma\tau']\!]^\rho_v) \in [\![\sqsubseteq]\!]_K$ by induction on the given subtyping derivation.
For the cases where $K = *$, by unrolling the definition of $[\![\sqsubseteq]\!]_*$, we need to show that $[\![\sigma\tau]\!]^\rho_v \subseteq [\![\sigma\tau']\!]^\rho_v$. Hence in these cases, by unfolding the mathematical definition of subset relation, we assume that $(m, w) \in [\![\sigma\tau]\!]^\rho_v$, and show that $(m, w) \in [\![\sigma\tau']\!]^\rho_v$. □

Case $\dfrac{\Psi;\Delta \vdash \tau_1 : * \qquad \Psi;\Delta \vdash \tau_2 : * \qquad \Delta \vdash \mu :: \mathbb{V} \qquad \Delta \vdash \kappa :: \mathbb{R}}{\Psi;\Delta;\Phi \models (\tau_1 \xrightarrow{\kappa} \tau_2)^\mu \sqsubseteq (\tau_1)^\mu \xrightarrow{\kappa} (\tau_2)^\mu : *} \to \mathbf{1}$

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $\models \sigma\Phi$ and $(m, w) \in [\![(\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2)^{\sigma\mu}]\!]^\rho_v$.
TS: $(m, w) \in [\![(\sigma\tau_1)^{\sigma\mu} \xrightarrow{\sigma\kappa} (\sigma\tau_2)^{\sigma\mu}]\!]^\rho_v$.
By definition, $w = \texttt{fix}\ f(x).æ$.
There are two possible cases for $\sigma\mu$.

subcase 1: $\sigma\mu = \mathbb{S}$
We know that $(m, w) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^\rho_v$ ($\diamond$) and $\texttt{stable}(w) = \texttt{stable}(\texttt{fix}\ f(x).æ)$, that is $\texttt{stable}(æ)$ (†).
TS: $(m, w) \in [\![(\sigma\tau_1)^{\mathbb{S}} \xrightarrow{\sigma\kappa} (\sigma\tau_2)^{\mathbb{S}}]\!]^\rho_v$.
Assume that $j < m$ and $(j, w') \in [\![(\sigma\tau_1)^{\mathbb{S}}]\!]^\rho_v$, i.e., $(j, w') \in [\![\sigma\tau_1]\!]^\rho_v$ and $\texttt{stable}(w')$ ($\diamond\diamond$).
STS: $(j, æ[w/f, w'/x]) \in [\![(\sigma\tau_2)^{\mathbb{S}}]\!]^{\rho,\sigma\kappa}_\varepsilon$
By Lemma 16, STS: $\texttt{stable}(æ[w/f, w'/x])$ and $(j, æ[w/f, w'/x]) \in [\![\sigma\tau_2]\!]^{\rho,\sigma\kappa}_\varepsilon$.
The requirement $\texttt{stable}(æ[w/f, w'/x])$ follows from the assumptions marked (†) and ($\diamond\diamond$).
The requirement $(j, æ[w/f, w'/x]) \in [\![\sigma\tau_2]\!]^{\rho,\sigma\kappa}_\varepsilon$ follows by unrolling assumption ($\diamond$) with $(j, w') \in [\![\sigma\tau_1]\!]^\rho_v$.

subcase 2: $\sigma\mu = \mathbb{C}$
We know that $(m, w) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^\rho_v$ ($\diamond$).
TS: $(m, w) \in [\![(\sigma\tau_1)^{\mathbb{C}} \xrightarrow{\sigma\kappa} (\sigma\tau_2)^{\mathbb{C}}]\!]^\rho_v$.
Assume that $j < m$ and $(j, w') \in [\![(\sigma\tau_1)^{\mathbb{C}}]\!]^\rho_v$, i.e., $(j, w') \in [\![\sigma\tau_1]\!]^\rho_v$.
STS: $(j, æ[w/f, w'/x]) \in [\![(\sigma\tau_2)^{\mathbb{C}}]\!]^{\rho,\sigma\kappa}_\varepsilon$
By Lemma 15, it STS $(j, æ[w/f, w'/x]) \in [\![\sigma\tau_2]\!]^{\rho,\sigma\kappa}_\varepsilon$, which follows by unrolling ($\diamond$) with $(j, w') \in [\![\sigma\tau_1]\!]^\rho_v$.

Case $\dfrac{\Psi;\Delta;\Phi \models \tau_1' \sqsubseteq \tau_1 : * \qquad \Delta;\Phi \models \tau_2 \sqsubseteq \tau_2' : * \qquad \Delta;\Phi \models \kappa \le \kappa'}{\Psi;\Delta;\Phi \models \tau_1 \xrightarrow{\kappa} \tau_2 \sqsubseteq \tau_1' \xrightarrow{\kappa'} \tau_2' : *} \to \mathbf{2}$

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, w) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^\rho_v$ ($\star$) and $\models \sigma\Phi$.
TS: $(m, w) \in [\![\sigma\tau_1' \xrightarrow{\sigma\kappa'} \sigma\tau_2']\!]^\rho_v$.
By definition, $w = \texttt{fix}\ f(x).æ$.
Assume $j < m$ and $(j, w') \in [\![\sigma\tau_1']\!]^\rho_v$.
STS: $(j, æ[w/f, w'/x]) \in [\![\sigma\tau_2']\!]^{\rho,\sigma\kappa'}_\varepsilon$.
Following the definition of $[\![\cdot]\!]^{\rho,\cdot}_\varepsilon$, suppose that $\mathrm{L}(æ[w/f, w'/x]) \Downarrow v, T$ ($\star\star$) and $j = |T| < m$. Our goal is to show (1)–(5) in the definition of $[\![\cdot]\!]^{\rho,\cdot}_\varepsilon$ below.
By IH on $\Psi;\Delta;\Phi \models \tau_1' \sqsubseteq \tau_1 : *$, using the assumption $(j, w) \in [\![\sigma\tau_1']\!]^\rho_v$, we get

$(j, w) \in [\![\sigma\tau_1]\!]^\rho_v$.
Unrolling the definition of the assumption ($\star$) with $(j, w) \in [\![\sigma\tau_1]\!]^\rho_v$, we get
$(j, @[w/f, w'/x]) \in [\![\sigma\tau_2]\!]^{\rho,\sigma\kappa}_\varepsilon$.
Unrolling the definition of $[\![\sigma\tau_2]\!]^{\rho,\sigma\kappa}_\varepsilon$ with ($\star\star$), we get

a) $\langle T, @[w/f, w'/x]\rangle \curvearrowright w'', T', c'$
b) $\mathrm{R}(@[w/f, w'/x]) \Downarrow v', T'$
c) $v = \mathrm{L}(w'') \ \wedge \ v' = \mathrm{R}(w'')$
d) $c' \leq \sigma\kappa$
e) $(m - j, w'') \in [\![\sigma\tau_2]\!]^\rho_v$

Then,

1. follows immediately from a)
2. follows immediately from b)
3. follows immediately from c)
4. $c' \leq \sigma\kappa'$ follows from Assumption 6 applied to $\Psi; \Delta; \Phi \models \kappa \leq \kappa'$ and d)
5. $(m - j, w'') \in [\![\sigma\tau_2']\!]^\rho_v$ by instantiating the IH on $\Delta; \Phi \models \tau_2 \sqsubseteq \tau_2' : *$ and e).

Case $\dfrac{\Psi; \Delta \vdash \tau_1 : * \qquad \Psi; \Delta \vdash \tau_2 : * \qquad \Delta \vdash \mu :: \mathbb{V}}{\Psi; \Delta; \Phi \models (\tau_1 \times \tau_2)^\mu \equiv (\tau_1)^\mu \times (\tau_2)^\mu : *} \times$ **1**

Here we only show the proof of $(\tau_1 \times \tau_2)^\mu \sqsubseteq (\tau_1)^\mu \times (\tau_2)^\mu : *$; the converse is similar.
Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, w) \in [\![(\sigma\tau_1 \times \sigma\tau_2)^{\sigma\mu}]\!]^\rho_v$ ($\star$) and $\models \sigma\Phi$.
TS: $(m, w) \in [\![(\sigma\tau_1)^{\sigma\mu} \times (\sigma\tau_2)^{\sigma\mu}]\!]^\rho_v$.
By definition of $[\![\cdot]\!]^\rho_v$, $w = (w_1, w_2)$.
STS: $(m, w_1) \in [\![(\sigma\tau_1)^{\sigma\mu}]\!]^\rho_v$ and $(m, w_2) \in [\![(\sigma\tau_2)^{\sigma\mu}]\!]^\rho_v$
There are two possible cases for $\sigma\mu$.

subcase 1: $\sigma\mu = \mathbb{S}$
By assumption ($\star$) we get, $\mathtt{stable}((w_1, w_2))$ and $(m, (w_1, w_2)) \in [\![\sigma\tau_1 \times \sigma\tau_2]\!]^\rho_v$.
Following the definition, we have $(m, w_1) \in [\![\sigma\tau_1]\!]^\rho_v$ ($\diamond$) and $(m, w_2) \in [\![\sigma\tau_2]\!]^\rho_v$ ($\diamond\diamond$).
Since $\mathtt{stable}((w_1, w_2))$, we also have that $\mathtt{stable}(w_1)$ and $\mathtt{stable}(w_2)$.
Combining these with ($\diamond$) and ($\diamond\diamond$), we get $(m, w_1) \in [\![(\sigma\tau_1)^{\mathbb{S}}]\!]^\rho_v$ and $(m, w_2) \in [\![(\sigma\tau_2)^{\mathbb{S}}]\!]^\rho_v$, as needed.

subcase 2: $\sigma\mu = \mathbb{C}$
From assumption ($\star$), we have $(m, w_1) \in [\![\sigma\tau_1]\!]^\rho_v$ and $(m, w_2) \in [\![\sigma\tau_2]\!]^\rho_v$, which are equivalent to $(m, w_1) \in [\![(\sigma\tau_1)^{\mathbb{C}}]\!]^\rho_v$ and $(m, w_2) \in [\![(\sigma\tau_2)^{\mathbb{C}}]\!]^\rho_v$, as needed.

Case $\dfrac{\Psi; \Delta \vdash \tau : * \qquad \Delta \vdash \mu :: \mathbb{V} \qquad \Delta \vdash n :: \mathbb{N} \qquad \Delta \vdash \alpha :: \mathbb{N}}{\Psi; \Delta; \Phi \models (\mathtt{list}\,[n]^\alpha\ \tau)^\mu \equiv \mathtt{list}\,[n]^\alpha\ (\tau)^\mu : *}$ **l1**

Here we only show only that $(\mathtt{list}\,[n]^\alpha\ \tau)^\mu \sqsubseteq \mathtt{list}\,[n]^\alpha\ (\tau)^\mu : *$; the converse is similar.
Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, w) \in [\![(\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau)^{\sigma\mu}]\!]^\rho_v$ and $\models \sigma\Phi$. We have to prove $(m, w) \in [\![\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ (\sigma\tau)^{\sigma\mu}]\!]^\rho_v$.
We prove the following more general statement by subinduction on w':
For all w', if $(m, w') \in [\![(\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau)^{\sigma\mu}]\!]^\rho_v$ ($\star$) then $(m, w') \in [\![\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ (\sigma\tau)^{\sigma\mu}]\!]^\rho_v$.

subcase 1: $w' = \mathtt{nil}$
From the assumption marked ($\star$), we get $(m, \mathtt{nil}) \in [\![(\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau)^{\sigma\mu}]\!]^\rho_v$.
Therefore, we have $\sigma n = 0$, and $(m, \mathtt{nil}) \in [\![\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ (\sigma\tau)^{\sigma\mu}]\!]^\rho_v$ by definition.

subcase 2: $w' = \mathtt{cons}(w_1, w_2)$

From the assumption marked ($\star$), we get $(m, \mathtt{cons}(w_1, w_2)) \in [\![(\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau)^{\sigma\mu}]\!]^\rho_v$.
Therefore, $\exists I.\ \sigma n = I + 1$.
We case analyze $\sigma\mu$:

case 1: $\sigma\mu = \mathbb{S}$

Then, we have $\mathtt{stable}(\mathtt{cons}(w_1, w_2))$ and $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[I+1]^{\sigma\alpha}\ \sigma\tau]\!]^\rho_v$.
TS: $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[I+1]^{\sigma\alpha}\ (\sigma\tau)^{\mathbb{S}}]\!]^\rho_v$.
We have two possible cases:

- $(m, w_1) \in [\![(\sigma\tau)^{\mathbb{S}}]\!]^\rho_v$ ($\dagger$) and $(m, w_2) \in [\![\mathtt{list}\,[I]^{\sigma\alpha}\ \sigma\tau]\!]^\rho_v$ ($\dagger\dagger$).
  From ($\dagger\dagger$) and $\mathtt{stable}(\mathtt{cons}(w_1, w_2))$, we get that $(m, w_2) \in [\![(\mathtt{list}\,[I]^{\sigma\alpha}\ \sigma\tau)^{\mathbb{S}}]\!]^\rho_v$.
  By the sub-IH, $(m, w_2) \in [\![\mathtt{list}\,[I]^{\sigma\alpha}\ (\sigma\tau)^{\mathbb{S}}]\!]^\rho_v$.
  From ($\dagger$), we get $(m, w_1) \in [\![((\sigma\tau)^{\mathbb{S}})^{\mathbb{S}}]\!]^\rho_v$.
  Combining the last two statements, we get $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[I+1]^{\sigma\alpha}\ (\sigma\tau)^{\mathbb{S}}]\!]^\rho_v$.
- $(m, w_1) \in [\![\sigma\tau]\!]^\rho_v$ ($\diamond$) and $(m, w_2) \in [\![\mathtt{list}\,[I]^{\sigma\alpha-1}\ \sigma\tau]\!]^\rho_v$ ($\diamond\diamond$).
  From ($\diamond\diamond$) and $\mathtt{stable}(\mathtt{cons}(w_1, w_2))$, we get $(m, w_2) \in [\![(\mathtt{list}\,[I]^{\sigma\alpha-1}\ \sigma\tau)^{\mathbb{S}}]\!]^\rho_v$.
  By the sub-IH, $(m, w_2) \in [\![\mathtt{list}\,[I]^{\sigma\alpha-1}\ (\sigma\tau)^{\mathbb{S}}]\!]^\rho_v$.
  From ($\diamond$) and $\mathtt{stable}(\mathtt{cons}(w_1, w_2))$, we get $(m, w_1) \in [\![(\sigma\tau)^{\mathbb{S}}]\!]^\rho_v$.
  Combining the last two statements, we get $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[I+1]^{\sigma\alpha}\ (\sigma\tau)^{\mathbb{S}}]\!]^\rho_v$.

case 2: $\sigma\mu = \mathbb{C}$

Then, we have $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[I+1]^{\sigma\alpha}\ \sigma\tau]\!]^\rho_v$.
TS: $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[I+1]^{\sigma\alpha}\ (\sigma\tau)^{\mathbb{C}}]\!]^\rho_v$.
We have two possible cases:

- $(m, w_1) \in [\![(\sigma\tau)^{\mathbb{S}}]\!]^\rho_v$ ($\dagger$) and $(m, w_2) \in [\![\mathtt{list}\,[I]^{\sigma\alpha}\ \sigma\tau]\!]^\rho_v = [\![(\mathtt{list}\,[I]^{\sigma\alpha}\ \sigma\tau)^{\mathbb{C}}]\!]^\rho_v$ ($\dagger\dagger$).
  By the sub-IH on ($\dagger\dagger$), we get $(m, w_2) \in [\![\mathtt{list}\,[I]^{\sigma\alpha}\ (\sigma\tau)^{\mathbb{C}}]\!]^\rho_v$.
  From the assumption ($\dagger$), we can trivially show that $(m, w_1) \in [\![((\sigma\tau)^{\mathbb{C}})^{\mathbb{S}}]\!]^\rho_v$.
  Combining the last two statements yields $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[I+1]^{\sigma\alpha}\ (\sigma\tau)^{\mathbb{C}}]\!]^\rho_v$.
- $(m, w_1) \in [\![\sigma\tau]\!]^\rho_v$ ($\diamond$) and $(m, w_2) \in [\![\mathtt{list}\,[I]^{\sigma\alpha-1}\ \sigma\tau]\!]^\rho_v = [\![(\mathtt{list}\,[I]^{\sigma\alpha-1}\ \sigma\tau)^{\mathbb{C}}]\!]^\rho_v$ ($\diamond\diamond$).
  By the sub-IH on ($\diamond\diamond$), we get that $(m, w_2) \in [\![\mathtt{list}\,[I]^{\sigma\alpha-1}\ (\sigma\tau)^{\mathbb{C}}]\!]^\rho_v$.
  From ($\diamond$), we get $(m, w_1) \in [\![(\sigma\tau)^{\mathbb{C}}]\!]^\rho_v$.
  Combining the last two statements, we get that $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[I+1]^{\sigma\alpha}\ (\sigma\tau)^{\mathbb{C}}]\!]^\rho_v$.

