State-Dependent Representation Independence (Technical Appendix)

Amal Ahmed
TTI-C
amal@tti-c.org

Derek Dreyer
MPI-SWS
dreyer@mpi-sws.mpg.de

Andreas Rossberg
MPI-SWS
rossberg@mpi-sws.mpg.de

August 4, 2008

Contents

1 The Language $\mathsf{F}^{\mu!}$

1.1 Syntax, Dynamic Semantics and Static Semantics

Types	τ	::=	$\alpha \mid \mathsf{unit} \mid \mathsf{int} \mid \mathsf{bool} \mid \tau_1 \times \tau_2 \mid \tau_1 + \tau_2 \mid \tau_1 \to \tau_2 \mid$ $\forall\alpha.\,\tau \mid \exists\alpha.\,\tau \mid \mu\alpha.\,\tau \mid \mathsf{ref}\,\tau$
Prim Ops	o	::=	$+ \mid - \mid = \mid < \mid \leq \mid \ldots$
Expressions	e	::=	$x \mid () \mid l \mid n \mid o(e_1, \ldots, e_n) \mid$ $\mathtt{true} \mid \mathtt{false} \mid \mathtt{if}\, e\, \mathtt{then}\, e_1\, \mathtt{else}\, e_2 \mid$ $\langle e_1, e_2\rangle \mid \mathtt{fst}\, e \mid \mathtt{snd}\, e \mid$ $\mathtt{inl}\, e \mid \mathtt{inr}\, e \mid \mathtt{case}\, e\, \mathtt{of}\, \mathtt{inl}\, x_1 \Rightarrow e_1 \mid \mathtt{inr}\, x_2 \Rightarrow e_2 \mid$ $\lambda x:\tau.\, e \mid e_1\, e_2 \mid \Lambda\alpha.\, e \mid e\,[\tau] \mid$ $\mathtt{pack}\,\tau_1, e\,\mathsf{as}\,\exists\alpha.\,\tau \mid \mathtt{unpack}\, e_1\,\mathsf{as}\,\alpha, x\,\mathtt{in}\, e_2 \mid$ $\mathtt{fold}\, e \mid \mathtt{unfold}\, e \mid$ $\mathtt{ref}\, e \mid \mathtt{!}e \mid e_1 \mathtt{:=} e_2 \mid e_1 \mathtt{==} e_2$
Values	v	::=	$() \mid l \mid n \mid \mathtt{true} \mid \mathtt{false} \mid \langle v_1, v_2\rangle \mid \mathtt{inl}\, v \mid \mathtt{inr}\, v \mid$ $\lambda x:\tau.\, e \mid \Lambda\alpha.\, e \mid \mathtt{pack}\,\tau_1, v\,\mathsf{as}\,\exists\alpha.\,\tau \mid \mathtt{fold}\, v$
Eval. Contexts	E	::=	$[\cdot] \mid o(v_1, \ldots, v_{i-1}, E, e_{i+1}, \ldots, e_n) \mid$ $\mathtt{if}\, E\, \mathtt{then}\, e_1\, \mathtt{else}\, e_2 \mid$ $\langle E, e_2\rangle \mid \langle v_1, E\rangle \mid \mathtt{fst}\, E \mid \mathtt{snd}\, E \mid$ $\mathtt{inl}\, E \mid \mathtt{inr}\, E \mid \mathtt{case}\, E\, \mathtt{of}\, \mathtt{inl}\, x_1 \Rightarrow e_1 \mid \mathtt{inr}\, x_2 \Rightarrow e_2 \mid$ $E\, e \mid v\, E \mid E\,[\tau] \mid$ $\mathtt{pack}\,\tau_1, E\,\mathsf{as}\,\exists\alpha.\,\tau \mid \mathtt{unpack}\, E\,\mathsf{as}\,\alpha, x\,\mathtt{in}\, e_2 \mid \mathtt{fold}\, E \mid$ $\mathtt{ref}\, E \mid \mathtt{!}E \mid E \mathtt{:=} e \mid v \mathtt{:=} E \mid E \mathtt{==} e \mid v \mathtt{==} E$

Figure 1: $\mathsf{F}^{\mu!}$ Syntax

$\boxed{s, e \longmapsto s', v}$

$$
\begin{array}{rcll}
s, \texttt{if true then } e_1 \texttt{ else } e_2 & \longmapsto & s, e_1 & \\
s, \texttt{if false then } e_1 \texttt{ else } e_2 & \longmapsto & s, e_2 & \\
s, \texttt{fst}\,\langle v_1, v_2\rangle & \longmapsto & s, v_1 & \\
s, \texttt{snd}\,\langle v_1, v_2\rangle & \longmapsto & s, v_2 & \\
s, \texttt{case}\,(\texttt{inl}\,v)\,\texttt{of inl}\,x_1 \Rightarrow e_1 \mid \texttt{inr}\,x_2 \Rightarrow e_2 & \longmapsto & s, [v/x_1]e_1 & \\
s, \texttt{case}\,(\texttt{inr}\,v)\,\texttt{of inl}\,x_1 \Rightarrow e_1 \mid \texttt{inr}\,x_2 \Rightarrow e_2 & \longmapsto & s, [v/x_2]e_2 & \\
s, (\lambda x : \tau.\, e)\, v & \longmapsto & s, [v/x]e & \\
s, (\Lambda\alpha.\, e)\,[\tau] & \longmapsto & s, [\tau/\alpha]e & \\
s, \texttt{unpack}\,(\texttt{pack}\,\tau, v\,\texttt{as}\,\exists\alpha.\,\tau_1)\,\texttt{as}\,\alpha, x\,\texttt{in}\,e & \longmapsto & s, [\tau/\alpha][v/x]e & \\
s, \texttt{unfold}\,(\texttt{fold}\,v) & \longmapsto & s, v & \\
s, l \texttt{ == } l & \longmapsto & s, \texttt{true} & \\
s, l \texttt{ == } l' & \longmapsto & s, \texttt{false} & \text{where } l \neq l'
\end{array}
$$

$$
\frac{l \notin \mathrm{dom}(s)}{s, \texttt{ref}\,v \;\longmapsto\; s[l \mapsto v], l}
\qquad
\frac{s(l) = v}{s, \texttt{!}l \;\longmapsto\; s, v}
\qquad
\frac{l \in \mathrm{dom}(s)}{s, l \texttt{ := } v \;\longmapsto\; s[l \mapsto v], ()}
$$

$$
\frac{s, e \;\longmapsto\; s', e'}{s, E[e] \;\longmapsto\; s', E[e']}
$$

Figure 2: $\mathsf{F}^{\mu\mathsf{I}}$ Dynamic Semantics

Notation The notation $s, e \longmapsto s', e'$ denotes a single operational step. We write $s, e \longmapsto^j s', e'$ to denote there there exists a chain of j steps of the form $s, e \longmapsto s_1, e_1 \longmapsto \ldots \longmapsto s_j, e_j$ where $s_j = s'$ and $e_j = e'$. We also use the following abbreviations (where $\mathrm{val}(e)$ denotes that e is a value).

$$
\begin{array}{rcl}
s, e \longmapsto^* s', e' & \stackrel{\text{def}}{=} & \exists k \geq 0.\ s, e \longmapsto^k s', e' \\
s, e \Downarrow s', e' & \stackrel{\text{def}}{=} & s, e \longmapsto^* s', e' \ \wedge\ \mathrm{val}(e') \\
s, e \Downarrow & \stackrel{\text{def}}{=} & \exists s', e'.\ s, e \Downarrow s', e'
\end{array}
$$

$$
\begin{array}{llll}
\textit{Type Context} & \Delta & ::= & \cdot \mid \Delta, \alpha \\
\textit{Value Context} & \Gamma & ::= & \cdot \mid \Gamma, x : \tau \\
\textit{Store Typing} & \Sigma & ::= & \cdot \mid \Sigma, l : \tau \qquad \text{where } FTV(\tau) = \emptyset
\end{array}
$$

$\boxed{\Delta \vdash \tau}$

$$
\frac{\alpha \in \Delta}{\Delta \vdash \alpha} \qquad \frac{}{\Delta \vdash \mathsf{unit}} \qquad \frac{}{\Delta \vdash \mathsf{int}} \qquad \frac{}{\Delta \vdash \mathsf{bool}} \qquad \frac{\Delta \vdash \tau_1 \qquad \Delta \vdash \tau_2}{\Delta \vdash \tau_1 \times \tau_2} \qquad \frac{\Delta \vdash \tau_1 \qquad \Delta \vdash \tau_2}{\Delta \vdash \tau_1 + \tau_2}
$$

$$
\frac{\Delta \vdash \tau_1 \qquad \Delta \vdash \tau_2}{\Delta \vdash \tau_1 \to \tau_2} \qquad \frac{\Delta, \alpha \vdash \tau}{\Delta \vdash \forall \alpha.\, \tau} \qquad \frac{\Delta, \alpha \vdash \tau}{\Delta \vdash \exists \alpha.\, \tau} \qquad \frac{\Delta, \alpha \vdash \tau}{\Delta \vdash \mu \alpha.\, \tau} \qquad \frac{\Delta \vdash \tau}{\Delta \vdash \mathsf{ref}\, \tau}
$$

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

$$
\frac{}{\Delta \vdash \cdot} \qquad \frac{\Delta \vdash \Gamma \qquad \Delta \vdash \tau}{\Delta \vdash \Gamma, x : \tau}
$$

Figure 3: $\mathsf{F}^{\mu!}$ Static Semantics I

$\boxed{\Delta; \Gamma; \Sigma \vdash e : \tau}$

$$\frac{\Gamma(x) = \tau}{\Delta; \Gamma; \Sigma \vdash x : \tau} \qquad \frac{}{\Delta; \Gamma; \Sigma \vdash () : \mathsf{unit}} \qquad \frac{\Sigma(l) = \tau}{\Delta; \Gamma; \Sigma \vdash l : \mathsf{ref}\, \tau} \qquad \frac{}{\Delta; \Gamma; \Sigma \vdash n : \mathsf{int}}$$

$$\frac{}{\Delta; \Gamma; \Sigma \vdash \mathtt{true} : \mathsf{bool}} \qquad \frac{}{\Delta; \Gamma; \Sigma \vdash \mathtt{false} : \mathsf{bool}} \qquad \frac{\Delta; \Gamma; \Sigma \vdash e : \mathsf{bool} \qquad \Delta; \Gamma; \Sigma \vdash e_1 : \tau \qquad \Delta; \Gamma; \Sigma \vdash e_2 : \tau}{\Delta; \Gamma; \Sigma \vdash \mathtt{if}\, e\, \mathtt{then}\, e_1\, \mathtt{else}\, e_2 : \tau}$$

$$\frac{\Delta; \Gamma; \Sigma \vdash e_1 : \tau_1 \qquad \Delta; \Gamma; \Sigma \vdash e_2 : \tau_2}{\Delta; \Gamma; \Sigma \vdash \langle e_1, e_2 \rangle : \tau_1 \times \tau_2} \qquad \frac{\Delta; \Gamma; \Sigma \vdash e : \tau_1 \times \tau_2}{\Delta; \Gamma; \Sigma \vdash \mathtt{fst}\, e : \tau_1} \qquad \frac{\Delta; \Gamma; \Sigma \vdash e : \tau_1 \times \tau_2}{\Delta; \Gamma; \Sigma \vdash \mathtt{snd}\, e : \tau_2}$$

$$\frac{\Delta; \Gamma; \Sigma \vdash e : \tau_1}{\Delta; \Gamma; \Sigma \vdash \mathtt{inl}\, e : \tau_1 + \tau_2} \qquad \frac{\Delta; \Gamma; \Sigma \vdash e : \tau_2}{\Delta; \Gamma; \Sigma \vdash \mathtt{inr}\, e : \tau_1 + \tau_2}$$

$$\frac{\Delta; \Gamma; \Sigma \vdash e : \tau_1 + \tau_2 \qquad \Delta; \Gamma, x_1 : \tau_1; \Sigma \vdash e_1 : \tau \qquad \Delta; \Gamma, x_2 : \tau_2; \Sigma \vdash e_2 : \tau}{\Delta; \Gamma; \Sigma \vdash \mathtt{case}\, e\, \mathtt{of}\, \mathtt{inl}\, x_1 \Rightarrow e_1 \mid \mathtt{inr}\, x_2 \Rightarrow e_2 : \tau}$$

$$\frac{\Delta; \Gamma, x : \tau_1; \Sigma \vdash e : \tau_2}{\Delta; \Gamma; \Sigma \vdash \lambda x\!:\!\tau_1.\, e : \tau_1 \to \tau_2} \qquad \frac{\Delta; \Gamma; \Sigma \vdash e_1 : \tau_2 \to \tau \qquad \Delta; \Gamma; \Sigma \vdash e_2 : \tau_2}{\Delta; \Gamma; \Sigma \vdash e_1\, e_2 : \tau}$$

$$\frac{\Delta, \alpha; \Gamma; \Sigma \vdash e : \tau}{\Delta; \Gamma; \Sigma \vdash \Lambda\alpha.\, e : \forall\alpha.\, \tau} \qquad \frac{\Delta; \Gamma; \Sigma \vdash e : \forall\alpha.\, \tau \qquad \Delta \vdash \tau_1}{\Delta; \Gamma; \Sigma \vdash e\, [\tau_1] : [\tau_1/\alpha]\tau}$$

$$\frac{\Delta \vdash \tau_1 \qquad \Delta; \Gamma; \Sigma \vdash e : [\tau_1/\alpha]\tau}{\Delta; \Gamma; \Sigma \vdash \mathtt{pack}\, \tau_1, e\, \mathtt{as}\, \exists\alpha.\, \tau : \exists\alpha.\, \tau} \qquad \frac{\Delta; \Gamma; \Sigma \vdash e_1 : \exists\alpha.\, \tau_1 \qquad \Delta \vdash \tau \qquad \Delta, \alpha; \Gamma, x : \tau_1; \Sigma \vdash e_2 : \tau}{\Delta; \Gamma; \Sigma \vdash \mathtt{unpack}\, e_1\, \mathtt{as}\, \alpha, x\, \mathtt{in}\, e_2 : \tau}$$

$$\frac{\Delta; \Gamma; \Sigma \vdash e : [\mu\alpha.\, \tau/\alpha]\tau}{\Delta; \Gamma; \Sigma \vdash \mathtt{fold}\, e : \mu\alpha.\, \tau} \qquad \frac{\Delta; \Gamma; \Sigma \vdash e : \mu\alpha.\, \tau}{\Delta; \Gamma; \Sigma \vdash \mathtt{unfold}\, e : [\mu\alpha.\, \tau/\alpha]\tau}$$

$$\frac{\Delta; \Gamma; \Sigma \vdash e : \tau}{\Delta; \Gamma; \Sigma \vdash \mathtt{ref}\, e : \mathsf{ref}\, \tau} \qquad \frac{\Delta; \Gamma; \Sigma \vdash e : \mathsf{ref}\, \tau}{\Delta; \Gamma; \Sigma \vdash\, !e : \tau} \qquad \frac{\Delta; \Gamma; \Sigma \vdash e_1 : \mathsf{ref}\, \tau \qquad \Delta; \Gamma; \Sigma \vdash e_2 : \tau}{\Delta; \Gamma; \Sigma \vdash e_1 := e_2 : \mathsf{unit}}$$

$$\frac{\Delta; \Gamma; \Sigma \vdash e_1 : \mathsf{ref}\, \tau \qquad \Delta; \Gamma; \Sigma \vdash e_2 : \mathsf{ref}\, \tau}{\Delta; \Gamma; \Sigma \vdash e_1 == e_2 : \mathsf{bool}}$$

$\boxed{\vdash s : \Sigma}$

$$\frac{\forall l \in \mathrm{dom}(\Sigma).\ \cdot; \cdot; \Sigma \vdash s(l) : \Sigma(l)}{\vdash s : \Sigma}$$

Figure 4: $\mathsf{F}^{\mu!}$ Static Semantics II

1.2 Contexts and Contextual Equivalence

$$
\begin{array}{lll}
\textit{Contexts} & C & ::= \\
 & & [\cdot] \mid o(e_1, \ldots, e_{i-1}, C, e_{i+1}, \ldots, e_n) \mid \\
 & & \texttt{if}\, C\, \texttt{then}\, e_1\, \texttt{else}\, e_2 \mid \texttt{if}\, e\, \texttt{then}\, C\, \texttt{else}\, e_2 \mid \texttt{if}\, e\, \texttt{then}\, e_1\, \texttt{else}\, C \mid \\
 & & \langle C, e_2 \rangle \mid \langle e_1, C \rangle \mid \texttt{fst}\, C \mid \texttt{snd}\, C \mid \\
 & & \texttt{inl}\, C \mid \texttt{inr}\, C \mid \texttt{case}\, C\, \texttt{of}\, \texttt{inl}\, x_1 \Rightarrow e_1 \mid \texttt{inr}\, x_2 \Rightarrow e_2 \mid \\
 & & \texttt{case}\, e\, \texttt{of}\, \texttt{inl}\, x_1 \Rightarrow C \mid \texttt{inr}\, x_2 \Rightarrow e_2 \mid \texttt{case}\, e\, \texttt{of}\, \texttt{inl}\, x_1 \Rightarrow e_1 \mid \texttt{inr}\, x_2 \Rightarrow C \mid \\
 & & \lambda x\!:\!\tau.\, C \mid C\, e \mid e\, C \mid \Lambda\alpha.\, C \mid C\,[\tau] \mid \\
 & & \texttt{pack}\, \tau_1, C\, \texttt{as}\, \exists\alpha.\, \tau \mid \texttt{unpack}\, C\, \texttt{as}\, \alpha, x\, \texttt{in}\, e_2 \mid \texttt{unpack}\, e_1\, \texttt{as}\, \alpha, x\, \texttt{in}\, C \mid \\
 & & \texttt{fold}\, C \mid \texttt{unfold}\, C \mid \\
 & & \texttt{ref}\, C \mid \texttt{!}C \mid C\, \texttt{:=}\, e \mid e\, \texttt{:=}\, C \mid C\, \texttt{==}\, e \mid e\, \texttt{==}\, C
\end{array}
$$

Figure 5: $\mathsf{F}^{\mu!}$ Syntax - Contexts

$\boxed{\vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau')}$

$$\frac{\Delta \subseteq \Delta' \qquad \Gamma \subseteq \Gamma' \qquad \Sigma \subseteq \Sigma'}{\vdash [\cdot] : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau)}$$

$$\frac{\vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \mathsf{bool}) \qquad \Delta'; \Gamma'; \Sigma' \vdash e_1 : \tau' \qquad \Delta'; \Gamma'; \Sigma' \vdash e_2 : \tau'}{\vdash \mathtt{if}\, C\, \mathtt{then}\, e_1\, \mathtt{else}\, e_2 : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau')}$$

$$\frac{\Delta'; \Gamma'; \Sigma' \vdash e : \mathsf{bool} \qquad \vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau') \qquad \Delta'; \Gamma'; \Sigma' \vdash e_2 : \tau'}{\vdash \mathtt{if}\, e\, \mathtt{then}\, C\, \mathtt{else}\, e_2 : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau')}$$

$$\frac{\Delta'; \Gamma'; \Sigma' \vdash e : \mathsf{bool} \qquad \Delta'; \Gamma'; \Sigma' \vdash e_1 : \tau' \qquad \vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau')}{\vdash \mathtt{if}\, e\, \mathtt{then}\, e_1\, \mathtt{else}\, C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau')}$$

$$\frac{\vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_1) \qquad \Delta'; \Gamma'; \Sigma' \vdash e_2 : \tau_2}{\vdash \langle C, e_2 \rangle : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_1 \times \tau_2)}$$

$$\frac{\Delta'; \Gamma'; \Sigma' \vdash e_1 : \tau_1 \qquad \vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_2)}{\vdash \langle e_1, C \rangle : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_1 \times \tau_2)}$$

$$\frac{\vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_1 \times \tau_2)}{\vdash \mathtt{fst}\, C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_1)} \qquad \frac{\vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_1 \times \tau_2)}{\vdash \mathtt{snd}\, C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_2)}$$

$$\frac{\vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_1)}{\vdash \mathtt{inl}\, C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_1 + \tau_2)} \qquad \frac{\vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_2)}{\vdash \mathtt{inr}\, C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_1 + \tau_2)}$$

$$\frac{\vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_1 + \tau_2) \qquad \Delta'; \Gamma', x_1 : \tau_1; \Sigma' \vdash e_1 : \tau' \qquad \Delta'; \Gamma', x_2 : \tau_2; \Sigma' \vdash e_2 : \tau'}{\vdash \mathtt{case}\, C\, \mathtt{of}\, \mathtt{inl}\, x_1 \Rightarrow e_1 \mid \mathtt{inr}\, x_2 \Rightarrow e_2 : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau')}$$

$$\frac{\Delta'; \Gamma'; \Sigma' \vdash e : \tau_1 + \tau_2 \qquad \vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma', x_1 : \tau_1; \Sigma' \vdash \tau') \qquad \Delta'; \Gamma', x_2 : \tau_2; \Sigma' \vdash e_2 : \tau'}{\vdash \mathtt{case}\, e\, \mathtt{of}\, \mathtt{inl}\, x_1 \Rightarrow C \mid \mathtt{inr}\, x_2 \Rightarrow e_2 : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau')}$$

$$\frac{\Delta'; \Gamma'; \Sigma' \vdash e : \tau_1 + \tau_2 \qquad \Delta'; \Gamma', x_1 : \tau_1; \Sigma' \vdash e_1 : \tau' \qquad \vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma', x_2 : \tau_2; \Sigma' \vdash \tau')}{\vdash \mathtt{case}\, e\, \mathtt{of}\, \mathtt{inl}\, x_1 \Rightarrow e_1 \mid \mathtt{inr}\, x_2 \Rightarrow C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau')}$$

$$\frac{\vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma', x : \tau_1; \Sigma' \vdash \tau_2)}{\vdash \lambda x : \tau_1 . C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_1 \to \tau_2)}$$

$$\frac{\vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_2 \to \tau') \qquad \Delta'; \Gamma'; \Sigma' \vdash e_2 : \tau_2}{\vdash C\, e_2 : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau')}$$

$$\frac{\Delta'; \Gamma'; \Sigma' \vdash e_1 : \tau_2 \to \tau' \qquad \vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau_2)}{\vdash e_1\, C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau')}$$

Figure 6: $\mathsf{F}^{\mu\mathsf{I}}$ Static Semantics - Contexts I

$\boxed{\vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \tau')}$ (contd.)

$$\frac{\vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta', \alpha;\Gamma';\Sigma' \vdash \tau')}{\vdash \Lambda\alpha.\, C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \forall\alpha.\, \tau')} \qquad \frac{\vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \forall\alpha.\, \tau') \qquad \Delta' \vdash \tau_1}{\vdash C\,[\tau_1] : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash [\tau_1/\alpha]\tau')}$$

$$\frac{\Delta' \vdash \tau_1 \qquad \vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash [\tau_1/\alpha]\tau')}{\vdash \mathtt{pack}\,\tau_1, C\,\mathtt{as}\,\exists\alpha.\,\tau' : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \exists\alpha.\,\tau')}$$

$$\frac{\vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \exists\alpha.\,\tau_1) \qquad \Delta' \vdash \tau' \qquad \Delta', \alpha;\Gamma', x : \tau_1;\Sigma' \vdash e_2 : \tau'}{\vdash \mathtt{unpack}\,C\,\mathtt{as}\,\alpha, x\,\mathtt{in}\,e_2 : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \tau')}$$

$$\frac{\Delta';\Gamma';\Sigma' \vdash e_1 : \exists\alpha.\,\tau_1 \qquad \Delta' \vdash \tau' \qquad \vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta', \alpha;\Gamma', x : \tau_1;\Sigma' \vdash \tau')}{\vdash \mathtt{unpack}\,e_1\,\mathtt{as}\,\alpha, x\,\mathtt{in}\,C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \tau')}$$

$$\frac{\vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash [\mu\alpha.\,\tau'/\alpha]\tau')}{\vdash \mathtt{fold}\,C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \mu\alpha.\,\tau')} \qquad \frac{\vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \mu\alpha.\,\tau')}{\vdash \mathtt{unfold}\,C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash [\mu\alpha.\,\tau'/\alpha]\tau')}$$

$$\frac{\vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \tau')}{\vdash \mathtt{ref}\,C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \mathsf{ref}\,\tau')} \qquad \frac{\vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \mathsf{ref}\,\tau')}{\vdash\, !C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \tau')}$$

$$\frac{\vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \mathsf{ref}\,\tau') \qquad \Delta';\Gamma';\Sigma' \vdash e_2 : \tau'}{\vdash C := e_2 : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \mathsf{unit})}$$

$$\frac{\Delta';\Gamma';\Sigma' \vdash e_1 : \mathsf{ref}\,\tau' \qquad \vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \tau')}{\vdash e_1 := C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \mathsf{unit})}$$

$$\frac{\vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \mathsf{ref}\,\tau') \qquad \Delta';\Gamma';\Sigma' \vdash e_2 : \mathsf{ref}\,\tau'}{\vdash C == e_2 : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \mathsf{bool})}$$

$$\frac{\Delta';\Gamma';\Sigma' \vdash e_1 : \mathsf{ref}\,\tau' \qquad \vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \mathsf{ref}\,\tau')}{\vdash e_1 := C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\Delta';\Gamma';\Sigma' \vdash \mathsf{bool})}$$

Figure 7: $\mathsf{F}^{\mu!}$ Static Semantics - Contexts II

Definition 1.1. (Contextual Approximation & Equivalence)

Let $\Delta;\Gamma;\Sigma \vdash e_1 : \tau$ *and* $\Delta;\Gamma;\Sigma \vdash e_2 : \tau$.

$$\Delta;\Gamma;\Sigma \vdash e_1 \preceq^{ctx} e_2 : \tau \quad \stackrel{\text{def}}{=} \quad \forall C, \Sigma', \tau', s.\ \vdash C : (\Delta;\Gamma;\Sigma \vdash \tau) \Rightarrow (\cdot;\cdot;\Sigma' \vdash \tau') \ \wedge\ \vdash s : \Sigma' \ \wedge\ s, C[e_1] \Downarrow \implies s, C[e_2] \Downarrow$$

$$\Delta;\Gamma;\Sigma \vdash e_1 \approx^{ctx} e_2 : \tau \quad \stackrel{\text{def}}{=} \quad \Delta;\Gamma;\Sigma \vdash e_1 \preceq^{ctx} e_2 : \tau \ \wedge\ \Delta;\Gamma;\Sigma \vdash e_2 \preceq^{ctx} e_1 : \tau$$

2 Step-Indexed Logical Relation for $\mathsf{F}^{\mu!}$

$$
\begin{array}{lrcl}
\textit{Type Interpretation} & \chi & ::= & \{(k, W, e_1, e_2), \dots\} \\
\textit{Store Relation} & \psi & ::= & \{(k, W, s_1, s_2), \dots\} \\
\textit{Population} & V & ::= & \{v_1, \dots\} \\
\textit{Knowledge} & \eta & ::= & (\psi, V, \Sigma_1, \Sigma_2) \\
\textit{Law} & \mathcal{L} & ::= & \{(j, \eta), \dots\} \\
\textit{Island} & w & ::= & (\eta, \mathcal{L}) \\
\textit{World} & W & ::= & \langle w_1, \dots, w_n \rangle
\end{array}
$$

Figure 8: Notation

Preliminaries

- We write $\Sigma \vdash e : \tau$ as shorthand for $\cdot; \cdot; \Sigma \vdash e : \tau$.
- If $W = \langle w_1, \dots, w_n \rangle$ and $1 \le j \le n$, we write $W[j]$ as shorthand for w_j.
- If $w = (\eta_i, \mathcal{L}_i)$ where $\eta_i = (\psi_i, V_i, \Sigma_{i1}, \Sigma_{i2})$, we use the following shorthand to extract various elements out of the island w:

$$
\begin{array}{lcllcl}
w.\eta & \equiv & \eta_i & w.V & \equiv & V_i \\
w.\mathcal{L} & \equiv & \mathcal{L}_i & w.\Sigma_1 & \equiv & \Sigma_{i1} \\
w.\psi & \equiv & \psi_i & w.\Sigma_2 & \equiv & \Sigma_{i2}
\end{array}
$$

- If W is a world with n islands, we also use the following shorthand:

$$
\begin{array}{lcl}
\Sigma_1(W) & \stackrel{\text{def}}{=} & \bigcup_{1 \le j \le n} W[j].\Sigma_1 \\
\Sigma_2(W) & \stackrel{\text{def}}{=} & \bigcup_{1 \le j \le n} W[j].\Sigma_2
\end{array}
$$

- We write *Val* for the set of all values, *Store* for the set of all stores (finite maps from locations to values), and *StoreTy* for the set of store typings (finite maps from locations to closed types).
- We write *Population* for the set of all subsets of *Val* (i.e., $\textit{Population} \stackrel{\text{def}}{=} \mathcal{P}(\textit{Val})$).
- We write *CTerm* for the set of all closed terms, (i.e., terms that may contain locations, but no free type or term variables.
- We use the metavariable χ to denote sets of the form (k, W, e_1, e_2) where k is a natural number (the step index), W is a world, and e_1 and e_2 are closed terms. Given a set χ of this form, we write χ^{val} to denote the subset of χ such that e_1 and e_2 are values.
- We write $S_1 \# S_2$ to denote that the sets S_1 and S_2 are disjoint.