Case $\dfrac{\Psi; \Delta \vdash \tau : *\qquad \Delta \vdash n :: \mathbb{N}\qquad \Delta \vdash \alpha :: \mathbb{N}\qquad \Delta; \Phi \models \mu \doteq \mathbb{S}}{\Psi; \Delta; \Phi \models (\mathtt{list}\,[n]^{\alpha}\ \tau)^{\mu} \equiv \mathtt{list}\,[n]^{0}\ \tau : *}\mathbf{l2}$

Here we show only that $(\mathtt{list}\,[n]^{\alpha}\ \tau)^{\mu} \sqsubseteq \mathtt{list}\,[n]^{0}\ \tau : *$; the converse is similar.
Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, w) \in [\![(\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau)^{\sigma\mu}]\!]^\rho_v$ and $\models \sigma\Phi$.
TS: $(m, w) \in [\![\mathtt{list}\,[\sigma n]^{0}\ \sigma\tau]\!]^\rho_v$.
We case analyze $\sigma\mu$:

subcase 1: $\sigma\mu = \mathbb{S}$

We have $(m, w) \in [\![(\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau)^{\mathbb{S}}]\!]^\rho_v$.
Following the definition, we have $\mathtt{stable}(w)$ and $(m, w) \in [\![\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau]\!]^\rho_v$.
We prove the following more general statement by subinduction on w':
For all w', if $(m, w') \in [\![(\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau)^{\mathbb{S}}]\!]^\rho_v$ ($\star$), then $(m, w') \in [\![\mathtt{list}\,[\sigma n]^{0}\ \sigma\tau]\!]^\rho_v$.

case: $w' = \mathtt{nil}$

From the assumption ($\star$), we get $(m, \mathtt{nil}) \in [\![(\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau)^{\mathbb{S}}]\!]^\rho_v$. Therefore, $\sigma n = 0$. The conclusion $(m, \mathtt{nil}) \in [\![\mathtt{list}\,[\sigma n]^{0}\ \sigma\tau]\!]^\rho_v$ follows by definition.

case: $w' = \mathtt{cons}(w_1, w_2)$

From $(\star)$, we have $\mathtt{stable}(\mathtt{cons}(w_1, w_2))$ and $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau]\!]^\rho_v$.
Therefore, $\exists I.\ \sigma n = I + 1$.
TS: $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[I+1]^0\ \sigma\tau]\!]^\rho_v$.
There are two possible cases for $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[I+1]^{\sigma\alpha}\ \sigma\tau]\!]^\rho_v$:

- $(m, w_1) \in [\![(\sigma\tau)^{\mathbb{S}}]\!]^\rho_v$ $(\dagger)$ and $(m, w_2) \in [\![\mathtt{list}\,[I]^{\sigma\alpha}\ \sigma\tau]\!]^\rho_v$ $(\dagger\dagger)$.
  From $(\dagger\dagger)$ and $\mathtt{stable}(\mathtt{cons}(w_1, w_2))$, we get $(m, w_2) \in [\![(\mathtt{list}\,[I]^{\sigma\alpha}\ \sigma\tau)^{\mathbb{S}}]\!]^\rho_v$.
  By the sub-IH, $(m, w_2) \in [\![\mathtt{list}\,[I]^0\ \sigma\tau]\!]^\rho_v$.
  Combining with $(\dagger)$, we get $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[I+1]^0\ \sigma\tau]\!]^\rho_v$.
- $(m, w_1) \in [\![\sigma\tau]\!]^\rho_v$ $(\diamond)$ and $(m, w_2) \in [\![\mathtt{list}\,[I]^{\sigma\alpha-1}\ \sigma\tau]\!]^\rho_v$ $(\diamond\diamond)$.
  From $(\diamond\diamond)$ and $\mathtt{stable}(\mathtt{cons}(w_1, w_2))$, $(m, w_2) \in [\![(\mathtt{list}\,[I]^{\sigma\alpha-1}\ \sigma\tau)^{\mathbb{S}}]\!]^\rho_v$. By the sub-IH, $(m, w_2) \in [\![\mathtt{list}\,[I]^0\ \sigma\tau]\!]^\rho_v$.
  From $(\diamond)$ and $\mathtt{stable}(\mathtt{cons}(w_1, w_2))$, we get $(m, w_1) \in [\![(\sigma\tau)^{\mathbb{S}}]\!]^\rho_v$.
  Combining the last two statements, we get $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[I+1]^0\ \sigma\tau]\!]^\rho_v$.

subcase 2: $\sigma\mu = \mathbb{C}$

From Assumption 6 applied to $\Psi; \Delta; \Phi \models \mu \doteq \mathbb{S}$, we get $\sigma\mu = \mathbb{S}$ which contradicts the case assumption.

Case $\dfrac{\Delta; \Phi \models n \doteq n' \qquad \Delta; \Phi \models \alpha \leq \alpha' \qquad \Psi; \Delta; \Phi \models \tau \sqsubseteq \tau' : *}{\Psi; \Delta; \Phi \models \mathtt{list}\,[n]^\alpha\ \tau \sqsubseteq \mathtt{list}\,[n']^{\alpha'}\ \tau' : *}\mathbf{l4}$

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, w) \in [\![\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau]\!]^\rho_v$ and $\models \sigma\Phi$.
TS: $(m, w) \in [\![\mathtt{list}\,[\sigma n']^{\sigma\alpha'}\ \sigma\tau']\!]^\rho_v$.
From Assumption 6 applied to the first premise, $\sigma n = \sigma n'$. Therefore,
STS: $(m, w) \in [\![\mathtt{list}\,[\sigma n]^{\sigma\alpha'}\ \sigma\tau']\!]^\rho_v$.
From Assumption 6 applied to the second premise, we get: $\sigma\alpha \leq \sigma\alpha'$. Therefore, it suffices to prove the following more general statement.
For all w', l, β, β', if $\beta \leq \beta'$ and $(m, w') \in [\![\mathtt{list}\,[l]^\beta\ \sigma\tau]\!]^\rho_v$, then $(m, w') \in [\![\mathtt{list}\,[l]^{\beta'}\ \sigma\tau']\!]^\rho_v$.
We establish this statement by subinduction on w'.

subcase 1: $w' = \mathtt{nil}$

The assumption $(m, w') \in [\![\mathtt{list}\,[l]^\beta\ \sigma\tau]\!]^\rho_v$ forces $l = 0$. Hence, $(m, w') \in [\![\mathtt{list}\,[l]^{\beta'}\ \sigma\tau']\!]^\rho_v$ follows immediately by definition.

subcase 2: $w' = \mathtt{cons}(w_1, w_2)$

By assumption, $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[l]^\beta\ \sigma\tau]\!]^\rho_v$. Therefore, $l = l' + 1$ for some l'.
TS: $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[l'+1]^{\beta'}\ \sigma\tau']\!]^\rho_v$.
There are two possible cases for $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[l]^\beta\ \sigma\tau]\!]^\rho_v$.

- $(m, w_1) \in [\![(\sigma\tau)^{\mathbb{S}}]\!]^\rho_v$ $(\dagger)$ and $(m, w_2) \in [\![\mathtt{list}\,[l']^\beta\ \sigma\tau]\!]^\rho_v$ $(\dagger\dagger)$.
  By IH on $\Psi; \Delta; \Phi \models \tau \sqsubseteq \tau' : *$ with $(\dagger)$, we get $(m, w_1) \in [\![(\sigma\tau')^{\mathbb{S}}]\!]^\rho_v$.
  By the sub-IH on $(\dagger\dagger)$, we get $(m, w_2) \in [\![\mathtt{list}\,[l']^{\beta'}\ \sigma\tau']\!]^\rho_v$.
  Combining, we get $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[l'+1]^{\beta'}\ \sigma\tau']\!]^\rho_v$.
- $(m, w_1) \in [\![\sigma\tau]\!]^\rho_v$ $(\diamond)$ and $(m, w_2) \in [\![\mathtt{list}\,[l']^{\beta-1}\ \sigma\tau]\!]^\rho_v$ $(\diamond\diamond)$.
  By IH on $\Psi; \Delta; \Phi \models \tau \sqsubseteq \tau' : *$ with $(\diamond)$, we get $(m, w_1) \in [\![\sigma\tau']\!]^\rho_v$
  By the sub-IH on $(\diamond\diamond)$, we get $(m, w_2) \in [\![\mathtt{list}\,[l']^{\beta'-1}\ \sigma\tau']\!]^\rho_v$.
  Combining these two yields $(m, \mathtt{cons}(w_1, w_2)) \in [\![\mathtt{list}\,[l'+1]^{\beta'}\ \sigma\tau']\!]^\rho_v$.

Case $\dfrac{\Psi; \Delta \vdash \tau : * \qquad \Delta \vdash \mu :: \mathbb{V} \qquad \Delta \vdash \kappa :: \mathbb{R}}{\Psi; \Delta; \Phi \models (\forall t \overset{\kappa}{::} S.\ \tau)^\mu \equiv \forall t \overset{\kappa}{::} S.\ (\tau)^\mu : *}\forall\mathbf{2}$

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, w) \in [\![(\forall t \overset{\sigma\kappa}{::} S.\ \sigma\tau)^{\sigma\mu}]\!]^\rho_v$ $(\star)$ and $\models \sigma\Phi$.

TS: $(m, w) \in [\![\forall t \overset{\sigma\kappa}{::} S.\ (\sigma\tau)^{\sigma\mu}]\!]^{\rho}_{v}$.
From ($\star$), $w = \Lambda.æ$.
Assume that $\vdash I :: S$.
STS: $(m, æ) \in [\![(\sigma\tau)^{\sigma\mu}\{I/t\}]\!]^{\rho,\sigma\kappa\{I/t\}}_{\varepsilon}$.
We case analyze $\sigma\mu$:

- $\sigma\mu = \mathbb{S}$
  Then we have $\texttt{stable}(\Lambda.æ)$ and $(m, \Lambda.æ) \in [\![\forall t \overset{\sigma\kappa}{::} S.\ \sigma\tau]\!]^{\rho}_{v}$.
  Unrolling the definition of $[\![\cdot]\!]^{\rho}_{v}$ with the assumption $\vdash I :: S$, we get $(m, æ) \in [\![\sigma\tau\{I/t\}]\!]^{\rho,\sigma\kappa\{I/t\}}_{\varepsilon}$.
  Instantiating Lemma 16 using $\texttt{stable}(æ)$, we get $(m, æ) \in [\![(\sigma\tau\{I/t\})^{\mathbb{S}}]\!]^{\rho,\sigma\kappa\{I/t\}}_{\varepsilon}$ or, equivalently, $(m, æ) \in [\![(\sigma\tau)^{\mathbb{S}}\{I/t\}]\!]^{\rho,\sigma\kappa\{I/t\}}_{\varepsilon}$.
- $\sigma\mu = \mathbb{C}$
  Then, we have $(m, \Lambda.æ) \in [\![\forall t \overset{\sigma\kappa}{::} S.\ \sigma\tau]\!]^{\rho}_{v}$.
  Unrolling the definition of $[\![\cdot]\!]^{\rho}_{v}$ with the assumption $\vdash I :: S$, we get $(m, æ) \in [\![\sigma\tau\{I/t\}]\!]^{\rho,\sigma\kappa\{I/t\}}_{\varepsilon}$.
  Hence by instantiating Lemma 15, we get $(m, æ) \in [\![(\sigma\tau\{I/t\})^{\mathbb{C}}]\!]^{\rho,\sigma\kappa\{I/t\}}_{\varepsilon}$ or, equivalently, $(m, æ) \in [\![(\sigma\tau)^{\mathbb{C}}\{I/t\}]\!]^{\rho,\sigma\kappa\{I/t\}}_{\varepsilon}$.

Case $\dfrac{\Psi; \Delta \vdash \tau : *\qquad \Delta \vdash \mu :: \mathbb{V}}{\Psi; \Delta; \Phi \models (\tau)^{\mu} \sqsubseteq \tau : *}\mathbf{T}$
Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $\models \sigma\Phi$.
TS: $([\![(\sigma\tau)^{\sigma\mu}]\!]^{\rho}_{v}, [\![\sigma\tau]\!]^{\rho}_{v}) \in [\![\subseteq]\!]_{*}$.
STS: $[\![(\sigma\tau)^{\sigma\mu}]\!]^{\rho}_{v} \subseteq [\![\sigma\tau]\!]^{\rho}_{v}$.
This follows by definition of $[\![\cdot]\!]^{\rho}_{v}$ both when $\sigma\mu = \mathbb{S}$ and when $\sigma\mu = \mathbb{C}$.

Case $\dfrac{\Psi; \Delta \vdash \tau : *}{\Psi; \Delta; \Phi \models \tau \sqsubseteq (\tau)^{\mathbb{C}} : *}\mathbf{I*}$
Immediate from the definition $[\![(\sigma\tau)^{\mathbb{C}}]\!]^{\rho}_{v} = [\![\sigma\tau]\!]^{\rho}_{v}$.

Case $\dfrac{\Psi; \Delta \vdash \tau : *\qquad \Delta \vdash I :: S}{\Psi; \Delta; \Phi \models (\lambda i :: S.\tau)\ I \equiv \tau[I/i] : K}\mathbf{ty\text{-}subst}$
Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $\models \sigma\Phi$.
TS: $([\![(\lambda i :: S.\sigma\tau)\ \sigma I]\!]^{\rho}_{v}, [\![\sigma\tau[\sigma I/i]]\!]^{\rho}_{v}) \in [\![\equiv]\!]_{K}$
By unrolling the definition of $[\![\cdot]\!]^{\rho}_{v}$, STS: $([\![(\lambda i :: S.\sigma\tau)]\!]^{\rho}_{v}\ \sigma I, [\![\sigma\tau[\sigma I/i]]\!]^{\rho}_{v}) \in [\![\equiv]\!]_{K}$
By semantic equivalence, this holds since $i \notin FTV(\rho)$.

Case $\dfrac{\Psi; i :: S, \Delta; \Phi \models \tau \sqsubseteq \tau' : K}{\Psi; \Delta; \Phi \models \lambda i :: S.\tau \sqsubseteq \lambda i :: S.\tau' : S{\to}K}\lambda\mathbf{\text{-}1}$
Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $\models \sigma\Phi$.
TS: $([\![\lambda i :: S.\sigma\tau]\!]^{\rho}_{v}, [\![\lambda i :: S.\sigma\tau']\!]^{\rho}_{v}) \in [\![\subseteq]\!]_{S\to K}$
By unrolling the definition of $[\![\cdot]\!]^{\rho}_{v}$, STS: $(\lambda i :: S.[\![\sigma\tau]\!]^{\rho}_{v}, \lambda i :: S.[\![\sigma\tau']\!]^{\rho}_{v}) \in [\![\subseteq]\!]_{S\to K}$
Suppose $\vdash I :: S$, then STS: $((\lambda i :: S.[\![\sigma\tau]\!]^{\rho}_{v})\ I, (\lambda i :: S.[\![\sigma\tau']\!]^{\rho}_{v})\ I) \in [\![\subseteq]\!]_{K}$
Since $i \notin FSV(\rho)$, STS:$([\![\sigma\tau[I/i]]\!]^{\rho}_{v}, [\![\sigma\tau'[I/i]]\!]^{\rho}_{v}) \in [\![\subseteq]\!]_{K}$
By instantiating IH on the premise of the λ**-1** using $\sigma[i \mapsto I]$, we get:
$([\![\sigma[i \mapsto I]\tau]\!]^{\rho}_{v}, [\![\sigma[i \mapsto I]\tau']\!]^{\rho}_{v}) \in [\![\subseteq]\!]_{K}$ which is equivalent to $([\![\sigma\tau[I/i]]\!]^{\rho}_{v}, [\![\sigma\tau'[I/i]]\!]^{\rho}_{v}) \in [\![\subseteq]\!]_{K}$.

Case $\dfrac{\Psi; \Delta; \Phi \models \tau \sqsubseteq \tau' : S{\to}K\qquad \Phi; \Delta \models I \doteq I'}{\Psi; \Delta; \Phi \models \tau\ I \sqsubseteq \tau'\ I' : K}\mathbf{ty\text{-}app1}$
Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $\models \sigma\Phi$.
TS: $([\![\sigma\tau\ \sigma I]\!]^{\rho}_{v}, [\![\sigma\tau'\ \sigma I']\!]^{\rho}_{v}) \in [\![\subseteq]\!]_{K}$

By unrolling the definition of $[\![\cdot]\!]^\rho_v$, STS: $([\![\sigma\tau]\!]^\rho_v\ \sigma I, [\![\sigma\tau']\!]^\rho_v\ \sigma I') \in [\![\subseteq]\!]_K$
By Lemma 7, we get $\sigma I = \sigma I'$. Therefore, STS: $([\![\sigma\tau]\!]^\rho_v\ \sigma I, [\![\sigma\tau']\!]^\rho_v\ \sigma I) \in [\![\subseteq]\!]_K$
By instantiating the IH, we get $([\![\sigma\tau]\!]^\rho_v, [\![\sigma\tau']\!]^\rho_v) \in [\![\subseteq]\!]_{S\to K}$.
By unrolling the definition of $[\![\subseteq]\!]_{S\to K}$ with σI, we get $([\![\sigma\tau]\!]^\rho_v\ \sigma I, [\![\sigma\tau']\!]^\rho_v\ \sigma I) \in [\![\subseteq]\!]_K$.

Lemma 18 (Subtyping Inversion Lemma)
If $\Psi; \Delta; \Phi \models \tau_1 \sqsubseteq \tau_2 : K$, then $\Psi; \Delta \vdash \tau_1 : K$ and $\Psi; \Delta \vdash \tau_2 : K$

Proof. By induction on the given subtyping derivation.

Case $\dfrac{\Psi; \Delta \vdash \tau_1 : * \qquad \Psi; \Delta \vdash \tau_2 : * \qquad \Delta \vdash \mu :: \mathbb{V} \qquad \Delta \vdash \kappa :: \mathbb{R}}{\Psi; \Delta; \Phi \models (\tau_1 \xrightarrow{\kappa} \tau_2)^\mu \sqsubseteq (\tau_1)^\mu \xrightarrow{\kappa} (\tau_2)^\mu : *} \to \mathbf{1}$

By instantiating the kinding rules **k-fun** and **k-mu** with the premises, we get

$$\dfrac{\dfrac{\Psi; \Delta \vdash \tau_1 : * \qquad \Psi; \Delta \vdash \tau_2 : * \qquad \Delta \vdash \kappa :: \mathbb{R}}{\Psi; \Delta \vdash \tau_1 \xrightarrow{\kappa} \tau_2 : *}\ \textbf{k-fun} \qquad \Delta \vdash \mu :: \mathbb{V}}{\Psi; \Delta \vdash (\tau_1 \xrightarrow{\kappa} \tau_2)^\mu : *}\ \textbf{k-mu}$$

Similarly, by instantiating the kinding rule **k-mu** on the first and second premises and then instantiating the **k-fun** rule, we get

$$\dfrac{\dfrac{\Psi; \Delta \vdash \tau_1 : *}{\Psi; \Delta \vdash (\tau_1)^\mu : *}\ \textbf{k-mu} \qquad \dfrac{\Psi; \Delta \vdash \tau_2 : *}{\Psi; \Delta \vdash (\tau_2)^\mu : *}\ \textbf{k-mu}}{\Psi; \Delta; \Phi \vdash (\tau_1)^\mu \xrightarrow{\kappa} (\tau_2)^\mu : *}\ \textbf{k-fun}$$

Case $\dfrac{\Psi; \Delta; \Phi \models \tau_1' \sqsubseteq \tau_1 : * \qquad \Delta; \Phi \models \tau_2 \sqsubseteq \tau_2' : * \qquad \Delta; \Phi \models \kappa \le \kappa'}{\Psi; \Delta; \Phi \models \tau_1 \xrightarrow{\kappa} \tau_2 \sqsubseteq \tau_1' \xrightarrow{\kappa'} \tau_2' : *} \to \mathbf{2}$

By IH on the first promise, we get $\Psi; \Delta \vdash \tau_1 : *$ and $\Psi; \Delta \vdash \tau_1' : *$.
By IH on the second promise, we get $\Psi; \Delta \vdash \tau_2 : *$ and $\Psi; \Delta \vdash \tau_2' : *$.
By instantiatinng **k-fun** kinding rule, we get

$$\dfrac{\Psi; \Delta \vdash \tau_1 : * \qquad \Psi; \Delta \vdash \tau_2 : * \qquad \Psi; \Delta \vdash \kappa :: \mathbb{R}}{\Psi; \Delta \vdash \tau_1 \xrightarrow{\kappa} \tau_2 : *}$$

and similarly

$$\dfrac{\Psi; \Delta \vdash \tau_1' : * \qquad \Psi; \Delta \vdash \tau_2' : * \qquad \Psi; \Delta \vdash \kappa' :: \mathbb{R}}{\Psi; \Delta \vdash \tau_1' \xrightarrow{\kappa'} \tau_2' : *}$$

Case $\dfrac{\Psi; \Delta \vdash \tau_1 : * \qquad \Psi; \Delta \vdash \tau_2 : * \qquad \Delta \vdash \mu :: \mathbb{V}}{\Psi; \Delta; \Phi \models (\tau_1 \times \tau_2)^\mu \equiv (\tau_1)^\mu \times (\tau_2)^\mu : *} \times\ \mathbf{1}$

By instantiating the **k-pair** and **k-mu** kinding rules, we get

$$\dfrac{\dfrac{\Psi; \Delta \vdash \tau_1 : * \qquad \Psi; \Delta \vdash \tau_2 : *}{\Psi; \Delta \vdash \tau_1 \times \tau_2 : *}\ \textbf{k-pair} \qquad \Delta \vdash \mu :: \mathbb{V}}{\Psi; \Delta \vdash (\tau_1 \times \tau_2)^\mu : *}\ \textbf{k-mu}$$

Similarly, by instantiating the **k-mu** and **k-pair** kinding rules, we get

$$\dfrac{\dfrac{\Psi; \Delta \vdash \tau_1 : * \qquad \Delta \vdash \mu :: \mathbb{V}}{\Psi; \Delta \vdash (\tau_1)^\mu : *}\ \textbf{k-mu} \qquad \dfrac{\Psi; \Delta \vdash \tau_2 : * \qquad \Delta \vdash \mu :: \mathbb{V}}{\Psi; \Delta \vdash (\tau_2)^\mu : *}\ \textbf{k-mu}}{\Psi; \Delta \vdash (\tau_1)^\mu \times (\tau_2)^\mu : *}\ \textbf{k-pair}$$

Case $\dfrac{\Psi; \Delta \vdash \tau : * \qquad \Delta \vdash \mu :: \mathbb{V} \qquad \Delta \vdash n :: \mathbb{N} \qquad \Delta \vdash \alpha :: \mathbb{N}}{\Psi; \Delta; \Phi \models (\mathtt{list}\ [n]^\alpha\ \tau)^\mu \equiv \mathtt{list}\ [n]^\alpha\ (\tau)^\mu : *}\ \mathbf{l1}$

By instantitating **k-list** and **k-mu** kinding rules, we get

$$\dfrac{\dfrac{\Psi;\Delta \vdash \tau : * \qquad \Delta \vdash n :: \mathbb{N} \qquad \Delta \vdash \alpha :: \mathbb{N}}{\Psi;\Delta \vdash \texttt{list}\,[n]^{\alpha}\ \tau : *}\ \textbf{k-list} \qquad \Delta \vdash \mu :: \mathbb{V}}{\Psi;\Delta \vdash (\texttt{list}\,[n]^{\alpha}\ \tau)^{\mu} : *}\ \textbf{k-mu}$$

Similarly, by instantiating the **k-mu** and **k-list** kinding rules, we get

$$\dfrac{\dfrac{\Psi;\Delta \vdash \tau : *}{\Psi;\Delta \vdash (\tau)^{\mu} : *}\ \textbf{k-mu} \qquad \Delta \vdash n :: \mathbb{N} \qquad \Delta \vdash \alpha :: \mathbb{N}}{\Psi;\Delta \vdash \texttt{list}\,[n]^{\alpha}\ (\tau)^{\mu} : *}\ \textbf{k-list}$$

Case $\dfrac{\Delta;\Phi \models n \doteq n' \qquad \Delta;\Phi \models \alpha \leq \alpha' \qquad \Psi;\Delta;\Phi \models \tau \sqsubseteq \tau' : *}{\Psi;\Delta;\Phi \models \texttt{list}\,[n]^{\alpha}\ \tau \sqsubseteq \texttt{list}\,[n']^{\alpha'}\ \tau' : *}\textbf{l4}$

By IH on the third premise, we get $\Psi;\Delta \vdash \tau : *(\star)$ and $\Psi;\Delta \vdash \tau' : *(\dagger)$.
By instantiating the **k-list** kinding rule with $(\star)$, we get

$$\dfrac{\Psi;\Delta \vdash \tau : * \qquad \Delta \vdash n :: \mathbb{N} \qquad \Delta \vdash \alpha :: \mathbb{N}}{\Psi;\Delta \vdash \texttt{list}\,[n]^{\alpha}\ \tau : *}\ \textbf{k-list}$$

Similarly, instantiating the **k-list** kinding rule with $(\dagger)$, we get

$$\dfrac{\Psi;\Delta \vdash \tau' : * \qquad \Delta \vdash n' :: \mathbb{N} \qquad \Delta \vdash \alpha' :: \mathbb{N}}{\Psi;\Delta \vdash \texttt{list}\,[n']^{\alpha'}\ \tau' : *}\ \textbf{k-list}$$

Case $\dfrac{\Psi;\Delta \vdash \tau : * \qquad \Delta \vdash \mu :: \mathbb{V} \qquad \Delta \vdash \kappa :: \mathbb{R}}{\Psi;\Delta;\Phi \models (\forall t :\overset{\kappa}{::} S.\ \tau)^{\mu} \equiv \forall t :\overset{\kappa}{::} S.\ (\tau)^{\mu} : *}\forall\textbf{2}$

By instantiating the **k-**$\forall$ and **k-mu** kinding rules with the premises, we get

$$\dfrac{\dfrac{\Psi;\Delta \vdash \tau : * \qquad \Delta \vdash \kappa :: \mathbb{R}}{\Psi;\Delta \vdash \forall t :\overset{\kappa}{::} S.\ \tau : *}\ \textbf{k-}\forall \qquad \Delta \vdash \mu :: \mathbb{V}}{\Psi;\Delta \vdash (\forall t :\overset{\kappa}{::} S.\ \tau)^{\mu} : *}$$

Similarly, by instantiating the **k-mu** and **k-**$\forall$ kinding rules with the premises, we get

$$\dfrac{\dfrac{\Psi;\Delta \vdash \tau : * \qquad \Delta \vdash \mu :: \mathbb{V}}{\Psi;\Delta \vdash \forall t :\overset{\kappa}{::} S.\ \tau : *}\ \textbf{k-mu} \qquad \Delta \vdash \kappa :: \mathbb{R}}{\Psi;\Delta \vdash \forall t :\overset{\kappa}{::} S.\ (\tau)^{\mu} : *}\ \textbf{k-}\forall$$

Case $\dfrac{\Psi;\Delta \vdash \tau : * \qquad \Delta \vdash \mu :: \mathbb{V}}{\Psi;\Delta;\Phi \models (\tau)^{\mu} \sqsubseteq \tau : *}\textbf{T}$

□

Lemma 19 (Stable context soundness)
Suppose $(\forall x \in \Gamma : \Psi;\Delta;\Phi \models \Gamma(x) \sqsubseteq (\Gamma(x))^{\mathbb{S}} : *)$ and $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $\models \sigma\Phi$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^{\rho}$. Then, the following hold.

1. If $\Psi;\Delta;\Phi;\Gamma \vdash e :_{\kappa} \tau$, then $\texttt{stable}(\theta^{\ulcorner} e^{\urcorner})$.
2. If $\Psi;\Delta;\Phi;\Gamma \vdash w \gg \tau$ and $\texttt{stable}(w)$, then $\texttt{stable}(\theta w)$.
3. If $\Psi;\Delta;\Phi;\Gamma \vdash \textit{æ} \gg_{\kappa} \tau$ and $\texttt{stable}(\textit{æ})$, then $\texttt{stable}(\theta \textit{æ})$.

Proof. All three statements have similar proofs. We show the proof of (1). By definition, $^{\ulcorner} e^{\urcorner}$ does not have any occurrence of `replace`. Therefore, it suffices to show that for any $x \in \Gamma$, $\texttt{stable}(\theta(x))$. Pick any $x \in \Gamma$. From the definition of $\mathcal{G}[\![\sigma\Gamma]\!]^{\rho}$, $(m, \theta(x)) \in [\![\sigma(\Gamma(x))]\!]^{\rho}_{v}$. By Lemma 17, $(m, \theta(x)) \in [\![(\sigma(\Gamma(x)))^{\mathbb{S}}]\!]^{\rho}_{v}$. From the definition of $[\![(\tau)^{\mathbb{S}}]\!]^{\rho}_{v}$, we get $\texttt{stable}(\theta(x))$, as needed. □

Our fundamental theorem relies on the assumption that the semantic interpretation of every primitive function lies in the interpretation of the function's type. This is explained below.

Assumption 20 (Soundness of primitive functions)
Suppose $\zeta : \forall\overline{X_i}, \overline{t_i}.\ \tau_1 \xrightarrow{\kappa} \tau_2$ and $\vdash \tau_i' : *$ and $(m, \boldsymbol{w}) \in [\![\tau_1[\overline{I_i/t_i}, \overline{\tau_i'/X_i}]]\!]_v^\rho$. Then, $\widehat{\zeta}(\mathrm{L}(\boldsymbol{w}))$ and $\widehat{\zeta}(\mathrm{R}(\boldsymbol{w}))$ are both defined. Further, if $\widehat{\zeta}(\mathrm{L}(\boldsymbol{w})) = (c_1, v_r)$ and $\widehat{\zeta}(\mathrm{R}(\boldsymbol{w})) = (c_2, v_r')$, then there must exist $\boldsymbol{w}'$ such that

- $\mathrm{L}(\boldsymbol{w}') = v_r$ and $\mathrm{R}(\boldsymbol{w}') = v_r'$
- $(m, w') \in [\![\tau_2[\overline{I_i/t_i}, \overline{\tau_i'/X_i}]]\!]_v^\rho$
- $c_1 \leq \kappa[\overline{I_i/t_i}]$ and $c_2 \leq \kappa[\overline{I_i/t_i}]$

Theorem 21 (Fundamental theorem)
The following hold.

1. If $\Psi; \Delta; \Phi; \Gamma \vdash e :_\kappa \tau$ and $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$, then $(m, \theta^{\ulcorner} e^{\urcorner}) \in [\![\sigma\tau]\!]_\varepsilon^{\rho,\sigma\kappa}$.

2. If $\Psi; \Delta; \Phi; \Gamma \vdash \boldsymbol{w} \gg \tau$ and $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$, then $(m, \theta\boldsymbol{w}) \in [\![\sigma\tau]\!]_v^\rho$.

3. If $\Psi; \Delta, \Phi, \Gamma \vdash \text{æ} \gg_\kappa \tau$ and $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$, then $(m, \theta(\text{æ})) \in [\![\sigma\tau]\!]_\varepsilon^{\rho,\sigma\kappa}$.

Proof. The first statement is proved by induction on e's typing with a sub-induction on step indices for recursive functions. The second and the third statements are proved by simultaneous induction on bi-value and bi-expression typing. We show select cases of the proofs. In these proofs, the numbers 1–5 represent the corresponding clauses in the definition of $[\![\tau]\!]_\varepsilon^{\rho,\kappa}$.

Proof of statement 1:

Case $\dfrac{}{\Psi; \Delta; \Phi; \Gamma, x : \tau \vdash x :_0 \tau}$ **var**

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma, x : \sigma\tau]\!]^\rho$ and $\models \sigma\Phi$.
TS: $(m, \theta^{\ulcorner} x^{\urcorner}) \in [\![\sigma\tau]\!]_\varepsilon^{\rho,0}$.
By Value Lemma (Lemma 14), STS: $(m, \theta x) \in [\![\sigma\tau]\!]_v^\rho$.
This follows from the definition of $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma, x : \sigma\tau]\!]^\rho$.

Case $\dfrac{}{\Psi; \Delta; \Phi; \Gamma \vdash \mathtt{r} :_0 (\mathtt{real})^{\mathbb{S}}}$ **int**

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$.
TS: $(m, \theta^{\ulcorner} \mathtt{r}^{\urcorner}) \in [\![\sigma\tau]\!]_\varepsilon^{\rho,0}$.
Since $\ulcorner \mathtt{r} \urcorner = \mathtt{keep}(\mathtt{r})$ STS:$(m, \mathtt{keep}(\mathtt{r})) \in [\![(\mathtt{real})^{\mathbb{S}}]\!]_\varepsilon^{\rho,0}$
By Value Lemma (Lemma 14), STS: $(m, \mathtt{keep}(\mathtt{r})) \in [\![(\mathtt{real})^{\mathbb{S}}]\!]_v^\rho$.
This follows from the definition of $[\![(\mathtt{real})^{\mathbb{S}}]\!]_v^\rho$.

Case $\dfrac{}{\Psi;\Delta;\Phi;\Gamma \vdash \texttt{nil} :_0 \texttt{list}\,[0]^0\ \tau}$ **nil**

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$.
TS: $(m, \theta^{\ulcorner}\texttt{nil}^{\urcorner}) \in\ [\![\texttt{list}\,[0]^0\ (\sigma\tau)]\!]^{\rho,0}_{\varepsilon}$.
Since $\ulcorner\texttt{nil}\urcorner = \texttt{nil}$, by the Value Lemma (Lemma 14),
STS: $(m, \texttt{nil}) \in\ [\![\texttt{list}\,[0]^0\ (\sigma\tau)]\!]^{\rho}_{v}$.
This follows from the definition of $[\![\texttt{list}\,[0]^0\ (\sigma\tau)]\!]^{\rho}_{v}$.