$$
\begin{array}{rcl}
\mathit{CandAtom}_k & \stackrel{\text{def}}{=} & \{(j, W, e_1, e_2) \in \mathbb{N} \times \bigcup_{j<k} \mathit{CandWorld}_j \times \mathit{CTerm} \times \mathit{CTerm} \mid \\
& & \quad j < k \ \wedge \ W \in \mathit{CandWorld}_j\} \\
\mathit{CandType}_k & \stackrel{\text{def}}{=} & \mathcal{P}(\mathit{CandAtom}_k^{\mathsf{val}}) \\
\mathit{CandStoreAtom}_k & \stackrel{\text{def}}{=} & \{(j, W, s_1, s_2) \in \mathbb{N} \times \bigcup_{j<k} \mathit{CandWorld}_j \times \mathit{Store} \times \mathit{Store} \mid \\
& & \quad j < k \ \wedge \ W \in \mathit{CandWorld}_j\} \\
\mathit{CandStoreRel}_k & \stackrel{\text{def}}{=} & \mathcal{P}(\mathit{CandStoreAtom}_k) \\
\mathit{CandKnowledge}_k & \stackrel{\text{def}}{=} & \mathit{CandStoreRel}_k \times \mathit{Population} \times \mathit{StoreTy} \times \mathit{StoreTy} \\
\mathit{CandLawAtom}_k & \stackrel{\text{def}}{=} & \{(j, \eta) \in \mathbb{N} \times \bigcup_{j \le k} \mathit{CandKnowledge}_j \mid \ j \le k \ \wedge \ \eta \in \mathit{CandKnowledge}_j\} \\
\mathit{CandLaw}_k & \stackrel{\text{def}}{=} & \mathcal{P}(\mathit{CandLawAtom}_k) \\
\mathit{CandIsland}_k & \stackrel{\text{def}}{=} & \mathit{CandKnowledge}_k \times \mathit{CandLaw}_k \\
\mathit{CandWorld}_k & \stackrel{\text{def}}{=} & \{W \in \mathit{CandIsland}_k^n \mid \ n \ge 0\}
\end{array}
$$

$$
\begin{array}{rcll}
\mathit{CandAtom}_\omega & \stackrel{\text{def}}{=} & \bigcup_{k\ge 0} \mathit{CandAtom}_k & \\
\mathit{CandType}_\omega & \stackrel{\text{def}}{=} & \mathcal{P}(\mathit{CandAtom}_\omega^{\mathsf{val}}) & \supseteq \ \bigcup_{k\ge 0} \mathit{CandType}_k \\
\mathit{CandStoreAtom}_\omega & \stackrel{\text{def}}{=} & \bigcup_{k\ge 0} \mathit{CandStoreAtom}_k & \\
\mathit{CandStoreRel}_\omega & \stackrel{\text{def}}{=} & \mathcal{P}(\mathit{CandStoreAtom}_\omega) & \supseteq \ \bigcup_{k\ge 0} \mathit{CandStoreRel}_k \\
\mathit{CandKnowledge}_\omega & \stackrel{\text{def}}{=} & \mathit{CandStoreRel}_\omega \times \mathit{Population} \times \mathit{StoreTy} \times \mathit{StoreTy} & \supseteq \ \bigcup_{k\ge 0} \mathit{CandKnowledge}_k \\
\mathit{CandLawAtom}_\omega & \stackrel{\text{def}}{=} & \bigcup_{k\ge 0} \mathit{CandLawAtom}_k & \\
\mathit{CandLaw}_\omega & \stackrel{\text{def}}{=} & \mathcal{P}(\mathit{CandLawAtom}_\omega) & \supseteq \ \bigcup_{k\ge 0} \mathit{CandLaw}_k \\
\mathit{CandIsland}_\omega & \stackrel{\text{def}}{=} & \mathit{CandKnowledge}_\omega \times \mathit{CandLaw}_\omega & \supseteq \ \bigcup_{k\ge 0} \mathit{CandIsland}_k \\
\mathit{CandWorld}_\omega & \stackrel{\text{def}}{=} & \bigcup_{k\ge 0} \mathit{CandWorld}_k &
\end{array}
$$

$$
\begin{array}{rcll}
\lfloor \chi \rfloor_k & \stackrel{\text{def}}{=} & \{(j, W, e_1, e_2) \mid \ j < k \ \wedge \ (j, W, e_1, e_2) \in \chi\} & \\
& \in & \mathit{CandType}_\omega \to \mathit{CandType}_k & \\
\lfloor \psi \rfloor_k & \stackrel{\text{def}}{=} & \{(j, W, s_1, s_2) \mid \ j < k \ \wedge \ (j, W, s_1, s_2) \in \psi\} & \\
& \in & \mathit{CandStoreRel}_\omega \to \mathit{CandStoreRel}_k & \\
\lfloor \eta \rfloor_k & \stackrel{\text{def}}{=} & (\lfloor \psi \rfloor_k, V, \Sigma_1, \Sigma_2) & \text{where } \eta = (\psi, V, \Sigma_1, \Sigma_2) \\
& \in & \mathit{CandKnowledge}_\omega \to \mathit{CandKnowledge}_k & \\
\lfloor \mathcal{L} \rfloor_k & \stackrel{\text{def}}{=} & \{(j, \eta) \mid \ j \le k \ \wedge \ (j, \eta) \in \mathcal{L}\} & \\
& \in & \mathit{CandLaw}_\omega \to \mathit{CandLaw}_k & \\
\lfloor w \rfloor_k & \stackrel{\text{def}}{=} & (\lfloor \eta \rfloor_k, \lfloor \mathcal{L} \rfloor_k) & \text{where } w = (\eta, \mathcal{L}) \\
\lfloor W \rfloor_k & \stackrel{\text{def}}{=} & \langle \lfloor w_1 \rfloor_k, \ldots, \lfloor w_n \rfloor_k \rangle & \text{where } W = \langle w_1, \ldots, w_n \rangle \\
& \in & \mathit{CandWorld}_\omega \to \mathit{CandWorld}_k &
\end{array}
$$

Figure 9: Auxiliary Definitions: Candidate Sets and k-Approximation

$$
\begin{array}{rcl}
(\psi', V', \Sigma_1', \Sigma_2') \sqsupseteq (\psi, V, \Sigma_1, \Sigma_2) & \stackrel{\text{def}}{=} & V' \supseteq V \ \wedge\ \Sigma_1' \supseteq \Sigma_1 \ \wedge\ \Sigma_2' \supseteq \Sigma_2 \\
(\eta', \mathcal{L}') \sqsupseteq (\eta, \mathcal{L}) & \stackrel{\text{def}}{=} & \eta' \sqsupseteq \eta \ \wedge\ \mathcal{L}' = \mathcal{L} \\
\langle w_1', \ldots, w_{n+m}' \rangle \sqsupseteq \langle w_1, \ldots, w_n \rangle & \stackrel{\text{def}}{=} & m \geq 0 \ \wedge\ \forall i \in \{1, \ldots, n\}.\ w_i' \sqsupseteq w_i \\
(j, W') \sqsupseteq (k, W) & \stackrel{\text{def}}{=} & j \leq k \ \wedge\ W' \sqsupseteq \lfloor W \rfloor_j \ \wedge\ W' \in \mathit{World}_j \ \wedge\ W \in \mathit{World}_k
\end{array}
$$

$$
\mathit{Atom}[\tau_1, \tau_2]_k \stackrel{\text{def}}{=} \{(j, W, e_1, e_2) \in \mathit{CandAtom}_k \mid\ W \in \mathit{World}_j \ \wedge\ \Sigma_1(W) \vdash e_1 : \tau_1 \ \wedge\ \Sigma_2(W) \vdash e_2 : \tau_2\}
$$

$$
\begin{array}{rcl}
\mathit{Type}[\tau_1, \tau_2]_k & \stackrel{\text{def}}{=} & \{\chi \in \mathcal{P}(\mathit{Atom}[\tau_1, \tau_2]_k^{\mathsf{val}}) \mid\ \forall (j, W, v_1, v_2) \in \chi. \\
& & \qquad \forall (i, W') \sqsupseteq (j, W).\ (i, W', v_1, v_2) \in \chi\}
\end{array}
$$

$$
\begin{array}{rcl}
\mathit{StoreAtom}_k & \stackrel{\text{def}}{=} & \{(j, W, s_1, s_2) \in \mathit{CandStoreAtom}_k \mid\ W \in \mathit{World}_j\} \\
& \subseteq & \mathit{CandStoreAtom}_k
\end{array}
$$

$$
\begin{array}{rcl}
\mathit{StoreRel}_k & \stackrel{\text{def}}{=} & \{\psi \in \mathcal{P}(\mathit{StoreAtom}_k) \mid\ \forall (j, W, s_1, s_2) \in \psi. \\
& & \qquad \forall (i, W') \sqsupseteq (j, W).\ (i, W', s_1, s_2) \in \psi\} \\
& \subseteq & \mathit{CandStoreRel}_k
\end{array}
$$

$$
\begin{array}{rcl}
\mathit{Knowledge}_k & \stackrel{\text{def}}{=} & \{(\psi, V, \Sigma_1, \Sigma_2) \in \mathit{CandKnowledge}_k \mid\ \psi \in \mathit{StoreRel}_k \ \wedge \\
& & \quad (\forall s_1, s_2, s_1', s_2'. \\
& & \qquad (\forall l \in \mathrm{dom}(\Sigma_1).\ s_1(l) = s_1'(l) \ \wedge\ \forall l \in \mathrm{dom}(\Sigma_2).\ s_2(l) = s_2'(l)\ ) \implies \\
& & \qquad \forall j, W.\ \ (j, W, s_1, s_2) \in \psi \iff (j, W, s_1', s_2') \in \psi\ )\} \\
& \subseteq & \mathit{CandKnowledge}_k
\end{array}
$$

$$
\begin{array}{rcl}
\mathit{LawAtom}_k & \stackrel{\text{def}}{=} & \{(j, \eta) \in \mathit{CandLawAtom}_k \mid\ \eta \in \mathit{Knowledge}_j\} \\
& \subseteq & \mathit{CandLawAtom}_k
\end{array}
$$

$$
\begin{array}{rcl}
\mathit{Law}_k & \stackrel{\text{def}}{=} & \{\mathcal{L} \in \mathcal{P}(\mathit{LawAtom}_k) \mid\ \forall (j, \eta) \in \mathcal{L}.\ \forall i < j.\ (i, \lfloor \eta \rfloor_i) \in \mathcal{L}\} \\
& \subseteq & \mathit{CandLaw}_k
\end{array}
$$

$$
\begin{array}{rcl}
\mathit{Island}_k & \stackrel{\text{def}}{=} & \{(\eta, \mathcal{L}) \in \mathit{Knowledge}_k \times \mathit{Law}_k \mid\ (k, \eta) \in \mathcal{L}\} \\
& \subseteq & \mathit{CandIsland}_k
\end{array}
$$

$$
\begin{array}{rcl}
\mathit{World}_k & \stackrel{\text{def}}{=} & \{W \in \mathit{Island}_k^n \mid\ n \geq 0 \ \wedge \\
& & \quad \forall a, b \in \{1, \ldots, n\}.\ a \neq b \implies \\
& & \qquad \mathrm{dom}(W[a].\Sigma_1) \# \mathrm{dom}(W[b].\Sigma_1) \ \wedge\ \mathrm{dom}(W[a].\Sigma_2) \# \mathrm{dom}(W[b].\Sigma_2)\} \\
& \subseteq & \mathit{CandWorld}_k
\end{array}
$$

$$
\mathit{Type}[\tau_1, \tau_2] \stackrel{\text{def}}{=} \{\chi \in \mathit{CandType}_\omega \mid\ \forall k \geq 0.\ \lfloor \chi \rfloor_k \in \mathit{Type}[\tau_1, \tau_2]_k\} \qquad \supseteq \quad \bigcup_{k \geq 0} \mathit{Type}[\tau_1, \tau_2]_k
$$

Figure 10: Auxiliary Definitions: World Extension and Well-Formedness Conditions

$$s_1, s_2 :_k W \quad \stackrel{\text{def}}{=} \quad \vdash s_1 : \Sigma_1(W) \ \wedge \ \vdash s_2 : \Sigma_2(W) \ \wedge \\ \forall w \in W.\, \forall j < k.\, (j, \lfloor W \rfloor_j, s_1, s_2) \in w.\psi$$

$$(i, W') \sqsupset (j, W) \quad \stackrel{\text{def}}{=} \quad i < j \ \wedge \ (i, W') \sqsupseteq (j, W)$$

Figure 11: Auxiliary Definitions: Relational Store Satisfaction and Strict World Extension

Notation

- A type substitution ρ is a finite map from type variables α to triples (χ, τ_1, τ_2), where τ_1 and τ_2 are closed types and $\chi \in Type[\tau_1, \tau_2]$.
- If $\rho(\alpha) = (\chi, \tau_1, \tau_2)$, then $\rho_1(\alpha)$ denotes τ_1 and $\rho_2(\alpha)$ denotes τ_2.
- Let $\rho = \{\alpha_1 \mapsto (\chi_1, \tau_{11}, \tau_{12}), \ldots, \alpha_n \mapsto (\chi_n, \tau_{n1}, \tau_{n2})\}$. Then
  - ρ_1 denotes $\{\alpha_1 \mapsto \tau_{11}, \ldots, \alpha_n \mapsto \tau_{n1}\}$
  - ρ_2 denotes $\{\alpha_1 \mapsto \tau_{12}, \ldots, \alpha_n \mapsto \tau_{n2}\}$
  - $\rho_1(\tau)$ is shorthand for $[\tau_{11}/\alpha_1, \ldots, \tau_{n1}/\alpha_n]\tau$
  - $\rho_2(\tau)$ is shorthand for $[\tau_{12}/\alpha_1, \ldots, \tau_{n2}/\alpha_n]\tau$
  - $\rho_1(e)$ is shorthand for $[\tau_{11}/\alpha_1, \ldots, \tau_{n1}/\alpha_n]e$
  - $\rho_2(e)$ is shorthand for $[\tau_{12}/\alpha_1, \ldots, \tau_{n2}/\alpha_n]e$
- A relational value substitution γ is a finite map from term variables x to pairs (v_1, v_2) where v_1 and v_2 are closed values (i.e., values that may have free locations, but no free type or term variables).
- If $\gamma(x) = (v_1, v_2)$, then $\gamma_1(x)$ denotes v_1 and $\gamma_2(x)$ denotes v_2.
- Let $\gamma = \{x_1 \mapsto (v_{11}, v_{12}), \ldots, x_n \mapsto (v_{n1}, v_{n2})\}$. Then
  - γ_1 denotes $\{x_1 \mapsto v_{11}, \ldots, x_n \mapsto v_{n1}\}$
  - γ_2 denotes $\{x_1 \mapsto v_{12}, \ldots, x_n \mapsto v_{n2}\}$
  - $\gamma_1(e)$ is shorthand for $[v_{11}/x_1, \ldots, v_{n1}/x_n]e$
  - $\gamma_2(e)$ is shorthand for $[v_{12}/x_1, \ldots, v_{n2}/x_n]e$

$$
\begin{array}{rcl}
\mathcal{V}_n[\![\tau]\!]\,\rho & = & \overline{\mathcal{V}}_n[\![\tau]\!]\,\rho \;\cap\; Atom[\rho_1(\tau),\rho_2(\tau)]_n^{\mathsf{val}} \\[2ex]
\overline{\mathcal{V}}_n[\![\alpha]\!]\,\rho & = & \chi \qquad \text{where } \rho(\alpha) = (\chi,\tau_1,\tau_2) \\[1ex]
\overline{\mathcal{V}}_n[\![\mathsf{unit}]\!]\,\rho & = & \{\,(k,W,(),())\,\} \\[1ex]
\overline{\mathcal{V}}_n[\![\mathsf{int}]\!]\,\rho & = & \{\,(k,W,n,n) \mid\; v \in \mathbb{N}\,\} \\[1ex]
\overline{\mathcal{V}}_n[\![\mathsf{bool}]\!]\,\rho & = & \{\,(k,W,v,v) \mid\; v = \mathtt{true} \;\vee\; v = \mathtt{false}\,\} \\[1ex]
\overline{\mathcal{V}}_n[\![\tau \times \tau']\!]\,\rho & = & \{\,(k,W,\langle v_1,v_1'\rangle,\langle v_2,v_2'\rangle) \mid\; (k,W,v_1,v_2) \in \mathcal{V}_n[\![\tau]\!]\,\rho \;\wedge\; (k,W,v_1',v_2') \in \mathcal{V}_n[\![\tau']\!]\,\rho\,\} \\[1ex]
\overline{\mathcal{V}}_n[\![\tau + \tau']\!]\,\rho & = & \{\,(k,W,\mathtt{inl}\,v_1,\mathtt{inl}\,v_2) \mid\; (k,W,v_1,v_2) \in \mathcal{V}_n[\![\tau]\!]\,\rho\,\} \\
& \cup & \{\,(k,W,\mathtt{inr}\,v_1,\mathtt{inr}\,v_2) \mid\; (k,W,v_1,v_2) \in \mathcal{V}_n[\![\tau']\!]\,\rho\,\} \\[1ex]
\overline{\mathcal{V}}_n[\![\tau \to \tau']\!]\,\rho & = & \{\,(k,W,\lambda x\!:\!\rho_1(\tau).\,e_1,\lambda x\!:\!\rho_2(\tau).\,e_2) \mid \\
& & \quad \forall (j,W') \sqsupset (k,W).\;\forall v_1,v_2. \\
& & \quad\quad (j,W',v_1,v_2) \in \mathcal{V}_n[\![\tau]\!]\,\rho \implies \\
& & \quad\quad (j,W',[v_1/x]e_1,[v_2/x]e_2) \in \mathcal{E}_n[\![\tau']\!]\,\rho\,\} \\[1ex]
\overline{\mathcal{V}}_n[\![\forall\alpha.\,\tau]\!]\,\rho & = & \{\,(k,W,\Lambda\alpha.\,e_1,\Lambda\alpha.\,e_2) \mid \\
& & \quad \forall (j,W') \sqsupset (k,W).\;\forall \tau_1,\tau_2,\chi \in \mathit{Type}[\tau_1,\tau_2]. \\
& & \quad\quad (j,W',[\tau_1/\alpha]e_1,[\tau_2/\alpha]e_2) \in \mathcal{E}_n[\![\tau]\!]\,\rho[\alpha \mapsto (\chi,\tau_1,\tau_2)]\,\} \\[1ex]
\overline{\mathcal{V}}_n[\![\exists\alpha.\,\tau]\!]\,\rho & = & \{\,(k,W,\mathtt{pack}\,\tau_1,v_1\;\mathtt{as}\;\exists\alpha.\,\rho_1(\tau),\mathtt{pack}\,\tau_2,v_2\;\mathtt{as}\;\exists\alpha.\,\rho_2(\tau)) \mid \\
& & \quad \exists\chi \in \mathit{Type}[\tau_1,\tau_2]. \\
& & \quad\quad (k,W,v_1,v_2) \in \mathcal{V}_n[\![\tau]\!]\,\rho[\alpha \mapsto (\chi,\tau_1,\tau_2)]\,\} \\[1ex]
\overline{\mathcal{V}}_n[\![\mu\alpha.\,\tau]\!]\,\rho & = & \{\,(k,W,\mathtt{fold}\,v_1,\mathtt{fold}\,v_2) \mid\; k < n \;\wedge \\
& & \quad \forall j < k.\;(j,\lfloor W\rfloor_j,v_1,v_2) \in \mathcal{V}_k[\![[\mu\alpha.\,\tau/\alpha]\tau]\!]\,\rho\,\} \\[1ex]
\overline{\mathcal{V}}_n[\![\mathsf{ref}\,\tau]\!]\,\rho & = & \{\,(k,W,l_1,l_2) \mid\; k < n \;\wedge\; w_{\mathsf{ref}}(k,\rho,\tau,l_1,l_2) \in W\,\} \\[1ex]
w_{\mathsf{ref}}(k,\rho,\tau,l_1,l_2) & = & (\eta,\mathcal{L}) \quad \text{where } \eta = (\psi,\{\},\{l_1 : \rho_1(\tau)\},\{l_2 : \rho_2(\tau)\}) \;\wedge \\
& & \qquad\qquad \psi = \{\,(j,W',s_1,s_2) \mid\; (j,W',s_1(l_1),s_2(l_2)) \in \mathcal{V}_k[\![\tau]\!]\,\rho\,\} \;\wedge \\
& & \qquad\qquad \mathcal{L} = \{(j,\lfloor\eta\rfloor_j) \mid\; j \le k\} \\[2ex]
\mathcal{E}_n[\![\tau]\!]\,\rho & = & \{\,(k,W,e_1,e_2) \in \mathit{Atom}[\rho_1(\tau),\rho_2(\tau)]_n \mid \\
& & \quad \forall j < k.\;\forall s_1,s_2,s_1',v_1. \\
& & \quad\quad s_1,s_2 :_k W \;\wedge\; s_1,e_1 \longmapsto^j s_1',v_1 \implies \\
& & \quad\quad \exists s_2',v_2,W'. \\
& & \quad\quad\quad s_2,e_2 \longmapsto^* s_2',v_2 \;\wedge \\
& & \quad\quad\quad (k-j,W') \sqsupseteq (k,W) \;\wedge \\
& & \quad\quad\quad s_1',s_2' :_{k-j} W' \;\wedge \\
& & \quad\quad\quad (k-j,W',v_1,v_2) \in \mathcal{V}_n[\![\tau]\!]\,\rho\,\}
\end{array}
$$

Figure 12: Step-Indexed Logical Relations I

$$
\begin{array}{rcl}
\mathcal{V}\,[\![\tau]\!]\,\rho & = & \bigcup_{n\geq 0}\mathcal{V}_n[\![\tau]\!]\,\rho \\
\mathcal{E}\,[\![\tau]\!]\,\rho & = & \bigcup_{n\geq 0}\mathcal{E}_n[\![\tau]\!]\,\rho
\end{array}
$$

$$
\begin{array}{rcl}
\mathcal{D}\,[\![\cdot]\!] & = & \{\,\emptyset\,\} \\
\mathcal{D}\,[\![\Delta,\alpha]\!] & = & \{\,\rho[\alpha\mapsto(\chi,\tau_1,\tau_2)]\mid\ \rho\in\mathcal{D}\,[\![\Delta]\!]\ \wedge\ \chi\in \mathit{Type}[\tau_1,\tau_2]\,\}
\end{array}
$$

$$
\begin{array}{rcl}
\mathcal{G}\,[\![\cdot]\!]\,\rho & = & \{\,(k,W,\emptyset)\mid\ W\in \mathit{World}_k\,\} \\
\mathcal{G}\,[\![\Gamma,x:\tau]\!]\,\rho & = & \{\,(k,W,\gamma[x\mapsto(v_1,v_2)])\mid \\
 & & \qquad (k,W,\gamma)\in\mathcal{G}\,[\![\Gamma]\!]\,\rho\ \wedge\ (k,W,v_1,v_2)\in\mathcal{V}\,[\![\tau]\!]\,\rho\,\}
\end{array}
$$

$$
\mathcal{S}\,[\![\Sigma]\!] \quad = \quad \{(k,W)\mid\ \forall(l:\tau)\in\Sigma.\ (k,W,l,l)\in\mathcal{V}\,[\![\mathsf{ref}\,\tau]\!]\,\emptyset\}
$$

$$
\Delta;\Gamma;\Sigma\vdash e_1\preceq^{log} e_2:\tau \quad\stackrel{\text{def}}{=}\quad \forall k\geq 0.\ \forall\rho,\gamma,W.\\
\qquad \rho\in\mathcal{D}\,[\![\Delta]\!]\ \wedge\ (k,W,\gamma)\in\mathcal{G}\,[\![\Gamma]\!]\,\rho\ \wedge\ (k,W)\in\mathcal{S}\,[\![\Sigma]\!]\implies\\
\qquad (k,W,\rho_1(\gamma_1(e_1)),\rho_2(\gamma_2(e_2)))\in\mathcal{E}\,[\![\tau]\!]\,\rho
$$

$$
\Delta;\Gamma;\Sigma\vdash e_1\approx^{log} e_2:\tau \quad\stackrel{\text{def}}{=}\quad \Delta;\Gamma;\Sigma\vdash e_1\preceq^{log} e_2:\tau\ \ \wedge\ \ \Delta;\Gamma;\Sigma\vdash e_2\preceq^{log} e_1:\tau
$$

Figure 13: Step-Indexed Logical Relations II

3 Logical Relation Proofs

3.1 Basic Properties

3.1.1 Properties of Step-Indexed Construction

Lemma 3.1.

Let $\Delta \vdash \tau$ *and* $\rho \in \mathcal{D}[\![\Delta]\!]$.
If $j \leq k$ *then* $\mathcal{V}_j[\![\tau]\!]\,\rho = \lfloor \mathcal{V}_k[\![\tau]\!]\,\rho \rfloor_j$.

Proof

Proof by induction on the derivation $\Delta \vdash \tau$. □

Lemma 3.2.

Let $\Delta \vdash \tau$ *and* $\rho \in \mathcal{D}[\![\Delta]\!]$ *and* $j, k \in \mathbb{N}$.
Then $\lfloor \mathcal{V}_k[\![\tau]\!]\,\rho \rfloor_j \subseteq \mathcal{V}_k[\![\tau]\!]\,\rho$.

Proof

By definition of $\lfloor \chi \rfloor_j$. □

Lemma 3.3.

Let $\Delta \vdash \tau$ *and* $\rho \in \mathcal{D}[\![\Delta]\!]$.
If $j < k$ *then* $\lfloor \mathcal{V}_j[\![\tau]\!]\,\rho \rfloor_k = \mathcal{V}_j[\![\tau]\!]\,\rho$.

Proof

By definition of $\mathcal{V}_j[\![\tau]\!]\,\rho$, for any $(i, W, v_1, v_2) \in \mathcal{V}_j[\![\tau]\!]\,\rho$, it must be that $i < j$. Furthermore, since we have $j < k$ as a premise, it follows that $i < k$.

Thus, from the definition of $\lfloor \chi \rfloor_k$, and since $i < j$ and $i < k$, it follows that
$(i, W, v_1, v_2) \in \lfloor \mathcal{V}_j[\![\tau]\!]\,\rho \rfloor_k$ iff $(i, W, v_1, v_2) \in \mathcal{V}_j[\![\tau]\!]\,\rho$. □

Lemma 3.4.

Let $\Delta \vdash \tau$ *and* $\rho \in \mathcal{D}[\![\Delta]\!]$.
Then $\lfloor \mathcal{V}[\![\tau]\!]\,\rho \rfloor_k = \mathcal{V}_k[\![\tau]\!]\,\rho$.

Proof

$\lfloor \mathcal{V}[\![\tau]\!]\,\rho \rfloor_k$		
$= \lfloor \bigcup_{n \geq 0} \mathcal{V}_n[\![\tau]\!]\,\rho \rfloor_k$		since $\mathcal{V}[\![\tau]\!]\,\rho = \bigcup_{n \geq 0} \mathcal{V}_n[\![\tau]\!]\,\rho$
$= \bigcup_{n \geq 0} \lfloor \mathcal{V}_n[\![\tau]\!]\,\rho \rfloor_k$		by distributivity of $\lfloor \cdot \rfloor_k$ over $\cup$
$= (\bigcup_{n<k} \lfloor \mathcal{V}_n[\![\tau]\!]\,\rho \rfloor_k) \cup (\bigcup_{n \geq k} \lfloor \mathcal{V}_n[\![\tau]\!]\,\rho \rfloor_k)$		
$= (\bigcup_{n<k} \lfloor \mathcal{V}_n[\![\tau]\!]\,\rho \rfloor_k) \cup (\bigcup_{n \geq k} \mathcal{V}_k[\![\tau]\!]\,\rho)$		since for $k \leq n$, $\lfloor \mathcal{V}_n[\![\tau]\!]\,\rho \rfloor_k = \mathcal{V}_k[\![\tau]\!]\,\rho$ by Lemma 3.1
$= (\bigcup_{n<k} \lfloor \mathcal{V}_n[\![\tau]\!]\,\rho \rfloor_k) \cup \mathcal{V}_k[\![\tau]\!]\,\rho$		
$= (\bigcup_{n<k} \mathcal{V}_n[\![\tau]\!]\,\rho) \cup \mathcal{V}_k[\![\tau]\!]\,\rho$		since for $n < k$, $\lfloor \mathcal{V}_n[\![\tau]\!]\,\rho \rfloor_k = \mathcal{V}_n[\![\tau]\!]\,\rho$ by Lemma 3.3
$= (\bigcup_{n<k} \lfloor \mathcal{V}_k[\![\tau]\!]\,\rho \rfloor_n) \cup \mathcal{V}_k[\![\tau]\!]\,\rho$		since for $n < k$, $\mathcal{V}_n[\![\tau]\!]\,\rho = \lfloor \mathcal{V}_k[\![\tau]\!]\,\rho \rfloor_n$ by Lemma 3.1
$= \mathcal{V}_k[\![\tau]\!]\,\rho$		since $\lfloor \mathcal{V}_k[\![\tau]\!]\,\rho \rfloor_n \subseteq \mathcal{V}_k[\![\tau]\!]\,\rho$ by Lemma 3.2

□

Lemma 3.5.

If $\psi \in StoreRel_k$ *then* $\psi = \lfloor \psi \rfloor_k$.

Lemma 3.6.

If $\eta \in Knowledge_k$ *then* $\eta = \lfloor \eta \rfloor_k$.

Lemma 3.7.

If $\mathcal{L} \in Law_k$ *then* $\mathcal{L} = \lfloor \mathcal{L} \rfloor_k$.

3.1.2 Approximation Yields Valid Semantic Objects

Lemma 3.8. (Store Relation Approximation Valid)

If $\psi \in StoreRel_k$ *and* $j \leq k$, *then* $\lfloor \psi \rfloor_j \in StoreRel_j$.

Lemma 3.9. (Knowledge Approximation Valid)

If $\eta \in Knowledge_k$ *and* $j \leq k$, *then* $\lfloor \eta \rfloor_j \in Knowledge_j$.

Lemma 3.10. (Law Approximation Valid)

If $\mathcal{L} \in Law_k$ *and* $j \leq k$, *then* $\lfloor \mathcal{L} \rfloor_j \in Law_j$.

Lemma 3.11. (Island Approximation Valid)

If $w \in Island_k$ *and* $j \leq k$, *then* $\lfloor w \rfloor_j \in Island_j$.

Lemma 3.12. (World Approximation Valid)

If $W \in World_k$ *and* $j \leq k$, *then* $\lfloor W \rfloor_j \in World_j$.

3.1.3 World Extension and Store Satisfaction Properties

Lemma 3.13. (Reflexivity: Island $\sqsupseteq$)

If $w \in \mathit{Island}_k$ *then* $w \sqsupseteq w$.

Lemma 3.14. (Reflexivity: World $\sqsupseteq$)

If $W \in \mathit{World}_k$ *then* $W \sqsupseteq W$.

Lemma 3.15. (Reflexivity of World Extension)

If $W \in \mathit{World}_k$ *then* $(k, W) \sqsupseteq (k, W)$.

Lemma 3.16. (World Approximation is Valid Extension)

If $W \in \mathit{World}_k$ *and* $j \leq k$, *then* $(j, \lfloor W \rfloor_j) \sqsupseteq (k, W)$.

Proof

We are required to show that

- $j \leq k$,
  which is a premise,
- $W \in \mathit{World}_k$,
  which is a premise,
- $\lfloor W \rfloor_j \in \mathit{World}_j$,
  which follows from Lemma 3.12 applied to $W \in \mathit{World}_k$ and $j \leq k$, and
- $\lfloor W \rfloor_j \sqsupseteq \lfloor W \rfloor_j$,
  which follows from Lemma 3.14 applied to $\lfloor W \rfloor_j \in \mathit{World}_j$.

□

Lemma 3.17.

If $(j, W') \sqsupseteq (k, W)$ *and* $j \leq i$,
then $(j, W') \sqsupseteq (i, \lfloor W \rfloor_i)$.

Lemma 3.18. (Transitivity of World Extension)

If $(i, W'') \sqsupseteq (j, W')$ *and* $(j, W') \sqsupseteq (k, W)$,
then $(i, W'') \sqsupseteq (k, W)$.

Lemma 3.19. (Store Satisfaction Downward Closed)

Suppose $W \in \mathit{World}_k$.
If $s_1, s_2 :_k W$ *and* $j \leq k$, *then* $s_1, s_2 :_j \lfloor W \rfloor_j$.

3.1.4 Validity of Type Interpretations

Lemma 3.20. (Closure Under World Extension)

Let $\Delta \vdash \tau$ *and* $\rho \in \mathcal{D}[\![\Delta]\!]$.
If $(k, W, v_1, v_2) \in \mathcal{V}_n[\![\tau]\!]\,\rho$ *and* $(j, W') \sqsupseteq (k, W)$,
then $(j, W', v_1, v_2) \in \mathcal{V}_n[\![\tau]\!]\,\rho$.

Proof

Proof by induction on n and nested induction on the derivation $\Delta \vdash \tau$. □

Lemma 3.21. (Logical Relations Closed Under World Extension)

Let $\Delta \vdash \tau$ *and* $\rho \in \mathcal{D}[\![\Delta]\!]$.
If $(k, W, v_1, v_2) \in \mathcal{V}[\![\tau]\!]\,\rho$ *and* $(j, W') \sqsupseteq (k, W)$,
then $(j, W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\,\rho$.

Proof

Follows from Lemmas 3.4 and 3.20. □

Lemma 3.22.

Let $\Delta \vdash \Gamma$ *and* $\rho \in \mathcal{D}[\![\Delta]\!]$.
If $(k, W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\,\rho$ *and* $(j, W') \sqsupseteq (k, W)$,
then $(j, W', \gamma) \in \mathcal{G}[\![\Gamma]\!]\,\rho$.

Proof

Proof by induction on Γ. Follows from Lemma 3.21. □

Lemma 3.23.

If $(k, W) \in \mathcal{S}[\![\Sigma]\!]$ *and* $(j, W') \sqsupseteq (k, W)$,
then $(j, W') \in \mathcal{S}[\![\Sigma]\!]$.

Proof

Follows from Lemma 3.21. □

Lemma 3.24. (Logical Relations Are Valid Type Interpretations)

If $\Delta \vdash \tau$ *and* $\rho \in \mathcal{D}[\![\Delta]\!]$, *then* $\mathcal{V}[\![\tau]\!]\,\rho \in \mathit{Type}[\rho_1(\tau), \rho_2(\tau)]$.