Case $\dfrac{\Psi;\Delta;\Phi;\Gamma \vdash e_1 :_{\kappa_1} (\tau)^{\mathbb{S}} \qquad \Psi;\Delta;\Phi;\Gamma \vdash e_2 :_{\kappa_2} \texttt{list}\,[n]^\alpha\ \tau}{\Psi;\Delta;\Phi;\Gamma \vdash \texttt{cons}(e_1,\, e_2) :_{\kappa_1+\kappa_2} \texttt{list}\,[n{+}1]^\alpha\ \tau}$ **cons1**

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$.
TS: $(m, \theta^{\ulcorner}\texttt{cons}(e_1, e_2)^{\urcorner}) \in\ [\![\texttt{list}\,[\sigma n{+}1]^{\sigma\alpha}\ \sigma\tau]\!]^{\rho,\sigma(\kappa_1+\kappa_2)}_{\varepsilon}$.
Following the definition of $[\![\cdot]\!]^{\rho,\cdot}_{\varepsilon}$, assume that:

$$\frac{\mathrm{L}(\theta^{\ulcorner}e_1{}^{\urcorner}) \Downarrow v_1, T_1\ (*) \qquad \mathrm{L}(\theta^{\ulcorner}e_2{}^{\urcorner}) \Downarrow v_2, T_2\ (\dagger)}{\texttt{cons}(\mathrm{L}(\theta^{\ulcorner}e_1{}^{\urcorner}),\, \mathrm{L}(\theta^{\ulcorner}e_2{}^{\urcorner})) \Downarrow \texttt{cons}(v_1,\, v_2), \texttt{cons}(T_1, T_2)}\ \textbf{cons}$$

where $j = |\texttt{cons}(T_1, T_2)| = |T_1| + |T_2| < m$
By IH on e_1, we get $(m, \theta^{\ulcorner}e_1{}^{\urcorner}) \in\ [\![(\tau)^{\mathbb{S}}]\!]^{\rho,\sigma\kappa_1}_{\varepsilon}$. Unrolling its definition using premise $(*)$ with $j_1 = |T_1| \leq j < m$, we get

a) $\langle T_1, \theta^{\ulcorner}e_1{}^{\urcorner}\rangle \curvearrowright \boldsymbol{w}_1', T_1', c_1'$
b) $\mathrm{R}(\theta^{\ulcorner}e_1{}^{\urcorner}) \Downarrow v_1', T_1'$
c) $v_1 = \mathrm{L}(\boldsymbol{w}_1')\ \wedge\ v_1' = \mathrm{R}(\boldsymbol{w}_1')$
d) $c_1' \leq \sigma\kappa_1$
e) $(m - j_1, \boldsymbol{w}_1') \in [\![(\sigma\tau)^{\mathbb{S}}]\!]^{\rho}_{v}$

By IH on e_2, we get $(m, \theta^{\ulcorner}e_2{}^{\urcorner}) \in\ [\![\texttt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau]\!]^{\rho,\sigma\kappa_2}_{\varepsilon}$. Unrolling its definition using premise $(\dagger)$ with $j_2 = |T_2| \leq j < m$, we get

f) $\langle T_2, \theta^{\ulcorner}e_2{}^{\urcorner}\rangle \curvearrowright \boldsymbol{w}_2', T_2', c_2'$
g) $\mathrm{R}(\theta^{\ulcorner}e_2{}^{\urcorner}) \Downarrow v_2', T_2'$
h) $v_2 = \mathrm{L}(\boldsymbol{w}_2')\ \wedge\ v_2' = \mathrm{R}(\boldsymbol{w}_2')$
i) $c_2' \leq \sigma\kappa_2$
j) $(m - j_2, \boldsymbol{w}_2') \in [\![\texttt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau]\!]^{\rho}_{v}$

Then,

1. Using a) and f)

$$\frac{\langle T_1, \theta^{\ulcorner}e_1{}^{\urcorner}\rangle \curvearrowright \boldsymbol{w}_1', T_1', c_1' \qquad \langle T_2, \theta^{\ulcorner}e_1{}^{\urcorner}\rangle \curvearrowright \boldsymbol{w}_2', T_2', c_2'}{\langle \texttt{cons}(T_1, T_2), \theta^{\ulcorner}\texttt{cons}(e_1,\, e_2)^{\urcorner}\rangle \curvearrowright \texttt{cons}(\boldsymbol{w}_1', \boldsymbol{w}_2'), \texttt{cons}(T_1', T_2'), c_1' + c_2'}\ \textbf{r-cons}$$

2. Using b) and g)
$$\frac{\mathrm{R}(\theta^{\ulcorner} e_1^{\urcorner}) \Downarrow v_1', T_1' \qquad \mathrm{R}(\theta^{\ulcorner} e_2^{\urcorner}) \Downarrow v_2', T_2'}{\mathtt{cons}(\mathrm{R}(\theta^{\ulcorner} e_1^{\urcorner}),\, \mathrm{L}(\theta^{\ulcorner} e_2^{\urcorner})) \Downarrow \mathtt{cons}(v_1',\, v_2'), \mathtt{cons}(T_1', T_2')}\ \textbf{cons}$$
3. Using c) and h), $\mathtt{cons}(v_1,\, v_2) = \mathrm{L}(\mathtt{cons}(w_1', w_2')) \ \wedge\ \mathtt{cons}(v_1',\, v_2') = \mathrm{R}(\mathtt{cons}(w_1', w_2'))$
4. By using d) and i), $c_1' + c_2' \leq \sigma(\kappa_1 + \kappa_2')$
5. By Lemma 11, we get $\Psi; \Delta; \Phi \vdash (\tau)^{\mathbb{S}}\ \mathtt{wf}$ and $\Psi; \Delta; \Phi \vdash \mathtt{list}\,[n]^{\alpha}\ \tau\ \mathtt{wf}$. By inversion on $\Psi; \Delta; \Phi \vdash (\tau)^{\mathbb{S}}\ \mathtt{wf}$, we get $\Psi; \Delta; \Phi \vdash \tau\ \mathtt{wf}$, hence by instantiating the Lemma 9 on the well-formedness judgments using e) and j) and noting that $m - j \leq m - j_1$ and $m - j \leq m - j_2$, we get
$(m - j, w_1') \in [\![(\sigma\tau)^{\mathbb{S}}]\!]_v^{\rho}$
$(m - j, w_2') \in [\![\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau]\!]_v^{\rho}$
$\therefore (m - j, \mathtt{cons}(w_1', w_2')) \in\ [\![\mathtt{list}\,[\sigma n{+}1]^{\sigma\alpha}\ \sigma\tau]\!]_v^{\rho}$

Case $\dfrac{\Psi; \Delta; \Phi; \Gamma \vdash e_1 :_{\kappa_1} \tau \qquad \Psi; \Delta; \Phi; \Gamma \vdash e_2 :_{\kappa_2} \mathtt{list}\,[n]^{\alpha-1}\ \tau \qquad \Delta; \Phi \models \alpha > 0}{\Psi; \Delta; \Phi; \Gamma \vdash \mathtt{cons}(e_1,\, e_2) :_{\kappa_1+\kappa_2} \mathtt{list}\,[n+1]^{\alpha}\ \tau}\ \textbf{cons2}$

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^{\rho}$ and $\models \sigma\Phi$.
TS: $(m, \theta^{\ulcorner} \mathtt{cons}(e_1, e_2)^{\urcorner}) \in\ [\![\mathtt{list}\,[\sigma n{+}1]^{\sigma\alpha}\ \sigma\tau]\!]_{\varepsilon}^{\rho, \sigma(\kappa_1+\kappa_2)}$.
Following the definition of $[\![\cdot]\!]_{\varepsilon}^{\rho,\cdot}$, assume that:
$$\frac{\mathrm{L}(\theta^{\ulcorner} e_1^{\urcorner}) \Downarrow v_1, T_1\ (*) \qquad \mathrm{L}(\theta^{\ulcorner} e_2^{\urcorner}) \Downarrow v_2, T_2\ (\dagger)}{\mathtt{cons}(\mathrm{L}(\theta^{\ulcorner} e_1^{\urcorner}),\, \mathrm{L}(\theta^{\ulcorner} e_2^{\urcorner})) \Downarrow \mathtt{cons}(v_1,\, v_2), \mathtt{cons}(T_1, T_2)}\ \textbf{cons}$$
where $j = |\mathtt{cons}(T_1, T_2)| = |T_1| + |T_2| < m$
By IH on e_1, we get $(m, \theta^{\ulcorner} e_1^{\urcorner}) \in\ [\![\sigma\tau]\!]_{\varepsilon}^{\rho, \sigma\kappa_1}$. Unrolling its definition and using the premise marked here $(*)$ with $j_1 = |T_1| \leq j < m$, we get

a) $\langle T_1, \theta^{\ulcorner} e_1^{\urcorner} \rangle \curvearrowright w_1', T_1', c_1'$
b) $\mathrm{R}(\theta^{\ulcorner} e_1^{\urcorner}) \Downarrow v_1', T_1'$
c) $v_1 = \mathrm{L}(w_1') \ \wedge\ v_1' = \mathrm{R}(w_1')$
d) $c_1' \leq \sigma\kappa_1$
e) $(m - j_1, w_1') \in [\![\sigma\tau]\!]_v^{\rho}$ *i.e.*

By IH on e_2, we get $(m, \theta^{\ulcorner} e_2^{\urcorner}) \in\ [\![\mathtt{list}\,[\sigma n]^{\sigma\alpha-1}\ \sigma\tau]\!]_{\varepsilon}^{\rho, \sigma\kappa_2}$. Unrolling its definition with the premise marked $(\dagger)$ with $j_2 = |T_2| \leq j < m$,

f) $\langle T_2, \theta^{\ulcorner} e_2^{\urcorner} \rangle \curvearrowright w_2', T_2', c_2'$
g) $\mathrm{R}(\theta^{\ulcorner} e_2^{\urcorner}) \Downarrow v_2', T_2'$
h) $v_2 = \mathrm{L}(w_2) \ \wedge\ v_2' = \mathrm{R}(w_2)$
i) $c_2' \leq \sigma\kappa_2$
j) $(m - j_2, w_2') \in [\![\mathtt{list}\,[\sigma n]^{\sigma\alpha-1}\ \sigma\tau]\!]_v^{\rho}$

Then,

1. Using a) and f)
$$\frac{\langle T_1, \theta^{\ulcorner} e_1 {}^{\urcorner}\rangle \curvearrowright \boldsymbol{w}_1', T_1', c_1' \qquad \langle T_2, \theta^{\ulcorner} e_2 {}^{\urcorner}\rangle \curvearrowright \boldsymbol{w}_2', T_2', c_2'}{\langle \mathtt{cons}(T_1, T_2), \theta^{\ulcorner} \mathtt{cons}(e_1,\ e_2)^{\urcorner}\rangle \curvearrowright \mathtt{cons}(\boldsymbol{w}_1', \boldsymbol{w}_2'), \mathtt{cons}(T_1', T_2'), c_1' + c_2'}\ \textbf{r-cons}$$
2. Using b) and g)
$$\frac{\mathrm{R}(\theta^{\ulcorner} e_1 {}^{\urcorner}) \Downarrow v_1', T_1' \qquad \mathrm{R}(\theta^{\ulcorner} e_2 {}^{\urcorner}) \Downarrow v_2', T_2'}{\mathtt{cons}(\mathrm{R}(\theta^{\ulcorner} e_1 {}^{\urcorner}),\ \mathrm{L}(\theta^{\ulcorner} e_2 {}^{\urcorner})) \Downarrow \mathtt{cons}(v_1',\ v_2'), \mathtt{cons}(T_1', T_2')}\ \textbf{cons}$$
3. Using c) and h), $\mathtt{cons}(v_1,\ v_2) = \mathrm{L}(\mathtt{cons}(\boldsymbol{w}_1', \boldsymbol{w}_2')) \ \wedge\ \mathtt{cons}(v_1',\ v_2') = \mathrm{R}(\mathtt{cons}(\boldsymbol{w}_1', \boldsymbol{w}_2'))$
4. Using d) and i), $c_1' + c_2' \leq \sigma(\kappa_1 + \kappa_2)$
5. By Lemma 11, we get $\Psi; \Delta; \Phi \vdash (\tau)^{\mathbb{S}}\ \mathtt{wf}$ and $\Psi; \Delta; \Phi \vdash \mathtt{list}\,[n]^{\alpha}\ \tau\ \mathtt{wf}$. By inversion on $\Psi; \Delta; \Phi \vdash (\tau)^{\mathbb{S}}\ \mathtt{wf}$, we get $\Psi; \Delta; \Phi \vdash \tau\ \mathtt{wf}$, hence by instantiating the Lemma 9 on the well-formedness judgments using e) and j) and noting that $m - j \leq m - j_1$ and $m - j \leq m - j_2$, we get
$(m - j, \boldsymbol{w}_1') \in [\![\sigma\tau]\!]_v^{\rho}$
$(m - j, \boldsymbol{w}_2') \in [\![\mathtt{list}\,[\sigma n]^{\sigma\alpha - 1}\ \sigma\tau]\!]_v^{\rho}$
$\therefore (m - j, \mathtt{cons}(\boldsymbol{w}_1', \boldsymbol{w}_2')) \in\ [\![\mathtt{list}\,[\sigma n{+}1]^{\sigma\alpha}\ \sigma\tau]\!]_v^{\rho}$

$$\textbf{Case}\ \frac{\begin{array}{c}\Psi; \Delta; \Phi; \Gamma \vdash e :_{\kappa} \mathtt{list}\,[n]^{\alpha}\ \tau \qquad \Psi; \Delta; \Phi \wedge n \doteq 0; \Gamma \vdash e_1 :_{\kappa'} \tau' \\ \Psi; i :: \iota, \Delta; \Phi \wedge n \doteq i + 1; h : (\tau)^{\mathbb{S}}, tl : \mathtt{list}\,[i]^{\alpha}\ \tau, \Gamma \vdash e_2 :_{\kappa'} \tau' \\ \Psi; i :: \iota, \beta :: \iota, \Delta; \Phi \wedge n \doteq i + 1 \wedge \alpha \doteq \beta + 1; h : (\tau)^{\mathbb{C}}, tl : \mathtt{list}\,[i]^{\beta}\ \tau, \Gamma \vdash e_2 :_{\kappa'} \tau'\end{array}}{\Psi; \Delta; \Phi; \Gamma \vdash \mathtt{case}_{\mathtt{L}}\ e\ \mathtt{of}\ \mathtt{nil}\ \rightarrow\ e_1 \mid \mathtt{cons}(h, tl)\ \rightarrow\ e_2 :_{\kappa + \kappa'} \tau'}\ \textbf{caseL}$$

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^{\rho}$ and $\models \sigma\Phi$.
TS: $(m, \theta^{\ulcorner}(\mathtt{case}_{\mathtt{L}}\ e\ \mathtt{of}\ \mathtt{nil}\ \rightarrow\ e_1 \mid \mathtt{cons}(h, tl)\ \rightarrow\ e_2)^{\urcorner}) \in\ [\![\sigma\tau']\!]_{\varepsilon}^{\rho, \sigma(\kappa + \kappa')}$.
Urolling the definition of $[\![\cdot]\!]_{\varepsilon}^{\rho, \cdot}$, we consider cases on the last rule in the evaluation of $\theta^{\ulcorner}(\mathtt{case}_{\mathtt{L}}\ e\ \mathtt{of}\ \mathtt{nil}\ \rightarrow\ e_1 \mid \mathtt{cons}(h, tl)\ \rightarrow\ e_2)^{\urcorner}$. There are two cases:

$$\textbf{subcase 1:}\ \frac{\mathrm{L}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow \mathtt{nil}, T\ (\star) \qquad \mathrm{L}(\theta^{\ulcorner} e_1 {}^{\urcorner}) \Downarrow v_1, T_1\ (\star\star)}{\mathrm{L}(\theta^{\ulcorner} \mathtt{case}_{\mathtt{L}}\ e\ \mathtt{of}\ \mathtt{nil}\ \rightarrow\ e_1 \mid \mathtt{cons}(h, tl)\ \rightarrow\ e_2 {}^{\urcorner}) \Downarrow v_1, \mathtt{case}_{\mathtt{nil}}(T, T_1)}\ \textbf{case-nil}$$
where $j = |\mathtt{case}_{\mathtt{nil}}(T, T_1)| = |T| + |T_1| + 1 < m$
By IH on e, $(m, \theta^{\ulcorner} e^{\urcorner}) \in\ [\![\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau]\!]_{\varepsilon}^{\rho, \sigma\kappa}$
Unrolling the definition using the premise $\star$ with $j_e = |T| < j < m$ we get

a) $\langle T, \theta^{\ulcorner} e^{\urcorner}\rangle \curvearrowright \boldsymbol{w}', T', c'$
b) $\mathrm{R}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow v', T'$
c) $\mathtt{nil} = \mathrm{L}(\boldsymbol{w}') \ \wedge\ v' = \mathrm{R}(\boldsymbol{w}')$ (this forces $v' = \mathtt{nil}$)
d) $c' \leq \sigma\kappa$
e) $(m - j_e, \boldsymbol{w}') \in [\![\mathtt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau]\!]_v^{\rho}$

Note that c) forces $\boldsymbol{w}' = \texttt{nil}$ and then e) forces $\sigma n \doteq 0$.
Hence, by IH on e_1, we get $(m, \theta^{\ulcorner} e_1{}^{\urcorner}) \in [\![\sigma\tau']\!]^{\rho,\sigma\kappa'}_{\varepsilon}$. Unrolling this with the premise marked ($\star\star$) and definition $j_1 = |T_1| < j < m$, we get

f) $\langle T_1, \theta^{\ulcorner} e_1{}^{\urcorner}\rangle \curvearrowright \boldsymbol{w}'_1, T'_1, c'_1$
g) $\mathrm{R}(\theta^{\ulcorner} e_1{}^{\urcorner}) \Downarrow v'_1, T'_1$
h) $v_1 = \mathrm{L}(\boldsymbol{w}'_1) \ \wedge \ v'_1 = \mathrm{R}(\boldsymbol{w}'_1)$
i) $c'_1 \leq \sigma\kappa'$
j) $(m - j_1, \boldsymbol{w}'_1) \in [\![\sigma\tau']\!]^{\rho}_{v}$

1. By a) and f)
$$\frac{\langle T, \theta^{\ulcorner} e^{\urcorner}\rangle \curvearrowright \texttt{nil}, T', c' \qquad \langle T_1, \theta^{\ulcorner} e_1{}^{\urcorner}\rangle \curvearrowright \boldsymbol{w}'_1, T'_1, c'_1}{\langle \texttt{case}_{\texttt{nil}}(T, T_1), \theta^{\ulcorner} \texttt{case}_{\texttt{L}}\ e\ \texttt{of nil} \ \to\ e_1 \mid \texttt{cons}(h, tl) \ \to\ e_2{}^{\urcorner}\rangle \curvearrowright \boldsymbol{w}'_1, \texttt{case}_{\texttt{nil}}(T', T'_1), c' + c'_1}\ \textbf{r-case-nil}$$
2. By b), c) and g)
$$\frac{\mathrm{R}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow \texttt{nil}, T' \qquad \mathrm{R}(\theta^{\ulcorner} e_1{}^{\urcorner}) \Downarrow v'_1, T'_1}{\mathrm{R}(\theta^{\ulcorner} \texttt{case}_{\texttt{L}}\ e\ \texttt{of nil} \ \to\ e_1 \mid \texttt{cons}(h, tl) \ \to\ e_2{}^{\urcorner}) \Downarrow v'_1, \texttt{case}_{\texttt{nil}}(T', T'_1)}\ \textbf{case-nil}$$
3. is immediate from h)
4. By d) and i), $c' + c'_1 \leq \sigma(\kappa + \kappa')$
5. By Lemma 11, we get $\Psi; \Delta; \Phi \wedge n \doteq 0 \vdash \tau'\ \texttt{wf}$. By instantiating the Lemma 9 on the well-formedness judgment and using j) and noting that $m - j < m - j_1$, we get $(m - j, \boldsymbol{w}'_1) \in [\![\sigma\tau']\!]^{\rho}_{v}$

subcase 2:
$$\frac{\mathrm{L}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow \texttt{cons}(v_h,\, v_{tl}), T\ (\star) \qquad \mathrm{L}(\theta^{\ulcorner} e_2{}^{\urcorner})[v_h/h, v_{tl}/tl] \Downarrow v_2, T_2\ (\star\star)}{\mathrm{L}(\theta^{\ulcorner} \texttt{case}_{\texttt{L}}\ e\ \texttt{of nil} \ \to\ e_1 \mid \texttt{cons}(h, tl) \ \to\ e_2{}^{\urcorner}) \Downarrow v_2, \texttt{case}_{\texttt{cons}}(T, T_2)}\ \textbf{case-cons}$$
where $j = |\texttt{case}_{\texttt{cons}}(T, T_2)| = |T| + |T_2| + 1 < m$
By IH on e, $(m, \theta^{\ulcorner} e^{\urcorner}) \in [\![\texttt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau]\!]^{\rho,\sigma\kappa}_{\varepsilon}$.
Unrolling the definition using the premise marked $\star$ and the definition
$j_e = |T| < j < m$, we get

a) $\langle T, \theta^{\ulcorner} e^{\urcorner}\rangle \curvearrowright \boldsymbol{w}', T', c'$
b) $\mathrm{R}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow v', T'$
c) $\texttt{cons}(v_h,\, v_{tl}) = \mathrm{L}(\boldsymbol{w}') \ \wedge \ v' = \mathrm{R}(\boldsymbol{w}')$
d) $c' \leq \sigma\kappa$
e) $(m - j_e, \boldsymbol{w}') \in [\![\texttt{list}\,[\sigma n]^{\sigma\alpha}\ \sigma\tau]\!]^{\rho}_{v}$
If $\sigma n = \texttt{0}$ then $\boldsymbol{w}' = \texttt{nil}$ however. This is impossible as it contradicts c).
If $\sigma n = I + 1$ then $\boldsymbol{w}' = \texttt{cons}(\boldsymbol{w}'_h, \boldsymbol{w}'_{tl})$ for some $\boldsymbol{w}'_h$ and $\boldsymbol{w}'_{tl}$. By c), $v_h = \mathrm{L}(\boldsymbol{w}'_h)$ and $v_{tl} = \mathrm{L}(\boldsymbol{w}'_{tl})$. Let $v'_h = \mathrm{R}(\boldsymbol{w}'_h)$ and $v'_{tl} = \mathrm{R}(vp'_{tl})$.
Now, $(m - j_e, \texttt{cons}(\boldsymbol{w}'_h, \boldsymbol{w}'_{tl})) \in [\![\texttt{list}\,[I+1]^{\sigma\alpha}\ \sigma\tau]\!]^{\rho}_{v}$ may hold in one to two ways:
case 1. $(m - j_e, \boldsymbol{w}'_h) \in [\![(\sigma\tau)^{\mathbb{S}}]\!]^{\rho}_{v}$ and $(m - j_e, \boldsymbol{w}'_{tl}) \in [\![\texttt{list}\,[I]^{\sigma\alpha}\ \sigma\tau]\!]^{\rho}_{v}$

case 2. $(m - j_e, \boldsymbol{w}'_h) \in [\![\sigma\tau]\!]^\rho_v$ and $(m - j_e, \boldsymbol{w}'_{tl}) \in [\![\texttt{list}\,[I]^{\sigma\alpha-1}\ \sigma\tau]\!]^\rho_v$

We analyze these cases separately:

case 1. $(m - j_e, \boldsymbol{w}'_h) \in [\![(\sigma\tau)^{\mathbb{S}}]\!]^\rho_v$ and $(m - j_e, \boldsymbol{w}'_{tl}) \in [\![\texttt{list}\,[I]^{\sigma\alpha}\ \sigma\tau]\!]^\rho_v$

By IH on e_2 (the third premise of the typing rule) using

- $\sigma[i \mapsto I] \in \mathcal{D}[\![i :: \iota, \Delta]\!]$
- $\models \sigma[i \mapsto I](\Phi \wedge n \doteq i + 1)$ since $\sigma n = I + 1$ by e)
- $(m - j_e, \theta[h \mapsto \boldsymbol{w}'_h, tl \mapsto \boldsymbol{w}'_{tl}]) \in \mathcal{G}[\![\sigma[i \mapsto I](\Gamma, h : (\tau)^{\mathbb{S}}, tl : \texttt{list}\,[i]^\alpha\ \tau)]\!]^\rho$ (using Lemma 8 and e) and noting that $i \notin FV(\tau')$),

we get $(m, \theta[\boldsymbol{w}'_h/h, \boldsymbol{w}'_{tl}/tl]\ulcorner e_2 \urcorner) \in [\![\sigma\tau']\!]^{\rho,\sigma\kappa'}_\varepsilon$.

Unrolling this definition with the premise marked ($\star\star$) and the definition $j_2 = |T_2| < m - j_e$, we get

f) $\langle T_2, \theta\ulcorner e_2 \urcorner[\boldsymbol{w}'_h/h, \boldsymbol{w}'_{tl}/tl]\rangle \curvearrowright \boldsymbol{w}'_2, T'_2, c'_2$

g) $\mathrm{R}(\theta\ulcorner e_2 \urcorner[\boldsymbol{w}'_h/h, \boldsymbol{w}'_{tl}/tl]) \Downarrow v'_2, T'_2$ or, alternatively, $\mathrm{R}(\theta\ulcorner e_2 \urcorner)[v'_h/h, v'_{tl}/tl] \Downarrow v'_2, T'_2$ since by e) $\mathrm{R}(\boldsymbol{w}'_h) = v'_h$ and $\mathrm{R}(\boldsymbol{w}'_{tl}) = v'_{tl}$

h) $v_2 = \mathrm{L}(\boldsymbol{w}'_2)\ \wedge\ v'_2 = \mathrm{R}(\boldsymbol{w}'_2)$

i) $c'_2 \leq \sigma\kappa'$

j) $(m - j_e - j_2, \boldsymbol{w}'_2) \in [\![\sigma\tau']\!]^\rho_v$

1. By a), e) and f)
$$\frac{\langle T, \theta\ulcorner e \urcorner\rangle \curvearrowright \texttt{cons}(\boldsymbol{w}'_h, \boldsymbol{w}'_{tl}), T', c' \qquad \langle T_2, \theta\ulcorner e_2 \urcorner[\boldsymbol{w}'_h/h, \boldsymbol{w}'_{tl}/tl]\rangle \curvearrowright \boldsymbol{w}'_2, T'_2, c'_2}{\langle \texttt{case}_{\texttt{cons}}(T, T_1), \theta\ulcorner \texttt{case}_{\texttt{L}}\ e\ \texttt{of nil}\ \to\ e_1 \mid \texttt{cons}(h, tl)\ \to\ e_2 \urcorner\rangle \curvearrowright \boldsymbol{w}'_2, \texttt{case}_{\texttt{cons}}(T', T'_2), c' + c'_2}\ \textbf{r-case-cons}$$
2. By b) and g)
$$\frac{\mathrm{R}(\theta\ulcorner e \urcorner) \Downarrow \texttt{cons}(v'_h, v'_{tl}), T' \qquad \mathrm{R}(\theta\ulcorner e_2 \urcorner)[v'_h/h, v'_{tl}/tl] \Downarrow v'_2, T'_2}{\mathrm{R}(\theta\ulcorner \texttt{case}_{\texttt{L}}\ e\ \texttt{of nil}\ \to\ e_1 \mid \texttt{cons}(h, tl)\ \to\ e_2 \urcorner) \Downarrow v'_2, \texttt{case}_{\texttt{cons}}(T', T'_2)}\ \textbf{case-cons}$$
3. is immediate from h)
4. By d) and i) $c' + c'_2 \leq \sigma(\kappa + \kappa')$
5. By Lemma 11, we get $\Psi; i :: \iota, \Delta; \Phi \wedge n \doteq i+1 \vdash \tau'\ \texttt{wf}$. By instantiating the Lemma 9 on the well-formedness judgment and using j) and noting that $m - j < m - j_e - j_2$, we get $(m - j, \boldsymbol{w}'_2) \in [\![\sigma\tau']\!]^\rho_v$

case 2. $(m - j_e, \boldsymbol{w}'_h) \in [\![\sigma\tau]\!]^\rho_v$ and $(m - j_e, \boldsymbol{w}'_{tl}) \in [\![\texttt{list}\,[I]^{\sigma\alpha-1}\ \sigma\tau]\!]^\rho_v$

By IH on e_2 (the fourth premise of the typing rule) using

- $\sigma[i \mapsto I, \beta \mapsto \alpha - 1] \in \mathcal{D}[\![i :: \iota, \beta :: \iota, \Delta]\!]$
- $\models \sigma[i \mapsto I, \beta \mapsto \alpha - 1](\Phi \wedge n \doteq i + 1 \wedge \alpha \doteq \beta + 1)$ since $n = I + 1$ by e)
- $(m - j_e, \theta[h \mapsto \boldsymbol{w}'_h, tl \mapsto \boldsymbol{w}'_{tl}]) \in \mathcal{G}[\![\sigma[i \mapsto I, \beta \mapsto \alpha - 1](\Gamma, h : \tau, tl : \texttt{list}\,[i]^\beta\ \tau)]\!]^\rho$ (using Lemma 8 and e) and noting that $i, \beta \notin FV(\tau')$),

we get $(m, \theta[\boldsymbol{w}'_h/h, \boldsymbol{w}'_{tl}/tl]\ulcorner e_2 \urcorner) \in [\![\sigma\tau']\!]^{\rho,\sigma\kappa'}_\varepsilon$.

Unrolling its definition the premise marked and the definition $j_2 = |T_2| < m - j_e$, we get

f) $\langle T_2, \theta^{\ulcorner} e_2 {}^{\urcorner}[\boldsymbol{w}'_h/h, \boldsymbol{w}'_{tl}/tl]\rangle \curvearrowright \boldsymbol{w}'_2, T'_2, c'_2$

g) $\mathrm{R}(\theta^{\ulcorner} e_2 {}^{\urcorner}[\boldsymbol{w}'_h/h, \boldsymbol{w}'_{tl}/tl]) \Downarrow v'_2, T'_2$ or, alternatively, $\mathrm{R}(\theta^{\ulcorner} e_2 {}^{\urcorner})[v'_h/h, v'_{tl}/tl] \Downarrow v'_2, T'_2$ since $\mathrm{R}(\boldsymbol{w}'_h) = v'_h$ and $\mathrm{R}(\boldsymbol{w}'_{tl}) = v'_{tl}$ by e)

h) $v_2 = \mathrm{L}(\boldsymbol{w}'_2) \ \wedge \ v'_2 = \mathrm{R}(\boldsymbol{w}'_2)$

i) $c'_2 \leq \sigma\kappa'$

j) $(m - j_e - j_2, \boldsymbol{w}'_2) \in [\![\sigma\tau']\!]^{\rho}_{v}$

1. By a), e) and f)
$$\frac{\langle T, \theta^{\ulcorner} e^{\urcorner}\rangle \curvearrowright \mathtt{cons}(\boldsymbol{w}'_h, \boldsymbol{w}'_{tl}), T', c' \qquad \langle T_2, \theta^{\ulcorner} e_2 {}^{\urcorner}[\boldsymbol{w}'_h/h, \boldsymbol{w}'_{tl}/tl]\rangle \curvearrowright \boldsymbol{w}'_2, T'_2, c'_2}{\begin{array}{c}\langle \mathtt{case}_{\mathtt{cons}}(T, T_1), \theta^{\ulcorner} \mathtt{case}_{\mathtt{L}}\ e\ \mathtt{of\ nil}\ \rightarrow\ e_1 \mid \mathtt{cons}(h, tl)\ \rightarrow\ e_2 {}^{\urcorner}\rangle \curvearrowright \\ \boldsymbol{w}'_2, \mathtt{case}_{\mathtt{cons}}(T', T'_2), c' + c'_2\end{array}}\ \textbf{r-case-cons}$$
2. By b) and g)
$$\frac{\mathrm{R}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow \mathtt{cons}(v'_h,\ v'_{tl}), T' \qquad \mathrm{R}(\theta^{\ulcorner} e_2 {}^{\urcorner})[v'_h/h, v'_{tl}/tl] \Downarrow v'_2, T'_2}{\mathrm{R}(\theta^{\ulcorner} \mathtt{case}_{\mathtt{L}}\ e\ \mathtt{of\ nil}\ \rightarrow\ e_1 \mid \mathtt{cons}(h, tl)\ \rightarrow\ e_2 {}^{\urcorner}) \Downarrow v'_2, \mathtt{case}_{\mathtt{cons}}(T', T'_2)}\ \textbf{case-cons}$$
3. follows immediately from h)
4. By d) and i) $c' + c'_2 \leq \sigma(\kappa + \kappa')$
5. By Lemma 11, we get $\Psi; i :: \iota, \beta :: \iota, \Delta; \Phi \wedge n \doteq i + 1 \vdash \tau'\ \mathtt{wf}$. By instantiating the Lemma 9 on the well-formedness judgment and using j) and noting that $m - j < m - j_e - j_2$, we get $(m - j, \boldsymbol{w}'_2) \in [\![\sigma\tau']\!]^{\rho}_{v}$

Case $\dfrac{\Psi; \Delta; \Phi; x : \tau_1, f : \tau_1 \xrightarrow{\kappa} \tau_2, \Gamma \vdash e :_{\kappa} \tau_2}{\Psi; \Delta; \Phi; \Gamma \vdash \mathtt{fix}\ \ f(x).\, e :_0 \tau_1 \xrightarrow{\kappa} \tau_2}\ \textbf{fix1}$

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^{\rho}$ and $\models \sigma\Phi$.
TS: $(m, \theta^{\ulcorner} \mathtt{fix}\ \ f(x).\, e^{\urcorner}) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^{\rho,0}_{\varepsilon}$.
STS: $(m, \theta^{\ulcorner} \mathtt{fix}\ \ f(x).\, e^{\urcorner}) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^{\rho}_{v}$ by Lemma 14.
We prove the more general statement $\forall k \leq m.\ (k, \theta^{\ulcorner} \mathtt{fix}\ \ f(x).\, e^{\urcorner}) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^{\rho}_{v}$ by subinduction on k.

subcase 1: $k = 0$ is vacuous from the definition $[\![\cdot]\!]^{\rho}_{v}\cdot$ at the function type.

subcase 2: $k + 1 \leq m$
Let $F = \theta^{\ulcorner} \mathtt{fix}\ \ f(x).\, e^{\urcorner}$.
Assume, by the sub-IH, that $(k, F) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^{\rho}_{v}$ $(*)$
STS: $(k + 1, F) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^{\rho}_{v}$
Following the definition, pick $j < k + 1$. Then $j \leq k$ and $j \leq m$.
Assume that $(j, w) \in [\![\sigma\tau_1]\!]^{\rho}_{v}$. Then, STS: $(j, \theta^{\ulcorner} e^{\urcorner}[F/f, w/x]) \in [\![\sigma\tau_2]\!]^{\rho,\sigma\kappa}_{\varepsilon}$ $(**)$.
Instantiate the IH on the premise of the typing rule using:

- $\sigma \in \mathcal{D}[\![\Delta]\!]$
- $(j, \theta[f \mapsto F, x \mapsto w]) \in \mathcal{G}[\![\sigma(\Gamma, x : \tau_1, f : \tau_1 \xrightarrow{\kappa} \tau_2)]\!]^\rho$, which holds because:
  $(j, \theta) \in \mathcal{G}[\![\Gamma]\!]^\rho$ by Lemma 8 and $(m, \theta) \in \mathcal{G}[\![\Gamma]\!]^\rho$,
  $(j, w) \in [\![\sigma\tau_1]\!]_v^\rho$ and
  $(j, F) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]_v^\rho$ by downward-closure on $(*)$ using $j \leq k$

We immediately get $(j, \theta[f \mapsto F, x \mapsto w]^\ulcorner e^\urcorner) \in [\![\sigma\tau_2]\!]_\varepsilon^{\rho,\sigma\kappa}$, which is the same as $(**)$.