Proof

Follows from Lemma 3.21. □

3.1.5 Substitution Property

Lemma 3.25. (Semantic Type Substitution)

Let $\Delta \vdash \tau'$ *and* $\rho \in \mathcal{D}[\![\Delta]\!]$ *and* $\Delta, \alpha \vdash \tau$.
Let $\chi = \mathcal{V}[\![\tau']\!]\,\rho$.
Then $\mathcal{V}[\![\tau]\!]\,\rho[\alpha \mapsto (\chi, \rho_1(\tau'), \rho_2(\tau'))] = \mathcal{V}[\![[\tau'/\alpha]\tau]\!]\,\rho$.

3.2 Fundamental Property

The Fundamental Property of the logical relation follows from the fact that the latter is a congruence [7]. To establish congruence we have to show that the logical relation satisfies the compatibility and substitutivity properties.

Note: Below we give detailed proofs of the compatibility lemmas that involve references—see Lemmas 3.29 (locations), 3.47 (allocation), 3.48 (dereferencing), and 3.49 (assignment). Proofs of the compatibility lemmas that do not involve references essentially follow the proofs given in Ahmed's earlier work [1].

Lemma 3.26. (Compatibility: Var)

If $\Gamma(x) = \tau$ *then* $\Delta; \Gamma; \Sigma \vdash x \preceq^{log} x : \tau$.

Lemma 3.27. (Compatibility: Unit)

$\Delta; \Gamma; \Sigma \vdash () \preceq^{log} () : \mathsf{unit}$.

Lemma 3.28. (Compatibility: Int)

$\Delta; \Gamma; \Sigma \vdash n \preceq^{log} n : \mathsf{int}$.

Lemma 3.29. (Compatibility: Loc)

If $\Sigma(l) = \tau$ *then* $\Delta; \Gamma; \Sigma \vdash l \preceq^{log} l : \mathsf{ref}\,\tau$.

Proof

Consider arbitrary k, ρ, γ, W such that

- $k \geq 0$,
- $\rho \in \mathcal{D}\,[\![\Delta]\!]$,
- $(k, W, \gamma) \in \mathcal{G}\,[\![\Gamma]\!]\,\rho$, and
- $(k, W) \in \mathcal{S}\,[\![\Sigma]\!]$.

We are required to show that $(k, W, \rho_1(\gamma_1(l)), \rho_2(\gamma_2(l))) \in \mathcal{E}\,[\![\mathsf{ref}\,\tau]\!]\,\rho$
$\equiv (k, W, l, l) \in \mathcal{E}\,[\![\mathsf{ref}\,\tau]\!]\,\rho$.

Consider arbitrary j, s_1, s_2, s_1', v_1 such that

- $j < k$,
- $s_1, s_2 :_k W$, and
- $s_1, l \longmapsto^j s_1', v_1$.

Since l is a value, we have that $j = 0$, $s_1' = s_1$, and $v_1 = l$.

Note that we have the following facts:

- $W \in \mathit{World}_k$,
  which follows from $(k, W, \gamma) \in \mathcal{G}\,[\![\Gamma]\!]\,\rho$ above, and
- $(k, W, l, l) \in \mathcal{V}\,[\![\mathsf{ref}\,\tau]\!]\,\emptyset$,
  which follows from $(k, W) \in \mathcal{S}\,[\![\Sigma]\!]$ since $\Sigma(l) = \tau$.

Take $s_2' = s_2$, $v_2 = l$, and $W' = W$.

We are required to show that

(1) $s_2, l \longmapsto^* s_2', v_2$
$\equiv s_2, l \longmapsto^* s_2, l$,
which is immediate,

(2) $(k - 0, W') \sqsupseteq (k, W)$
$\equiv (k, W) \sqsupseteq (k, W)$,
which follows from Lemma 3.15 (reflexivity of $\sqsupseteq$, page 18) applied to $W \in \mathit{World}_k$,

(3) $s_1', s_2' :_{k-0} W'$
$\equiv s_1, s_2 :_k W$,
which follows from above, and

(4) $(k - 0, W', v_1, v_2) \in \mathcal{V}\,[\![\mathsf{ref}\,\tau]\!]\,\rho$
$\equiv (k, W, l, l) \in \mathcal{V}\,[\![\mathsf{ref}\,\tau]\!]\,\rho$
$\equiv (k, W, l, l) \in \mathcal{V}\,[\![\mathsf{ref}\,\tau]\!]\,\emptyset$ (since we can conclude from the premise that $FTV(\tau) = \emptyset$),
which follows from above.

□

Lemma 3.30. (Compatibility: True)

$\Delta; \Gamma; \Sigma \vdash \texttt{true} \preceq^{log} \texttt{true} : \texttt{bool}$.

Lemma 3.31. (Compatibility: False)

$\Delta; \Gamma; \Sigma \vdash \texttt{false} \preceq^{log} \texttt{false} : \texttt{bool}$.

Lemma 3.32. (Compatibility: If)

If $\Delta; \Gamma; \Sigma \vdash e_{10} \preceq^{log} e_{20} : \texttt{bool}$, $\Delta; \Gamma; \Sigma \vdash e_{11} \preceq^{log} e_{21} : \tau$, *and* $\Delta; \Gamma; \Sigma \vdash e_{12} \preceq^{log} e_{22} : \tau$,
then $\Delta; \Gamma; \Sigma \vdash \texttt{if}\, e_{10}\, \texttt{then}\, e_{11}\, \texttt{else}\, e_{12} \preceq^{log} \texttt{if}\, e_{20}\, \texttt{then}\, e_{21}\, \texttt{else}\, e_{22} : \tau$.

Lemma 3.33. (Compatibility: Pair)

If $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau$ *and* $\Delta; \Gamma; \Sigma \vdash e_1' \preceq^{log} e_2' : \tau'$,
then $\Delta; \Gamma; \Sigma \vdash \langle e_1, e_1' \rangle \preceq^{log} \langle e_2, e_2' \rangle : \tau \times \tau'$.

Lemma 3.34. (Compatibility: Fst)

If $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau \times \tau'$,
then $\Delta; \Gamma; \Sigma \vdash \texttt{fst}\, e_1 \preceq^{log} \texttt{fst}\, e_2 : \tau$.

Lemma 3.35. (Compatibility: Snd)

If $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau \times \tau'$,
then $\Delta; \Gamma; \Sigma \vdash \texttt{snd}\, e_1 \preceq^{log} \texttt{snd}\, e_2 : \tau'$.

Lemma 3.36. (Compatibility: Inl)

If $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau$,
then $\Delta; \Gamma; \Sigma \vdash \texttt{inl}\, e_1 \preceq^{log} \texttt{inl}\, e_2 : \tau + \tau'$.

Lemma 3.37. (Compatibility: Inr)

If $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau'$,
then $\Delta; \Gamma; \Sigma \vdash \texttt{inr}\, e_1 \preceq^{log} \texttt{inr}\, e_2 : \tau + \tau'$.

Lemma 3.38. (Compatibility: Case)

If $\Delta; \Gamma; \Sigma \vdash e_{10} \preceq^{log} e_{20} : \tau + \tau'$, $\Delta; \Gamma, x : \tau; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau''$, *and* $\Delta; \Gamma, x' : \tau'; \Sigma \vdash e_1' \preceq^{log} e_2' : \tau''$,
then $\Delta; \Gamma; \Sigma \vdash \texttt{case}\, e_{10}\, \texttt{of}\, \texttt{inl}\, x \Rightarrow e_1 \mid \texttt{inr}\, x' \Rightarrow e_1' \preceq^{log} \texttt{case}\, e_{20}\, \texttt{of}\, \texttt{inl}\, x \Rightarrow e_2 \mid \texttt{inr}\, x' \Rightarrow e_2' : \tau''$.

Lemma 3.39. (Compatibility: Fun)

If $\Delta; \Gamma, x : \tau; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau'$,
then $\Delta; \Gamma; \Sigma \vdash \lambda x\!:\!\tau.\, e_1 \preceq^{log} \lambda x\!:\!\tau.\, e_2 : \tau \to \tau'$.

Lemma 3.40. (Compatibility: App)

If $\Delta; \Gamma; \Sigma \vdash e_1' \preceq^{log} e_2' : \tau \to \tau'$ *and* $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau$,
then $\Delta; \Gamma; \Sigma \vdash e_1'\, e_1 \preceq^{log} e_2'\, e_2 : \tau'$.

Lemma 3.41. (Compatibility: All)

If $\Delta, \alpha; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau$,
then $\Delta; \Gamma; \Sigma \vdash \Lambda\alpha.\, e_1 \preceq^{log} \Lambda\alpha.\, e_2 : \forall\alpha.\, \tau$.

Lemma 3.42. (Compatibility: Type App)

If $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \forall\alpha.\, \tau$ *and* $\Delta \vdash \tau'$,
then $\Delta; \Gamma; \Sigma \vdash e_1\,[\tau'] \preceq^{log} e_2\,[\tau'] : [\tau'/\alpha]\tau$.

Lemma 3.43. (Compatibility: Pack)

If $\Delta \vdash \tau'$ *and* $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : [\tau'/\alpha]\tau$,
then $\Delta; \Gamma; \Sigma \vdash \mathtt{pack}\,\tau', e_1\,\mathtt{as}\,\exists\alpha.\, \tau \preceq^{log} \mathtt{pack}\,\tau', e_2\,\mathtt{as}\,\exists\alpha.\, \tau : \exists\alpha.\, \tau$.

Lemma 3.44. (Compatibility: Unpack)

If $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \exists\alpha.\, \tau$, $\Delta \vdash \tau'$, *and* $\Delta, \alpha; \Gamma, x : \tau; \Sigma \vdash e_1' \preceq^{log} e_2' : \tau'$
then $\Delta; \Gamma; \Sigma \vdash \mathtt{unpack}\, e_1\, \mathtt{as}\, \alpha, x\, \mathtt{in}\, e_1' \preceq^{log} \mathtt{unpack}\, e_2\, \mathtt{as}\, \alpha, x\, \mathtt{in}\, e_2' : \tau'$.

Lemma 3.45. (Compatibility: Fold)

If $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : [\mu\alpha.\, \tau/\alpha]\tau$,
then $\Delta; \Gamma; \Sigma \vdash \mathtt{fold}\, e_1 \preceq^{log} \mathtt{fold}\, e_2 : \mu\alpha.\, \tau$.

Lemma 3.46. (Compatibility: Unfold)

If $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \mu\alpha.\, \tau$,
then $\Delta; \Gamma; \Sigma \vdash \mathtt{unfold}\, e_1 \preceq^{log} \mathtt{unfold}\, e_2 : [\mu\alpha.\, \tau/\alpha]\tau$.

Lemma 3.47. (Compatibility: Ref)

If $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau$,
then $\Delta; \Gamma; \Sigma \vdash \texttt{ref}\, e_1 \preceq^{log} \texttt{ref}\, e_2 : \mathsf{ref}\, \tau$.

Proof

Consider arbitrary k, ρ, γ, W such that

- $k \geq 0$,
- $\rho \in \mathcal{D}\,[\![\Delta]\!]$,
- $(k, W, \gamma) \in \mathcal{G}\,[\![\Gamma]\!]\,\rho$, and
- $(k, W) \in \mathcal{S}\,[\![\Sigma]\!]$.

We are required to show that $(k, W, \rho_1(\gamma_1(\texttt{ref}\, e_1)), \rho_2(\gamma_2(\texttt{ref}\, e_2))) \in \mathcal{E}\,[\![\mathsf{ref}\, \tau]\!]\,\rho$
$\equiv (k, W, \texttt{ref}\, (\rho_1(\gamma_1(e_1))), \texttt{ref}\, (\rho_2(\gamma_2(e_2)))) \in \mathcal{E}\,[\![\mathsf{ref}\, \tau]\!]\,\rho$.

Consider arbitrary j, s_1, s_2, s_1', v_1 such that

- $j < k$,
- $s_1, s_2 :_k W$, and
- $s_1, \texttt{ref}\, (\rho_1(\gamma_1(e_1))) \longmapsto^j s_1', v_1$.

Hence, by inspection of the operational semantics, it follows that there exist j_1, s_{1a}, v_{1a}, and l_1 such that

- $s_1, \rho_1(\gamma_1(e_1)) \longmapsto^{j_1} s_{1a}, v_{1a}$,
- $s_{1a}, \texttt{ref}\, v_{1a} \longmapsto^1 s_{1a}[l_1 \mapsto v_{1a}], l_1$,
- $l_1 \notin \mathrm{dom}(s_{1a})$,
- $j = j_1 + 1$,
- $s_1' = s_{1a}[l_1 \mapsto v_{1a}]$, and
- $v_1 = l_1$.

Instantiate the premise $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau$ with k, ρ, γ, and W. Note that

- $k \geq 0$,
- $\rho \in \mathcal{D}\,[\![\Delta]\!]$,
- $(k, W, \gamma) \in \mathcal{G}\,[\![\Gamma]\!]\,\rho$, and
- $(k, W) \in \mathcal{S}\,[\![\Sigma]\!]$.

Hence, $(k, W, \rho_1(\gamma_1(e_1)), \rho_2(\gamma_2(e_2))) \in \mathcal{E}\,[\![\tau]\!]\,\rho$.
Instantiate this with j_1, s_1, s_2, s_{1a}, v_{1a}. Note that

- $j_1 < k$, which follows from $j_1 = j - 1$ and $j < k$,
- $s_1, s_2 :_k W$ and

- $s_1, \rho_1(\gamma_1(e_1)) \longmapsto^{j_1} s_{1a}, v_{1a}$.

Hence, there exist s_{2a}, v_{2a}, and W_a such that

- $s_2, \rho_2(\gamma_2(e_2)) \longmapsto^* s_{2a}, v_{2a}$,
- $(k - j_1, W_a) \sqsupseteq (k, W)$,
- $s_{1a}, s_{2a} :_{k-j_1} W_a$, and
- $(k - j_1, W_a, v_{1a}, v_{2a}) \in \mathcal{V}[\![\tau]\!]\,\rho$.

Take $s_2' = s_{2a}[l_2 \mapsto v_{2a}]$, where $l_2 \notin \mathrm{dom}(s_{2a})$, and $v_2 = l_2$.
If $W_a = \langle w_{a1}, \ldots, w_{an}\rangle$, then
take $W' = \langle \lfloor w_{a1}\rfloor_{k-j}, \ldots, \lfloor w_{an}\rfloor_{k-j}, w'\rangle$,
where $w' = (\eta', \mathcal{L}')$,
$\eta' = (\psi', \langle\rangle, \{l_1 : \rho_1(\tau)\}, \{l_2 : \rho_2(\tau)\})$
$\psi' = \{(i, W'', s_1'', s_2'') \mid (i, W'', s_1''(l_1), s_2''(l_2)) \in \lfloor \mathcal{V}[\![\tau]\!]\,\rho\rfloor_{k-j}\}$
$\mathcal{L}' = \{(i, \lfloor \eta'\rfloor_i) \mid i \leq k - j\}$.

Note that we have the following facts:

- $\vdash s_{1a} : \Sigma_1(W_a)$ and $\vdash s_{2a} : \Sigma_2(W_a)$,
  which follow from $s_{1a}, s_{2a} :_{k-j_1} W_a$,
- $W_a \in \mathit{World}_{k-j_1}$,
  which follows from $(k - j_1, W_a) \sqsupseteq (k, W)$ above,
- $\lfloor w_{ai}\rfloor_{k-j} \in \mathit{Island}_{k-j}$ for all i such that $1 \leq i \leq n$,
  which follows from Lemma 3.11 (page 17) applied to
  - $w_{ai} \in \mathit{Island}_{k-j_1}$,
    which follows from $w_{ai} \in W_a$ and the fact that $W_a \in \mathit{World}_{k-j_1}$, and
  - $k - j \leq k - j_1$.
- $W' \in \mathit{World}_{k-j}$,
  which follows from **(i)** and **(ii)** below:
  - **(i)** $\langle \lfloor w_{a1}\rfloor_{k-j}, \ldots, \lfloor w_{an}\rfloor_{k-j}, w'\rangle \in \mathit{Island}_{k-j}^{n+1}$,
    which follows from
    - $\lfloor w_{ai}\rfloor_{k-j} \in \mathit{Island}_{k-j}$ for all i such that $1 \leq i \leq n$,
      which follows from above, and
    - $w' \in \mathit{Island}_{k-j}$,
      which follows from **(a)**, **(b)**, and **(c)** below:
      - **(a)** $\eta' \in \mathit{Knowledge}_{k-j}$, which follows from
        - $\psi' \in \mathit{StoreRel}_{k-j}$,
          which follows from the closure of ψ' under world extension; the latter, given the definition of ψ', follows from the closure of $\lfloor \mathcal{V}[\![\tau]\!]\,\rho\rfloor_{k-j}$ under world extension (i.e., from Lemma 3.21 (page 19) applied to $\Delta \vdash \tau$ and $\rho \in \mathcal{D}[\![\Delta]\!]$).

- $\forall s_1, s_2, s_1', s_2'.$
  $(\forall l_1 \in \mathrm{dom}(\eta'.\Sigma_1).s_1(l_1) = s_1'(l_1) \ \wedge \ \forall l_2 \in \mathrm{dom}(\eta'.\Sigma_2).s_2(l_2) = s_2'(l_2)) \implies$
  $\forall j'', W''.\ (j'', W'', s_1, s_2) \in \psi' \Leftrightarrow (j'', W'', s_1', s_2') \in \psi'),$
  which is immediate from the definition of η' since $\mathrm{dom}(\eta'.\Sigma_1) = \{l_1\}$ and $\mathrm{dom}(\eta'.\Sigma_2) = \{l_2\}$ and since ψ' is defined to rely only on the contents of location l_1 in the first store and the contents of l_2 in the second store. More formally, note that from the definition of ψ' it follows that

$$\begin{array}{rcl} & & (j'', W'', s_1, s_2) \in \psi' \ \Leftrightarrow \ (j'', W'', s_1', s_2') \in \psi' \\ \equiv & & (j'', W'', s_1(l_1), s_2(l_2)) \in \lfloor \mathcal{V}[\![\tau]\!]\,\rho \rfloor_{k-j} \ \Leftrightarrow \ (j'', W'', s_1'(l_1), s_2'(l_2)) \in \lfloor \mathcal{V}[\![\tau]\!]\,\rho \rfloor_{k-j} \end{array}$$

  The latter is clearly a tautology when $s_1(l_1) = s_1'(l_1)$ and $s_2(l_2) = s_2'(l_2)$.

(b) $\mathcal{L}' \in \mathit{Law}_{k-j}$,
which follows from the downward closure of $\mathcal{L}'$ (i.e., the property that $\forall (i, \eta) \in \mathcal{L}'.\ \forall i' < i.\ (i', \lfloor \eta' \rfloor_{i'}) \in \mathcal{L}'$), which is immediate from the definition of $\mathcal{L}'$.

(c) $(k-j, \eta') \in \mathcal{L}'$
$\equiv (k-j, \lfloor \eta' \rfloor_{k-j}) \in \mathcal{L}'$ (since $\eta' = \lfloor \eta' \rfloor_{k-j}$ by Lemma 3.6 (page 16) applied to $\eta' \in \mathit{Knowledge}_{k-j}$),
which is immediate from the definition of $\mathcal{L}'$.

(ii) $\forall c, d \in \{1, \ldots, n+1\}.\ c \neq d \implies \mathrm{dom}(W'[c].\Sigma_1) \,\#\, \mathrm{dom}(W'[d].\Sigma_1) \ \wedge \ \mathrm{dom}(W'[c].\Sigma_2) \,\#\, \mathrm{dom}(W'[d].\Sigma_2),$
which we conclude as follows:
Suppose $c, d \in \{1, \ldots, n\}$ and $c \neq d$. Note that

$$\begin{array}{rl} & \mathrm{dom}(W'[c].\Sigma_1) \,\#\, \mathrm{dom}(W'[d].\Sigma_1) \ \wedge \ \mathrm{dom}(W'[c].\Sigma_2) \,\#\, \mathrm{dom}(W'[d].\Sigma_2) \\ \equiv & \mathrm{dom}(W_a[c].\Sigma_1) \,\#\, \mathrm{dom}(W_a[d].\Sigma_1) \ \wedge \ \mathrm{dom}(W_a[c].\Sigma_2) \,\#\, \mathrm{dom}(W_a[d].\Sigma_2) \\ & \text{(since } W'[i].\Sigma_1 = W_a[i].\Sigma_1 \text{ and } W'[i].\Sigma_2 = W_a[i].\Sigma_2 \text{ for } i \in \{1, \ldots, n\}\text{, by defn of } W') \\ \equiv & \mathrm{dom}(w_{ac}.\Sigma_1) \,\#\, \mathrm{dom}(w_{ad}.\Sigma_1) \ \wedge \ \mathrm{dom}(w_{ac}.\Sigma_2) \,\#\, \mathrm{dom}(w_{ad}.\Sigma_2) \\ & \text{(since } W_a[i] = w_{ai} \text{ for } i \in \{1, \ldots, n\}\text{)} \end{array}$$

Note that the latter follows from $W_a \in \mathit{World}_{k-j_1}$ (which follows from above).
Thus, it remains for us to show that the last island in W', namely $W'[n+1] \equiv w'$ is such that

$$\begin{array}{rrcl} & \forall i \in \{1, \ldots, n\}.\ \mathrm{dom}(w'.\Sigma_1) \,\#\, \mathrm{dom}(W'[i].\Sigma_1) & \wedge & \mathrm{dom}(w'.\Sigma_2) \,\#\, \mathrm{dom}(W'[i].\Sigma_2) \\ & \forall i \in \{1, \ldots, n\}.\ \mathrm{dom}(w'.\Sigma_1) \,\#\, \mathrm{dom}(W_a[i].\Sigma_1) & \wedge & \mathrm{dom}(w'.\Sigma_2) \,\#\, \mathrm{dom}(W_a[i].\Sigma_2) \\ \equiv & \mathrm{dom}(w'.\Sigma_1) \,\#\, \mathrm{dom}(\textstyle\bigcup_{1 \leq i \leq n} W_a[i].\Sigma_1) & \wedge & \mathrm{dom}(w'.\Sigma_2) \,\#\, \mathrm{dom}(\textstyle\bigcup_{1 \leq i \leq n} W_a[i].\Sigma_2) \\ \equiv & \mathrm{dom}(w'.\Sigma_1) \,\#\, \mathrm{dom}(\Sigma_1(W_a)) & \wedge & \mathrm{dom}(w'.\Sigma_2) \,\#\, \mathrm{dom}(\Sigma_2(W_a)) \\ \equiv & \{l_1\} \,\#\, \mathrm{dom}(\Sigma_1(W_a)) & \wedge & \{l_2\} \,\#\, \mathrm{dom}(\Sigma_2(W_a)) \\ \equiv & l_1 \notin \mathrm{dom}(\Sigma_1(W_a)) & \wedge & l_2 \notin \mathrm{dom}(\Sigma_2(W_a)) \end{array}$$

Note that from $s_{1a}, s_{2a} :_{k-j_1} W_a$ it follows that $\vdash s_{1a} : \Sigma_1(W_a)$ and $\vdash s_{2a} : \Sigma_2(W_a)$.
Hence, it follows that $\mathrm{dom}(s_{1a}) \supseteq \mathrm{dom}(\Sigma_1(W_a))$ and $\mathrm{dom}(s_{2a}) \supseteq \mathrm{dom}(\Sigma_2(W_a))$.
Hence, we can conclude that

- $l_1 \notin \Sigma_1(W_a)$,
  which follows from $l_1 \notin \mathrm{dom}(s_{1a})$ (from above) and $\mathrm{dom}(s_{1a}) \supseteq \mathrm{dom}(\Sigma_1(W_a))$, and
- $l_2 \notin \Sigma_2(W_a)$,
  which follows from $l_2 \notin \mathrm{dom}(s_{2a})$ (from above) and $\mathrm{dom}(s_{2a}) \supseteq \mathrm{dom}(\Sigma_2(W_a))$.

We are required to show that

(1) $s_2, \mathtt{ref}\,(\rho_2(\gamma_2(e_2))) \longmapsto^* s_2', v_2$
$\equiv s_2, \mathtt{ref}\,(\rho_2(\gamma_2(e_2))) \longmapsto^* s_{2a}[l_2 \mapsto v_{2a}], l_2,$
which follows from

$$\begin{array}{lll} s_2, \mathtt{ref}\,(\rho_2(\gamma_2(e_2))) & \longmapsto^* & s_{2a}, \mathtt{ref}\, v_{2a} \\ & \longmapsto^1 & s_{2a}[l_2 \mapsto v_{2a}], l_2, \quad \text{where } l_2 \notin \mathrm{dom}(s_{2a}) \text{ as required.} \end{array}$$

(2) $(k-j, W') \sqsupseteq (k, W)$,
which follows from Lemma 3.18 (transitivity of $\sqsupseteq$, page 18) applied to

- $(k-j, W') \sqsupseteq (k-j_1, W_a)$,
which follows (by the definition of $\sqsupseteq$) from:
  - $k-j \leq k-j_1$, which follows from $k-j = k-j_1-1$ (since $j = j_1+1$),
  - $W_a \in \mathit{World}_{k-j_1}$,
which follows from above,
  - $W' \in \mathit{World}_{k-j}$,
which follows from above, and
  - $W' \sqsupseteq \lfloor W_a \rfloor_{k-j}$
$\equiv \langle \lfloor w_{a1} \rfloor_{k-j}, \ldots, \lfloor w_{an} \rfloor_{k-j}, w' \rangle \sqsupseteq \lfloor \langle w_{a1}, \ldots, w_{an} \rangle \rfloor_{k-j}$
$\equiv \langle \lfloor w_{a1} \rfloor_{k-j}, \ldots, \lfloor w_{an} \rfloor_{k-j}, w' \rangle \sqsupseteq \langle \lfloor w_{a1} \rfloor_{k-j}, \ldots, \lfloor w_{an} \rfloor_{k-j} \rangle$,
which we conclude as follows:
Note that it suffices to show $\forall i \in \{1, \ldots, n\}.\ \lfloor w_{ai} \rfloor_{k-j} \sqsupseteq \lfloor w_{ai} \rfloor_{k-j}$.
Applying Lemma 3.13 (page 18) to $\lfloor w_{ai} \rfloor_{k-j} \in \mathit{Island}_{k-j}$ (from above), we conclude that $\lfloor w_{ai} \rfloor_{k-j} \sqsupseteq \lfloor w_{ai} \rfloor_{k-j}$.

  and
- $(k-j_1, W_a) \sqsupseteq (k, W)$,
which follows from above.

(3) $s_1', s_2' :_{k-j} W'$
$\equiv s_{1a}[l_1 \mapsto v_{1a}], s_{2a}[l_2 \mapsto v_{2a}] :_{k-j} W'$,
which follows (by definition of the store satisfaction relation) from

- $\vdash s_{1a}[l_1 \mapsto v_{1a}] : \Sigma_1(W')$
$\equiv\ \forall l \in \mathrm{dom}(\Sigma_1(W')).\ \cdot;\cdot;\Sigma_1(W') \vdash s_{1a}[l_1 \mapsto v_{1a}](l) : \Sigma_1(W')(l)$,
which, since $\Sigma_1(W') \equiv \Sigma_1(W_a) \uplus \{l_1 : \rho_1(\tau)\}$, follows from **(I)** and **(II)** below:

  (I) $\forall l \in \mathrm{dom}(\Sigma_1(W_a)).\ \cdot;\cdot;\Sigma_1(W') \vdash s_{1a}[l_1 \mapsto v_{1a}](l) : (\Sigma_1(W'))(l)$,
  which follows from:
  Consider $l \in \mathrm{dom}(\Sigma_1(W_a))$. Hence, note that $l \neq l_1$.
  We are required to show that

$$\begin{array}{lll} & \cdot;\cdot;\Sigma_1(W') \vdash s_{1a}[l_1 \mapsto v_{1a}](l) : (\Sigma_1(W'))(l) & \\ \equiv & \cdot;\cdot;\Sigma_1(W') \vdash s_{1a}(l) : (\Sigma_1(W'))(l) & (\text{since } l \neq l_1 \text{ and } l_1 \notin \mathrm{dom}(s_{1a})) \\ \equiv & \cdot;\cdot;\Sigma_1(W') \vdash s_{1a}(l) : (\Sigma_1(W_a))(l) & (\text{since } l \neq l_1 \text{ and } l_1 \notin \mathrm{dom}(\Sigma_1(W_a))) \\ \equiv & \cdot;\cdot;\Sigma_1(W_a) \uplus \{l_1 : \rho_1(\tau)\} \vdash s_{1a}(l) : (\Sigma_1(W_a))(l) & \end{array}$$

  which follows from $\cdot;\cdot;\Sigma_1(W_a) \vdash s_{1a}(l) : (\Sigma_1(W_a))(l)$,
  which in turn follows from $\vdash s_{1a} : \Sigma_1(W_a)$ since $l \in \mathrm{dom}(\Sigma_1(W_a))$.

  (II) $\forall l \in \mathrm{dom}(\{l_1 : \rho_1(\tau)\}).\ \cdot;\cdot;\Sigma_1(W') \vdash s_{1a}[l_1 \mapsto v_{1a}](l) : (\Sigma_1(W'))(l)$
  $\equiv \cdot;\cdot;\Sigma_1(W') \vdash s_{1a}[l_1 \mapsto v_{1a}](l_1) : (\Sigma_1(W'))(l_1)$
  $\equiv \cdot;\cdot;\Sigma_1(W') \vdash v_{1a} : \rho_1(\tau)$,
  which follows from $\cdot;\cdot;\Sigma_1(W_a) \vdash v_{1a} : \rho_1(\tau)$,
  which in turn follows from $(k-j_1, W_a, v_{1a}, v_{2a}) \in \mathcal{V}\,[\![\tau]\!]\,\rho$.

- $\vdash s_{2a}[l_2 \mapsto v_{2a}] : \Sigma_2(W')$,
  which follows by reasoning analogous to that used for $\vdash s_{1a}[l_1 \mapsto v_{1a}] : \Sigma_1(W')$ above.
- $\forall w \in W'.\ \forall i' < k - j.\ (i', \lfloor W' \rfloor_{i'}, s_{1a}[l_1 \mapsto v_{1a}], s_{2a}[l_2 \mapsto v_{2a}]) \in w.\psi$,
  which we conclude as follows:

  Consider arbitrary $w \in W'$ and $i' < k - j$.
  We are required to show $(i', \lfloor W' \rfloor_{i'}, s_{1a}[l_1 \mapsto v_{1a}], s_{2a}[l_2 \mapsto v_{2a}]) \in w.\psi$.

  Note that by the definition of W', there are two cases to consider:
  either $w = W'[i]$ (where $1 \leq i \leq n$), or $w = W'[n+1]$.

  Case $w = W'[i] = \lfloor w_{ai} \rfloor_{k-j}$ (where $1 \leq i \leq n$) :
  We are required to show that

  $$\begin{aligned}
  &(i', \lfloor W' \rfloor_{i'}, s_{1a}[l_1 \mapsto v_{1a}], s_{2a}[l_2 \mapsto v_{2a}]) \in (\lfloor w_{ai} \rfloor_{k-j}).\psi \\
  &\equiv (i', \lfloor W' \rfloor_{i'}, s_{1a}[l_1 \mapsto v_{1a}], s_{2a}[l_2 \mapsto v_{2a}]) \in \lfloor w_{ai}.\psi \rfloor_{k-j} \\
  &\equiv (i', \lfloor W' \rfloor_{i'}, s_{1a}[l_1 \mapsto v_{1a}], s_{2a}[l_2 \mapsto v_{2a}]) \in w_{ai}.\psi \qquad \text{(since } i' < k - j\text{)}
  \end{aligned}$$

  Note that from $s_{1a}, s_{2a} :_{k-j_1} W_a$ it follows that
  - $\forall w_{ai} \in W_a.\ \forall i' < k - j_1.\ (i', \lfloor W' \rfloor_{i'}, s_{1a}, s_{2a}) \in w_{ai}.\psi$.

  Hence, since $w_{ai} \in W_a$ (where $1 \leq i \leq n$) and since $k - j < k - j_1$ (which follows from $j = j_1 + 1$), it follows that
  - $(k - j, \lfloor W' \rfloor_{k-j}, s_{1a}, s_{2a}) \in w_{ai}.\psi$.

  Let $w_{ai}.\Sigma_1 = \Sigma_{ai1}$ and let $w_{ai}.\Sigma_2 = \Sigma_{ai2}$. Then it must be that
  - $l_1 \notin \mathrm{dom}(\Sigma_{ai1})$,
    which follows from
    - $l_1 \notin \mathrm{dom}(\Sigma_1(W_a))$,
      which follows from above, and
    - $\Sigma_{ai1} \subseteq \Sigma_1(W_a)$,
      which follows from the definition of $\Sigma_1(W_a)$ since $w_{ai} \in W_a$ and $w_{ai}.\Sigma_1 = \Sigma_{ai1}$.
  - $l_2 \notin \mathrm{dom}(\Sigma_{ai2})$,
    which follows from
    - $l_2 \notin \mathrm{dom}(\Sigma_2(W_a))$,
      which follows from above, and
    - $\Sigma_{ai2} \subseteq \Sigma_2(W_a)$,
      which follows from the definition of $\Sigma_2(W_a)$ since $w_{ai} \in W_a$ and $w_{ai}.\Sigma_2 = \Sigma_{ai2}$.

  Hence, note that
  - $\forall l \in \mathrm{dom}(\Sigma_{ai1}).\ s_{1a}(l) = s_{1a}[l_1 \mapsto v_{1a}](l)$, and
  - $\forall l \in \mathrm{dom}(\Sigma_{ai2}).\ s_{2a}(l) = s_{2a}[l_2 \mapsto v_{2a}](l)$.

  Note that $w_{ai}.\eta \in \mathit{Knowledge}_{k-j_1}$, which follows from $W_a \in \mathit{World}_{k-j_1}$ since $W_a[i] = w_{ai}$.
  Now, from $W_a.\eta \in \mathit{Knowledge}_{k-j_1}$, together with
  - $\forall l \in \mathrm{dom}(\Sigma_{ai1}).\ s_{1a}(l) = s_{1a}[l_1 \mapsto v_{1a}](l)$,
  - $\forall l \in \mathrm{dom}(\Sigma_{ai2}).\ s_{2a}(l) = s_{2a}[l_2 \mapsto v_{2a}](l)$, and
  - $(k - j, \lfloor W_a \rfloor_{k-j}, s_{1a}, s_{2a}) \in w_{ai}.\psi$ (from above),

  it follows that $(k - j, \lfloor W_a \rfloor_{k-j}, s_{1a}[l_1 \mapsto v_{1a}], s_{2a}[l_2 \mapsto v_{2a}]) \in w_{ai}.\psi$.

  Note that
  - $(i', \lfloor W' \rfloor_{i'}) \sqsupseteq (k - j, \lfloor W_a \rfloor_{k-j})$,
    which follows from Lemma 3.18 (page 18) applied to

- $(i', \lfloor W' \rfloor_{i'}) \sqsupseteq (k-j, W')$,
  which follows from Lemma 3.16 (page 18) applied to $W' \in \mathit{World}_{k-j}$ and $i' < k-j$, and
- $(k-j, W') \sqsupseteq (k-j, \lfloor W_a \rfloor_{k-j})$,
  which follows from Lemma 3.17 (page 18) applied to
  - $(k-j, W') \sqsupseteq (k-j_1, W_a)$,
    which follows from above, and
  - $k-j \leq k-j$.

Next, note that $w_{ai}.\psi \in \mathit{StoreRel}_{k-j_1}$, which follows from $w_{ai}.\eta \in \mathit{Knowledge}_{k-j_1}$. Since $w_{ai}.\psi$ is closed under world extension, and since we have that

- $(k-j, \lfloor W_a \rfloor_{k-j}, s_{1a}[l_1 \mapsto v_{1a}], s_{2a}[l_2 \mapsto v_{2a}]) \in w_{ai}.\psi$ (from above) and
- $(i', \lfloor W' \rfloor_{i'}) \sqsupseteq (k-j, \lfloor W_a \rfloor_{k-j})$,

it follows that $(i', \lfloor W' \rfloor_{i'}, s_{1a}[l_1 \mapsto v_{1a}], s_{2a}[l_2 \mapsto v_{2a}]) \in w_{ai}.\psi$ as required.

Case $w = W'[n+1] = w'$:

We are required to show that

$$
\begin{array}{ll}
(i', \lfloor W' \rfloor_{i'}, s_{1a}[l_1 \mapsto v_{1a}], s_{2a}[l_2 \mapsto v_{2a}]) \in w'.\psi & \\
\equiv (i', \lfloor W' \rfloor_{i'}, s_{1a}[l_1 \mapsto v_{1a}], s_{2a}[l_2 \mapsto v_{2a}]) \in \psi' & \text{(since } w'.\psi = \psi') \\
\equiv (i', \lfloor W' \rfloor_{i'}, s_{1a}[l_1 \mapsto v_{1a}](l_1), s_{2a}[l_2 \mapsto v_{2a}](l_2)) \in \lfloor \mathcal{V}[\![\tau]\!]\rho \rfloor_{k-j} & \text{(by definition of } \psi') \\
\equiv (i', \lfloor W' \rfloor_{i'}, v_{1a}, v_{2a}) \in \lfloor \mathcal{V}[\![\tau]\!]\rho \rfloor_{k-j} & \\
\equiv (i', \lfloor W' \rfloor_{i'}, v_{1a}, v_{2a}) \in \mathcal{V}[\![\tau]\!]\rho & \text{(since } i' < k-j)
\end{array}
$$

Note that

- $(i', \lfloor W' \rfloor_{i'}) \sqsupseteq (k-j_1, W_a)$,
  which follows from Lemma 3.18 (page 18) applied to
  - $(i', \lfloor W' \rfloor_{i'}) \sqsupseteq (k-j, W')$
    which follows from Lemma 3.16 (page 18) applied to $W' \in \mathit{World}_{k-j}$ and $i' < k-j$, and
  - $(k-j, W') \sqsupseteq (k-j_1, W_a)$,
    which follows from above.

Applying Lemma 3.21 (page 19) to $(k-j_1, W_a, v_{1a}, v_{2a}) \in \mathcal{V}[\![\tau]\!]\rho$ (from above) and $(i', \lfloor W' \rfloor_{i'}) \sqsupseteq (k-j_1, W_a)$, we conclude that $(i', \lfloor W' \rfloor_{i'}, v_{1a}, v_{2a}) \in \mathcal{V}[\![\tau]\!]\rho$ as required.

(4) $(k-j, W', v_1, v_2) \in \mathcal{V}[\![\mathsf{ref}\,\tau]\!]\rho$
$\equiv (k-j, W', l_1, l_2) \in \mathcal{V}[\![\mathsf{ref}\,\tau]\!]\rho$,
which follows (by the definition of $\mathcal{V}[\![\mathsf{ref}\,\tau]\!]\rho$) from

- $w_{\mathsf{ref}}(k-j, \rho, \tau, l_1, l_2) \in W'$
  $\equiv (\eta', \mathcal{L}') \in W'$ (since $w_{\mathsf{ref}}(k-j, \rho, \tau, l_1, l_2) = (\eta', \mathcal{L}') = w'$)
  $\equiv w' \in W'$,
  which follows from $W'[n+1] = w'$.

□

Lemma 3.48. (Compatibility: Deref)

If $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \mathsf{ref}\ \tau$,
then $\Delta; \Gamma; \Sigma \vdash\ !e_1 \preceq^{log}\ !e_2 : \tau$.

Proof

Consider arbitrary k, ρ, γ, W such that

- $k \geq 0$,
- $\rho \in \mathcal{D}\,[\![\Delta]\!]$,
- $(k, W, \gamma) \in \mathcal{G}\,[\![\Gamma]\!]\,\rho$, and
- $(k, W) \in \mathcal{S}\,[\![\Sigma]\!]$.

We are required to show that $(k, W, \rho_1(\gamma_1(!e_1)), \rho_2(\gamma_2(!e_2))) \in \mathcal{E}\,[\![\tau]\!]\,\rho$
$\equiv (k, W, !(\rho_1(\gamma_1(e_1))), !(\rho_2(\gamma_2(e_2)))) \in \mathcal{E}\,[\![\tau]\!]\,\rho$.

Consider arbitrary j, s_1, s_2, s_1', v_1 such that

- $j < k$,
- $s_1, s_2 :_k W$, and
- $s_1, !(\rho_1(\gamma_1(e_1))) \longmapsto^j s_1', v_1$.

Hence, by inspection of the operational semantics, it follows that there exist j_1, s_{1a}, and l_1 such that

- $s_1, \rho_1(\gamma_1(e_1)) \longmapsto^{j_1} s_{1a}, l_1$,
- $s_{1a}(l_1) = v_1$,
- $s_{1a}, !l_1 \longmapsto^1 s_{1a}, v_1$,
- $j = j_1 + 1$, and
- $s_1' = s_{1a}$.

Instantiate the premise $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \mathsf{ref}\ \tau$ with k, ρ, γ, and W. Note that

- $k \geq 0$,
- $\rho \in \mathcal{D}\,[\![\Delta]\!]$,
- $(k, W, \gamma) \in \mathcal{G}\,[\![\Gamma]\!]\,\rho$, and
- $(k, W) \in \mathcal{S}\,[\![\Sigma]\!]$.

Hence, $(k, W, \rho_1(\gamma_1(e_1)), \rho_2(\gamma_2(e_2))) \in \mathcal{E}\,[\![\mathsf{ref}\ \tau]\!]\,\rho$.
Instantiate this with j_1, s_1, s_2, s_{1a}, l_1. Note that

- $j_1 < k$, which follows from $j_1 = j - 1$ and $j < k$,
- $s_1, s_2 :_k W$ and
- $s_1, \rho_1(\gamma_1(e_1)) \longmapsto^{j_1} s_{1a}, l_1$.

Hence, there exist s_{2a}, v_{2a}, and W_a such that

- $s_2, \rho_2(\gamma_2(e_2)) \longmapsto^* s_{2a}, v_{2a}$,
- $(k - j_1, W_a) \sqsupseteq (k, W)$,
- $s_{1a}, s_{2a} :_{k-j_1} W_a$, and
- $(k - j_1, W_a, l_1, v_{2a}) \in \mathcal{V}\,[\![\mathsf{ref}\,\tau]\!]\,\rho$.

Hence, $v_{2a} \equiv l_2$.
Note that we have the following facts:

- $k - j < k - j_1$,
  which follows from $j < k$ and $j = j_1 + 1$, and
- $W_a \in \mathit{World}_{k-j_1}$,
  which follows from $(k - j_1, W_a) \sqsupseteq (k, W)$.

Also, note that $w_{\mathsf{ref}}(k - j_1, \rho, \tau, l_1, l_2) \in W_a$ (which follows from $(k - j_1, W_a, l_1, v_{2a}) \in \mathcal{V}\,[\![\mathsf{ref}\,\tau]\!]\,\rho$), where $w_{\mathsf{ref}}(k - j_1, \rho, \tau, l_1, l_2) = (\eta, \mathcal{L})$
$\eta = (\psi, \langle\rangle, \{l_1 : \rho_1(\tau)\}, \{l_2 : \rho_2(\tau)\})$
$\psi = \{(i, W'', s_1'', s_2'') \mid (i, W'', s_1''(l_1), s_2''(l_2)) \in \lfloor \mathcal{V}\,[\![\tau]\!]\,\rho \rfloor_{k-j_1}\}$
$\mathcal{L} = \{(i, \lfloor \eta \rfloor_i) \mid i \leq k - j_1\}$
Note that

- $\forall w \in W_a.\ \forall i < k - j_1.\ (i, \lfloor W_a \rfloor_i, s_{1a}, s_{2a}) \in w.\psi$,
  which follows from $s_{1a}, s_{2a} :_{k-j_1} W_a$.

Hence, since $(\eta, \mathcal{L}) \in W_a$, it follows that

- $\forall i < k - j_1.\ (i, \lfloor W_a \rfloor_i, s_{1a}, s_{2a}) \in (\eta, \mathcal{L}).\psi$
  $\equiv \forall i < k - j_1.\ (i, \lfloor W_a \rfloor_i, s_{1a}, s_{2a}) \in \psi \quad (\text{since } (\eta, \mathcal{L}).\psi \equiv \psi)$

Hence, since $k - j < k - j_1$, it follows that

- $(k - j, \lfloor W_a \rfloor_{k-j}, s_{1a}, s_{2a}) \in \psi$

Hence, from the definition of ψ, it follows that

- $(k - j, \lfloor W_a \rfloor_{k-j}, s_{1a}(l_1), s_{2a}(l_2)) \in \lfloor \mathcal{V}\,[\![\tau]\!]\,\rho \rfloor_{k-j_1}$.

Note that, from the latter, it follows that $l_2 \in \mathrm{dom}(s_{2a})$.

Take $s_2' = s_{2a}$, $v_2 = s_{2a}(l_2)$, and $W' = \lfloor W_a \rfloor_{k-j}$.

We are required to show that

(1) $s_2, !(\rho_2(\gamma_2(e_2))) \longmapsto^* s_2', v_2$
$\equiv s_2, !(\rho_2(\gamma_2(e_2))) \longmapsto^* s_{2a}, s_{2a}(l_2)$,
which follows from

$$\begin{array}{lll} s_2, !(\rho_2(\gamma_2(e_2))) & \longmapsto^* & s_{2a}, !v_{2a} \\ & \equiv & s_{2a}, !l_2, \quad \text{where } l_2 \in \mathrm{dom}(s_{2a}) \text{ as required} \\ & \longmapsto^1 & s_{2a}, s_{2a}(l_2). \end{array}$$

(2) $(k-j, W') \sqsupseteq (k, W)$
$\equiv (k-j, \lfloor W_a \rfloor_{k-j}) \sqsupseteq (k, W)$,
which follows from Lemma 3.18 (transitivity of $\sqsupseteq$, page 18) applied to

- $(k-j, \lfloor W_a \rfloor_{k-j}) \sqsupseteq (k-j_1, W_a)$,
  which follows from Lemma 3.16 (page 18) applied to $W_a \in \mathit{World}_{k-j_1}$ and $k-j < k-j_1$, and
- $(k-j_1, W_a) \sqsupseteq (k, W)$,
  which follows from above.

(3) $s_1', s_2' :_{k-j} W'$
$\equiv s_{1a}, s_{2a} :_{k-j} \lfloor W_a \rfloor_{k-j}$,
which follows from Lemma 3.19 (page 18) applied to $s_{1a}, s_{2a} :_{k-j_1} W_a$ and $k-j < k-j_1$.

(4) $(k-j, W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$
$\equiv (k-j, \lfloor W_a \rfloor_{k-j}, s_{1a}(l_1), s_{2a}(l_2)) \in \mathcal{V}[\![\tau]\!]\rho$,
which follows from $(k-j, \lfloor W_a \rfloor_{k-j}, s_{1a}(l_1), s_{2a}(l_2)) \in \lfloor \mathcal{V}[\![\tau]\!]\rho \rfloor_{k-j_1}$ (since $k-j < k-j_1$).

□

Lemma 3.49. (Compatibility: Assign)

If $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \mathsf{ref}\,\tau$ *and* $\Delta; \Gamma; \Sigma \vdash e_1' \preceq^{log} e_2' : \tau$,
then $\Delta; \Gamma; \Sigma \vdash e_1 := e_1' \preceq^{log} e_2 := e_2' : \mathsf{unit}$.

Proof

Consider arbitrary k, ρ, γ, W such that

- $k \geq 0$,
- $\rho \in \mathcal{D}\,[\![\Delta]\!]$,
- $(k, W, \gamma) \in \mathcal{G}\,[\![\Gamma]\!]\,\rho$, and
- $(k, W) \in \mathcal{S}\,[\![\Sigma]\!]$.

We are required to show that $(k, W, \rho_1(\gamma_1(e_1 := e_1')), \rho_2(\gamma_2(e_2 := e_2'))) \in \mathcal{E}\,[\![\mathsf{unit}]\!]\,\rho$
$\equiv (k, W, \rho_1(\gamma_1(e_1)) := \rho_1(\gamma_1(e_1')), \rho_2(\gamma_2(e_2)) := \rho_2(\gamma_2(e_2'))) \in \mathcal{E}\,[\![\mathsf{unit}]\!]\,\rho$.

Consider arbitrary j, s_1, s_2, s_1', v_1 such that

- $j < k$,
- $s_1, s_2 :_k W$, and
- $s_1, \rho_1(\gamma_1(e_1)) := \rho_1(\gamma_1(e_1')) \longmapsto^j s_1', v_1$.

Hence, by inspection of the operational semantics, it follows that there exist j_1, j_2, s_{1a}, s_{1b}, l_1, and v_{1b} such that

- $s_1, \rho_1(\gamma_1(e_1)) \longmapsto^{j_1} s_{1a}, l_1$,
- $s_{1a}, \rho_1(\gamma_1(e_1')) \longmapsto^{j_2} s_{1b}, v_{1b}$,
- $l_1 \in \mathrm{dom}(s_{1b})$,
- $s_{1b}, l_1 := v_{1b} \longmapsto^1 s_{1b}[l_1 \mapsto v_{1b}], ()$,
- $j = j_1 + j_2 + 1$,
- $s_1' = s_{1b}[l_1 \mapsto v_{1b}]$, and
- $v_1 = ()$.

Instantiate the premise $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \mathsf{ref}\,\tau$ with k, ρ, γ, and W. Note that

- $k \geq 0$,
- $\rho \in \mathcal{D}\,[\![\Delta]\!]$,
- $(k, W, \gamma) \in \mathcal{G}\,[\![\Gamma]\!]\,\rho$, and
- $(k, W) \in \mathcal{S}\,[\![\Sigma]\!]$.

Hence, $(k, W, \rho_1(\gamma_1(e_1)), \rho_2(\gamma_2(e_2))) \in \mathcal{E}\,[\![\mathsf{ref}\,\tau]\!]\,\rho$.
Instantiate this with j_1, s_1, s_2, s_{1a}, l_1. Note that

- $j_1 < k$, which follows from $j_1 = j - j_2 - 1$ and $j < k$,

- $s_1, s_2 :_k W$ and
- $s_1, \rho_1(\gamma_1(e_1)) \longmapsto^{j_1} s_{1a}, l_1$.

Hence, there exist s_{2a}, v_{2a}, and W_a such that

- $s_2, \rho_2(\gamma_2(e_2)) \longmapsto^* s_{2a}, v_{2a}$,
- $(k - j_1, W_a) \sqsupseteq (k, W)$,
- $s_{1a}, s_{2a} :_{k-j_1} W_a$, and
- $(k - j_1, W_a, l_1, v_{2a}) \in \mathcal{V}\,[\![\mathsf{ref}\ \tau]\!]\,\rho$.

Hence, $v_{2a} \equiv l_2$.

Instantiate the premise $\Delta; \Gamma; \Sigma \vdash e_1' \preceq^{log} e_2' : \tau$ with $k - j_1$, ρ, γ, and W_a. Note that

- $k - j_1 \geq 0$,
  which follows from $j_1 = j - j_2 - 1$ and $j < k$,
- $\rho \in \mathcal{D}\,[\![\Delta]\!]$,
- $(k - j_1, W_a, \gamma) \in \mathcal{G}\,[\![\Gamma]\!]\,\rho$,
  which follows from Lemma 3.22 (page 19) applied to $(k, W, \gamma) \in \mathcal{G}\,[\![\Gamma]\!]\,\rho$ and $(k - j_1, W_a) \sqsupseteq (k, W)$, and
- $(k - j_1, W_a) \in \mathcal{S}\,[\![\Sigma]\!]$,
  which follows from Lemma 3.23 (page 19) applied to $(k, W) \in \mathcal{S}\,[\![\Sigma]\!]$ and $(k - j_1, W_a) \sqsupseteq (k, W)$.

Hence, $(k - j_1, W_a, \rho_1(\gamma_1(e_1')), \rho_2(\gamma_2(e_2'))) \in \mathcal{E}\,[\![\tau]\!]\,\rho$.
Instantiate this with j_2, s_{1a}, s_{2a}, s_{1b}, v_{1b}. Note that

- $j_2 < k - j_1$,
  which follows from $j_2 = j - j_1 - 1$ and $j < k$,
- $s_{1a}, s_{2a} :_{k-j_1} W_a$,
  which follows from above, and
- $s_{1a}, \rho_1(\gamma_1(e_1')) \longmapsto^{j_2} s_{1b}, v_{1b}$,
  which follows from above.

Hence, there exist s_{2b}, v_{2b}, and W_b such that

- $s_{2a}, \rho_2(\gamma_2(e_2')) \longmapsto^* s_{2b}, v_{2b}$,
- $(k - j_1 - j_2, W_b) \sqsupseteq (k - j_1, W_a)$,
- $s_{1b}, s_{2b} :_{k-j_1-j_2} W_b$, and
- $(k - j_1 - j_2, W_b, v_{1b}, v_{2b}) \in \mathcal{V}\,[\![\tau]\!]\,\rho$.

Note that we have the following facts:

- $\vdash s_{1b} : \Sigma_1(W_b)$ and $\vdash s_{2b} : \Sigma_2(W_b)$,
  which follow from $s_{1b}, s_{2b} :_{k-j_1-j_2} W_b$,

- $k - j < k - j_1 - j_2$,
  which follows from $j < k$ and $j = j_1 + j_2 + 1$,

- $W_b \in \mathit{World}_{k-j_1-j_2}$,
  which follows from $(k - j_1 - j_2, W_b) \sqsupseteq (k - j_1, W_a)$,

- $\lfloor W_b \rfloor_{k-j} \in \mathit{World}_{k-j}$,
  which follows from Lemma 3.12 (page 17) applied to $W_b \in \mathit{World}_{k-j_1-j_2}$ and $k - j \leq k - j_1 - j_2$,

- Suppose $W_a = \langle w_{a1}, \ldots, w_{an} \rangle$. Then

  $$\exists m \in \{1, \ldots, n\}.\ \ W_a[m] = w_{\mathsf{ref}}(k - j_1, \rho, \tau, l_1, l_2)$$

  (or alternatively, $w_{\mathsf{ref}}(k-j_1, \rho, \tau, l_1, l_2) \in W_a$, which follows from $(k-j_1, W_a, l_1, v_{2a}) \in \mathcal{V}\,[\![\mathsf{ref}\ \tau]\!]\,\rho)$,
  where $w_{\mathsf{ref}}(k - j_1, \rho, \tau, l_1, l_2) = (\eta, \mathcal{L})$
  $\eta = (\psi, \langle\rangle, \{l_1 : \rho_1(\tau)\}, \{l_2 : \rho_2(\tau)\})$
  $\psi = \{(i, W'', s_1'', s_2'') \mid (i, W'', s_1''(l_1), s_2''(l_2)) \in \lfloor \mathcal{V}\,[\![\tau]\!]\,\rho \rfloor_{k-j_1}\}$
  $\mathcal{L} = \{(i, \lfloor \eta \rfloor_i) \mid i \leq k - j_1\}$

- $\{l_1 : \rho_1(\tau)\} \subseteq \Sigma_1(W_a)$ and $\{l_2 : \rho_2(\tau)\} \subseteq \Sigma_2(W_a)$,
  which follow from the definitions of $\Sigma_1(W_a)$ and $\Sigma_2(W_a)$ and the fact that $(\eta, \mathcal{L}) \in W_a$ (above) where $(\eta, \mathcal{L}).\Sigma_1 = \{l_1 : \rho_1(\tau)\}$ and $(\eta, \mathcal{L}).\Sigma_2 = \{l_2 : \rho_2(\tau)\}$.

- $\Sigma_1(W_b) \supseteq \Sigma_1(W_a)$ and $\Sigma_2(W_b) \supseteq \Sigma_2(W_a)$,
  which follow from $(k - j_1 - j_2, W_b) \sqsupseteq (k - j_1, W_a)$.

- $\{l_1 : \rho_1(\tau)\} \subseteq \Sigma_1(W_b)$ and $\{l_2 : \rho_2(\tau)\} \subseteq \Sigma_2(W_b)$,
  which follow, respectively, from $\{l_1 : \rho_1(\tau)\} \subseteq \Sigma_1(W_a)$ since $\Sigma_1(W_b) \supseteq \Sigma_1(W_a)$, and from $\{l_2 : \rho_2(\tau)\} \subseteq \Sigma_2(W_a)$ since $\Sigma_2(W_b) \supseteq \Sigma_2(W_a)$.

- $l_2 \in \mathrm{dom}(s_{2b})$,
  which follows from the fact that $\forall l \in \mathrm{dom}(\Sigma_2(W_b)).\ \cdot;\cdot;\Sigma_2(W_b) \vdash s_{2b}(l) : \Sigma_2(W_b)(l)$ (which follows, by definition, from $\vdash s_{2b} : \Sigma_2(W_b)$), since $l_2 \in \mathrm{dom}(\Sigma_2(W_b))$.

Take $s_2' = s_{2b}[l_2 \mapsto v_{2b}]$, $v_2 = ()$, and $W' = \lfloor W_b \rfloor_{k-j}$.

We are required to show that

(1) $s_2, (\rho_2(\gamma_2(e_2))) := (\rho_2(\gamma_2(e_2'))) \longmapsto^* s_2', v_2$
$\equiv s_2, (\rho_2(\gamma_2(e_2))) := (\rho_2(\gamma_2(e_2'))) \longmapsto^* s_{2b}[l_2 \mapsto v_{2b}], ()$,
which follows from

$$\begin{array}{lll} s_2, (\rho_2(\gamma_2(e_2))) := (\rho_2(\gamma_2(e_2'))) & \longmapsto^* & s_{2a}, v_{2a} := (\rho_2(\gamma_2(e_2'))) \\ & \equiv & s_{2a}, l_2 := (\rho_2(\gamma_2(e_2'))) \\ & \longmapsto^* & s_{2b}, l_2 := v_{2b}, \quad \text{where } l_2 \in \mathrm{dom}(s_{2b}) \text{ as required} \\ & \longmapsto^1 & s_{2b}[l_2 \mapsto v_{2b}], () . \end{array}$$

(2) $(k - j, W') \sqsupseteq (k, W)$
$\equiv (k - j, \lfloor W_b \rfloor_{k-j}) \sqsupseteq (k, W)$,
which follows from Lemma 3.18 (transitivity of $\sqsupseteq$, page 18) applied to

- $(k - j, \lfloor W_b \rfloor_{k-j}) \sqsupseteq (k - j_1 - j_2, W_b)$,
  which follows from Lemma 3.16 (page 18) applied to $W_b \in \mathit{World}_{k-j_1-j_2}$ and $k - j < k - j_1 - j_2$, and

- $(k - j_1 - j_2, W_b) \sqsupseteq (k, W)$,
  which follows from Lemma 3.18 (transitivity of $\sqsupseteq$, page 18) applied to
  - $(k - j_1 - j_2, W_b) \sqsupseteq (k - j_1, W_a)$,
    which follows from above, and
  - $(k - j_1, W_a) \sqsupseteq (k, W)$,
    which follows from above.

(3) $s_1', s_2' :_{k-j} W'$
$\equiv s_{1b}[l_1 \mapsto v_{1b}], s_{2b}[l_2 \mapsto v_{2b}] :_{k-j} \lfloor W_b \rfloor_{k-j}$,
which follows (by definition of the store satisfaction relation) from

- $\vdash s_{1b}[l_1 \mapsto v_{1b}] : \Sigma_1(\lfloor W_b \rfloor_{k-j})$
  $\equiv \vdash s_{1b}[l_1 \mapsto v_{1b}] : \Sigma_1(W_b)$
  $\equiv \forall l \in \mathrm{dom}(\Sigma_1(W_b)).\ \cdot;\cdot;\Sigma_1(W_b) \vdash s_{1b}[l_1 \mapsto v_{1b}](l) : (\Sigma_1(W_b))(l)$,
  which, since $l_1 \in \mathrm{dom}(\Sigma_1(W_b))$, follows from **(I)** and **(II)** below:

  (I) $\forall l \in (\mathrm{dom}(\Sigma_1(W_b)) \setminus \{l_1\}).\ \cdot;\cdot;\Sigma_1(W_b) \vdash s_{1b}[l_1 \mapsto v_{1b}](l) : (\Sigma_1(W_b))(l)$,
  which follows from:
  Consider $l \in \mathrm{dom}(\Sigma_1(W_b)) \setminus \{l_1\})$. Hence, note that $l \neq l_1$.
  We are required to show that

  $$\begin{array}{rl} & \cdot;\cdot;\Sigma_1(W_b) \vdash s_{1b}[l_1 \mapsto v_{1b}](l) : (\Sigma_1(W_b))(l) \\ \equiv & \cdot;\cdot;\Sigma_1(W_b) \vdash s_{1b}(l) : (\Sigma_1(W_b))(l) \qquad (\text{since } l \neq l_1) \end{array}$$

  which follows from $\forall l \in \mathrm{dom}(\Sigma_1(W_b)).\ \cdot;\cdot;\Sigma_1(W_b) \vdash s_{1b}(l) : (\Sigma_1(W_b))(l)$,
  which in turn follows from $\vdash s_{1b} : \Sigma_1(W_b)$ since $l \in \mathrm{dom}(\Sigma_1(W_b))$.

  (II) $\forall l \in \{l_1\}.\ \cdot;\cdot;\Sigma_1(W_b) \vdash s_{1b}[l_1 \mapsto v_{1b}](l) : (\Sigma_1(W_b))(l)$
  $\equiv \cdot;\cdot;\Sigma_1(W_b) \vdash s_{1b}[l_1 \mapsto v_{1b}](l_1) : (\Sigma_1(W_b))(l_1)$
  $\equiv \cdot;\cdot;\Sigma_1(W_b) \vdash v_{1b} : (\Sigma_1(W_b))(l_1)$
  $\equiv \cdot;\cdot;\Sigma_1(W_b) \vdash v_{1b} : \rho_1(\tau) \qquad (\text{since } \{l_1 : \rho_1(\tau)\} \subseteq \Sigma_1(W_b))$
  which follows from $(k - j_1 - j_2, W_b, v_{1b}, v_{2b}) \in \mathcal{V}[\![\tau]\!]\rho$.

- $\vdash s_{2b}[l_2 \mapsto v_{2b}] : \Sigma_2(\lfloor W_b \rfloor_{k-j})$,
  which follows by reasoning analogous to that used for $\vdash s_{1b}[l_1 \mapsto v_{1b}] : \Sigma_1(\lfloor W_b \rfloor_{k-j})$ above.

- $\forall w \in W'.\ \forall i' < k - j.\ (i', \lfloor W' \rfloor_{i'}, s_{1b}[l_1 \mapsto v_{1b}], s_{2b}[l_2 \mapsto v_{2b}]) \in w.\psi$
  $\equiv \forall w \in \lfloor W_b \rfloor_{k-j}.\ \forall i' < k - j.\ (i', \lfloor \lfloor W_b \rfloor_{k-j} \rfloor_{i'}, s_{1b}[l_1 \mapsto v_{1b}], s_{2b}[l_2 \mapsto v_{2b}]) \in w.\psi$
  $\equiv \forall w \in \lfloor W_b \rfloor_{k-j}.\ \forall i' < k - j.\ (i', \lfloor W_b \rfloor_{i'}, s_{1b}[l_1 \mapsto v_{1b}], s_{2b}[l_2 \mapsto v_{2b}]) \in w.\psi$,
  which we conclude as follows:

  Suppose $W_b = \langle w_{b1}, \ldots, w_{bn'} \rangle$. Note that we have the following facts:

  - $m \leq n \leq n'$,
    which follows from $(k - j_1 - j_2, W_b) \sqsupseteq (k - j_1, W_a)$ together with $1 \leq m \leq n$ (from above) and $W_a = \langle w_{a1}, \ldots, w_{an} \rangle$ (from above).
  - $\lfloor W_b \rfloor_{k-j} = \langle \lfloor w_{b1} \rfloor_{k-j}, \ldots, \lfloor w_{bn'} \rfloor_{k-j} \rangle$,
    which is immediate from the definition of world approximation.