Case $\dfrac{\Psi; \Delta; \Phi; \Gamma \vdash e_1 :_{\kappa_1} \tau_1 \xrightarrow{\kappa} \tau_2 \qquad \Psi; \Delta; \Phi; \Gamma \vdash e_2 :_{\kappa_2} \tau_1}{\Psi; \Delta; \Phi; \Gamma \vdash e_1\ e_2 :_{(\kappa_1+\kappa_2+\kappa)} \tau_2}$ **app**

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$.
TS: $(m, \theta^\ulcorner e_1\ e_2^\urcorner) \in [\![\sigma\tau_2]\!]_\varepsilon^{\rho,\sigma(\kappa_1+\kappa_2+\kappa)}$.
Following the definition of $[\![\cdot]\!]_\varepsilon^{\rho,\cdot}$, assume that

$$\dfrac{\mathrm{L}(\theta^\ulcorner e_1^\urcorner) \Downarrow \texttt{fix}\ \ f(x).\, e, T_1\ (\star) \qquad \mathrm{L}(\theta^\ulcorner e_2^\urcorner) \Downarrow v_2, T_2\ (\star\star) \qquad e[v_2/x, (\texttt{fix}\ \ f(x).\, e)/f] \Downarrow v_r, T_r\ (\star\star\star)}{\mathrm{L}(\theta^\ulcorner e_1\ e_2^\urcorner) \Downarrow v_r, \texttt{app}(T_1, T_2, T_r)}\ \textbf{app}$$

where $j = |\texttt{app}(T_1, T_2, T_r)| = |T_1| + |T_2| + |T_r| + 1 < m$
By IH on e_1, we get $(m, \theta^\ulcorner e_1^\urcorner) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]_\varepsilon^{\rho,\sigma\kappa_1}$.
Unrolling its definition using the premise marked $(\star)$ and the definition $j_1 = |T_1| < j < m$, we get

a) $\langle T_1, \theta^\ulcorner e_1^\urcorner \rangle \curvearrowright w_1', T_1', c_1'$
b) $\mathrm{R}(\theta^\ulcorner e_1^\urcorner) \Downarrow v_1', T_1'$
c) $\texttt{fix}\ \ f(x).\, e = \mathrm{L}(w_1')\ \wedge\ v_1' = \mathrm{R}(w_1')$
   Therefore, $w_1' = \texttt{fix}\ \ f(x).\, æ$ for some $æ$ and $v_1' = \texttt{fix}\ \ f(x).\, e'$ for $e' = \mathrm{R}(æ)$
d) $c_1' \leq \sigma\kappa_1$
e) $(m - j_1, w_1') \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]_v^\rho$

By IH on e_2 , we get $(m, \theta^\ulcorner e_2^\urcorner) \in [\![\sigma\tau_1]\!]_\varepsilon^{\rho,\sigma\kappa_2}$
Unrolling its definition, using the premise $(\star\star)$ and the definition $j_2 = |T_2| < j < m$, we get

f) $\langle T_2, \theta^\ulcorner e_2^\urcorner \rangle \curvearrowright w_2', T_2', c_2'$
g) $\mathrm{R}(\theta^\ulcorner e_2^\urcorner) \Downarrow v_2', T_2'$
h) $v_2 = \mathrm{L}(w_2')\ \wedge\ v_2' = \mathrm{R}(w_2')$
i) $c_2' \leq \sigma\kappa_2$
j) $(m - j_2, w_2') \in [\![\sigma\tau_1]\!]_v^\rho$

Unrolling e) and $(m - j_1 - j_2 - 1, w_2') \in [\![\sigma\tau_1]\!]_v^\rho$ (downward-closure on j) using $m - j_1 - j_2 - 1 < m - j_2$), we get
$(m - j_1 - j_2 - 1, æ[(\texttt{fix}\ \ f(x).\, æ)/f, w_2'/x]) \in [\![\sigma\tau_2]\!]_v^\rho$.

Unrolling its definition with the premise ($\star\star\star$), noting that
$\mathrm{L}(\text{æ}[(\texttt{fix}\ \ f(x).\,\text{æ})/f, w_2'/x]) = e[v_2/x, (\texttt{fix}\ \ f(x).\,e)/f]$ from c) and h), we get

k) $\langle T_r, \text{æ}[(\texttt{fix}\ \ f(x).\,\text{æ})/f, w_2'/x]\rangle \curvearrowright w_r', T_r', c_r'$
l) $\mathrm{R}(\text{æ}[(\texttt{fix}\ \ f(x).\,\text{æ})/f, w_2'/x] = e'[(\texttt{fix}\ \ f(x).\,e')/f, v_2'/x]) \Downarrow v_r', T_r'$
m) $v_r = \mathrm{L}(w_r')\ \wedge\ v_r' = \mathrm{R}(w_r')$
n) $c_r' \le \sigma\kappa$
o) $(m - j_1 - j_2 - j_r - 1, w_r') \in [\![\sigma\tau_2]\!]_v^\rho$

Then,

1. By a), f) and k)
$$\frac{\langle T_2, \theta^\ulcorner e_2 \urcorner\rangle \curvearrowright w_2', T_2', c_2' \qquad \langle T_r, \text{æ}[(\texttt{fix}\ \ f(x).\,\text{æ})/f, w_2'/x]\rangle \curvearrowright w_r', T_r', c_r'}{\langle \texttt{app}(T_1, T_2, T_r), \theta^\ulcorner e_1\ e_2 \urcorner\rangle \curvearrowright w_r', \texttt{app}(T_1', T_2', T_r'), c_1' + c_2' + c_r'}\ \textbf{r-app}$$
2. By b), g) and l)
$$\frac{\mathrm{R}(\theta^\ulcorner e_1 \urcorner) \Downarrow \texttt{fix}\ \ f(x).\,e', T_1' \qquad \mathrm{R}(\theta^\ulcorner e_2 \urcorner) \Downarrow v_2', T_2' \qquad e'[(\texttt{fix}\ \ f(x).\,e')/f, v_2'/x] \Downarrow v_r', T_r'}{\mathrm{R}(\theta^\ulcorner e_1\ e_2 \urcorner) \Downarrow v_r', \texttt{app}(T_1', T_2', T_r')}\ \textbf{app}$$
3. follows immediately from m)
4. By d), i), n) $c_1 + c_2 + c_r \le \sigma(\kappa_1 + \kappa_2 + \kappa)$
5. Since $j = j_1 + j_2 + j_r + 1$, by o), we get $(m - j, w_r') \in [\![\sigma\tau_2]\!]_v^\rho$, noting that $m - j = m - j_1 - j_2 - j_r - 1$.

Case $\dfrac{\Psi; t :: S, \Delta; \Phi; \Gamma \vdash e :_\kappa \tau}{\Psi; \Delta; \Phi; \Gamma \vdash \Lambda.\, e :_0 \forall t \overset{\kappa}{::} S.\ \tau}\ \forall\mathbf{I}$

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$.
TS: $(m, \theta^\ulcorner \Lambda.\, e \urcorner) \in [\![\forall t \overset{\sigma\kappa}{::} S.\ \sigma\tau]\!]_\varepsilon^{\rho,0}$.
STS: $(m, \theta^\ulcorner \Lambda.\, e \urcorner) \in [\![\forall t \overset{\sigma\kappa}{::} S.\ \sigma\tau]\!]_v^\rho$ by Lemma 14.
Unrolling the definition of $[\![\cdot]\!]_v^\rho$, assume that $\vdash I :: S$.
STS: $(m, \theta^\ulcorner e \urcorner) \in [\![\sigma\tau\{I/t\}]\!]_\varepsilon^{\rho, \sigma\kappa\{I/t\}}$
This follows from the IH instantiated with the substitution $\sigma[t \mapsto I] \in \mathcal{D}[\![t :: S, \Delta]\!]$. Note that $\models \sigma[t \mapsto I]\Phi$ is the same as $\models \sigma\Phi$ since $t \notin FV(\Phi; \Gamma)$.

Case $\dfrac{\Psi; \Delta; \Phi; \Gamma \vdash e :_\kappa \forall t \overset{\kappa'}{::} S.\ \tau \qquad \Delta \vdash I :: S}{\Psi; \Delta; \Phi; \Gamma \vdash e[] :_{\kappa + \kappa'\{I/t\}} \tau\{I/t\}}\ \forall\mathbf{E}$

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$.
TS: $(m, \theta^\ulcorner e[] \urcorner) \in [\![\sigma\tau\{\sigma I/t\}]\!]_\varepsilon^{\rho, \sigma(\kappa + \kappa'\{\sigma I/t\})}$
Following the definition of $[\![\cdot]\!]_\varepsilon^{\rho,\cdot}$, assume that

$$\frac{\mathrm{L}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow \Lambda.\, e', T \ (\star) \qquad e' \Downarrow v_r, T_r \ (\star\star)}{\mathrm{L}(\theta^{\ulcorner} e[]^{\urcorner}) \Downarrow v_r, \mathtt{iApp}(T, T_r)}\ \textbf{App}$$

where $j = |T| + |T_r| + 1 < m$

By IH on e, $(m, \theta^{\ulcorner} e^{\urcorner}) \in \ [\![\forall t \overset{\sigma\kappa'}{::} S.\ \sigma\tau]\!]_{\varepsilon}^{\rho,\sigma\kappa}$.

Unrolling this, using the premise marked $\star$ with the definition $j_e = |T| < j < m$, we get

a) $\langle T, \theta^{\ulcorner} e^{\urcorner} \rangle \curvearrowright \boldsymbol{w}', T', c'$

b) $\mathrm{R}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow v', T'$

c) $\Lambda.\, e' = \mathrm{L}(\boldsymbol{w}') \ \wedge \ v' = \mathrm{R}(\boldsymbol{w}')$

Hence, $\boldsymbol{w}' = \Lambda.\text{æ}$, $e' = \mathrm{L}(\text{æ})$, $v' = \Lambda.e''$ where $e'' = \mathrm{R}(\text{æ})$

d) $c' \leq \sigma\kappa$

e) $(m - j_e, \boldsymbol{w}') \in [\![\forall t \overset{\sigma\kappa'}{::} S.\ \sigma\tau]\!]_v^{\rho}$

By Lemma 7, $\vdash \sigma I :: S$.

Unrolling e) with $\vdash \sigma I :: S$, we get $(m - j_e, \text{æ}) \in \ [\![\sigma\tau\{\sigma I/t\}]\!]_{\varepsilon}^{\rho,\sigma\kappa'\{\sigma I/t\}}$.

Unrolling this with the premise marked $(\star\star)$ and defining $j_r = |T_r| < m - j_e$, we get

f) $\langle T_r, \text{æ} \rangle \curvearrowright \boldsymbol{w}_r', T_r', c_r'$

g) $e'' \Downarrow v_r', T_r'$

h) $v_r = \mathrm{L}(\boldsymbol{w}_r') \ \wedge \ v_r' = \mathrm{R}(\boldsymbol{w}_r')$

i) $c_r' \leq \sigma\kappa'\{\sigma I/t\}$

j) $(m - j_e - j_r, w_r) \in \ [\![\sigma\tau\{\sigma I/t\}]\!]_v^{\rho}$

Then,

1. By a) and f)
$$\frac{\langle T, \theta^{\ulcorner} e^{\urcorner} \rangle \curvearrowright \Lambda.\text{æ}, T', c' \qquad \langle T_r, \text{æ} \rangle \curvearrowright \boldsymbol{w}_r', T_r', c_r'}{\langle \mathtt{iApp}(T, T_r), \theta^{\ulcorner} \text{æ}[]^{\urcorner} \rangle \curvearrowright \boldsymbol{w}_r', \mathtt{iApp}(T', T_r'), c' + c_r'}\ \textbf{r-App}$$
2. By b) and g)
$$\frac{\mathrm{R}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow \Lambda.\, e'', T' \qquad e'' \Downarrow v_r', T_r'}{\mathrm{R}(\theta^{\ulcorner} e[]^{\urcorner}) \Downarrow v_r', \mathtt{iApp}(T', T_r')}\ \textbf{App}$$
3. follows immediately from h)
4. By d) and i), $c' + c_r' \leq \sigma(\kappa + \kappa')$
5. $(m - j, w_r) \in \ [\![\sigma\tau\{\sigma I/t\}]\!]_v^{\rho}$ by downward-closure on j) since $m - j < m - j_e - j_r$

Case $\dfrac{X : K, \Psi; \Delta; \Phi; \Gamma \vdash e :_{\kappa} \tau}{\Psi; \Delta; \Phi; \Gamma \vdash \nu.\, e :_0 \forall X \overset{\kappa}{:} K.\tau}\ \textbf{t-forall}$

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^{\rho}$ and $\models \sigma\Phi$.

TS: $(m, \theta^{\ulcorner} \nu.\, e^{\urcorner}) \in \ [\![\forall X \overset{\sigma\kappa}{:} K.\sigma\tau]\!]_{\varepsilon}^{\rho,0}$.

STS: $(m, \theta^{\ulcorner} \nu.\, e^{\urcorner}) \in \ [\![\forall X \overset{\sigma\kappa}{:} K.\sigma\tau]\!]_v^{\rho}$ by Lemma 14.

Unrolling the definition of $[\![\cdot]\!]^{\rho}_{v}$, assume that $R \in [\![K]\!]_K$.
STS: $(m, \theta^{\ulcorner} e^{\urcorner}) \in [\![\sigma\tau]\!]^{\sigma\kappa, \rho[X \mapsto R]}_{\varepsilon}$
This follows from the IH instantiated with the substitution $\rho[X \mapsto R] \in \mathcal{T}[\![X : K, \Psi]\!]$.

Case $\dfrac{\Psi; \Delta; \Phi; \Gamma \vdash e :_{\kappa} \forall X \overset{\kappa'}{:} K.\tau \qquad \Psi; \Delta \vdash \tau' : K}{\Psi; \Delta; \Phi; \Gamma \vdash e[-] :_{\kappa+\kappa'} \tau[\tau'/X]}$ **t-app**

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^{\rho}$ and $\models \sigma\Phi$.
TS: $(m, \theta^{\ulcorner} e[-]^{\urcorner}) \in [\![\sigma\tau\{\sigma\tau'/X\}]\!]^{\rho, \sigma(\kappa+\kappa')}_{\varepsilon}$
Following the definition of $[\![\cdot]\!]^{\rho,\cdot}_{\varepsilon}$, assume that

$\dfrac{\mathrm{L}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow \nu.\, e', T \ (\star) \qquad e' \Downarrow v_r, T_r \ (\star\star)}{\mathrm{L}(\theta^{\ulcorner} e[-]^{\urcorner}) \Downarrow v_r, \mathtt{tApp}(T, T_r)}$ **t-App**

where $j = |T| + |T_r| + 1 < m$
By IH on e, $(m, \theta^{\ulcorner} e^{\urcorner}) \in [\![\forall X \overset{\sigma\kappa'}{:} K.\sigma\tau]\!]^{\rho, \sigma\kappa}_{\varepsilon}$.
Unrolling this, using the premise marked $\star$ with the definition $j_e = |T| < j < m$, we get

a) $\langle T, \theta^{\ulcorner} e^{\urcorner} \rangle \curvearrowright \boldsymbol{w}', T', c'$
b) $\mathrm{R}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow v', T'$
c) $\nu.\, e' = \mathrm{L}(\boldsymbol{w}') \ \wedge \ v' = \mathrm{R}(\boldsymbol{w}')$
   Hence, $\boldsymbol{w}' = \nu.\text{æ}$, $e' = \mathrm{L}(\text{æ})$, $v' = \nu.e''$ where $e'' = \mathrm{R}(\text{æ})$
d) $c' \leq \sigma\kappa$
e) $(m - j, \boldsymbol{w}') \in [\![\forall X \overset{\sigma\kappa'}{:} K.\sigma\tau]\!]^{\rho}_{v}$

By soundness of the kinding judgement $\Psi; \Delta \vdash \tau' : K$ (Lemma 9), we get $[\![\sigma\tau']\!]^{\rho}_{v} \in [\![K]\!]_K$.
Unrolling e) with $[\![\sigma\tau']\!]^{\rho}_{v}$, we get $(m, \text{æ}) \in [\![\sigma\tau\{\sigma\tau'/X\}]\!]^{\rho, \sigma\kappa'}_{\varepsilon}$.
Unrolling this with the premise marked $(\star\star)$ and defining $j_r = |T_r| < m - j_e$, we get

f) $\langle T_r, \text{æ} \rangle \curvearrowright \boldsymbol{w}'_r, T'_r, c'_r$
g) $e'' \Downarrow v'_r, T'_r$
h) $v_r = \mathrm{L}(\boldsymbol{w}'_r) \ \wedge \ v'_r = \mathrm{R}(\boldsymbol{w}'_r)$
i) $c'_r \leq \sigma\kappa'$
j) $(m - j_e - j_r, \boldsymbol{w}_r) \in [\![\sigma\tau\{\sigma\tau'/X\}]\!]^{\rho}_{v}$

Then,

1. By a) and f)
   $\dfrac{\langle T, \theta^{\ulcorner} e^{\urcorner} \rangle \curvearrowright \nu.\text{æ}, T', c' \qquad \langle T_r, \text{æ} \rangle \curvearrowright \boldsymbol{w}'_r, T'_r, c'_r}{\langle \mathtt{tApp}(T, T_r), \theta^{\ulcorner} \text{æ}[-]^{\urcorner} \rangle \curvearrowright \boldsymbol{w}'_r, \mathtt{tApp}(T', T'_r), c' + c'_r}$ **r-tyApp**
2. By b) and g)
   $\dfrac{\mathrm{R}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow \nu.\, e'', T' \qquad e'' \Downarrow v'_r, T'_r}{\mathrm{R}(\theta^{\ulcorner} e[-]^{\urcorner}) \Downarrow v'_r, \mathtt{tApp}(T', T'_r)}$ **tyApp**

3. follows immediately from h)
4. By d) and i), $c' + c'_r \leq \sigma(\kappa + \kappa')$
5. By Lemma 11, we get $\Psi; \Delta; \Phi; \Gamma \vdash \forall X \overset{\kappa'}{:} K.\tau : *$.
   By inversion, we get $X : K; \Psi; \Delta; \Phi; \Gamma \vdash \tau : *$.
   By instantiating Lemma 9 on the previous statement, we get $[\![\sigma\tau]\!]_v^{\rho[X \mapsto \sigma\tau']} \in [\![*]\!]_K$.
   By unrolling the definition using j), we get $(m - j, \boldsymbol{w}_r) \in [\![\sigma\tau\{\sigma\tau'/X\}]\!]_v^\rho$ since $m - j < m - j_e - j_r$.