  Note that since $W_a[m] = (\eta, \mathcal{L})$ and since $(k - j, \lfloor W_b \rfloor_{k-j}) \sqsupseteq (k - j_1, W_a)$, it follows from the definition of the latter that there exist η', $\mathcal{L}'$ such that

  - $(\lfloor W_b \rfloor_{k-j})[m] = (\eta', \mathcal{L}')$ (or alternatively $(\eta', \mathcal{L}') \in \lfloor W_b \rfloor_{k-j}$),
  - $(\eta', \mathcal{L}') \sqsupseteq \lfloor (\eta, \mathcal{L}) \rfloor_{k-j}$,
    which follows from $(\lfloor W_b \rfloor_{k-j})[m] \sqsupseteq \lfloor W_a \rfloor_{k-j}[m]$,
    which in turn follows from $\lfloor W_b \rfloor_{k-j} \sqsupseteq \lfloor W_a \rfloor_{k-j}$,
    which in turn is immediate from the definition of $(k - j, \lfloor W_b \rfloor_{k-j}) \sqsupseteq (k - j_1, W_a)$,

- $(\eta', \mathcal{L}') \in \mathit{Island}_{k-j}$,
  which follows from $\lfloor W_b \rfloor_{k-j} \in \mathit{World}_{k-j}$ since $(\eta', \mathcal{L}') = (\lfloor W_b \rfloor_{k-j})[m]$,
- $\{l_1 : \rho_1(\tau)\} \subseteq (\eta', \mathcal{L}').\Sigma_1$,
  which follows from the fact that
  - $(\eta, \mathcal{L}).\Sigma_1 = \{l_1 : \rho_1(\tau)\}$, and
  - $(\eta', \mathcal{L}').\Sigma_1 \supseteq (\eta, \mathcal{L}).\Sigma_1$
    $\equiv (\eta', \mathcal{L}').\Sigma_1 \supseteq \lfloor (\eta, \mathcal{L}) \rfloor_{k-j}.\Sigma_1$,
    which follows, by definition, from $(\eta', \mathcal{L}') \sqsupseteq \lfloor (\eta, \mathcal{L}) \rfloor_{k-j}$,
- $\{l_2 : \rho_2(\tau)\} \subseteq (\eta', \mathcal{L}').\Sigma_2$,
  which follows from the fact that
  - $(\eta, \mathcal{L}).\Sigma_2 = \{l_2 : \rho_2(\tau)\}$, and
  - $(\eta', \mathcal{L}').\Sigma_2 \supseteq (\eta, \mathcal{L}).\Sigma_2$
    $\equiv (\eta', \mathcal{L}').\Sigma_2 \supseteq \lfloor (\eta, \mathcal{L}) \rfloor_{k-j}.\Sigma_2$,
    which follows, by definition, from $(\eta', \mathcal{L}') \sqsupseteq \lfloor (\eta, \mathcal{L}) \rfloor_{k-j}$,
- $\mathcal{L}' = \lfloor \mathcal{L} \rfloor_{k-j}$,
  which follows from $(\eta', \mathcal{L}') \sqsupseteq \lfloor (\eta, \mathcal{L}) \rfloor_{k-j}$, and
- $\eta' = \lfloor \eta \rfloor_{k-j}$,
  which we conclude from:

	$(k-j, \eta') \in \mathcal{L}'$	(which follows from $(\eta', \mathcal{L}') \in \mathit{Island}_{k-j}$)
$\equiv$	$(k-j, \eta') \in \lfloor \mathcal{L} \rfloor_{k-j}$	(since $\mathcal{L}' = \lfloor \mathcal{L} \rfloor_{k-j}$)
$\equiv$	$(k-j, \eta') \in \lfloor \{(i, \lfloor \eta \rfloor_i) \mid \ i \leq k - j_1\} \rfloor_{k-j}$	(since $\mathcal{L} = \{(i, \lfloor \eta \rfloor_i) \mid \ i \leq k - j_1\}$)
$\equiv$	$(k-j, \eta') \in \{(i, \lfloor \eta \rfloor_i) \mid \ i \leq k - j\}$	(by the defn of law approximation)

- $(\eta', \mathcal{L}').\psi = \lfloor \psi \rfloor_{k-j}$,
  which follows from $\eta' = \lfloor \eta \rfloor_{k-j}$ since $\eta = (\psi, \langle\rangle, \{l_1 : \rho_1(\tau)\}, \{l_2 : \rho_2(\tau)\})$.
  (Recall from above that $\psi = \{(i, W'', s_1'', s_2'') \mid (i, W'', s_1''(l_1), s_2''(l_2)) \in \lfloor \mathcal{V}\, [\![\tau]\!]\, \rho \rfloor_{k-j_1}\}$.)

Consider arbitrary $w \in \lfloor W_b \rfloor_{k-j}$ and $i' < k - j$.
We are required to show $(i', \lfloor W_b \rfloor_{i'}, s_{1b}[l_1 \mapsto v_{1b}], s_{2b}[l_2 \mapsto v_{2b}]) \in w.\psi$.
There are two cases to consider: either $w = (\lfloor W_b \rfloor_{k-j})[i]$ where $1 \leq i \leq n'$ and $i \neq m$, or $w = (\lfloor W_b \rfloor_{k-j})[m]$.

Case $w = (\lfloor W_b \rfloor_{k-j})[i] = \lfloor w_{bi} \rfloor_{k-j}$ (where $1 \leq i \leq n'$ and $i \neq m$) :

We are required to show that

$$
\begin{array}{l}
(i', \lfloor W_b \rfloor_{i'}, s_{1b}[l_1 \mapsto v_{1b}], s_{2b}[l_2 \mapsto v_{2b}]) \in (\lfloor w_{bi} \rfloor_{k-j}).\psi \\
\equiv (i', \lfloor W_b \rfloor_{i'}, s_{1b}[l_1 \mapsto v_{1b}], s_{2b}[l_2 \mapsto v_{2b}]) \in \lfloor w_{bi}.\psi \rfloor_{k-j} \\
\equiv (i', \lfloor W_b \rfloor_{i'}, s_{1b}[l_1 \mapsto v_{1b}], s_{2b}[l_2 \mapsto v_{2b}]) \in w_{bi}.\psi \qquad \text{(since } i' < k - j\text{)}
\end{array}
$$

Note that from $s_{1b}, s_{2b} :_{k-j_1-j_2} W_b$ it follows that

- $\forall w \in W_b.\ \forall i' < k - j_1 - j_2.\ (i', \lfloor W_b \rfloor_{i'}, s_{1b}, s_{2b}) \in w.\psi$.

Hence, since $w_{bi} \in W_b$ (where $1 \leq i \leq n$) and since $k - j < k - j_1 - j_2$ (which follows from $j = j_1 + j_2 + 1$), it follows that

- $(k - j, \lfloor W_b \rfloor_{k-j}, s_{1a}, s_{2a}) \in w_{bi}.\psi$.

Let $w_{bi}.\Sigma_1 = \Sigma_{bi1}$ and let $w_{bi}.\Sigma_2 = \Sigma_{bi2}$. Then it must be that

- $l_1 \notin \mathrm{dom}(\Sigma_{bi1})$
  $\equiv l_1 \notin \mathrm{dom}(\lfloor W_b \rfloor_{k-j}[i].\Sigma_1)$,
  which follows from
  - $l_1 \in \mathrm{dom}(\lfloor W_b \rfloor_{k-j}[m].\Sigma_1)$
    $\equiv l_1 \in \mathrm{dom}((\eta', \mathcal{L}').\Sigma_1)$ (since $\lfloor W_b \rfloor_{k-j}[m] = (\eta', \mathcal{L}')$)
    which follows from $\{l_1 : \rho_1(\tau)\} \subseteq (\eta', \mathcal{L}').\Sigma_1$, and
  - $\mathrm{dom}(\lfloor W_b \rfloor_{k-j}[m].\Sigma_1) \# \mathrm{dom}(\lfloor W_b \rfloor_{k-j}[i].\Sigma_1)$,
    which follows from $i \neq m$ and $\lfloor W_b \rfloor_{k-j} \in \mathit{World}_{k-j}$ (since the locations that distinct islands in $\lfloor W_b \rfloor_{k-j}$ "care about" must be disjoint),
- $l_2 \notin \mathrm{dom}(\Sigma_{bi2})$
  $\equiv l_2 \notin \mathrm{dom}(\lfloor W_b \rfloor_{k-j}[i].\Sigma_2)$,
  which follows from
  - $l_2 \in \mathrm{dom}(\lfloor W_b \rfloor_{k-j}[m].\Sigma_2)$
    $\equiv l_2 \in \mathrm{dom}((\eta', \mathcal{L}').\Sigma_2)$ (since $\lfloor W_b \rfloor_{k-j}[m] = (\eta', \mathcal{L}')$)
    which follows from $\{l_2 : \rho_2(\tau)\} \subseteq (\eta', \mathcal{L}').\Sigma_2$, and
  - $\mathrm{dom}(\lfloor W_b \rfloor_{k-j}[m].\Sigma_2) \# \mathrm{dom}(\lfloor W_b \rfloor_{k-j}[i].\Sigma_2)$,
    which follows from $i \neq m$ and $\lfloor W_b \rfloor_{k-j} \in \mathit{World}_{k-j}$ (since the locations that distinct islands in $\lfloor W_b \rfloor_{k-j}$ "care about" must be disjoint),

Hence, note that

- $\forall l \in \mathrm{dom}(\Sigma_{bi1}).\ s_{1b}(l) = s_{1b}[l_1 \mapsto v_{1b}](l)$, and
- $\forall l \in \mathrm{dom}(\Sigma_{bi2}).\ s_{2b}(l) = s_{2b}[l_2 \mapsto v_{2b}](l)$.

Note that $w_{bi}.\eta \in \mathit{Knowledge}_{k-j_1-j_2}$, which follows from $W_b \in \mathit{World}_{k-j_1-j_2}$ since $W_b[i] = w_{bi}$.
Now, from $W_b.\eta \in \mathit{Knowledge}_{k-j_1-j_2}$, together with

- $\forall l \in \mathrm{dom}(\Sigma_{bi1}).\ s_{1b}(l) = s_{1b}[l_1 \mapsto v_{1b}](l)$,
- $\forall l \in \mathrm{dom}(\Sigma_{bi2}).\ s_{2b}(l) = s_{2b}[l_2 \mapsto v_{2b}](l)$, and
- $(k-j, \lfloor W_b \rfloor_{k-j}, s_{1b}, s_{2b}) \in w_{bi}.\psi$ (from above),

it follows that $(k-j, \lfloor W_b \rfloor_{k-j}, s_{1b}[l_1 \mapsto v_{1b}], s_{2b}[l_2 \mapsto v_{2b}]) \in w_{bi}.\psi$.

Note that

- $(i', \lfloor W_b \rfloor_{i'}) \sqsupseteq (k-j, \lfloor W_b \rfloor_{k-j})$
  $\equiv (i', \lfloor \lfloor W_b \rfloor_{k-j} \rfloor_{i'}) \sqsupseteq (k-j, \lfloor W_b \rfloor_{k-j})$ (since $i' < k-j$)
  which follows from Lemma 3.16 (page 18) applied to $\lfloor W_b \rfloor_{k-j} \in \mathit{World}_{k-j}$ and $i' < k-j$.

Next, note that $w_{bi}.\psi \in \mathit{StoreRel}_{k-j_1-j_2}$, which follows from $w_{bi}.\eta \in \mathit{Knowledge}_{k-j_1-j_2}$. Since $w_{bi}.\psi$ is closed under world extension, and since we have that

- $(k-j, \lfloor W_b \rfloor_{k-j}, s_{1b}[l_1 \mapsto v_{1b}], s_{2b}[l_2 \mapsto v_{2b}]) \in w_{bi}.\psi$ (from above) and
- $(i', \lfloor W_b \rfloor_{i'}) \sqsupseteq (k-j, \lfloor W_b \rfloor_{k-j})$,

it follows that $(i', \lfloor W_b \rfloor_{i'}, s_{1b}[l_1 \mapsto v_{1b}], s_{2b}[l_2 \mapsto v_{2b}]) \in w_{bi}.\psi$ as required.

Case $w = (\lfloor W_b \rfloor_{k-j})[m] = (\eta', \mathcal{L}')$:

We are required to show that

$$
\begin{array}{ll}
(i', \lfloor W_b \rfloor_{i'}, s_{1b}[l_1 \mapsto v_{1b}], s_{2b}[l_2 \mapsto v_{2b}]) \in (\eta', \mathcal{L}').\psi & \\
\equiv (i', \lfloor W_b \rfloor_{i'}, s_{1b}[l_1 \mapsto v_{1b}], s_{2b}[l_2 \mapsto v_{2b}]) \in \lfloor \psi \rfloor_{k-j} & (\text{since } (\eta', \mathcal{L}').\psi = \lfloor \psi \rfloor_{k-j}) \\
\equiv (i', \lfloor W_b \rfloor_{i'}, s_{1b}[l_1 \mapsto v_{1b}], s_{2b}[l_2 \mapsto v_{2b}]) \in \psi & (\text{since } i' < k - j) \\
\equiv (i', \lfloor W_b \rfloor_{i'}, s_{1b}[l_1 \mapsto v_{1b}](l_1), s_{2b}[l_2 \mapsto v_{2b}](l_2)) \in \lfloor \mathcal{V}[\![\tau]\!]\rho \rfloor_{k-j_1} & (\text{by definition of } \psi) \\
\equiv (i', \lfloor W_b \rfloor_{i'}, s_{1b}[l_1 \mapsto v_{1b}](l_1), s_{2b}[l_2 \mapsto v_{2b}](l_2)) \in \mathcal{V}[\![\tau]\!]\rho & (\text{since } i' < k - j_1) \\
\equiv (i', \lfloor W_b \rfloor_{i'}, v_{1b}, v_{2b}) \in \mathcal{V}[\![\tau]\!]\rho &
\end{array}
$$

Note that

- $(i', \lfloor W_b \rfloor_{i'}) \sqsupseteq (k - j_1 - j_2, W_b)$,
  which follows from Lemma 3.18 (page 18) applied to
  - $(i', \lfloor W_b \rfloor_{i'}) \sqsupseteq (k - j, \lfloor W_b \rfloor_{k-j})$
    $\equiv (i', \lfloor \lfloor W_b \rfloor_{k-j} \rfloor_{i'}) \sqsupseteq (k - j, \lfloor W_b \rfloor_{k-j})$ (since $i' < k - j$)
    which follows from Lemma 3.16 (page 18) applied to $\lfloor W_b \rfloor_{k-j} \in \mathit{World}_{k-j}$ and $i' < k - j$, and
  - $(k - j, \lfloor W_b \rfloor_{k-j}) \sqsupseteq (k - j_1 - j_2, W_b)$,
    which follows from above.

Applying Lemma 3.21 (page 19) to $(k - j_1 - j_2, W_b, v_{1b}, v_{2b}) \in \mathcal{V}[\![\tau]\!]\rho$ (from above) and $(i', \lfloor W_b \rfloor_{i'}) \sqsupseteq (k - j_1 - j_2, W_b)$, we conclude that $(i', \lfloor W_b \rfloor_{i'}, v_{1b}, v_{2b}) \in \mathcal{V}[\![\tau]\!]\rho$ as required.

(4) $(k - j, W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$
$\equiv (k - j, \lfloor W_b \rfloor_{k-j}, (), ()) \in \mathcal{V}[\![\mathsf{unit}]\!]\rho$,
which follows from the definition of $\mathcal{V}[\![\mathsf{unit}]\!]\rho$ since $\lfloor W_b \rfloor_{k-j} \in \mathit{World}_{k-j}$ (from above) and since it is immediate from the typing rules that $\Sigma_1(\lfloor W_b \rfloor_{k-j}) \vdash () : \mathsf{unit}$ and $\Sigma_2(\lfloor W_b \rfloor_{k-j}) \vdash () : \mathsf{unit}$.

□

Lemma 3.50. (Compatibility: Ref Equality)

If $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \mathsf{ref}\,\tau$ *and* $\Delta; \Gamma; \Sigma \vdash e_1' \preceq^{log} e_2' : \mathsf{ref}\,\tau$,
then $\Delta; \Gamma; \Sigma \vdash e_1 == e_1' \preceq^{log} e_2 == e_2' : \mathsf{bool}$.

Proof

To be filled in. □

Theorem 3.51. (Fundamental Property)

If $\Delta; \Gamma; \Sigma \vdash e : \tau$ *then* $\Delta; \Gamma; \Sigma \vdash e \preceq^{log} e : \tau$.

Proof

Proof by induction on the derivation $\Delta; \Gamma; \Sigma \vdash e : \tau$.
Each case follows from the corresponding compatibility lemma (i.e., Lemmas 3.26 through 3.50). □

3.3 Soundness w.r.t. Contextual Equivalence

Lemma 3.52. (Logically Related Terms Are Related in Any Context)

If $\vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau')$ *and* $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau$,
then $\Delta'; \Gamma'; \Sigma' \vdash C[e_1] \preceq^{log} C[e_2] : \tau'$.

Proof

Proof by induction on the derivation $\vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\Delta'; \Gamma'; \Sigma' \vdash \tau')$.
The base case (i.e., when $C = [\cdot]$) follows easily from the premise $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau$. The remaining cases follow from the induction hypothesis and application of the appropriate compatibility lemma (i.e., one of Lemmas 3.32 through 3.50). □

Value Parametricity and Store Parametricity

To prove that the logical relation is sound with respect to contextual equivalance, we will need a notion of store parametricity (see Lemma 3.58 on page 46). Informally, this is the property that if $\vdash s : \Sigma$ and W is a world comprised of one w_{ref} island for each location $l \in \mathrm{dom}(\Sigma)$ (see Definition 3.55, page 45), then s is related to itself at world W for any number of steps k. Notice that to prove this lemma, we will need to show that if $\Sigma(l) = \tau$, then the value stored at location l in store s (where we know that $\cdot;\cdot;\Sigma \vdash s(l) : \tau$) is related to itself at the type τ (i.e., $(k, W, s(l), s(l)) \in \mathcal{V}\,[\![\tau]\!]\,\emptyset$). To show the latter, we define a notion of value relatedness below and prove that any well typed value is related to itself in the appropriate value relation $\mathcal{V}\,[\![\tau]\!]\,\rho$, not just in the computation relation $\mathcal{E}\,[\![\tau]\!]\,\rho$ as established by the Fundamental Property.

Definition 3.53. (Value Relatedness)

Let $\Delta;\Gamma;\Sigma \vdash v_1 : \tau$ *and* $\Delta;\Gamma;\Sigma \vdash v_2 : \tau$.

$$\Delta;\Gamma;\Sigma \vdash v_1 \preceq^{log}_{\mathsf{val}} v_2 : \tau \quad \stackrel{\text{def}}{=} \quad \forall k \geq 0.\ \forall \rho, \gamma, W.\\ \rho \in \mathcal{D}\,[\![\Delta]\!] \ \wedge\ (k, W, \gamma) \in \mathcal{G}\,[\![\Gamma]\!]\,\rho \ \wedge\ (k, W) \in \mathcal{S}\,[\![\Sigma]\!] \implies\\ (k, W, \rho_1(\gamma_1(v_1)), \rho_2(\gamma_2(v_2))) \in \mathcal{V}\,[\![\tau]\!]\,\rho$$

Lemma 3.54. (Well-typed Values in Value Relation $\mathcal{V}\,[\![\tau]\!]$)

If $\Delta;\Gamma;\Sigma \vdash v : \tau$ *then* $\Delta;\Gamma;\Sigma \vdash v \preceq^{log}_{\mathsf{val}} v : \tau$.

Proof

Proof by induction on the derivation $\Delta;\Gamma;\Sigma \vdash v : \tau$.

The proofs of all cases are similar to the corresponding compatibility lemmas.

In all cases where the value v contains only values as subexpressions, the proof follows by application of the induction hypothesis. However, this is not the case when the value v contains a term e as a subexpression as in the case for functions and type abstraction (which we discuss next).

Consider the function case. Suppose $\Delta;\Gamma;\Sigma \vdash \lambda x : \tau_1.\, e : \tau_1 \to \tau_2$. Then we know that $\Delta;\Gamma, x : \tau_1;\Sigma \vdash e : \tau_2$. Here we make use of the Fundamental Property (Lemma 3.51, page 42) to conclude that $\Delta;\Gamma, x : \tau_1;\Sigma \vdash e \preceq^{log} e : \tau_2$. The rest of the proof is similar to the proof of Lemma 3.39 (compatibility lemma for functions).

Similarly, in the case of type abstraction, suppose $\Delta;\Gamma;\Sigma \vdash \Lambda\alpha.\, e : \forall\alpha.\, \tau_1$. Then we have that $\Delta, \alpha;\Gamma;\Sigma \vdash e : \tau_1$. Now from the Fundamental Property (Lemma 3.51, page 42) it follows that $\Delta, \alpha;\Gamma;\Sigma \vdash e \preceq^{log} e : \tau_1$. The rest of the proof is similar to that of the Lemma 3.41 (compatibility lemma for type abstraction). □

Definition 3.55. (Canonical World for Store Typing Σ)

If $\Sigma = \{l_1 : \tau_1, \ldots, l_n : \tau_n\}$ *and* $k \geq 0$, *then*
$W_{\mathsf{can}}(k, \Sigma) \stackrel{\text{def}}{=} \langle w_1, \ldots, w_n \rangle$, *where each* $w_i = w_{\mathsf{ref}}(k, \emptyset, \tau_i, l_i, l_i)$.

Lemma 3.56.

$W_{\mathsf{can}}(k, \Sigma) \in \mathit{World}_k$.

Proof

Let $\Sigma = \{l_1 : \tau_1, \ldots, l_n : \tau_n\}$. Then $W_{\mathsf{can}}(k, \Sigma) = \langle w_1, \ldots, w_n \rangle$, where each $w_i = w_{\mathsf{ref}}(k, \emptyset, \tau_i, l_i, l_i)$.

From the definition of w_{ref}, we have that each $w_i = (\eta_i, \mathcal{L}_i)$ where

$$\begin{array}{rcl} \eta_i & = & (\psi_i, \{\}, \{l_i : \tau_i\}, \{l_i : \tau_i\}) \\ \psi_i & = & \{(j, W', s_1, s_2) \mid \ (j, W', s_1(l_i), s_2(l_i)) \in \mathcal{V}_k[\![\tau_i]\!]\,\emptyset\} \\ \mathcal{L}_i & = & \{(j, \lfloor \eta_i \rfloor_j) \mid j \leq k\} \end{array}$$

Let $W = W_{\mathsf{can}}(k, \Sigma)$. We are required to show that

- $W \in \mathit{Island}_k^n$, which follows from the fact that each $w_i \in \mathit{Island}_k$, which in turn follows from:
  - $(\eta_i, \mathcal{L}_i) \in \mathit{Knowledge}_k \times \mathit{Law}_k$, which follows from the definition of η_i and $\mathcal{L}_i$, and
  - $(k, \eta_i) \in \mathcal{L}_i$
    $\equiv (k, \lfloor \eta_i \rfloor_k) \in \mathcal{L}_i$ (since $\eta_i = \lfloor \eta_i \rfloor_k$ by Lemma 3.6 (page 16) applied to $\eta_i \in \mathit{Knowledge}_k$)
    which is immediate from the definition of $\mathcal{L}_i$.
- $n \geq 0$, which is immediate since $\mathrm{dom}(\Sigma)$ contains $n \geq 0$ locations, and
- $\forall a, b \in \{1, \ldots, n\}.\ a \neq b \implies \mathrm{dom}(W[a].\Sigma_1) \,\#\, \mathrm{dom}(W[b].\Sigma_1) \ \wedge\ \mathrm{dom}(W[a].\Sigma_2) \,\#\, \mathrm{dom}(W[b].\Sigma_2)$, which follows from our choice of W above, since $\mathrm{dom}(W[a].\Sigma_1) = \mathrm{dom}(W[a].\Sigma_2 = \{l_a\}$ and $\mathrm{dom}(W[b].\Sigma_1) = \mathrm{dom}(W[b].\Sigma_2 = \{l_b\}$, and $l_a \neq l_b$ whenever $a \neq b$.

□

Lemma 3.57.

Let $W = W_{\mathsf{can}}(k, \Sigma)$. *Then* $(k, W) \in \mathcal{S}[\![\Sigma]\!]$.

Proof

Suppose $(l : \tau) \in \Sigma$.
We are required to show that $(k, W, l, l) \in \mathcal{V}[\![\mathsf{ref}\ \tau]\!]\,\emptyset$.

By the definition of $\mathcal{V}[\![\mathsf{ref}\ \tau]\!]\,\emptyset$, it suffices to show that $w_{\mathsf{ref}}(k, \emptyset, \tau, l, l) \in W$.
The latter is immediate from the premise and the definition of $W_{\mathsf{can}}(k, \Sigma)$. □

Lemma 3.58. (Store Parametricity)

If $\vdash s : \Sigma$ *and* $W = W_{\mathsf{can}}(k, \Sigma)$*, then* $s, s :_k W$*.*

Proof

Let $\Sigma = \{l_1 : \tau_1, \ldots, l_n : \tau_n\}$. Then $W = W_{\mathsf{can}}(k, \Sigma) = \langle w_1, \ldots, w_n \rangle$, where each $w_i = w_{\mathsf{ref}}(k, \emptyset, \tau_i, l_i, l_i)$.
From the definition of w_{ref}, we have that each $w_i = (\eta_i, \mathcal{L}_i)$ where

$$\begin{array}{rcl} \eta_i & = & (\psi_i, \{\}, \{l_i : \tau_i\}, \{l_i : \tau_i\}) \\ \psi_i & = & \{(j, W', s_1, s_2) \mid \ (j, W', s_1(l_i), s_2(l_i)) \in \mathcal{V}_k[\![\tau_i]\!]\,\emptyset \\ \mathcal{L}_i & = & \{(j, \lfloor \eta_i \rfloor_j) \mid j \leq k\} \end{array}$$

Hence, note that $w_i.\Sigma_1 = w_i.\Sigma_2 = \{l_i : \tau_i\}$.
Furthermore, $\Sigma_1(W) = \bigcup_{1 \leq i \leq n} w_i.\Sigma_1 = \bigcup_{1 \leq i \leq n} \{l_i : \tau_i\} = \Sigma$, and
$\Sigma_2(W) = \bigcup_{1 \leq i \leq n} w_i.\Sigma_2 = \bigcup_{1 \leq i \leq n} \{l_i : \tau_i\} = \Sigma$.
Finally, note that $W \in \mathit{World}_k$, which follows from Lemma 3.56 applied to $W_{\mathsf{can}}(k, \Sigma)$.

We are required to show that

- $\vdash s : \Sigma_1(W)$
  $\equiv \ \vdash s : \Sigma$,
  which is immediate,
- $\vdash s : \Sigma_1(W)$
  $\equiv \ \vdash s : \Sigma$,
  which is again immediate, and
- $\forall w_i \in W.\ \forall j < k.(j, \lfloor W \rfloor_j, s, s) \in w_i.\psi$
  $\equiv \ \forall w_i \in W.\ \forall j < k.(j, \lfloor W \rfloor_j, s, s) \in \psi_i$,
  which we conclude as follows:

  Consider arbitrary w_i and j such that $w_i \in W$ and $j < k$.

  From the definition of ψ_i above, it suffices to show that $(j, \lfloor W \rfloor_j, s(l_i), s(l_i)) \in \mathcal{V}_k[\![\tau_i]\!]\,\emptyset$.

  Note that from $\vdash s : \Sigma$ and $\Sigma(l_i) = \tau_i$, it follows that $\cdot; \cdot; \Sigma \vdash s(l_i) : \tau_i$.

  Applying Lemma 3.54 (page 44) to $\cdot; \cdot; \Sigma \vdash s(l_i) : \tau_i$, we have that $\cdot; \cdot; \Sigma \vdash s(l_i) \preceq^{log}_{\mathsf{val}} s(l_i) : \tau_i$.

  Instantiate the latter with k, $\emptyset$, $\emptyset$, and W. Note that

  - $k \geq 0$,
  - $\emptyset \in \mathcal{D}[\![\cdot]\!]$,
  - $(k, W, \emptyset) \in \mathcal{G}[\![\cdot]\!]\,\emptyset$,
    which follows from $W \in \mathit{World}_k$ (from above), and
  - $(k, W) \in \mathcal{S}[\![\Sigma]\!]$,
    which follows from Lemma 3.57 applied to $W_{\mathsf{can}}(k, \Sigma)$.

  Hence, $(k, W, s(l_i), s(l_i)) \in \mathcal{V}[\![\tau_i]\!]\,\emptyset$.

Applying Lemma 3.21 (page 19) to

- $\cdot \vdash \tau_i$,
- $\emptyset \in \mathcal{D}[\![\cdot]\!]$,
- $(k, W, s(l_i), s(l_i)) \in \mathcal{V}[\![\tau_i]\!]\emptyset$, and
- $(j, \lfloor W \rfloor_j) \sqsupseteq (k, W)$,
  which follows from Lemma 3.16 applied to $W \in \mathit{World}_k$,

we conclude that $(j, \lfloor W \rfloor_j, s(l_i), s(l_i)) \in \mathcal{V}[\![\tau_i]\!]\emptyset$.

Hence, $(j, \lfloor W \rfloor_j, s(l_i), s(l_i)) \in \lfloor \mathcal{V}[\![\tau_i]\!]\emptyset \rfloor_k$ since $j < k$.

Note that $\lfloor \mathcal{V}[\![\tau_i]\!]\emptyset \rfloor_k = \mathcal{V}_k[\![\tau_i]\!]\emptyset$ (from Lemma 3.4 (page 15) applied to $\cdot \vdash \tau_i$ and $\emptyset \in \mathcal{D}[\![\cdot]\!]$).

Finally, from $(j, \lfloor W \rfloor_j, s(l_i), s(l_i)) \in \lfloor \mathcal{V}[\![\tau_i]\!]\emptyset \rfloor_k$ together with $\lfloor \mathcal{V}[\![\tau_i]\!]\emptyset \rfloor_k = \mathcal{V}_k[\![\tau_i]\!]\emptyset$, it follows that $(j, \lfloor W \rfloor_j, s(l_i), s(l_i)) \in \mathcal{V}_k[\![\tau_i]\!]\emptyset$, as required.

□

Theorem 3.59. (Soundness w.r.t. Contextual Equivalence)

If $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau$ *then* $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{ctx} e_2 : \tau$.

Proof

Consider arbitrary C, Σ', τ', and s such that

- $\vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\cdot; \cdot; \Sigma' \vdash \tau')$,
- $\vdash s : \Sigma'$, and
- $s, C[e_1] \Downarrow$.

Hence, there exists some store s_1, some value v_1, and some k such that

- $s, C[e_1] \longmapsto^k s_1, v_1$.

We are required to show that $s, C[e_2] \Downarrow$.

Note that $\cdot; \cdot; \Sigma' \vdash C[e_1] \preceq^{log} C[e_2] : \tau'$, which follows from Lemma 3.52 (page 43) applied to $\vdash C : (\Delta; \Gamma; \Sigma \vdash \tau) \Rightarrow (\cdot; \cdot; \Sigma' \vdash \tau')$ and $\Delta; \Gamma; \Sigma \vdash e_1 \preceq^{log} e_2 : \tau$.

Let $W = W_{\mathsf{can}}(k+1, \Sigma')$.

Note that $W \in \mathit{World}_{k+1}$, which follows from Lemma 3.56 applied to $W_{\mathsf{can}}(k+1, \Sigma')$.

Instantiate $\cdot; \cdot; \Sigma' \vdash C[e_1] \preceq^{log} C[e_2] : \tau'$ with $k+1$, $\emptyset$, $\emptyset$, and W. Note that

- $k + 1 \geq 0$,
- $\emptyset \in \mathcal{D}[\![\cdot]\!]$,
- $(k+1, W, \emptyset) \in \mathcal{G}[\![\cdot]\!]$,
  which follows from $W \in \mathit{World}_{k+1}$ (from above), and
- $(k+1, W) \in \mathcal{S}[\![\Sigma']\!]$,
  which follows from Lemma 3.57 applied to $W_{\mathsf{can}}(k+1, \Sigma')$.