Case $\dfrac{\Psi; \Delta; \Phi; \Gamma \vdash e :_\kappa \tau \qquad \Psi; \Delta; \Phi \models \tau \sqsubseteq \tau' : * \qquad \Delta; \Phi \models \kappa \leq \kappa'}{\Psi; \Delta; \Phi; \Gamma \vdash e :_{\kappa'} \tau'} \sqsubseteq : *$

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$.
TS: $(m, \theta^\ulcorner e^\urcorner) \in [\![\sigma\tau']\!]_\varepsilon^{\rho, \sigma\kappa'}$
Following the definition of $[\![\cdot]\!]_\varepsilon^{\rho,\cdot}$, assume that $\mathrm{L}(\theta^\ulcorner e^\urcorner) \Downarrow v, T$ ($\star$) where $j = |T| < m$.
By IH on premise, we get $(m, \theta^\ulcorner e^\urcorner) \in [\![\sigma\tau]\!]_\varepsilon^{\rho, \sigma\kappa}$.
Unrolling this and using the assumption marked ($\star$), we get

a) $\langle T, \theta^\ulcorner e^\urcorner \rangle \curvearrowright \boldsymbol{w}', T', c'$
b) $\mathrm{R}(\theta^\ulcorner e^\urcorner) \Downarrow v', T'$
c) $v = \mathrm{L}(\boldsymbol{w}') \ \wedge \ v' = \mathrm{R}(\boldsymbol{w}')$
d) $c' \leq \sigma\kappa$
e) $(m - j, \boldsymbol{w}') \in [\![\sigma\tau]\!]_v^\rho$

Then,

1. follows immediately from a)
2. follows immediately from b)
3. follows immediately from c)
4. Applying Assumption 6 to $\Delta; \Phi \models \kappa \leq \kappa'$ and the assumptions $\models \sigma\Phi$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$, we get $\sigma\kappa \leq \sigma\kappa'$. Therefore, using d), $c' \leq \sigma\kappa \leq \sigma\kappa'$.
5. Applying Lemma 17 $\Delta; \Phi \models \tau \sqsubseteq \tau' : *$, we get $([\![\sigma\tau]\!]_v^\rho, [\![\sigma\tau']\!]_v^\rho) \in [\![\sqsubseteq]\!]_*$. Hence using e), we get $(m - j, \boldsymbol{w}') \in [\![\sigma\tau]\!]_v^\rho \subseteq [\![\sigma\tau']\!]_v^\rho$.

Case $\dfrac{\begin{array}{c}\Upsilon(\zeta) = \zeta : \forall \overline{t_i}, \overline{X_i}.\ \tau_1 \xrightarrow{\kappa} \tau_2 \\ \Psi; \Delta \vdash \tau'_i : * \qquad \Delta \vdash \overline{I_i} :: S \qquad \Psi; \Delta; \Phi; \Gamma \vdash e :_{\kappa_e} \tau_1[\overline{I_i/t_i}, \overline{\tau'_i/X_i}]\end{array}}{\Psi; \Delta; \Phi; \Gamma \vdash \zeta\ e :_{\kappa_e + \kappa[\overline{I_i/t_i}]} \tau_2[\overline{I_i/t_i}, \overline{\tau'_i/X_i}]}$ **primApp**

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$.
TS: $(m, \theta^\ulcorner \zeta\ e^\urcorner) \in [\![\sigma\tau_2[\overline{\sigma I_i/t_i}, \overline{\sigma\tau'_i/X_i}]]\!]_\varepsilon^{\rho, \sigma\kappa_e + \sigma\kappa[\overline{\sigma I_i/t_i}]}$
Assume that

$$\frac{\mathrm{L}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow v, T \ (\star) \qquad \widehat{\zeta}(v) = (\_, v_r) \ (\star\star)}{\mathrm{L}(\theta^{\ulcorner} \zeta\ e^{\urcorner}) \Downarrow v_r, \mathtt{primApp}(T, v_r, \zeta)}\ \textbf{primapp}$$

Let $j = |T| + 1 < m$

By IH on e, we get $(m, \theta^{\ulcorner} e^{\urcorner}) \in \ [\![\sigma\tau_1[\overline{\sigma I_i/t_i}, \overline{\sigma\tau_i'/X_i}]]\!]_{\varepsilon}^{\rho, \sigma\kappa_e}$.

Unrolling this with the premise $(\star)$ and defining $j_e = |T| < j < m$, we get

a) $\langle T, \theta^{\ulcorner} e^{\urcorner}\rangle \curvearrowright \boldsymbol{w}', T', c'$

b) $\mathrm{R}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow v', T'$

c) $v = \mathrm{L}(\boldsymbol{w}') \ \wedge \ v' = \mathrm{R}(\boldsymbol{w}')$

d) $c' \leq \sigma\kappa_e$

e) $(m - j_e, \boldsymbol{w}') \in \ [\![\sigma\tau_1[\overline{\sigma I_i/t_i}, \overline{\sigma\tau_i'/X_i}]]\!]_v^{\rho}$

There are two cases depending on whether $\mathtt{stable}(\theta^{\ulcorner} e^{\urcorner})$ or not.

case: $\mathtt{stable}(\theta^{\ulcorner} e^{\urcorner})$

1. $$\frac{\mathtt{stable}(\theta^{\ulcorner} e^{\urcorner})}{\langle \mathtt{primApp}(T, v_r, \zeta), \theta^{\ulcorner} \zeta\ æ^{\urcorner}\rangle \curvearrowright {}^{\ulcorner} v_r {}^{\urcorner}, \mathtt{primApp}(T, v_r, \zeta), 0}\ \textbf{r-prim-s}$$
2. Since $\mathtt{stable}(\theta^{\ulcorner} e^{\urcorner})$, we also have $\mathtt{stable}(\theta^{\ulcorner} \zeta\ e^{\urcorner})$. So, $\mathrm{L}(\theta^{\ulcorner} \zeta\ e^{\urcorner}) = \mathrm{R}(\theta^{\ulcorner} \zeta\ e^{\urcorner})$. Hence, from the evaluation judgment for $\mathrm{L}(\theta^{\ulcorner} \zeta\ e^{\urcorner})$, we also get:
   $$\frac{\mathrm{R}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow v, T \qquad \widehat{\zeta}(v) = (\_, v_r)}{\mathrm{R}(\theta^{\ulcorner} \zeta\ e^{\urcorner}) \Downarrow v_r, \mathtt{primApp}(T, v_r, \zeta)}\ \textbf{primapp}$$
3. We choose $w_r' = {}^{\ulcorner} v_r {}^{\urcorner}$. $v_r = \mathrm{L}({}^{\ulcorner} v_r {}^{\urcorner}) \ \wedge \ v_r = \mathrm{R}({}^{\ulcorner} v_r {}^{\urcorner})$ by definition of ${}^{\ulcorner}\cdot{}^{\urcorner}$.
4. $0 \leq \sigma\kappa_e + \sigma\kappa[\overline{\sigma I_i/t_i}]$, trivially.
5. We have to show $(m - j, {}^{\ulcorner} v_r {}^{\urcorner}) \in \ [\![\sigma\tau_2[\overline{\sigma I_i/t_i}, \overline{\sigma\tau_i'/X_i}]]\!]_v^{\rho}$. From Assumption 20, observing that $(m - j_e, \boldsymbol{w}') \in \ [\![\sigma\tau_1[\overline{\sigma I_i/t_i}, \overline{\sigma\tau_i'/X_i}]]\!]_v^{\rho}$ and that $\mathrm{L}(\boldsymbol{w}') = \mathrm{R}(\boldsymbol{w}') = v = v'$, we derive that $(m - j, {}^{\ulcorner} v_r {}^{\urcorner}) \in \ [\![\sigma\tau_2[\overline{\sigma I_i/t_i}, \overline{\sigma\tau_i'/X_i}]]\!]_v^{\rho}$. Noting that $\mathtt{merge}(v_r, v_r) = {}^{\ulcorner} v_r {}^{\urcorner}$, we are done.

case: $\neg\mathtt{stable}(\theta^{\ulcorner} e^{\urcorner})$

Since $\zeta : \forall\overline{t_i}, \overline{X_i}.\ \tau_1 \xrightarrow{\kappa} \tau_2$ and $\vdash \sigma\tau_i' : *$ and $(m - j_e, \boldsymbol{w}') \in \ [\![\sigma\tau_1[\overline{\sigma I_i/t_i}, \overline{\sigma\tau_i'/X_i}]]\!]_v^{\rho}$, Assumption 20 and the premise $(\star\star)$ together yield some c_1, c_2 and v_r' such that $\widehat{\zeta}(v) = (c_1, v_r)$ and $\widehat{\zeta}(v') = (c_2, v_r')$ $(\dagger)$ and a $\boldsymbol{w}_r'$ such that

f) $\mathrm{L}(\boldsymbol{w}_r') = v_r$ and $\mathrm{R}(\boldsymbol{w}_r') = v_r'$. Hence, $\boldsymbol{w}_r' = \mathtt{merge}(v_r, v_r')$.

g) $(m - j_e, \boldsymbol{w}_r') \in \ [\![\sigma\tau_2[\overline{\sigma I_i/t_i}, \overline{\sigma\tau_i'/X_i}]]\!]_v^{\rho}$

h) $c_1 \leq \sigma\kappa[\overline{\sigma I_i/t_i}]$ and $c_2 \leq \sigma\kappa[\overline{\sigma I_i/t_i}]$

1. By a), c), f) and $(*)$,
   $$\frac{\neg\mathtt{stable}(\theta^{\ulcorner} e^{\urcorner}) \qquad \langle T, \theta^{\ulcorner} e^{\urcorner}\rangle \curvearrowright \boldsymbol{w}', T', c' \qquad (c_2, v_r') = \widehat{\zeta}(\mathrm{R}(\boldsymbol{w}'))}{\langle \mathtt{primApp}(T, v_r, \zeta), \theta^{\ulcorner} \zeta\ e^{\urcorner}\rangle \curvearrowright \boldsymbol{w}_r',\ \mathtt{primApp}(T', v_r', \zeta),\ c' + c_2}\ \textbf{r-prim}$$

2. By using b), c) and $(*)$
$$\frac{\mathrm{R}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow v', T' \qquad \widehat{\zeta}(v') = (\_, v'_r)}{\mathrm{R}(\theta^{\ulcorner} \zeta\ e^{\urcorner}) \Downarrow v'_r, \mathtt{primApp}(T', v'_r, \zeta)}\ \textbf{primapp}$$
3. $v_r = \mathrm{L}(\boldsymbol{w}'_r) \ \wedge\ v'_r = \mathrm{R}(\boldsymbol{w}'_r)$ by f).
4. From d) and h), $c' + c_2 \leq \sigma\kappa_e + \sigma\kappa[\overline{\sigma I_i/t_i}]$
5. From g) we get $(m - j_e, \boldsymbol{w}'_r) \in \ [\![\sigma\tau_2[\overline{\sigma I_i/t_i}, \overline{\sigma\tau'_i/X_i}]]\!]^{\rho}_{v}$.
By Lemma 11, we get $\Psi; \Delta \vdash \tau_2[\overline{I_i/t_i}, \overline{\tau'_i/X_i}] : *$. By instantiating the Lemma 9, we get $[\![\sigma\tau_2[\overline{\sigma I_i/t_i}, \overline{\sigma\tau'_i/X_i}]]\!]^{\rho}_{v} \in [\![*]\!]_K$. By unrolling the definition with j) and noting that $m - j < m - j_e$, we get $(m - j, \boldsymbol{w}'_r) \in \ [\![\sigma\tau_2[\overline{\sigma I_i/t_i}, \overline{\sigma\tau'_i/X_i}]]\!]^{\rho}_{v}$.

Case $\dfrac{\Psi; \Delta; \Phi; \Gamma \vdash e :_{\kappa} \tau \qquad \forall y \in \Gamma.\ \ \Psi; \Delta; \Phi \models \Gamma(y) \sqsubseteq (\Gamma(y))^{\mathbb{S}} : *}{\Psi; \Delta; \Phi; \Gamma, \Gamma' \vdash e :_0 (\tau)^{\mathbb{S}}}$ **nochange**

Assume that $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma, \sigma\Gamma']\!]^{\rho}$ and $\models \sigma\Phi$.
Let $\theta = \theta_1 \cup \theta_2$ where $(m, \theta_1) \in \mathcal{G}[\![\sigma\Gamma]\!]^{\rho}$ and $(m, \theta_2) \in \mathcal{G}[\![\sigma\Gamma']\!]^{\rho}$.
TS: $(m, \theta^{\ulcorner} e^{\urcorner}) \in \ [\![(\sigma\tau)^{\mathbb{S}}]\!]^{\rho,0}_{\varepsilon}$
STS: $(m, \theta_1{}^{\ulcorner} e^{\urcorner}) \in \ [\![(\sigma\tau)^{\mathbb{S}}]\!]^{\rho,0}_{\varepsilon}$ since e doesn't have any free variables from Γ'.
Unrolling the definition of $[\![\cdot]\!]^{\rho,\cdot}_{\varepsilon}$, assume that $\mathrm{L}(\theta^{\ulcorner} e^{\urcorner}) \Downarrow v, T$ $(\star)$ where $j = |T| < m$.
By IH on premise with θ_1, we get $(m, \theta_1{}^{\ulcorner} e^{\urcorner}) \in \ [\![\sigma\tau]\!]^{\rho,\sigma\kappa}_{\varepsilon}$.
Unrolling this definition the premise marked $(\star)$, we get

a) $\langle T, \theta_1{}^{\ulcorner} e^{\urcorner} \rangle \curvearrowright \boldsymbol{w}', T', c'$
b) $\mathrm{R}(\theta_1{}^{\ulcorner} e^{\urcorner}) \Downarrow v', T'$
c) $v = \mathrm{L}(\boldsymbol{w}') \ \wedge\ v' = \mathrm{R}(\boldsymbol{w}')$
d) $c' \leq \sigma\kappa$
e) $(m - j, \boldsymbol{w}') \in \ [\![\sigma\tau]\!]^{\rho}_{v}$

Then,

1. follows immediately from a)
2. follows immediately from b)
3. follows immediately from c)
4. $c' = 0$ as shown in 5.
5. TS: $(m - j, \boldsymbol{w}') \in \ [\![(\sigma\tau)^{\mathbb{S}}]\!]^{\rho}_{v}$. Using e), STS: $\mathtt{stable}(\boldsymbol{w}')$. From Lemma 19 and the premises of the typing rule, we get $\mathtt{stable}(\theta_1{}^{\ulcorner} e^{\urcorner})$. Using Lemma Lemma 12 and a), we get $\mathtt{stable}(\boldsymbol{w}')$, we get $\mathtt{stable}(\boldsymbol{w}')$ and $c' = 0$.

Case $\dfrac{\Delta; \Phi; x : \tau_1, f : (\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{S}}, \Gamma \vdash e :_{\kappa} \tau_2 \qquad \forall y \in \Gamma.\ \ \Psi; \Delta; \Phi \models \Gamma(y) \sqsubseteq (\Gamma(y))^{\mathbb{S}} : *}{\Psi; \Delta; \Phi; \Gamma, \Gamma' \vdash \mathtt{fix}\ \ f(x).\, e :_0 (\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{S}}}$ **fix2**

Assume that $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma, \sigma\Gamma']\!]^\rho$ and $\models \sigma\Phi$.
Let $\theta = \theta_1 \cup \theta_2$ where $(m, \theta_1) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $(m, \theta_2) \in \mathcal{G}[\![\sigma\Gamma']\!]^\rho$.
TS: $(m, \theta \ulcorner \texttt{fix}\ \ f(x).\, e \urcorner) \in\ [\![(\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2)^{\mathbb{S}}]\!]^{\rho,0}_{\varepsilon}$.
STS: $(m, \theta_1 \ulcorner \texttt{fix}\ \ f(x).\, e \urcorner) \in\ [\![(\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2)^{\mathbb{S}}]\!]^{\rho}_{v}$ by Lemma 14 and $\forall z \in \Gamma', z \notin FV(e)$.
We prove by subinduction on k that $\forall k \leq m.\ (k, \theta_1 \ulcorner \texttt{fix}\ \ f(x).\, e \urcorner) \in\ [\![(\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2)^{\mathbb{S}}]\!]^{\rho}_{v}$.
Let $F = \theta_1 \ulcorner \texttt{fix}\ \ f(x).\, e \urcorner$.

subcase 1: $k = 0$.