Hence $(k, W, C[e_1], C[e_2]) \in \mathcal{E}[\![\tau']\!]\emptyset$.

Instantiate the latter with k and s, s, s_1, and v_1. Note that

- $k < k + 1$,
- $s, s :_{k+1} W$,
  which follows from Lemma 3.58 (page 46) applied to $\vdash s : \Sigma'$ and W, and
- $s, C[e_1] \longmapsto^k s_1, v_1$,
  which follows from above.

Hence, there exist s_2, v_2, and W' such that

- $s, C[e_2] \longmapsto^* s_2, v_2$,
- $(k + 1 - k, W') \sqsupseteq (k+1, W)$,
- $s_1, s_2 :_{k+1-k} W'$, and
- $(k + 1 - k, W', v_1, v_2) \in \mathcal{V}[\![\tau']\!]\rho$.

Hence, $s, C[e_2] \Downarrow$. □

4 A Small Catalogue of Examples

The following is a list of examples that can be proved equivalent with our logical relation. Besides the ones considered in the main paper, it contains some additional cases from the literature, both monomorphic and polymorphic.

For each example we give a suitable island definition and, where needed, type relations for existential quantifiers, that form the core of the proof. In giving these definitions, we assume that k_0 is the current step level at which we have to introduce the respective island in the proof. Furthermore, we assume that the world at that point consists of p islands, so that the new one has index $p+1$.

Full details for some of the examples can be found in Section 5.

4.1 Redundant State

This is the most basic example, which appears in Meyer & Sieber (Example 1) [6], Koutavas & Wand (Section 6.1) [5], and Benton & Leperchey [3]. It shows that unused local state is irrelevant.

$$\begin{array}{rcl} e_1 & = & \lambda z:\tau.\, z \\ e_2 & = & \lambda z:\tau.\, \mathtt{let}\, x = \mathtt{ref}\, z\, \mathtt{in}\, z \end{array}$$

The store relation simply includes all possible stores:

$$\begin{array}{rcl} w_{p+1} & = & (\eta_{k_0}, \mathcal{L}_{k_0}) \\ \eta_k & = & (\psi_k, \emptyset, \{\}, \{l_x : \tau\}) \\ \psi_k & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k\} \\ \mathcal{L}_k & = & \{(j, \eta_j) \in \mathit{LawAtom}_k\} \end{array}$$

4.2 Higher-Order Function

The next example is a simple higher-order function that appears similarly in Koutavas & Wand (Section 6.2) [5] and Bohr & Birkedal [4]. It shows that the content of a local reference cannot be changed by the context.

$$\begin{array}{rcl} e_1 & = & \lambda f : (\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}. \\ & & \quad f\,(\lambda z : \mathsf{unit}.\,()) \\ & & \quad \mathtt{true} \\ e_2 & = & \lambda f : (\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}. \\ & & \quad \mathtt{let}\, x = \mathtt{ref}\, 0\, \mathtt{in} \\ & & \quad f\,(\lambda z : \mathsf{unit}.\, x := !\,x + 2); \\ & & \quad !\,x \bmod 2 = 0 \end{array}$$

The island's store relation simply includes all stores valid under the invariant:

$$\begin{array}{rcl} w_{p+1} & = & (\eta_{k_0}, \mathcal{L}_{k_0}) \\ \eta_k & = & (\psi_k, \emptyset, \{\}, \{l_x : \mathsf{int}\}) \\ \psi_k & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid \exists n \in \mathbb{N}, s'(l_x) = 2n\} \\ \mathcal{L}_k & = & \{(j, \eta_j) \in \mathit{LawAtom}_k\} \end{array}$$

The full proof for this example appears in Section 5.3.

4.3 Private Location

The following example also is due to Meyer & Sieber (Example 6) [6]. Related to the previous example, it demonstrates that the *identity* of a local reference cannot leak unexpectedly either.

$$
\begin{array}{rcl}
e_1 & = & \lambda f : (\mathsf{ref\ int} \to \mathsf{unit}) \to \mathsf{unit}. \\
& & \quad f\,(\lambda x : \mathsf{ref\ int}.\,()) \\
& & \quad \mathtt{true} \\
e_2 & = & \lambda f : (\mathsf{ref\ int} \to \mathsf{unit}) \to \mathsf{unit}. \\
& & \quad \mathtt{let}\, x = \mathtt{ref}\, 1\, \mathtt{in} \\
& & \quad f\,(\lambda x' : \mathsf{ref\ int}.\, \mathtt{if}\, x == x'\, \mathtt{then}\, x := 0\, \mathtt{else}\,()); \\
& & \quad !x \geq 0
\end{array}
$$

Again, the island's store relation simply includes all stores that are faithful to the invariant:

$$
\begin{array}{rcl}
w_{p+1} & = & (\eta_{k_0}, \mathcal{L}_{k_0}) \\
\eta_k & = & (\psi_k, \emptyset, \{\}, \{l_x : \mathsf{int}\}) \\
\psi_k & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid s'(l) > 0\} \\
\mathcal{L}_k & = & \{(j, \eta_j) \in \mathit{LawAtom}_k\}
\end{array}
$$

4.4 Fixpoint

We show that Landin's knot is a suitable implementation of a fixpoint operator by proving it equivalent to a built-in fixpoint operator (which we assume has been added to the language with obvious semantics).

$$
\begin{array}{rcl}
e_1 & = & \Lambda\alpha.\, \Lambda\beta.\, f \to (\alpha \to \beta) \times \alpha \to \beta \\
& & \quad \mathtt{fix}\,(\lambda g : \alpha \to \beta.\, \lambda x : \alpha.\, f\,\langle g, x\rangle) \\
e_2 & = & \Lambda\alpha.\, \Lambda\beta.\, f \to (\alpha \to \beta) \times \alpha \to \beta \\
& & \quad \mathtt{let}\, g = \mathtt{ref}\,(\lambda x : \alpha.\, \mathtt{diverge})\, \mathtt{in} \\
& & \quad g := \lambda x : \alpha.\, f\,\langle !\, g, x\rangle; \\
& & \quad !\, g
\end{array}
$$

The island definition for this example, is straightforward, it simply states that, once assigned, the location l_g holds the same function in all future worlds:

$$
\begin{array}{rcl}
w_{p+1} & = & (\eta_{k_0}, \mathcal{L}_{k_0}) \\
\eta_k & = & (\psi_k, \emptyset, \{\}, \{l_g : \tau'_\alpha \to \tau'_\beta\}) \\
\psi_k & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid s'(l_g) = (\lambda x : \tau'_\alpha.\, v_3\,\langle !\, l_g, x\rangle)\} \\
\mathcal{L}_k & = & \{(j, \eta_j) \in \mathit{LawAtom}_k\}
\end{array}
$$

We assume here that α and β have been instantiated with $\chi_\alpha \in \mathit{Type}[\tau_\alpha, \tau'_\alpha]$ and $\chi_\beta \in \mathit{Type}[\tau_\beta, \tau'_\beta]$, respectively, and that v_3, v'_3 are passed for f.

The actual proof is not difficult, but unlike the others requires induction on the step level to show that the two functions are related in all reachable future worlds.

4.5 Callback with Lock

The following example (from the main paper) is similar to the callback example given by Banerjee & Naumann [2]. It is interesting because it involves state that can be accessed recursively through a higher-order

argument.

$$
\begin{array}{rcl}
e_1 & = & \texttt{let}\, b = \texttt{ref}\, \texttt{true}\, \texttt{in} \\
& & \texttt{let}\, x = \texttt{ref}\, 0\, \texttt{in} \\
& & \langle \lambda f : \mathsf{unit} \to \mathsf{unit}. \\
& & \quad (\texttt{if}\, !b\, \texttt{then}\, (b := \texttt{false}; f\,(); x := !x + 1; b := \texttt{true})\, \texttt{else}\, ()) \\
& & \lambda z : \mathsf{unit}.\, !x \rangle \\
e_2 & = & \texttt{let}\, b = \texttt{ref}\, \texttt{true}\, \texttt{in} \\
& & \texttt{let}\, x = \texttt{ref}\, 0\, \texttt{in} \\
& & \langle \lambda f : \mathsf{unit} \to \mathsf{unit}. \\
& & \quad (\texttt{if}\, !b\, \texttt{then}\, (b := \texttt{false}; \texttt{let}\, n = !x\, \texttt{in}\, f\,(); x := n + 1; b := \texttt{true})\, \texttt{else}\, ()) \\
& & \lambda z : \mathsf{unit}.\, !x \rangle
\end{array}
$$

As explained in the main paper, we establish an island that allows dynamic addition of time windows in which the reference is locked and may not change.

$$
\begin{array}{rcl}
w_{p+1} & = & (\eta_{k_0}^{\{(k_0+1,k_0+1,0)\}}, \mathcal{L}_{k_0}) \\
\eta_k^V & = & (\psi_k^{\min(V)}, V, \{l_b : \mathsf{bool}, l_n : \mathsf{int}\}, \{l'_b : \mathsf{bool}, l'_n : \mathsf{int}\}) \\
\psi_k^{(k_1,k_2,v)} & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid (k_1 \geq j \geq k_2 \ \wedge s(l_b) = s'(l'_b) = \texttt{false} \ \wedge s(l_n) = s'(l'_n) = v) \vee \\
& & \qquad\qquad\qquad\qquad (k_1 \geq k_2 > j \ \wedge s(l_b) = s'(l'_b) \qquad\quad \wedge s(l_n) = s'(l'_n))\} \\
\mathcal{L}_k & = & \{(j, \eta_k^{\{\langle k_1, k'_1, v_1\rangle, \ldots, \langle k_n, k'_n, v_n\rangle\}}) \in \mathit{LawAtom}_k \mid k_1 \geq k'_1 > k_2 \geq \cdots \geq k'_{n-1} > k_n \geq k'_n\}
\end{array}
$$

The full proof can be found in Section 5.4.

4.6 Cell Object

The following is a polymorphic variation on the higher-order cell example from Koutavas & Wand (Section 6.3) [5] and Bohr & Birkedal [4]:

$$
\begin{array}{rcl}
e_1 & = & \Lambda\alpha.\, \lambda z : \alpha. \\
& & \quad \texttt{let}\, x = \texttt{ref}\, z\, \texttt{in} \\
& & \quad \langle \lambda z' : \alpha.\, (x := z'), \\
& & \quad\ \lambda z' : \mathsf{unit}.\, !x \rangle \\
e_2 & = & \Lambda\alpha.\, \lambda z : \alpha. \\
& & \quad \texttt{let}\, x_0 = \texttt{ref}\, 1\, \texttt{in} \\
& & \quad \texttt{let}\, x_1 = \texttt{ref}\, z\, \texttt{in} \\
& & \quad \texttt{let}\, x_2 = \texttt{ref}\, z\, \texttt{in} \\
& & \quad \langle \lambda z' : \alpha.\, \texttt{if}\, !x_0 = 1\, \texttt{then}\, (x_0 := 2; x_2 := z')\, \texttt{else}\, (x_0 := 1; x_1 := z'), \\
& & \quad\ \lambda z' : \mathsf{unit}.\, \texttt{if}\, !x_0 = 1\, \texttt{then}\, !x_1\, \texttt{else}\, !x_2 \rangle
\end{array}
$$

Assuming that α has been instantiated with $\chi_\alpha \in \mathit{Type}[\tau_\alpha, \tau'_\alpha]$, the island is straightforward:

$$
\begin{array}{rcl}
w_{p+1} & = & (\eta_{k_0}, \mathcal{L}_{k_0}) \\
\eta_k & = & (\psi_k, \emptyset, \{l_x : \tau_\alpha\}, \{l'_0 : \mathsf{int}, l'_1 : \tau'_\alpha, l'_2 : \tau'_\alpha\}) \\
\psi_k & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid \exists i \in \{1, 2\}, s'(l'_0) = i \wedge (j, W, s(l_x), s'(l'_i)) \in \chi_\alpha\} \\
\mathcal{L}_k & = & \{(j, \eta_j) \in \mathit{LawAtom}_k\}
\end{array}
$$

4.7 Cell Class

We can also generalize the previous example to an encoding of an actual *class* (which is generic):

$$
\begin{array}{rcl}
e_1 & = & \Lambda\alpha.\,\mathtt{pack}\,\mathsf{ref}\,\alpha, \\
& & \quad \langle \lambda x:\alpha.\,\mathtt{ref}\,x, \\
& & \quad\ \lambda o:\mathsf{ref}\,\alpha.\,!o, \\
& & \quad\ \lambda o:\mathsf{ref}\,\alpha.\,\lambda x:\alpha.\,(o := x)\rangle\,\mathsf{as}\,\sigma \\
e_2 & = & \Lambda\alpha.\,\mathtt{pack}\,(\mathsf{ref}\,\mathsf{int}\times(\mathsf{ref}\,\alpha\times\mathsf{ref}\,\alpha)), \\
& & \quad \langle \lambda x:\alpha.\,\langle \mathtt{ref}\,1, \langle \mathtt{ref}\,x, \mathtt{ref}\,x\rangle\rangle, \\
& & \quad\ \lambda o:(\mathsf{ref}\,\mathsf{int}\times(\mathsf{ref}\,\alpha\times\mathsf{ref}\,\alpha)). \\
& & \quad\quad \mathtt{if}\,!(\mathtt{fst}\,o) = 1 \\
& & \quad\quad \mathtt{then}\,!(\mathtt{fst}\,(\mathtt{snd}\,o)) \\
& & \quad\quad \mathtt{else}\,!(\mathtt{snd}\,(\mathtt{snd}\,o)), \\
& & \quad\ \lambda o:(\mathsf{ref}\,\mathsf{int}\times(\mathsf{ref}\,\alpha\times\mathsf{ref}\,\alpha)).\,\lambda x:\alpha. \\
& & \quad\quad \mathtt{if}\,!(\mathtt{fst}\,o) = 1 \\
& & \quad\quad \mathtt{then}\,(\mathtt{fst}\,o := 2; \mathtt{snd}\,(\mathtt{snd}\,o) := x) \\
& & \quad\quad \mathtt{else}\,(\mathtt{fst}\,o := 1; \mathtt{fst}\,(\mathtt{snd}\,o) := x)\rangle\,\mathsf{as}\,\sigma \\
\sigma & = & \exists\beta.\,(\alpha\to\beta)\times(\beta\to\alpha)\times(\beta\to\alpha\to\mathsf{unit})
\end{array}
$$

This time, the island definition is more involved, because arbitrary many objects can be allocated. The allocated objects are recorded in the population, which also relates both sides:

$$
\begin{array}{rcl}
w_{p+1} & = & (\eta^{\emptyset}_{k_0}, \mathcal{L}_{k_0}) \\
\eta^L_k & = & (\psi^L_k, L, \Sigma_L, \Sigma'_L) \\
\psi^L_k & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid \forall\langle l, l'_0, l'_1, l'_2\rangle \in L, \exists i \in \{1,2\}, s'(l'_0) = i \wedge (j, W, s(l), s'(l'_i)) \in \chi_\alpha\} \\
\Sigma_L & = & \{l : \tau_\alpha \mid \langle l, l'_0, l'_1, l'_2\rangle \in L\} \\
\Sigma'_L & = & \{l'_0 : \mathsf{int}, l'_1 : \tau'_\alpha, l'_2 : \tau'_\alpha \mid \langle l, l'_0, l'_1, l'_2\rangle \in L\} \\
\mathcal{L}_k & = & \{(j, \eta^L_j) \in \mathit{LawAtom}_k\} \\
\chi_\beta & = & \{(j, W, l, \langle l'_0, l'_1, l'_2\rangle) \in \mathit{Atom}[\mathsf{ref}\,\tau_\alpha, \mathsf{ref}\,\mathsf{int}\times\mathsf{ref}\,\tau'_\alpha\times\mathsf{ref}\,\tau'_\alpha]_{k_0} \mid \langle l, l'_0, l'_1, l'_2\rangle \in W[p+1].V\}
\end{array}
$$

where all locations in a set L are disjoint.

4.8 Name Generator

This is the main example from our paper, where the interpretation of an abstract types depends on the current state:

$$
\begin{array}{rcl}
e_1 & = & \mathtt{let}\,x = \mathtt{ref}\,0\,\mathtt{in} \\
& & \mathtt{pack}\,\mathsf{int}, \langle \lambda z:\mathsf{unit}.\,(x := !x + 1; !x), \\
& & \qquad \lambda z:\mathsf{int}.\,(z \le !x)\rangle\,\mathsf{as}\,\sigma \\
e_2 & = & \mathtt{let}\,x = \mathtt{ref}\,0\,\mathtt{in} \\
& & \mathtt{pack}\,\mathsf{int}, \langle \lambda z:\mathsf{unit}.\,(x := !x + 1; !x), \\
& & \qquad \lambda z:\mathsf{int}.\,\mathtt{true}\rangle\,\mathsf{as}\,\sigma \\
\sigma & = & \exists\alpha.\,(\mathsf{unit}\to\alpha)\times(\alpha\to\mathsf{bool})
\end{array}
$$

The island's population records the "valid" names generated s far:

$$\begin{array}{rcl} w_{p+1} & = & (\eta^0_{k_0}, \mathcal{L}_{k_0}) \\ \eta^n_k & = & (\psi^n_k, V_n, \{l_x : \mathsf{int}\}, \{l'_x : \mathsf{int}\}) \\ \psi^n_k & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid s(l_x) = s'(l'_x) = n\} \\ V_n & = & \{i \mid 1 \le i \le n\} \\ \mathcal{L}_k & = & \{(j, \eta^n_j) \in \mathit{LawAtom}_k \mid n \in \mathbb{N}\} \\ \chi_\alpha & = & \{(j, W, i, i) \in \mathit{Atom}[\mathsf{int}, \mathsf{int}]_{k_0} \mid i \in W[p+1].V\} \end{array}$$

A fully detailed proof for this example is given in Section 5.1.

4.9 Dynamic Data Structures

The following variation of the name generator implements the counter using a mutable recursive type to represent naturals. Although its use of actual mutation is limited, the example demonstrates the treatment of dynamically allocated data structures.

$$\begin{array}{rcl} e_1 & = & \mathtt{let}\, x = \mathtt{ref}\, (\mathtt{fold}\, \mathtt{inl}\, ())\, \mathtt{in} \\ & & \mathtt{pack}\, \mu\alpha.\, \mathsf{unit} + \mathsf{ref}\, \alpha, \langle \lambda z : \mathsf{unit}.\, (x := \mathtt{fold}\, (\mathtt{inr}\, (!x)); \mathit{toInt}\, (!x)), \\ & & \qquad \lambda z : \mathsf{int}.\, (z \le \mathit{toInt}\, (!x))\rangle\, \mathsf{as}\, \sigma \\ e_2 & = & \mathtt{let}\, x = \mathtt{ref}\, 0\, \mathtt{in} \\ & & \mathtt{pack}\, \mathsf{int}, \langle \lambda z : \mathsf{unit}.\, (x := !x + 1; !x), \\ & & \qquad \lambda z : \mathsf{int}.\, \mathtt{true}\rangle\, \mathsf{as}\, \sigma \\ \sigma & = & \exists\alpha.\, (\mathsf{unit} \to \alpha) \times (\alpha \to \mathsf{bool}) \end{array}$$

We assume that the helper function $\mathit{toInt} : (\mu\alpha.\, \mathsf{unit} + \mathsf{ref}\, \alpha) \to \mathsf{int}$ is defined in the obvious way.

The law has to allow the data structure to grow, relative to some constraints on its inner structure, which is encoded in the side condition of the store relation:

$$\begin{array}{rcl} w_{p+1} & = & (\eta^{\emptyset}_{k_0}, \mathcal{L}_{k_0}) \\ \eta^{\{l_1,\ldots,l_n\}}_k & = & (\psi^{\{l_1,\ldots,l_n\}}_k, V_n, \{l_0 : (\mu\alpha.\, 1 + \mathsf{ref}\, \alpha), \ldots, l_n : (\mu\alpha.\, 1 + \mathsf{ref}\, \alpha)\}, \{l'_x : \mathsf{int}\}) \\ \psi^{\{l_1,\ldots,l_n\}}_k & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid s'(l'_x) = n \wedge s(l_n) = \mathtt{fold}\, (\mathtt{inl}\, ()) \\ & & \qquad \wedge \forall i \in \{0, \ldots, n-1\}, s(l_i) = \mathtt{fold}\, (\mathtt{inr}\, l_{i+1})\} \\ V_n & = & \{i \mid 1 \le i \le n\} \\ \mathcal{L}_k & = & \{(j, \eta^{\{l_1,\ldots,l_n\}}_j) \in \mathit{LawAtom}_k \mid l_0 \notin \{l_1, \ldots, l_n\}\} \\ \chi_\alpha & = & \{(j, W, i, i) \in \mathit{Atom}[\mathsf{int}, \mathsf{int}]_{k_0} \mid i \in W[p+1].V\} \end{array}$$

Here, l_0 is supposed to be the location allocated for x in e_1.

4.10 Name Generator with References

Another implementation of a name generator relies on the generativity of references. We can show it equivalent to the one using integers:

$$\begin{array}{rcl} e_1 & = & \mathtt{let}\, x = \mathtt{ref}\, 0\, \mathtt{in} \\ & & \mathtt{pack}\, \mathsf{int}, \langle \lambda z : \mathsf{unit}.\, (x := !x + 1; !x), \\ & & \qquad \lambda p : (\mathsf{int} \times \mathsf{int}).\, (\mathtt{fst}\, p = \mathtt{snd}\, p)\rangle\, \mathsf{as}\, \sigma \\ e_2 & = & \mathtt{pack}\, \mathsf{ref\ unit}, \langle \lambda z : \mathsf{unit}.\, (\mathtt{ref}\, ()), \\ & & \qquad \lambda p : (\mathsf{ref\ unit} \times \mathsf{ref\ unit}).\, (\mathtt{fst}\, p == \mathtt{snd}\, p)\rangle\, \mathsf{as}\, \sigma \\ \sigma & = & \exists\alpha.\, (\mathsf{unit} \to \alpha) \times (\alpha \times \alpha \to \mathsf{bool}) \end{array}$$

The island not only has to record the valid integer names, it also has to relate them to the references allocated on the other side. We therefor encode a partial bijection in the population V:

$$\begin{array}{rcl}
w_{p+1} & = & (\eta_{k_0}^{\langle\rangle}, \mathcal{L}_{k_0}) \\
\eta_k^{\langle l_1,\ldots,l_n\rangle} & = & (\psi_k^n, \{\langle 1, l_1\rangle, \ldots, \langle n, l_n\rangle\}, \{l_x : \mathsf{int}\}, \{l_1 : \mathsf{unit}, \ldots, l_n : \mathsf{unit}\}) \\
\psi_k^n & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid s(l_x) = n\} \\
\mathcal{L}_k & = & \{(j, \eta_j^{\langle l_1,\ldots,l_n\rangle}) \in \mathit{LawAtom}_k \mid n \in \mathbb{N}\} \\
\chi_\alpha & = & \{(j, W, i, l) \in \mathit{Atom}[\mathsf{int}, \mathsf{ref}\ \mathsf{unit}]_{k_0} \mid \langle i, l\rangle \in W[p+1].V\}
\end{array}$$

We require that $l_1, \ldots, l_n$ are pairwise disjoint.

The full proof can be found in Section 5.2.

4.11 Twin Abstraction

An island may be associated with several abstract types, with non-trivial interdependencies:

$$\begin{array}{rcl}
e_1 & = & \mathtt{let}\, x = \mathtt{ref}\, 0\, \mathtt{in} \\
& & \mathtt{pack}\, \mathsf{int}, \mathsf{int}, \langle \lambda z : \mathsf{unit}.\, (x := !x + 1; !x), \\
& & \qquad\qquad \lambda z : \mathsf{unit}.\, (x := !x + 1; !x), \\
& & \qquad\qquad \lambda p : (\mathsf{int} \times \mathsf{int}).\, \mathtt{false}\rangle\, \mathsf{as}\, \sigma \\
e_2 & = & \mathtt{let}\, x = \mathtt{ref}\, 0\, \mathtt{in} \\
& & \mathtt{pack}\, \mathsf{int}, \mathsf{int}, \langle \lambda z : \mathsf{unit}.\, (x := !x + 1; !x), \\
& & \qquad\qquad \lambda z : \mathsf{unit}.\, (x := !x + 1; !x), \\
& & \qquad\qquad \lambda p : (\mathsf{int} \times \mathsf{int}).\, (\mathtt{fst}\, p = \mathtt{snd}\, p)\rangle\, \mathsf{as}\, \sigma \\
\sigma & = & \exists \alpha, \beta.\, (\mathsf{unit} \to \alpha) \times (\mathsf{unit} \to \beta) \times (\alpha \times \beta \to \mathsf{bool})
\end{array}$$

We need to establish that the values inhabiting the two abstract types are disjoint, which we do by partitioning the island's population properly:

$$\begin{array}{rcl}
w_{p+1} & = & (\eta_{k_0}^{0,\emptyset}, \mathcal{L}_{k_0}) \\
\eta_k^{n,S} & = & (\psi_k^n, V_{n,S}, \{l_x : \mathsf{int}\}, \{l'_x : \mathsf{int}\}) \\
\psi_k^n & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid s(l_x) = s'(l'_x) = n\} \\
V_{n,S} & = & \{\langle 1, i\rangle \mid i \in S\} \cup \{\langle 2, i\rangle \mid i \in \{1, \ldots, n\} \setminus S\} \\
\mathcal{L}_k & = & \{(j, \eta_j^{n,S}) \in \mathit{LawAtom}_k \mid S \subseteq \{1, \ldots, n\}\} \\
\chi_\alpha & = & \{(j, W, i, i) \in \mathit{Atom}[\mathsf{int}, \mathsf{int}]_{k_0} \mid \langle 1, i\rangle \in W[p+1].V\} \\
\chi_\beta & = & \{(j, W, i, i) \in \mathit{Atom}[\mathsf{int}, \mathsf{int}]_{k_0} \mid \langle 2, i\rangle \in W[p+1].V\}
\end{array}$$

4.12 Abstract References

We can prove invariants about references even if they leak to the context — as long as their content type is hidden (we chose a rather trivial invariant for this example):

$$\begin{array}{rcl}
e_1 & = & \mathtt{let}\, x = \mathtt{ref}\, 7\, \mathtt{in} \\
& & \mathtt{pack}\, \mathsf{int}, \langle x, \lambda z : \mathsf{ref}\, \mathsf{int}.\, \mathtt{true}\rangle\, \mathsf{as}\, \sigma \\
e_2 & = & \mathtt{let}\, x = \mathtt{ref}\, 7\, \mathtt{in} \\
& & \mathtt{pack}\, \mathsf{int}, \langle x, \lambda z : \mathsf{ref}\, \mathsf{int}.\, (!x = !z)\rangle\, \mathsf{as}\, \sigma \\
\sigma & = & \exists \alpha.\, \mathsf{ref}\, \alpha \times (\alpha \to \mathsf{bool})
\end{array}$$

The island definition, but also the type relation, are straightforward in this case:

$$\begin{array}{rcl} w_{p+1} & = & (\eta_{k_0}, \mathcal{L}_{k_0}) \\ \eta_k & = & (\psi_k, \emptyset, \{l_x : \mathsf{int}\}, \{l'_x : \mathsf{int}\}) \\ \psi_k & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid s(l_x) = s'(l'_x) = 7\} \\ \mathcal{L}_k & = & \{(j, \eta_j) \in \mathit{LawAtom}_k\} \\ \chi_\alpha & = & \{(j, W, 7, 7) \in \mathit{Atom}[\mathsf{int}, \mathsf{int}]_{k_0}\} \end{array}$$

4.13 Symbol

Finally, we give an island and type interpretation that would be suitable for proving the invariant of the motivating `Symbol` example from the main paper (assuming an appropriate encoding of the example into our language). Note that it is a straightforward generalization of the island for the name generator:

$$\begin{array}{rcl} w_{p+1} & = & (\eta^0_{k_0}, \mathcal{L}_{k_0}) \\ \eta^n_k & = & (\psi^n_k, V_n, \{l_{size} : \mathsf{int}, l_{table} : \mu\alpha.\, \mathsf{unit} + \mathsf{string} \times \alpha\}, \{l'_{size} : \mathsf{int}, l'_{table} : \mu\alpha.\, \mathsf{unit} + \mathsf{string} \times \alpha\}) \\ \psi^n_k & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid s(l_{size}) = s'(l'_{size}) = n \wedge \\ & & \qquad\qquad s(l_{table}) = s'(l'_{table}) \wedge \\ & & \qquad\qquad \mathit{length}(s(l_{table})) = \mathit{length}(s'(l'_{table})) = n\} \\ V_n & = & \{i \mid 1 \le i \le n\} \\ \mathcal{L}_k & = & \{(j, \eta^n_j) \in \mathit{LawAtom}_k \mid n \in \mathbb{N}\} \\ \chi_t & = & \{(j, W, i, i) \in \mathit{Atom}[\mathsf{int}, \mathsf{int}]_{k_0} \mid i \in W[p+1].V\} \end{array}$$

The auxiliary meta-function *length* computes the length of a list and is defined in the obvious way.

5 Example Proofs

In the following, we present several examples of reasoning with our logical relation in all gory detail. In Section 5.1, we redo the proof for the name generator example from the main paper, with omissions filled in. In the other subsections, we show a couple of other proofs for examples from the main paper and the catalogue in Section 4.

5.1 Name Generator

Recall the name generator from the main paper:

$$\begin{array}{rcl} e & = & P[\lambda z : \mathsf{int}.\, z \leq\, !x] \\ e' & = & P[\lambda z : \mathsf{int}.\, \mathtt{true}] \\ \text{where } P[E] & = & \mathtt{let}\, x = \mathtt{ref}\, 0\, \mathtt{in}\, (\mathtt{pack}\, \mathit{int}, \langle \lambda z : \mathsf{unit}.\, (x := !x + 1; !x), E\rangle\, \mathtt{as}\, \sigma) \\ \sigma & = & \exists \alpha.\, (\mathsf{unit} \to \alpha) \times (\alpha \to \mathsf{bool}) \end{array}$$

We want to show that:

$$\vdash e \preceq e' : \sigma$$

By definition of approximation, we have to show:

$$\forall k_0 \geq 0, W_0, \quad (k_0, W_0, e, e') \in \mathcal{E}\,[\![\sigma]\!]\,\emptyset$$

By definition of $\mathcal{E}\,[\![\tau]\!]$, we need to show:

$$\begin{array}{rlll} \forall k_1 < k_0, s_0, s_0', s_1, v_1, & s_0, s_0' :_{k_0} W_0 & \wedge & s_0, P[\lambda z : \mathsf{int}.\, z \leq\, !x] \longmapsto^{k_1} s_1, v_1 \implies \\ \exists s_1', v_1', W_1, & s_1, s_1' :_{k_0 - k_1} W_1 & \wedge & s_0', P[\lambda z : \mathsf{int}.\, \mathtt{true}] \longmapsto^{*} s_1', v_1' \wedge \\ & (k_0 - k_1, W_1) \sqsupseteq (k_0, W_0) & \wedge & (k_0 - k_1, W_1, v_1, v_1') \in \mathcal{V}\,[\![\sigma]\!]\,\emptyset \end{array}$$

Assume $s_0, s_0' :_{k_0} W_0$ and $s_0, P[\lambda z : \mathsf{int}.\, z \leq\, !x] \longmapsto^{k_1} s_1, v_1$. By definition of reduction, the following has to hold for some $l \notin \mathrm{dom}(s_0)$ and $l' \notin \mathrm{dom}(s_0')$:

$$\begin{array}{rclcrcl} s_1 & = & s_0[l \mapsto 0], & \quad & v_1 & = & (\mathtt{pack}\, \mathsf{int}, \langle \lambda z : \mathsf{unit}.\, (l := !l + 1; !l), \lambda z : \mathsf{int}.\, z \leq\, !l\rangle\, \mathtt{as}\, \sigma) \\ s_1' & = & s_0'[l' \mapsto 0], & & v_1' & = & (\mathtt{pack}\, \mathsf{int}, \langle \lambda z : \mathsf{unit}.\, (l' := !l' + 1; !l'), \lambda z : \mathsf{int}.\, \mathtt{true}\rangle\, \mathtt{as}\, \sigma) \end{array}$$

Assume $W_0 = \langle w_1, \ldots, w_p\rangle$. Now let:

$$\begin{array}{rcl} W_1 & = & \langle w_1, \ldots, w_p, w_{p+1}\rangle \\ \text{where } w_{p+1} & = & (\eta^0_{k_0-k_1}, \mathcal{L}_{k_0-k_1}) \\ \eta^n_k & = & (\psi^n_k, V_n, \{l : \mathsf{int}\}, \{l' : \mathsf{int}\}) \\ \psi^n_k & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid s(l) = s'(l') = n\} \\ V_n & = & \{i \mid 1 \leq i \leq n\} \\ \mathcal{L}_k & = & \{(j, \eta^n_j) \in \mathit{LawAtom}_k \mid n \in \mathbb{N}\} \end{array}$$

We have to show the necessary properties for this definition:

1. $W_1 \in \mathit{World}_{k_0-k_1}$:
   - It is easy to see that, for all k and n, we have $\psi^n_k \in \mathit{StoreRel}_k$ and $V_n \in \mathit{Population}$.
   - Hence, for all k and n, $\eta^n_k \in \mathit{Knowledge}_{k_0-k_1}$.
   - Note that, for all n, k, $k' < k$, we have $\lfloor \psi^n_k \rfloor_{k'} = \psi^n_{k'}$, and thus also $\lfloor \eta^n_k \rfloor_{k'} = \eta^n_{k'}$.
   - Hence, $\mathcal{L}_k$ is downward closed and thus in Law_k.

- Consequently, also $(k_0 - k_1, \eta^0_{k_0-k_1}) \in \mathcal{L}_{k_0-k_1}$.
- So, $w_{p+1} \in \mathit{Island}_{k_0-k_1}$.
- And since l and l' are fresh wrt. s_0 and s_0', and $s_0, s_0' :_{k_0} W_0$, we know that $l \notin \mathrm{dom}(\Sigma_1(W_0))$ and $l' \notin \mathrm{dom}(\Sigma_2(W_0))$.

2. $(k_0 - k_1, W_1) \sqsupseteq (k_0, W_0)$:
   - Trivial, since $k_0 - k_1 \leq k_0$ and $w_1, \ldots, w_p$ are unchanged.
3. $s_1, s_1' :_{k_0-k_1} W_1$:
   - Obviously, $\vdash s_1 : \{l : \mathsf{int}\}$ and $\vdash s_1' : \{l' : \mathsf{int}\}$.
   - Clearly, for all $j < k_0 - k_1$, $(j, \lfloor W \rfloor_j, s_1, s_1') \in \psi^0_{k_0-k_1} = w_{p+1}.\psi$.
   - From the definition of *StoreRel* and *Island* we know that $w_1.\psi, \ldots, w_p.\psi$ are downward closed. It follows that for all $1 \leq i \leq p$ and $j < k_0 - k_1$, $(j, \lfloor W_1 \rfloor_j, s_1, s_1') \in \psi(w_i)$ (because for all $j \leq k$, $(j, \lfloor W \rfloor_k) \sqsupseteq (k, W)$).

Also note that, for all $n' \geq n$ and $k' \leq k$, it holds that $\eta^{n'}_{k'} \sqsupseteq \eta^n_k$.

By definition of $\mathcal{V}[\![\exists\alpha.\tau]\!]$, it now remains to be shown that:

$$\exists \chi \in \mathit{Type}[\mathsf{int}, \mathsf{int}],\quad (k_0 - k_1, W_1, \langle \lambda z : \mathsf{unit}.\, (l := !l + 1; !l), \lambda z : \mathsf{int}.\, z \leq !l \rangle, \\ \langle \lambda z : \mathsf{unit}.\, (l' := !l' + 1; !l'), \lambda z : \mathsf{int}.\, \mathtt{true} \rangle) \in \mathcal{V}[\![(\mathsf{unit} \to \alpha) \times (\alpha \to \mathsf{bool})]\!]\,\rho$$

for $\rho = [\alpha \mapsto (\chi, \mathsf{int}, \mathsf{int})]$. Define:

$$\chi = \{(j, W, i, i) \in \mathit{Atom}[\mathsf{int}, \mathsf{int}]_{k_0-k_1} \mid i \in W[p+1].V\}$$

We need to check that $\chi \in \mathit{Type}[\mathsf{int}, \mathsf{int}]_{k_0-k_1}$. That is straightforward:

- Assume $(j, W, i, i) \in \chi$ and $(j', W') \sqsupseteq (j, W)$.
- From the former it follows that $i \in W[p+1].V$.
- From the latter it follows that $W'[p+1].V \supseteq W[p+1].V$ and $j' \leq j$.
- Hence, $(j', W', i, i) \in \chi$.

By definition of $\mathcal{V}[\![\tau \times \tau']\!]$, we now have to show that:

1. $(k_0 - k_1, W_1, \lambda z : \mathsf{unit}.\, (l := !l + 1; !l), \lambda z : \mathsf{unit}.\, (l' := !l' + 1; !l')) \in \mathcal{V}[\![\mathsf{unit} \to \alpha]\!]\,\rho$
2. $(k_0 - k_1, W_1, \lambda z : \mathsf{int}.\, z \leq !l, \lambda z : \mathsf{int}.\, \mathtt{true}) \in \mathcal{V}[\![\alpha \to \mathsf{bool}]\!]\,\rho$

First consider (1). By definition of $\mathcal{V}[\![\tau \to \tau']\!]$, we have to show that:

$$\forall (k_2, W_2) \sqsupset (k_0 - k_1, W_1),\quad (k_2, W_2, v_2, v_2') \in \mathcal{V}[\![\mathsf{unit}]\!]\,\rho \implies \\ (k_2, W_2, (l := !l + 1; !l), (l' := !l' + 1; !l')) \in \mathcal{E}[\![\alpha]\!]\,\rho$$

Assume $(k_2, W_2) \sqsupset (k_0 - k_1, W_1)$. By definition of $\mathcal{E}[\![\tau]\!]$, we have to show:

$$\begin{array}{rlll} \forall k_3 < k_2, s_2, s_2', s_3, v_3, & s_2, s_2' :_{k_2} W_2 & \wedge & s_2, (l := !l + 1; !l) \longmapsto^{k_3} s_3, v_3 \implies \\ \exists s_3', v_3', W_3, & s_3, s_3' :_{k_2-k_3} W_3 & \wedge & s_2', (l' := !l' + 1; !l') \longmapsto^{*} s_3', v_3' \wedge \\ & (k_2 - k_3, W_3) \sqsupseteq (k_2, W_2) & \wedge & (k_2 - k_3, W_3, v_3, v_3') \in \mathcal{V}[\![\alpha]\!]\,\emptyset \end{array}$$

Assume $s_2, s_2' :_{k_2} W_2$ and $s_2, (l := !l + 1; !l) \longmapsto^{k_3} s_3, v_3$. From $(k_2, W_2) \sqsupseteq (k_0 - k_1, W_1)$ it follows that $W_2[p+1].\mathcal{L} = \lfloor W_1[p+1].\mathcal{L} \rfloor_{k_2} = \lfloor \mathcal{L}_{k_0-k_1} \rfloor_{k_2} = \mathcal{L}_{k_2}$. From that, by definition of $Island_{k_2}$, we know $(k_2, W_2[p+1].\eta) \in \mathcal{L}_{k_2}$, and there exists n, such that

$$\begin{array}{rcl} W_2[p+1].\eta & = & \eta^n_{k_2} \\ \text{that is, } W_2[p+1].\psi & = & \psi^n_{k_2} \\ W_2[p+1].V & = & V_n \end{array}$$

as defined above. Because $k_2 > k_3$, apparently, $k_2 > 0$. From $s_2, s_2' :_{k_2} W_2$ and we can thereby conclude $(k_2 - 1, \lfloor W_2 \rfloor_{k_2-1}, s_2, s_2') \in \psi^n_{k_2}$ and thus

$$s_2(l) = s_2'(l') = n$$

By definition of reduction, the following must hold:

$$\begin{array}{rclcrcl} s_3 & = & s_2[l \mapsto n+1], & & v_3 & = & n+1 \\ s_3' & = & s_2'[l' \mapsto n+1], & & v_3' & = & n+1 \end{array}$$

Now choose W_3 such that w_{p+1} is updated as follows:

$$\begin{array}{rcl} W_3[p+1].\mathcal{L} & = & \mathcal{L}_{k_2-k_3} \\ W_3[p+1].\eta & = & \eta^{n+1}_{k_2-k_3} \\ \text{that is, } W_3[p+1].\psi & = & \psi^{n+1}_{k_2-k_3} \\ W_3[p+1].V & = & V_{n+1} \end{array}$$

Again, we have to show that this definition has the necessary properties:

1. $W_3 \in World_{k_2-k_3}$:
   - Follows by the same reasoning as above. In particular, it is obvious from the definition of $\mathcal{L}_k$ that $W_3[p+1].\eta \in \lfloor \mathcal{L} \rfloor_{k_2-k_3} = \mathcal{L}_{k_2-k_3}$.
2. $(k_2 - k_3, W_3) \sqsupseteq (k_2, W_2)$:
   - Obviously, $W_3[p+1].V \supset W_2[p+1].V$. Hence, $W_3[p+1].\eta \sqsupseteq W_2[p+1].\eta$.
   - Because $W_3[p+1].\mathcal{L} = \lfloor W_2[p+1].\mathcal{L} \rfloor_{k_2-k_3}$ and $k_2 - k_3 \leq k_2$, we have $W_3 \sqsupseteq W_2$.
3. $s_3, s_3' :_{k_2-k_3} W_3$:
   - As before. Specifically, for all $j < k_2 - k_3$, $(j, \lfloor W_3 \rfloor_j, s_3, s_3') \in \psi^{n+1}_{k_2-k_3}$.

By definition of $\mathcal{V}[\![\alpha]\!]$, it remains to be shown that:

$$(k_2 - k_3, W_3, n+1, n+1) \in \chi$$

Since $k_2 - k_3 \leq k_2 < k_0 - k_1$ and $n + 1 \in W_3[p+1].V$, this follows directly from the definition of χ.

Now consider (2). By definition of $\mathcal{V}[\![\tau \to \tau']\!]$, we have to show that:

$$\begin{array}{rl} \forall (k_2, W_2) \sqsupset (k_0 - k_1, W_1), v_2, v_2', & (k_2, W_2, v_2, v_2') \in \mathcal{V}[\![\alpha]\!]\,\rho \implies \\ & (k_2, W_2, \lambda z : \mathsf{int}.\, z \leq !l, \lambda z : \mathsf{int}.\, \mathtt{true}) \in \mathcal{E}[\![\mathsf{bool}]\!]\,\rho \end{array}$$

Assume $(k_2, W_2) \sqsupset (k_0 - k_1, W_1)$ and $(k_2, W_2, v_2, v_2') \in \mathcal{V}[\![\alpha]\!]\,\rho$. By definition of $\mathcal{E}[\![\tau]\!]$, we are required to show:

$$\begin{array}{rlcll} \forall k_3 < k_2, s_2, s_2', s_2, v_3, & s_2, s_2' :_{k_2} W_2 & \wedge & s_2, (v_2 \leq !l) \longmapsto^{k_3} s_3, v_3 & \implies \\ \exists s_3', v_3', W_3, & s_3, s_3' :_{k_2-k_3} W_3 & \wedge & s_2', \mathtt{true} \longmapsto^* s_3', v_3' & \wedge \\ & (k_2 - k_3, W_3) \sqsupseteq (k_2, W_2) & \wedge & (k_2 - k_3, W_3, v_3, v_3') \in \mathcal{V}[\![\mathsf{bool}]\!]\,\rho & \end{array}$$

Assume $s_2, s_2' :_{k_2} W_2$ and $s_2, (v_2 \leq \texttt{!}l) \longmapsto^{k_3} s_3, v_3$. As for part (1), from $(k_2, W_2) \sqsupseteq (k_0 - k_1, W_1)$ it follows that there exist n and $k \geq k_2$, such that

$$\begin{array}{rcl} W_2[p+1].\eta & = & \eta_k^n \\ \text{that is,} \quad W_2[p+1].\psi & = & \psi_k^n \\ W_2[p+1].V & = & V_n \end{array}$$

as defined above. From $s_2, s_2' :_{k_2} W_2$ and $k_2 > k_3$ we can once more conclude $(k_2 - 1, \lfloor W_2 \rfloor_{k_2-1}, s_2, s_2') \in \psi_k^n$ and thus

$$s_2(l) = s_2'(l') = n$$

By definition of $\mathcal{V}[\![\alpha]\!]$, from $(k_2, W_2, v_2, v_2') \in \mathcal{V}[\![\alpha]\!]\,\rho$ it follows that:

$$(k_2, W_2, v_2, v_2') \in \chi$$

and from the definition of χ it follows that:

$$v_2 = v_2' = i \quad \text{such that} \quad i \in W_2[p+1].V$$

Because $W_2[p+1].V = V_n$, clearly $i \leq n$. By definition of reduction, it then must hold that:

$$\begin{array}{rclcrcl} s_3 & = & s_2, & & v_3 & = & \texttt{true} \\ s_3' & = & s_2', & & v_3' & = & \texttt{true} \end{array}$$

Let $W_3 = W_2$, which trivially is valid and extends W_2. Likewise, $s_3, s_3' :_{k_2-k_3} W_3$ is immediate. It remains to be shown that

$$(k_2 - k_3, W_3, \texttt{true}, \texttt{true}) \in \mathcal{V}[\![\mathsf{bool}]\!]\,\rho$$

which obviously is the case. □

5.2 Name Generator with References

Now let us go through the equivalence proof for the two different name generator implementations:

$$\begin{array}{rcl} e & = & \texttt{let}\, x = \texttt{ref}\, 0\, \texttt{in}\, (\texttt{pack}\, \mathit{int}, \langle \lambda z : \mathsf{unit}.\, (x := \texttt{!}x + 1; \texttt{!}x), \lambda p : \mathsf{int} \times \mathsf{int}.\, \texttt{fst}\, p = \texttt{snd}\, p \rangle\, \texttt{as}\, \sigma) \\ e' & = & (\texttt{pack}\, \mathsf{ref\ unit}, \langle \lambda z : \mathsf{unit}.\, \texttt{ref}\, (), \lambda p : \mathsf{ref\ unit} \times \mathsf{ref\ unit}.\, \texttt{fst}\, p \equiv \texttt{snd}\, p \rangle\, \texttt{as}\, \sigma) \\ \text{where} \quad \sigma & = & \exists \alpha.\, (\mathsf{unit} \to \alpha) \times (\alpha \times \alpha \to \mathsf{bool}) \end{array}$$

We only show one direction, the other proceeds analogously. That is, we want to show that:

$$\vdash e \preceq e' : \sigma$$

By definition of approximation, we have to show:

$$\forall k_0 \geq 0, W_0, \quad (k_0, W_0, e, e') \in \mathcal{E}[\![\sigma]\!]\,\emptyset$$

By definition of $\mathcal{E}[\![\tau]\!]$, we need to show:

$$\begin{array}{rlcll} \forall k_1 < k_0, s_0, s_0', s_1, v_1, & s_0, s_0' :_{k_0} W_0 & \wedge & s_0, P[\lambda z : \mathsf{int}.\, z \leq \texttt{!}x] \longmapsto^{k_1} s_1, v_1 & \Longrightarrow \\ \exists s_1', v_1', W_1, & s_1, s_1' :_{k_0-k_1} W_1 & \wedge & s_0', P[\lambda z : \mathsf{int}.\, \texttt{true}] \longmapsto^{*} s_1', v_1' & \wedge \\ & (k_0 - k_1, W_1) \sqsupseteq (k_0, W_0) & \wedge & (k_0 - k_1, W_1, v_1, v_1') \in \mathcal{V}[\![\sigma]\!]\,\emptyset & \end{array}$$

Assume $s_0, s_0' :_{k_0} W_0$ and $s_0, P[e] \longmapsto^{k_1} s_1, v_1$. By definition of reduction, the following has to hold for some $l \notin \mathrm{dom}(s_0)$:

$$\begin{array}{rclcrcl} s_1 & = & s_0[l \mapsto 0], & & v_1 & = & (\texttt{pack}\, \mathsf{int}, \langle \lambda z : \mathsf{unit}.\, (l := \texttt{!}l + 1; \texttt{!}l), \lambda p : \mathsf{int} \times \mathsf{int}.\, \texttt{fst}\, p = \texttt{snd}\, p \rangle\, \texttt{as}\, \sigma) \\ s_1' & = & s_0', & & v_1' & = & e' \end{array}$$

Assume $W_0 = \langle w_1, \ldots, w_p \rangle$. Now let:

$$\begin{array}{rcl} W_1 & = & \langle w_1, \ldots, w_p, w_{p+1} \rangle \\ \text{where } w_{p+1} & = & (\eta^{\langle\rangle}_{k_0-k_1}, \mathcal{L}_{k_0-k_1}) \\ \eta^{\langle l_1,\ldots,l_n\rangle}_k & = & (\psi^n_k, V_{\langle l_1,\ldots,l_n\rangle}, \{l : \mathsf{int}\}, \{l_1 : \mathsf{unit}, \ldots, l_n : \mathsf{unit}\}) \\ \psi^n_k & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid s(l) = n\} \\ V_{\langle l_1,\ldots,l_n\rangle} & = & \{\langle i, l_i\rangle \mid 1 \le i \le n\} \\ \mathcal{L}_k & = & \{(j, \eta^{\langle l_1,\ldots,l_n\rangle}_j) \in \mathit{LawAtom}_k \mid n \in \mathbb{N}\} \end{array}$$

As a notational convention, we implicitly require that all locations in a list $\langle l_1, \ldots, l_n \rangle$ used here are pairwise disjoint. We have to show the necessary properties for this definition:

1. $W_1 \in \mathit{World}_{k_0-k_1}$:
   - Obviously, for all k and n, we have $\psi^n_k \in \mathit{StoreRel}_k$ and $V_{\langle l_1,\ldots,l_n\rangle} \in \mathit{Population}$.
   - Hence, for all k and n, $\eta^{\langle l_1,\ldots,l_n\rangle}_k \in \mathit{Knowledge}_{k_0-k_1}$.
   - Note that, for all n, k, $k' < k$, we have $\lfloor \psi^n_k \rfloor_{k'} = \psi^n_{k'}$, and thus also $\lfloor \eta^{\langle l_1,\ldots,l_n\rangle}_k \rfloor_{k'} = \eta^{\langle l_1,\ldots,l_n\rangle}_{k'}$.
   - Hence, $\mathcal{L}_k$ is downward closed and thus in Law_k.
   - Consequently, also $(k_0 - k_1, \eta^{\langle\rangle}_{k_0-k_1}) \in \mathcal{L}_{k_0-k_1}$.
   - So, $w_{p+1} \in \mathit{Island}_{k_0-k_1}$.
   - And since l is fresh wrt. s_0, and $s_0, s'_0 :_{k_0} W_0$, we know that $l \notin \mathrm{dom}(\Sigma_1(W_0))$.
2. $(k_0 - k_1, W_1) \sqsupseteq (k_0, W_0)$:
   - Obvious, since $k_0 - k_1 \le k_0$ and $w_1, \ldots, w_p$ are unchanged.
3. $s_1, s'_1 :_{k_0-k_1} W_1$:
   - Obviously, $\vdash s_1 : \{l : \mathsf{int}\}$ and $\vdash s'_1 : \{\}$.
   - Clearly, for all $j < k_0 - k_1$, $(j, \lfloor W \rfloor_j, s_1, s'_1) \in \psi^{\langle\rangle}_{k_0-k_1} = w_{p+1}.\psi$.
   - From the definition of *StoreRel* and *Island* we know that $w_1.\psi, \ldots, w_p.\psi$ are downward closed. It follows that for all $1 \le i \le p$ and $j < k_0 - k_1$, $(j, \lfloor W_1 \rfloor_j, s_1, s'_1) \in \psi(w_i)$ (because for all $j \le k$, $(j, \lfloor W \rfloor_k) \sqsupseteq (k, W)$).

Also note that, for all $n' \ge n, k' \le k$, it holds that $\eta^{\langle l_1,\ldots,l_{n'}\rangle}_{k'} \sqsupseteq \eta^{\langle l_1,\ldots,l_n\rangle}_k$.

By definition of $\mathcal{V}[\![\exists\alpha.\tau]\!]$, it remains to be shown that:

$$\begin{array}{l} \exists \chi \in \mathit{Type}[\mathsf{int}, \mathsf{ref\ unit}], \quad (k_0 - k_1, W_1, \langle \lambda z : \mathsf{unit}.\, (l := !\, l + 1;\, !\, l), \lambda p : \mathsf{int} \times \mathsf{int}.\, \mathtt{fst}\, p = \mathtt{snd}\, p\rangle, \\ \qquad\qquad \langle \lambda z : \mathsf{unit}.\, \mathtt{ref}\ (), \lambda p : \mathsf{ref\ unit} \times \mathsf{ref\ unit}.\, \mathtt{fst}\, p \equiv \mathtt{snd}\, p\rangle) \\ \qquad\qquad\qquad \in \mathcal{V}[\![(\mathsf{unit} \to \alpha) \times (\alpha \to \mathsf{bool})]\!]\, \rho \end{array}$$

for $\rho = [\alpha \mapsto (\chi, \mathsf{int}, \mathsf{ref\ unit})]$. Define:

$$\chi = \{(j, W, i, l) \in \mathit{Atom}[\mathsf{int}, \mathsf{ref\ unit}]_{k_0-k_1} \mid \langle i, l\rangle \in W[p+1].V\}$$

We need to check that $\chi \in \mathit{Type}[\mathsf{int}, \mathsf{int}]_{k_0-k_1}$. That is straightforward:

- Assume $(j, W, i, l) \in \chi$ and $(j', W') \sqsupseteq (j, W)$.
- From the former it follows that $\langle i, l\rangle \in W[p+1].V$.

- From the latter it follows that $W'[p+1].V \supseteq W[p+1].V$ and $j' \leq j$.
- Hence, $(j', W', i, l) \in \chi$.

By definition of $\mathcal{V}\,[\![\tau \times \tau']\!]$, we now need to show that:

1. $(k_0 - k_1, W_1, \lambda z : \mathsf{unit}.\,(l := !l + 1; !l), \lambda z : \mathsf{unit}.\,\mathtt{ref}\,()) \in \mathcal{V}\,[\![\mathsf{unit} \to \alpha]\!]\,\rho$
2. $(k_0 - k_1, W_1, \lambda p : \mathsf{int} \times \mathsf{int}.\,\mathtt{fst}\,p = \mathtt{snd}\,p, \lambda p : \mathsf{ref\ unit} \times \mathsf{ref\ unit}.\,\mathtt{fst}\,p \equiv \mathtt{snd}\,p) \in \mathcal{V}\,[\![\alpha \times \alpha \to \mathsf{bool}]\!]\,\rho$

First consider (1). By definition of $\mathcal{V}\,[\![\tau \to \tau']\!]$, we have to show that:

$$\begin{array}{ll} \forall (k_2, W_2) \sqsupset (k_0 - k_1, W_1), & (k_2, W_2, v_2, v_2') \in \mathcal{V}\,[\![\mathsf{unit}]\!]\,\rho \implies \\ & (k_2, W_2, (l := !l + 1; !l), \mathtt{ref}\,()) \in \mathcal{E}\,[\![\alpha]\!]\,\rho \end{array}$$

Assume $(k_2, W_2) \sqsupset (k_0 - k_1, W_1)$. By definition of $\mathcal{E}\,[\![\tau]\!]$, we have to show:

$$\begin{array}{lllll} \forall k_3 < k_2, s_2, s_2', s_3, v_3, & s_2, s_2' :_{k_2} W_2 & \wedge & s_2, (l := !l + 1; !l) \longmapsto^{k_3} s_3, v_3 & \implies \\ \exists s_3', v_3', W_3, & s_3, s_3' :_{k_2 - k_3} W_3 & \wedge & s_2', \mathtt{ref}\,() \longmapsto^{*} s_3', v_3' & \wedge \\ & (k_2 - k_3, W_3) \sqsupseteq (k_2, W_2) & \wedge & (k_2 - k_3, W_3, v_3, v_3') \in \mathcal{V}\,[\![\alpha]\!]\,\emptyset & \end{array}$$

Assume $s_2, s_2' :_{k_2} W_2$ and $s_2, (l := !l + 1; !l) \longmapsto^{k_3} s_3, v_3$. From $(k_2, W_2) \sqsupseteq (k_0 - k_1, W_1)$ it follows that $W_2[p+1].\mathcal{L} = \lfloor W_1[p+1].\mathcal{L} \rfloor_{k_2} = \lfloor \mathcal{L}_{k_0 - k_1} \rfloor_{k_2} = \mathcal{L}_{k_2}$ and $W_2[p+1].\eta \sqsupseteq \lfloor W_1[p+1].\eta \rfloor_{k_2}$. From that, by definition of *Island*, we know $(k_2, W_2[p+1].\eta) \in \mathcal{L}_{k_2}$, and there exists $\langle l_1, \ldots, l_n \rangle$, such that

$$\begin{array}{rrcl} & W_2[p+1].\eta & = & \eta_{k_2}^{\langle l_1, \ldots, l_n \rangle} \\ \text{that is,} & W_2[p+1].\psi & = & \psi_{k_2}^{n} \\ & W_2[p+1].V & = & V_{\langle l_1, \ldots, l_n \rangle} \\ & W_2[p+1].\Sigma_2 & = & \{l_1 : \mathsf{unit}, \ldots, l_n : \mathsf{unit}\} \end{array}$$

as defined above. Because $k_2 > k_3$, apparently $k_2 > 0$. From $s_2, s_2' :_{k_2} W_2$ we can thereby conclude $(k_2 - 1, \lfloor W_2 \rfloor_{k_2 - 1}, s_2, s_2') \in \psi_{k_2}^n$ and thus

$$s_2(l) = n \quad \wedge \quad \{l_1, \ldots, l_n\} \subseteq \mathrm{dom}(s_2')$$

By definition of reduction, the following must hold, for some $l_{n+1} \notin \mathrm{dom}(s_2')$:

$$\begin{array}{rclrcl} s_3 & = & s_2[l \mapsto n+1], & v_3 & = & n+1 \\ s_3' & = & s_2'[l_{n+1} \mapsto ()], & v_3' & = & l_{n+1} \end{array}$$

Now choose W_3 such that w_{p+1} is updated as follows:

$$\begin{array}{rrcl} & W_3[p+1].\eta & = & \eta_{k_2 - k_3}^{\langle l_1, \ldots, l_{n+1} \rangle} \\ \text{that is,} & W_3[p+1].\psi & = & \psi_{k_2 - k_3}^{n+1} \\ & W_3[p+1].V & = & V_{\langle l_1, \ldots, l_{n+1} \rangle} \\ & W_3[p+1].\Sigma_2 & = & \{l_1 : \mathsf{unit}, \ldots, l_{n+1} : \mathsf{unit}\} \end{array}$$

Again, we have to show that this definition has the necessary properties:

1. $W_3 \in \mathit{World}_{k_2 - k_3}$:
   - Follows by the same reasoning as above. In particular, it is obvious from the definition of $\mathcal{L}_k$ that $(k_2 - k_3, W_3[p+1].\eta) \in \mathcal{L}_{k_2 - k_3}$.
2. $(k_2 - k_3, W_3) \sqsupseteq (k_2, W_3)$:

- Obviously, $W_3[p+1].V \supset W_2[p+1].V$ and $W_3[p+1].\Sigma_2 \supset W_2[p+1].\Sigma_2$. Hence, $W_3[p+1].\eta \sqsupseteq W_2[p+1].\eta$.
- Because $W_3[p+1].\mathcal{L} = W_2[p+1].\mathcal{L}$ and $k_2 - k_3 \leq k_2$, we have $W_3 \sqsupseteq W_2$.

3. $s_3, s_3' :_{k_2-k_3} W_3$:
   - As before. Specifically, for all $j < k_2 - k_3$, $(j, \lfloor W_3 \rfloor_j, s_3, s_3') \in \psi^{n+1}_{k_2-k_3}$.

By definition of $\mathcal{V}[\![\alpha]\!]$, it remains to be shown that:

$$(k_2 - k_3, W_3, n+1, l_{n+1}) \in \chi$$

Since $k_2 - k_3 \leq k_2 < k_0 - k_1$ and $(n+1, l_{n+1}) \in W_3[p+1].V$, this follows directly from the definition of χ.