Unfolding the definition of $[\![\cdot]\!]^\rho_v$ at function types, we only need to show that $\texttt{stable}(F)$.
This follows from Lemma 19 and the assumption $\forall y \in \Gamma.\ \Delta; \Phi \models \Gamma(y) \sqsubseteq (\Gamma(y))^{\mathbb{S}} : *$.

subcase 2: $k + 1 \leq m$

By subinduction hypothesis, $(k, F) \in\ [\![(\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2)^{\mathbb{S}}]\!]^{\rho}_{v}$, i.e. $(k, F) \in\ [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^{\rho}_{v}$ ($\star$) and $\texttt{stable}(F)$ ($\star\star$)
STS: $(k + 1, F) \in\ [\![(\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2)^{\mathbb{S}}]\!]^{\rho}_{v}$
STS: $(k + 1, F) \in\ [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^{\rho}_{v}$ and $\texttt{stable}(F)$
By ($\star\star$), $\texttt{stable}(F)$. STS: $(k + 1, F) \in\ [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^{\rho}_{v}$.
Following the definition $[\![\cdot]\!]^\rho_v$, pick $j < k + 1$. Then, $j \leq k$ and $j \leq m$.
Assume that $(j, w) \in\ [\![\sigma\tau_1]\!]^{\rho}_{v}$.
STS: $(j, \theta_1 \ulcorner e \urcorner[F/f, w/x]) \in\ [\![\sigma\tau_2]\!]^{\rho,\sigma\kappa}_{\varepsilon}$ ($\star\star\star$).
We instantiate the IH on the premise using:

- $\sigma \in \mathcal{D}[\![\Delta]\!]$
- $(j, \theta_1[f \mapsto F, x \mapsto w]) \in \mathcal{G}[\![\sigma(\Gamma, x : \tau_1, f : F)]\!]^\rho$, which holds because
  $(j, \theta_1) \in \mathcal{G}[\![\Gamma]\!]^\rho$ by Lemma 8 applied to $(m, \theta_1) \in \mathcal{G}[\![\Gamma]\!]^\rho$ and $j < m$,
  $(j, w) \in\ [\![\sigma\tau_1]\!]^{\rho}_{v}$ and
  $(j, F) \in\ [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^{\rho}_{v}$ (obtained by instantiating Lemma 9 applied to $\Psi; \Delta; \Phi \vdash \tau_1 \xrightarrow{\kappa} \tau_2 : *$ (obtained by Lemma 11) using ($\star$) and $j \leq k$)

We immediately get $(j, \theta[f \mapsto F, x \mapsto w] \ulcorner e \urcorner) \in\ [\![\sigma\tau_2]\!]^{\rho,\sigma\kappa}_{\varepsilon}$ which is the same as ($\star\star\star$).

Proof of statement 2:

Case $\dfrac{}{\Psi; \Delta; \Phi; \Gamma \vdash \texttt{keep(r)} \gg (\texttt{real})^{\mathbb{S}}}$ **keep-r**
TS: $(m, \theta\ \texttt{keep(r)}) \in\ [\![(\texttt{real})^{\mathbb{S}}]\!]^{\rho}_{v}$.
This follows from the definition of $[\![(\texttt{real})^{\mathbb{S}}]\!]^{\rho}_{v}$.

Case $\dfrac{}{\Psi; \Delta; \Phi; \Gamma \vdash \texttt{repl(r, r')} \gg (\texttt{real})^{\mathbb{C}}}$ **repl-r**
TS: $(m, \theta\ \texttt{repl(r, r')}) \in\ [\![(\texttt{real})^{\mathbb{C}}]\!]^{\rho}_{v}$.
This follows from the definition of $[\![(\texttt{real})^{\mathbb{C}}]\!]^{\rho}_{v}$.

Case $\dfrac{\Psi; \Delta; \Phi; x : \tau_1, f : \tau_1 \xrightarrow{\kappa} \tau_2, \Gamma \vdash \text{æ} \gg_\kappa \tau_2}{\Psi; \Delta; \Phi; \Gamma \vdash \texttt{fix}\ f(x).\text{æ} \gg \tau_1 \xrightarrow{\kappa} \tau_2}$ **fix1**

Assume that $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$.

TS: $(m, \theta(\texttt{fix}\ f(x).\text{æ})) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^\rho_v$.

Let $F = \theta(\texttt{fix}\ f(x).\text{æ})$.

We prove by subinduction on k that $\forall k \leq m.\ (k, F) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^\rho_v$.

subcase 1: $k = 0$ is vacuous by the definition of $[\![\cdot]\!]^\rho_v$.

subcase 2: $k + 1 \leq m$

From the subinduction hypothesis, we assume that $(k, F) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^\rho_v$ ($\star$).

STS: $(k+1, F) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^\rho_v$.

Following the definition of $[\![\cdot]\!]^\rho_v$, pick $j < k + 1$. Then, $j \leq k$ and $j \leq m$.

Assume that $(j, \boldsymbol{w}) \in [\![\sigma\tau_1]\!]^\rho_v$.

STS: $(j, \theta\text{æ}[F/f, \boldsymbol{w}/x]) \in [\![\sigma\tau_2]\!]^{\rho,\sigma\kappa}_\varepsilon$ ($\star\star$).

Now, we instantiate IH(3) on the premise using:

- $\sigma \in \mathcal{D}[\![\Delta]\!]$
- $(j, \theta[f \mapsto F, x \mapsto \boldsymbol{w}]) \in \mathcal{G}[\![\sigma(\Gamma, x : \tau_1, f : F)]\!]^\rho$, which holds because
  $(j, \theta) \in \mathcal{G}[\![\Gamma]\!]^\rho$ by Lemma 8 on $(m, \theta) \in \mathcal{G}[\![\Gamma]\!]^\rho$,
  $(j, \boldsymbol{w}) \in [\![\sigma\tau_1]\!]^\rho_v$ and
  $(j, F) \in [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^\rho_v$ (obtained by instantiating Lemma 9 applied to $\Psi; \Delta; \Phi \vdash \tau_1 \xrightarrow{\kappa} \tau_2 : *$ (obtained by Lemma 11) using ($\star$) and $j \leq k$)

We immediately get $(j, \theta[f \mapsto F, x \mapsto \boldsymbol{w}]\text{æ}) \in [\![\sigma\tau_2]\!]^{\rho,\sigma\kappa}_\varepsilon$, which is the same as ($\star\star$).

Case $\dfrac{X : K, \Psi; \Delta; \Phi; \Gamma \vdash \text{æ} \gg_\kappa \tau}{\Psi; \Delta; \Phi; \Gamma \vdash \nu.\text{æ} \gg \forall X \overset{\kappa}{:} K.\tau}$ **tylam**

Assume that $\rho \in \mathcal{T}[\![\Psi]\!]$ and $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$.

TS: $(m, \nu.\theta\text{æ}) \in [\![\forall X \overset{\sigma\kappa}{:} K.\sigma\tau]\!]^\rho_v$.

Unrolling the definition of $[\![\cdot]\!]^\rho_v$, assume that $R \in [\![K]\!]_K$.

STS: $(m, \theta\text{æ}) \in [\![\sigma\tau]\!]^{\sigma\kappa, \rho[X \mapsto R]}_\varepsilon$

This follows from the IH instantiated with the substitution $\rho[X \mapsto R] \in \mathcal{T}[\![X : K, \Psi]\!]$.

Case $\dfrac{\Psi; \Delta; \Phi; \Gamma \vdash \boldsymbol{w} \gg \tau \qquad \forall z \in \Gamma.\ \ \Psi; \Delta; \Phi \models \Gamma(z) \sqsubseteq (\Gamma(z))^{\mathbb{S}} : * \qquad \texttt{stable}(\boldsymbol{w})}{\Psi; \Delta; \Phi; \Gamma, \Gamma' \vdash \boldsymbol{w} \gg (\tau)^{\mathbb{S}}}$ **nochange**

Assume that $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m, \theta) \in \mathcal{G}[\![\sigma\Gamma, \sigma\Gamma']\!]^\rho$ and $\models \sigma\Phi$.

Let $\theta = \theta_1 \cup \theta_2$ where $(m, \theta_1) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $(m, \theta_2) \in \mathcal{G}[\![\sigma\Gamma']\!]^\rho$.

TS: $(m, \theta\boldsymbol{w}) \in [\![(\sigma\tau)^{\mathbb{S}}]\!]^\rho_v$.

STS: $(m, \theta_1\boldsymbol{w}) \in [\![\sigma\tau]\!]^\rho_v$ and $\texttt{stable}(\theta_1\boldsymbol{w})$, since $\boldsymbol{w}$ doesn't have any free variables from Γ'.

By Lemma 19 on $\texttt{stable}(\boldsymbol{w})$ and $\forall z \in \Gamma.\ \Delta; \Phi \models \Gamma(z) \sqsubseteq (\Gamma(z))^{\mathbb{S}} : *$, we get $\texttt{stable}(\theta_1\boldsymbol{w})$.

By IH on $\boldsymbol{w}$, we get $(m, \theta_1\boldsymbol{w}) \in [\![\sigma\tau]\!]^\rho_v$.

Case $\dfrac{\begin{array}{c}\Psi;\Delta;\Phi;x:\tau_1, f:(\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{S}}, \Gamma \vdash \text{æ} \gg_\kappa \tau_2 \\ \forall z \in \Gamma.\quad \Psi;\Delta;\Phi \models \Gamma(z) \sqsubseteq (\Gamma(z))^{\mathbb{S}} : * \qquad \texttt{stable}(\text{æ})\end{array}}{\Psi;\Delta;\Phi;\Gamma,\Gamma' \vdash \texttt{fix}\ \ f(x).\,\text{æ} \gg (\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{S}}}$ **fix2**

Assume that $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m,\theta) \in \mathcal{G}[\![\sigma\Gamma, \sigma\Gamma']\!]^\rho$ and $\models \sigma\Phi$.
Let $\theta = \theta_1 \cup \theta_2$ where $(m,\theta_1) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $(m,\theta_2) \in \mathcal{G}[\![\sigma\Gamma']\!]^\rho$.
TS: $(m, \theta(\texttt{fix}\ f(x).\text{æ})) \in\ [\![(\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2)^{\mathbb{S}}]\!]^\rho_v$
STS: $(m, \theta_1(\texttt{fix}\ f(x).\text{æ})) \in\ [\![(\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2)^{\mathbb{S}}]\!]^\rho_v$ since æ doesn't have any free variables from Γ'.
Let $F = \theta_1(\texttt{fix}\ f(x).\text{æ})$.
We prove by subinduction on k that $\forall k \leq m.\ (k, F) \in\ [\![(\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2)^{\mathbb{S}}]\!]^\rho_v$.

subcase 1: $k = 0$

We only need to show $\texttt{stable}(F)$. This follows from Lemma 19 applied to the premise $\texttt{stable}(\text{æ})$ and $\forall z \in \Gamma.\ \Delta;\Phi \models \Gamma(z) \sqsubseteq (\Gamma(z))^{\mathbb{S}} : *$.

subcase 2: $k + 1 \leq m$

By subinduction hypothesis, assume that $(k, F) \in\ [\![(\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2)^{\mathbb{S}}]\!]^\rho_v$, i.e., $(k, F) \in\ [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^\rho_v$ $(*)$ and $\texttt{stable}(F)$ $(**)$.
STS: $(k+1, F) \in\ [\![(\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2)^{\mathbb{S}}]\!]^\rho_v$.
STS: $(k+1, F) \in\ [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^\rho_v$ and $\texttt{stable}(F)$.
By $(**)$, $\texttt{stable}(F)$. STS: $(k+1, F) \in\ [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^\rho_v$.
Following the definition of $[\![\cdot]\!]^\rho_v$, pick $j < k+1$. Then, $j \leq k$ and $j \leq m$.
Assume that $(j, w) \in\ [\![\sigma\tau_1]\!]^\rho_v$.
TS: $(j, \theta_1 \text{æ}[F/f, w/x]) \in\ [\![\sigma\tau_2]\!]^{\rho,\sigma\kappa}_\varepsilon$ $(***)$.
We instantiate IH(3) on the premise $\Delta;\Phi;x:\tau_1, f:(\tau_1 \xrightarrow{\kappa} \tau_2)^{\mathbb{S}}, \Gamma \vdash \text{æ} \gg_\kappa \tau_2$ using:

- $\sigma \in \mathcal{D}[\![\Delta]\!]$
- $(j, \theta_1[f \mapsto F, x \mapsto w]) \in \mathcal{G}[\![\sigma(\Gamma, x:\tau_1, f:F)]\!]^\rho$, which holds since
  $(j, \theta_1) \in \mathcal{G}[\![\Gamma]\!]^\rho$ by Lemma 8 applied to $(m, \theta_1) \in \mathcal{G}[\![\Gamma]\!]^\rho$ and $j \leq m$,
  $(j, w) \in\ [\![\sigma\tau_1]\!]^\rho_v$ and
  $(j, F) \in\ [\![\sigma\tau_1 \xrightarrow{\sigma\kappa} \sigma\tau_2]\!]^\rho_v$ (obtained by instantiating Lemma 9 applied to $\Psi;\Delta;\Phi \vdash \tau_1 \xrightarrow{\kappa} \tau_2 : *$ (obtained by Lemma 11) using ($\star$) and $j \leq k$)

We immediately get $(j, \theta_1[f \mapsto F, x \mapsto w]\text{æ}) \in\ [\![\sigma\tau_2]\!]^{\rho,\sigma\kappa}_\varepsilon$ which is the same as $(***)$.

Case $\dfrac{\Psi;\Delta;\Phi;\Gamma \vdash w \gg \tau \qquad \Psi;\Delta;\Phi \models \tau \sqsubseteq \tau' : *}{\Psi;\Delta;\Phi;\Gamma \vdash w \gg \tau'}$ $\sqsubseteq : *$

Assume that $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m,\theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$.
TS: $(m, \theta w) \in\ [\![\sigma\tau']\!]^\rho_v$.
By IH on the premise, $(m, \theta w) \in\ [\![\sigma\tau]\!]^\rho_v$.
By Lemma 17 $(m, \theta w) \in\ [\![\sigma\tau']\!]^\rho_v$.

Proof of statement 3:

There is only one case:

Case $\dfrac{\Psi;\Delta;\Phi;\Gamma \vdash \boldsymbol{w}_i \gg \tau_i \qquad \Psi;\Delta;\Phi;\overline{x_i : \tau_i},\Gamma \vdash e :_\kappa \tau}{\Psi;\Delta;\Phi;\Gamma \vdash \ulcorner e \urcorner[\overline{\boldsymbol{w}_i/x_i}] \gg_\kappa \tau}$ **exp**

Assume that $\sigma \in \mathcal{D}[\![\Delta]\!]$ and $(m,\theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$ and $\models \sigma\Phi$.

TS: $(m, \theta\ulcorner e \urcorner[\overline{\theta \boldsymbol{w}_i/x_i}]) \in \ [\![\sigma\tau]\!]_\varepsilon^{\rho,\sigma\kappa}$ $(*)$.

By IH(2) on premise $\Psi;\Delta;\Phi;\Gamma \vdash \boldsymbol{w}_i \gg \tau_i$, we get $(m, \theta\boldsymbol{w}_i) \in \ [\![\sigma\tau_i]\!]_v^\rho$.

By IH(1) on premise $\Delta;\Phi;\overline{x_i : \tau_i},\Gamma \vdash e :_\kappa \tau$ using

$\sigma \in \mathcal{D}[\![\Delta]\!]$,

$(m, \theta[x_i \mapsto \theta\boldsymbol{w}_i]) \in \mathcal{G}[\![x_i : \sigma\tau_i, \sigma\Gamma]\!]^\rho$ (since $(m, \theta\boldsymbol{w}_i) \in \ [\![\sigma\tau_i]\!]_v^\rho$ and $(m,\theta) \in \mathcal{G}[\![\sigma\Gamma]\!]^\rho$) and

$\models \sigma\Phi$,

we get $(m, \theta[x_i \mapsto \theta\boldsymbol{w}_i]\ulcorner e \urcorner) \in \ [\![\sigma\tau]\!]_\varepsilon^{\rho,\sigma\kappa}$ which is the same as $(*)$.

□

Corollary 22 (Type soundness)
Suppose:

$x : \tau \vdash e :_\kappa \tau'$

$\vdash \boldsymbol{w} \gg \tau$

$e[\mathrm{L}(\boldsymbol{w})/x] \Downarrow v', T$

Then, there exist T', c and $\boldsymbol{w}'$ such that

1: $\langle T, \ulcorner e \urcorner[\boldsymbol{w}/x]\rangle \curvearrowright \boldsymbol{w}', T', c$

2: $e[\mathrm{R}(\boldsymbol{w})/x] \Downarrow \mathrm{R}(\boldsymbol{w}'), T'$

3: $c \leq \kappa$

Proof. Immediate from the fundamental theorem (Theorem 21) statements (1) and (2), choosing any step index m greater than $|T|$. □