Now consider (2). By definition of $\mathcal{V}[\![\tau \to \tau']\!]$, we have to show that:

$$\begin{array}{l}\forall (k_2, W_2) \sqsupset (k_0 - k_1, W_1), v_2, v_2', \ (k_2, W_2, v_2, v_2') \in \mathcal{V}[\![\alpha \times \alpha]\!]\,\rho \implies \\ \qquad\qquad (k_2, W_2, \lambda p : \mathsf{int} \times \mathsf{int}.\, \mathtt{fst}\, p = \mathtt{snd}\, p, \lambda p : \mathsf{ref\ unit} \times \mathsf{ref\ unit}.\, \mathtt{fst}\, p \equiv \mathtt{snd}\, p) \in \mathcal{E}[\![\mathsf{bool}]\!]\,\rho\end{array}$$

Assume $(k_2, W_2) \sqsupset (k_0 - k_1, W_1)$ and $(k_2, W_2, v_2, v_2') \in \mathcal{V}[\![\alpha \times \alpha]\!]\,\rho$. By definition of $\mathcal{E}[\![\tau]\!]$, we are required to show:

$$\begin{array}{rlcl}\forall k_3 < k_2, s_2, s_2', s_2, v_3, & s_2, s_2' :_{k_2} W_2 & \wedge & s_2, (\mathtt{fst}\, v_2 = \mathtt{snd}\, v_2) \longmapsto^{k_3} s_3, v_3 \implies \\ \exists s_3', v_3', W_3, & s_3, s_3' :_{k_2-k_3} W_3 & \wedge & s_2', (\mathtt{fst}\, v_2' \equiv \mathtt{snd}\, v_2') \longmapsto^{*} s_3', v_3' \ \wedge \\ & (k_2 - k_3, W_3) \sqsupseteq (k_2, W_2) & \wedge & (k_2 - k_3, W_3, v_3, v_3') \in \mathcal{V}[\![\mathsf{bool}]\!]\,\rho\end{array}$$

Assume $s_2, s_2' :_{k_2} W_2$ and $s_2, (\mathtt{fst}\, v_2 = \mathtt{snd}\, v_2) \longmapsto^{k_3} s_3, v_3$. As for part (1), from $(k_2, W_2) \sqsupseteq (k_0 - k_1, W_1)$ it follows that there exist $\langle l_1, \ldots, l_n \rangle$ and k, such that

$$\begin{array}{rrcl} & W_2[p+1].\eta & = & \eta_k^{\langle l_1, \ldots, l_n \rangle} \\ \text{that is,} & W_2[p+1].\psi & = & \psi_k^n \\ & W_2[p+1].V & = & V_{\langle l_1, \ldots, l_n \rangle}\end{array}$$

as defined above. From $s_2, s_2' :_{k_2} W_2$ and $k_2 > k_3$ we can once more conclude $(k_2 - 1, \lfloor W_2 \rfloor_{k_2-1}, s_2, s_2') \in \psi_k^n$ and thus

$$s_2(l) = n$$

By definition of $\mathcal{V}[\![\tau \times \tau']\!]$, from $(k_2, W_2, v_2, v_2') \in \mathcal{V}[\![\alpha \times \alpha]\!]\,\rho$ it follows that:

$$\begin{array}{rcl} v_2 & = & \langle v_{21}, v_{22} \rangle \\ v_2' & = & \langle v_{21}', v_{22}' \rangle\end{array}$$

for some $v_{21}, v_{22}, v_{21}', v_{22}'$, such that

$$\begin{array}{l}(k_2, W_2, v_{21}, v_{21}') \in \mathcal{V}[\![\alpha]\!]\,\rho \\ (k_2, W_2, v_{22}, v_{22}') \in \mathcal{V}[\![\alpha]\!]\,\rho\end{array}$$

From the definition of $\mathcal{V}[\![\alpha]\!]$ we hence know:

$$\begin{array}{l}(k_2, W_2, v_{21}, v_{21}') \in \chi \\ (k_2, W_2, v_{22}, v_{22}') \in \chi\end{array}$$

and from the definition of χ it follows that:

$$\begin{array}{l}v_{21} = i \wedge v_{21}' = l_i \ \text{ such that } \ (i, l_i) \in W_2[p+1].V \\ v_{22} = j \wedge v_{21}' = l_j \ \text{ such that } \ (j, l_j) \in W_2[p+1].V\end{array}$$

Because $W_2[p+1].V = V_{\langle l_1,\ldots,l_n\rangle}$ and the assumption was that all locations are disjoint, we know that $i = j \Leftrightarrow l_i = l_j$. By definition of reduction, it either of the following must then hold:

$$\begin{array}{rclcrcl} s_3 & = & s_2, & & v_3 & = & \texttt{true} \\ s_3' & = & s_2', & & v_3' & = & \texttt{true} \end{array}$$

or

$$\begin{array}{rclcrcl} s_3 & = & s_2, & & v_3 & = & \texttt{false} \\ s_3' & = & s_2', & & v_3' & = & \texttt{false} \end{array}$$

Let $W_3 = W_2$, which trivially is valid in both cases and extends W_2. Likewise, $s_3, s_3' :_{k_2-k_3} W_3$ is immediate. It remains to be shown that both

$$(k_2 - k_3, W_3, \texttt{true}, \texttt{true}) \in \mathcal{V}\,[\![\mathsf{bool}]\!]\,\rho$$
$$(k_2 - k_3, W_3, \texttt{false}, \texttt{false}) \in \mathcal{V}\,[\![\mathsf{bool}]\!]\,\rho$$

hold, which obviously is the case. □

5.3 Higher-Order Function

The next example is a variation on Koutavas & Wand, Section 6.2:

$$\begin{array}{rcl} e & = & \lambda f : (\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}.\, \texttt{let}\, x = \texttt{ref}\, 0\, \texttt{in}\, (f\, (\lambda z : \mathsf{unit}.\, x := !x + 2); !x \,\texttt{mod}\, 2 = 0) \\ e' & = & \lambda f : (\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}.\, (f\, (\lambda z : \mathsf{unit}.\, ()); \texttt{true}) \end{array}$$

We want to show that:

$$\vdash e \preceq e' : ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{bool}$$

By definition of approximation, we have to show:

$$\forall k_0 \geq 0, W_0, \quad (k_0, W_0, e, e') \in \mathcal{E}\,[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{bool}]\!]\,\emptyset$$

Since e and e' are values, it suffices to show, by definition of $\mathcal{V}\,[\![\tau \to \tau']\!]$:

$$\begin{array}{rll} \forall (k_1, W_1) \sqsupset (k_0, W_0), v_1, v_1', & (k_1, W_1, v_1, v_1') \in \mathcal{V}\,[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\,\emptyset & \implies \\ & (k_1, W_1, e_1, e_1') \in \mathcal{E}\,[\![\mathsf{bool}]\!]\,\emptyset & \end{array}$$

where $e_1 = (\texttt{let}\, x = \texttt{ref}\, 0\, \texttt{in}\, v_1\, (\lambda z : \mathsf{unit}.\, x := !x + 2); !x \,\texttt{mod}\, 2 = 0)$ and $e_1' = (v_1'\, (\lambda z : \mathsf{unit}.\, ()); \texttt{true})$. By definition of $\mathcal{E}\,[\![\tau]\!]$, this requires showing that:

$$\begin{array}{rlcl} \forall k_2 < k_1, s_1, s_1', s_2, v_2, & s_1, s_1' :_{k_1} W_1 & \wedge & s_1, e_1 \longmapsto^{k_2} s_2, v_2 \implies \\ \exists s_2', v_2', W_2, & s_2, s_2' :_{k_1-k_2} W_2 & \wedge & s_1', e_1' \longmapsto^{*} s_2', v_2' \;\wedge \\ & (k_1 - k_2, W_2) \sqsupseteq (k_1, W_1) & \wedge & (k_1 - k_2, W_2, v_2, v_2') \in \mathcal{V}\,[\![\mathsf{bool}]\!]\,\emptyset \end{array}$$

Assume $s_1, s_1' :_{k_1} W_1$ and $s_1, e_1 \longmapsto^{k_2} s_2, v_2$. We see that the first step in reducing e_1 must be, for some label $l \notin \mathrm{dom}(s_1)$:

$$s_1, e_1 \longmapsto^{1} s_1[l \mapsto 0], (\texttt{let}\, x = l\, \texttt{in}\, v_1\, (\lambda z : \mathsf{unit}.\, x := !x + 2); !x \,\texttt{mod}\, 2 = 0)$$

The proof proceeds as follows. Before doing the higher-order call to v_1, we have to set up a new island controlling that $!x$ is even. Call the new world W_1', and observe that $s_1[l \mapsto 0], s_1' :_{k_1-1} W_1'$. Then show that

$$\begin{array}{rlcl} \exists s_2', v_2', W_2, & s_2, s_2' :_{k_1-k_2} W_2 & \wedge & s_1', e_1' \longmapsto^{*} s_2', v_2' \;\wedge \\ & (k_1 - k_2, W_2) \sqsupseteq (k_1 - 1, W_1') & \wedge & (k_1 - k_2, W_2, v_2, v_2') \in \mathcal{V}\,[\![\mathsf{bool}]\!]\,\emptyset \end{array}$$

This is possible, because we know that f will terminate in less than $k_2 - 1$ steps and return in a future world of W_1' where $!x$ is still even. The original proof obligation then follows by transitivity of world extension.

Assume $W_1 = \langle w_1, \ldots, w_p \rangle$. Now define:

$$\begin{array}{rcl} W_1' & = & \langle w_1, \ldots, w_p, w_{p+1} \rangle \\ \text{where } w_{p+1} & = & (\eta_{k_1-1}, \mathcal{L}_{k_1-1}) \\ \eta_k & = & (\psi_k, \emptyset, \{l : \mathsf{int}\}, \{\}) \\ \psi_k & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid \exists n \in \mathbb{N}, s(l) = 2n\} \\ \mathcal{L}_k & = & \{(j, \eta_j) \in \mathit{Law}_k\} \end{array}$$

We can show the following properties for this definition:

1. $W_1' \in \mathit{World}_{k_1-1}$:
   - Obviously, for all k, we have $\psi_k \in \mathit{StoreRel}_k$.
   - Hence, for all k, $\eta_k \in \mathit{Knowledge}_{k_1-1}$.
   - Note that, for all n, k, $k' < k$, we have $\lfloor \psi_k \rfloor_{k'} = \psi_{k'}$, and thus also $\lfloor \eta_k \rfloor_{k'} = \eta_{k'}$.
   - Hence, $\mathcal{L}_k$ is downward closed and thus in Law_k.
   - Consequently, also $(k_1 - 1, \eta_{k_1-1}) \in \mathcal{L}_{k_1-1}$.
   - So, $w_{p+1} \in \mathit{Island}_{k_1-1}$.
   - And since l is fresh wrt. s_1, and $s_1, s_1' :_{k_1} W_1$, we know that $l \notin \mathrm{dom}(\Sigma_1(W_1'))$.
2. $(k_1 - 1, W_1') \sqsupseteq (k_1, W_1)$:
   - Obvious, since $k_1 - 1 \leq k_1$ and $w_1, \ldots, w_p$ are unchanged.
3. $s_1[l \mapsto 0], s_1' :_{k_1-1} W_1'$:
   - Obviously, $\vdash s_1[l \mapsto 0] : \{l : \mathsf{int}\}$ and $\vdash s_1' : \{\}$.
   - Clearly, for all $j < k_1 - 1$, $(j, \lfloor W \rfloor_j, s_1[l \mapsto 0], s_1') \in \psi_{k_1-1}^{\langle\rangle} = w_{p+1}.\psi$.
   - From the definition of *StoreRel* and *Island* we know that $w_1.\psi, \ldots, w_p.\psi$ are downward closed. It follows that for all $1 \leq i \leq p$ and $j < k_1 - 1$, $(j, \lfloor W_1' \rfloor_j, s_1[l \mapsto 0], s_1') \in \psi(w_i)$ (because for all $j \leq k$, $(j, \lfloor W \rfloor_k) \sqsupseteq (k, W)$).

We next show that $(k_1 - 1, W_1', (\lambda z : \mathsf{unit}.\, l := !\, l + 2), (\lambda z : \mathsf{unit}.\, ())) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$:

- By definition of $\mathcal{V}[\![\tau \to \tau']\!]$, this amounts to showing:

$$\begin{array}{ll} \forall (k_2, W_2) \sqsupseteq (k_1 - 1, W_1'), & (k_2, W_2, v_2, v_2') \in \mathcal{V}[\![\mathsf{unit}]\!] \implies \\ & (k_2, W_2, (l := !\, l + 2), ()) \in \mathcal{E}[\![\mathsf{unit}]\!] \end{array}$$

- By definition of $\mathcal{E}[\![\tau]\!]$, this requires showing:

$$\begin{array}{rlcl} \forall k_3 < k_2, s_2, s_2', s_3, v_3, & s_2, s_2' :_{k_2} W_2 & \wedge & s_2, (l := !\, l + 2) \longmapsto^{k_3} s_3, v_3 \implies \\ \exists s_3', v_3', W_3, & s_3, s_3' :_{k_2 - k_3} W_3 & \wedge & s_2', () \longmapsto^* s_3', v_3' \ \wedge \\ & (k_2 - k_3, W_3) \sqsupseteq (k_2, W_2) & \wedge & (k_2 - k_3, W_3, v_3, v_3') \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset \end{array}$$

- Assume $s_2, s_2' :_{k_2} W_2$ and $s_2, (l := !\, l + 2) \longmapsto^{k_3} s_3, v_3$. By inspection of the reduction relation we see that:

$$\begin{array}{rcll} v_3 & = & (), & s_3 = s_2[l \mapsto s_2(l) + 2] \\ v_3' & = & (), & s_3' = s_2' \end{array}$$

- Let $W_3 = W_2$. Then obviously $(k_2 - k_3, W_3) \sqsupseteq (k_2, W_2)$. We have to show $s_3, s_3' :_{k_2-k_3} W_3$:

– From $(k_2, W_2) \sqsupseteq (k_1 - 1, W_1')$ it follows that $W_2[p+1].\mathcal{L} = \lfloor W_1'[p+1].\mathcal{L} \rfloor_{k_2} = \lfloor \mathcal{L}_{k_1-1} \rfloor_{k_2} = \mathcal{L}_{k_2}$.
– From that, by definition of *Island*, we know $(k_2, W_2[p+1].\eta) \in \mathcal{L}_{k_2}$, so

$$\begin{array}{rrcl} & W_2[p+1].\eta & = & \eta_{k_2} \\ \text{that is,} & W_2[p+1].\psi & = & \psi_{k_2} \end{array}$$

as defined above.
– From $s_2, s_2' :_{k_2} W_2$ and $k_2 > k_3 \geq 0$ we can conclude $(k_2 - 1, \lfloor W_2 \rfloor_{k_2-1}, s_2, s_2') \in \psi_{k_2}$ and thus

$$s_2(l) = 2n$$

– Because $s_3(l) = 2(n+1)$, clearly, for all $j < k_2 - k_3$, $(j, \lfloor W_3 \rfloor_j, s_3, s_3') \in \psi_{k_2} = W_3[p+1].\psi$.

- Finally, it is trivial that

$$(k_2 - k_3, W_3, (), ()) \in \mathcal{V}\,[\![\mathsf{unit}]\!]\,\emptyset$$

Now, because $(k_1, W_1, v_1, v_1') \in \mathcal{V}\,[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\,\emptyset$ and $(k_1 - 1, W_1') \sqsupset (k_1, W_1)$, by definition of $\mathcal{V}\,[\![\tau \to \tau']\!]$ we can conclude that $v_1 = \lambda z : \mathsf{unit} \to \mathsf{unit}.\, e_2$ and $v_1' = \lambda z : \mathsf{unit} \to \mathsf{unit}.\, e_2'$, and:

$$(k_1 - 1, W_1', [(\lambda z : \mathsf{unit}.\, l := !\, l + 2)/z]e_1, [(\lambda z : \mathsf{unit}.\, ())/z]e_1') \in \mathcal{E}\,[\![\mathsf{unit}]\!]\,\emptyset$$

Because we know that s_1, e_1 terminates in k_2 steps, and performs at least one further step after returning from v_1, there exists $j \leq k_2 - 2$ such that $s_1[l \mapsto 0], [(\lambda z : \mathsf{unit}.\, l := !\, l + 2)/z]e_1$ terminates in j steps. Furthermore, the final state of the former computation has to be s_2, because there are no further assignments in e. From the definition of $\mathcal{E}\,[\![\tau]\!]$ it follows that $s_1', [(\lambda z : \mathsf{unit}.\, ())/z]e_1'$ terminates likewise, in state s_2', such that

$$s_2, s_2' :_{k_1-1-j} W_2 \quad \wedge \quad (k_1 - 1 - j, W_2) \sqsupseteq (k_1 - 1, W_1')$$

Because $k_1 - 1 - j > k_1 - k_2 \geq 0$, we can conclude that $(k_1 - j - 2, \lfloor W_2 \rfloor_{k_1-j-2}, s_2, s_2') \in W_2[p+1].\psi$ for some $n \in \mathbb{N}$, i.e.,

$$s_2(l) = 2n$$

Thus the result of the whole computation is $v_2 = \texttt{true}$. Because the other side terminates as well, $v_2' = \texttt{true}$, and obviously,

$$(k_1 - k_2, W_2, \texttt{true}, \texttt{true}) \in \mathcal{V}\,[\![\mathsf{bool}]\!]\,\emptyset$$

Finally, because $1 + j < k_2$, we have:

$$(k_1 - k_2, W_2) \sqsupset (k_1 - 1 - j, W_2) \sqsupseteq (k_1 - 1, W_1') \sqsupset (k_1, W_1)$$

and thanks to downward closure also

$$s_2, s_2' :_{k_1-k_2} W_2$$

which is all that we needed to conclude $(k_1, W_1, e_1, e_1') \in \mathcal{E}\,[\![\mathsf{bool}]\!]\,\rho$. □

5.4 Callback with Lock

The last proof addresses the callback example from the main paper:

$$\begin{array}{rrcl} & e & = & P[f\,(); x := !\, x + 1] \\ & e' & = & P[\texttt{let}\, n = !\, x\, \texttt{in}\, f\,(); x := n + 1] \\ \text{where} & P[E] & = & \texttt{let}\, b = \texttt{ref}\, \texttt{true}\, \texttt{in}\, \texttt{let}\, x = \texttt{ref}\, 0\, \texttt{in} \\ & & & \langle \lambda f : \mathsf{unit} \to \mathsf{unit}.\, (\texttt{if}\, \mathit{not}\, (!\, b)\, \texttt{then}\, ()\, \texttt{else}\, (b := \texttt{false}; E; b := \texttt{true})), \lambda z : \mathsf{unit}.\, !\, x \rangle \\ & \tau & = & ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \times (\mathsf{unit} \to \mathsf{int}) \end{array}$$

We want to show that:

$$\vdash e \preceq e' : \tau$$

By definition of approximation, we have to show:

$$\forall k_0 \geq 0, W_0, \quad (k_0, W_0, e, e') \in \mathcal{E}\,[\![\tau]\!]\,\emptyset$$

By definition of $\mathcal{E}\,[\![\tau]\!]$, we need to show:

$$\begin{array}{lllll} \forall k_1 < k_0, s_0, s_0', s_1, v_1, & s_0, s_0' :_{k_0} W_0 & \wedge & s_0, P[f\,(); x := !\,x + 1] \longmapsto^{k_1} s_1, v_1 & \Longrightarrow \\ \exists s_1', v_1', W_1, & s_1, s_1' :_{k_0 - k_1} W_1 & \wedge & s_0', P[\mathtt{let}\, n = !\,x\, \mathtt{in}\, f\,(); x := n + 1] \longmapsto^{*} s_1', v_1' & \wedge \\ & (k_0 - k_1, W_1) \sqsupseteq (k_0, W_0) & \wedge & (k_0 - k_1, W_1, v_1, v_1') \in \mathcal{V}\,[\![\tau]\!]\,\emptyset & \end{array}$$

Assume $s_0, s_0' :_{k_0} W_0$ and $s_0, P[f\,(); x := !\,x + 1] \longmapsto^{k_1} s_1, v_1$. By definition of reduction, the following has to hold for some $l_b, l_x \notin \mathrm{dom}(s_0)$ and $l_b', l_x' \notin \mathrm{dom}(s_0')$:

$$\begin{array}{rcl@{\qquad}rcl} s_1 & = & s_0[l_b \mapsto \mathtt{true}, l_x \mapsto 0], & v_1 & = & P'[l_b, l_x, f\,(); l_x := !\,l_x + 1] \\ s_1' & = & s_0'[l_b' \mapsto \mathtt{true}, l_x' \mapsto 0], & v_1' & = & P'[l_b', l_x', \mathtt{let}\, n = !\,l_x'\, \mathtt{in}\, f\,(); l_x' := n + 1] \\ \text{where}\ \ P'[l_1, l_2, E] & = & \langle \lambda f : \mathsf{unit} \to \mathsf{unit}.\, (\mathtt{if}\ \mathit{not}\ (!\,l_1)\ \mathtt{then}\ ()\ \mathtt{else}\ (l_1 := \mathtt{false}; E; l_1 := \mathtt{true})), \lambda z : \mathsf{unit}.\, !\,l_2 \rangle & & & \end{array}$$

Assume $W_0 = \langle w_1, \ldots, w_p \rangle$. Now let:

$$\begin{array}{rcl} W_1 & = & \langle w_1, \ldots, w_p, w_{p+1} \rangle \\ w_{p+1} & = & (\eta_{k_0-k_1}^{\{(k_0,k_0,0)\}}, \mathcal{L}_{k_0-k_1}) \\ \eta_k^V & = & (\psi_k^{\min(V)}, V, \{l_b : \mathsf{bool}, l_n : \mathsf{int}\}, \{l_b' : \mathsf{bool}, l_n' : \mathsf{int}\}) \\ \psi_k^{(k_1,k_2,v)} & = & \{(j, W, s, s') \in \mathit{StoreAtom}_k \mid (k_1 \geq j \geq k_2 \ \wedge s(l_b) = s'(l_b') = \mathtt{false} \ \wedge s(l_n) = s'(l_n') = v) \vee \\ & & \qquad\qquad (k_1 \geq k_2 > j \ \wedge s(l_b) = s'(l_b') \qquad\quad \wedge s(l_n) = s'(l_n'))\} \\ \mathcal{L}_k & = & \{(j, \eta_j^{\{(k_1,k_1',v_1),\ldots,(k_n,k_n',v_n)\}}) \in \mathit{LawAtom}_k \mid k_1 \geq k_1' > k_2 \geq \cdots \geq k_{n-1}' > k_n \geq k_n'\} \end{array}$$

where $\min(V)$ denotes the $(k_1, k_2, v) \in V$ with the smallest k_1 (by the definition of $\mathcal{L}_k$, it will also have the smallest k_2). We have to show the necessary properties for this definition:

1. $W_1 \in \mathit{World}_{k_0-k_1}$:
   - First, we need to show that for all k and all (k_1, k_2, v) with $k_1 \geq k_2$, we have $\psi_k^{(k_1,k_2,v)} \in \mathit{StoreRel}_k$. This requires showing that $\psi_k^{(k_1,k_2,v)}$ is downward closed. Assume that $(j, W, s, s') \in \psi_k^{(k_1,k_2,v)}$ and $(j', W') \sqsupseteq (j, W)$. There are three possible cases:
     (a) $j \geq j' \geq k_2$: from $j \geq k_2$ it follows that $s(l_b) = s'(l_b') = \mathtt{false} \wedge s(l_n) = s'(l_n') = v$, and since also $j' \geq k_2$, we know that $(j', W', s, s') \in \psi_k^{(k_1,k_2,v)}$, too.
     (b) $k_2 > j \geq j'$: from $k_2 > j$ it follows that $s(l_b) = s'(l_b') \wedge s(l_n) = s'(l_n')$, and since also $k_2 > j'$, we know that $(j', W', s, s') \in \psi_k^{(k_1,k_2,v)}$, too.
     (c) $j \geq k_2 > j'$: from $j \geq k_2$ it follows that $s(l_b) = s'(l_b')$ $(= \mathtt{false}) \wedge s(l_n) = s'(l_n')$ $(= v)$, and since also $k_2 > j'$, we know that $(j', W', s, s') \in \psi_k^{(k_1,k_2,v)}$, too (note that it is crucial here that we do not require $s(l_b) = s'(l_b') = \mathtt{true}$ in the case $k_2 > j$).
   - Hence, for all k and all V (that obey the side condition in $\mathcal{L}_k$), $\eta_k^V \in \mathit{Knowledge}_{k_0-k_1}$.
   - Note that, for all V, k, $k' < k$, we have $\lfloor \psi_k^{\min V} \rfloor_{k'} = \psi_{k'}^{\min V}$, and thus also $\lfloor \eta_k^V \rfloor_{k'} = \eta_{k'}^V$.
   - Hence, $\mathcal{L}_k$ is downward closed and thus in Law_k.
   - Because the dummy $(k_0, k_0, 0)$ obeys the side condition, $(k_0 - k_1, \eta_{k_0-k_1}^{(k_0,k_0,0)}) \in \mathcal{L}_{k_0-k_1}$.
   - So, $w_{p+1} \in \mathit{Island}_{k_0-k_1}$.

- And since l_b, l_x and l'_b, l'_x are fresh wrt. s_0 and s'_0 respectively, and $s_0, s'_0 :_{k_0} W_0$, we know that $l_b, l_x \notin \mathrm{dom}(\Sigma_1(W_0))$ and $l'_b, l'_x \notin \mathrm{dom}(\Sigma_2(W_0))$.

2. $(k_0 - k_1, W_1) \sqsupseteq (k_0, W_0)$:
   - Obvious, since $k_0 - k_1 \leq k_0$ and $w_1, \ldots, w_p$ are unchanged.
3. $s_1, s'_1 :_{k_0-k_1} W_1$:
   - Obviously, $\vdash s_1 : \{l_b : \mathsf{bool}, l_x : \mathsf{int}\}$ and $\vdash s'_1 : \{l'_b : \mathsf{bool}, l'_x : \mathsf{int}\}$.
   - Clearly, for all $j < k_0 - k_1$, $(j, \lfloor W \rfloor_j, s_1, s'_1) \in \psi^{(k_0,k_0,0)}_{k_0-k_1} = w_{p+1}.\psi$.
   - From the definition of *StoreRel* and *Island* we know that $w_1.\psi, \ldots, w_p.\psi$ are downward closed. It follows that for all $1 \leq i \leq p$ and $j < k_0 - k_1$, $(j, \lfloor W_1 \rfloor_j, s_1, s'_1) \in \psi(w_i)$ (because for all $j \leq k$, $(j, \lfloor W \rfloor_k) \sqsupseteq (k, W)$).

By definition of $\mathcal{V}[\![\tau \times \tau']\!]$, it remains to be shown that:

1. $(k_0 - k_1, W_1, \lambda f : \mathsf{unit} \to \mathsf{unit}.\, P''[l_b, l_x, (f\,(); l_x := !\,l_x + 1)],$
   $\lambda f : \mathsf{unit} \to \mathsf{unit}.\, P''[l'_b, l'_x, (\mathtt{let}\, n = !\,l'_x\, \mathtt{in}\, f\,(); l'_x := n + 1)]) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit} \to \mathsf{unit}]\!]\,\emptyset$
2. $(k_0 - k_1, W_1, \lambda z : \mathsf{unit}.\, !\,l_x, \lambda z : \mathsf{unit}.\, !\,l'_x) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{int}]\!]\,\emptyset$

where $P''[l_1, l_2, E] = (\mathtt{if}\ \mathit{not}\ (!\,l_1)\ \mathtt{then}\ ()\ \mathtt{else}\ (l_1 := \mathtt{false}; E; l_1 := \mathtt{true}))$.

First consider (1). By definition of $\mathcal{V}[\![\tau \to \tau']\!]$, we have to show that:

$$\forall (k_2, W_2) \sqsupset (k_0 - k_1, W_1),\ (k_2, W_2, v_2, v'_2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\,\emptyset \implies (k_2, W_2, P''[l_b, l_x, (f\,(); l_x := !\,l_x + 1)], P''[l'_b, l'_x, (\mathtt{let}\, n = !\,l'_x\, \mathtt{in}\, f\,(); l'_x := n + 1)]) \in \mathcal{E}[\![\mathsf{unit}]\!]\,\emptyset$$

Assume $(k_2, W_2) \sqsupset (k_0 - k_1, W_1)$ and $(k_2, W_2, v_2, v'_2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\,\emptyset$. By definition of $\mathcal{E}[\![\tau]\!]$, we have to show:

$$\begin{array}{lllll} \forall k_3 < k_2, s_2, s'_2, s_3, v_3, & s_2, s'_2 :_{k_2} W_2 & \wedge & s_2, P''[l_b, l_x, (v_2\,(); l_x := !\,l_x + 1)] \longmapsto^{k_3} s_3, v_3 & \implies \\ \exists s'_3, v'_3, W_3, & s_3, s'_3 :_{k_2-k_3} W_3 & \wedge & s'_2, P''[l'_b, l'_x, (\mathtt{let}\, n = !\,l'_x\, \mathtt{in}\, v'_2\,(); l'_x := n + 1)] \longmapsto^* s'_3, v'_3 & \wedge \\ & (k_2 - k_3, W_3) \sqsupseteq (k_2, W_2) & \wedge & (k_2 - k_3, W_3, v_3, v'_3) \in \mathcal{V}[\![\mathsf{unit}]\!]\,\emptyset & \end{array}$$

Assume $s_2, s'_2 :_{k_2} W_2$ and $s_2, P''[l_b, l_x, (v_2\,(); l_x := !\,l_x + 1)] \longmapsto^{k_3} s_3, v_3$. From $(k_2, W_2) \sqsupseteq (k_0 - k_1, W_1)$ it follows that $W_2[p+1].\mathcal{L} = \lfloor W_1[p+1].\mathcal{L} \rfloor_{k_2} = \lfloor \mathcal{L} \rfloor_{k_2} = \mathcal{L}_{k_2}$ and $W_2[p+1].\eta \sqsupseteq \lfloor W_1[p+1].\eta \rfloor_{k_2}$. From that, by definition of *Island*, we know $(k_2, W_2[p+1].\eta) \in \mathcal{L}_{k_2}$, and there exists V, such that

$$\begin{array}{rcl} W_2[p+1].\eta & = & \eta^V_{k_2} \\ \text{that is, } W_2[p+1].\psi & = & \psi^{\min(V)}_{k_2} \end{array}$$

as defined above. Apparently, $k_2 > k_3$ implies $k_2 > 0$. From $s_2, s'_2 :_{k_2} W_2$ we can therefor conclude $(k_2 - 1, \lfloor W_2 \rfloor_{k_2-1}, s_2, s'_2) \in \psi^{\min(V)}_{k_2}$ and thus, for some b and m:

$$\begin{array}{rcl} s_2(l_b) = s'_2(l'_b) & = & b \\ s_2(l_x) = s'_2(l'_x) & = & m \end{array}$$

There are two cases: either $b = \mathtt{false}$. Then obviously, $s_3 = s_2$ and $v_3 = ()$. Hence, $P''[l'_b, l'_x, (\mathtt{let}\, n = !\,l'_x\, \mathtt{in}\, v'_2\,(); l'_x := n + 1)]$ terminates, too, with $s'_3 = s'_2$ and $v'_3 = ()$. Obviously, these results are related and the stores remain related in the unchanged world $W_3 = W_2$.

Now consider the other case, $b = \mathtt{true}$. By definition of the reduction rules, termination in k_3 steps implies that there are j_1, j_2, j_3 with $j_1 + j_2 + j_3 = k_3$ such that

$$\begin{array}{rcl} s_2, P''[l_b, l_x, v_2\,(); l_x := !\,l_x + 1] & \longmapsto^{j_1} & s_{21}, (v_2\,(); l_x := !\,l_x + 1; l_b := \mathtt{true}) \\ & \longmapsto^{j_2} & s_{22}, (v_{22}; l_x := !\,l_x + 1; l_b := \mathtt{true}) \\ & \longmapsto^{j_3} & s_3, () \end{array}$$

for $s_{21} = s_2[l_b \mapsto \texttt{false}]$ and some s_{22}, such that $s_3 = s_{22}[l_b \mapsto \texttt{true}, l_x \mapsto s_{22}(l_x) + 1]$. Note that $j_i \geq 1$ for all three $i \in \{1, 2, 3\}$. Likewise, there is at least a reduction sequence

$$s_2', P''[l_b', l_x', (\texttt{let}\, n = !\, l_x'\, \texttt{in}\, v_2'\, (); l_x' := n + 1)] \longmapsto^* s_{21}', (v_2'\, (); l_x' := m + 1; l_1 := \texttt{true})$$

with $s_{21}' = s_2'[l_b' \mapsto \texttt{false}]$. Assume $W_2 = \langle w_1, \ldots, w_p, w_{p+1}, \ldots, w_q \rangle$. Now define:

$$\begin{array}{rcl} W_2' & = & \langle w_1, \ldots, w_p, w_{p+1}', \ldots, w_q \rangle \\ w_{p+1}' & = & (\eta_{p+1}', \mathcal{L}_{k_2 - j_1}) \\ \eta_{p+1}' & = & \eta_{k_2 - j_1}^{V \cup \{(k_2 - j_1, k_2 - j_1 - j_2 - 1, m)\}} \end{array}$$

We have to show:

- $W_2' \in \mathit{World}_{k_2}$:
  - From the definition of w_{p+1} we know that V obeys the side conditions of $\mathcal{L}_k$.
  - Since $s_2(l_b) = \texttt{true}$, we know that $k' > k_2 > k_2 - j_1$, where $(k, k', m) = \min(V)$.
  - Thus, $V \cup \{(k_2 - j_1, k_2 - j_1 - j_2 - 1, m)\}$ obeys the side conditions of $\mathcal{L}_k$.
  - Also, it follows that $(k_2 - j_1, k_2 - j_1 - j_2 - 1, m) = \min(V \cup \{(k_2 - j_1, k_2 - j_1 - j_2 - 1, m)\})$ and hence, $w_{p+1}'.\psi = \psi_{k_2 - j_1}^{(k_2 - j_1, k_2 - j_1 - j_2 - 1, m)}$.
  - So $(k_2 - j_1, \eta_{p+1}') \in \mathcal{L}_{k_2 - j_1}$.
- $(k_2, W_2') \sqsupseteq (k_2, W_2)$:
  - Because $V \cup \{(k_2 - j_1, k_2 - j_1 - j_2 - 1, m)\} \supset V$, we have $\eta_{p+1}' \sqsupseteq W_2[p+1].\eta$ and thus $w_{p+1}' \sqsupseteq w_{p+1}$.
  - Furthermore, the other islands are unchanged, and $k_2 \leq k_2$.
- $s_{21}, s_{21}' :_{k_2 - j_1} W_2'$:
  - Because $s_{21}(l_b) = s_{21}'(l_b') = \texttt{false}$ and $s_{21}(l_x) = s_{21}'(l_x') = m$ and $k_2 \geq j_1$, clearly $(k_2 - j_1 - 1, \lfloor W_2' \rfloor_{k_2 - j_1 - 1}, s_{21}, s_{21}') \in \psi_{k_2 - j_1}^{(k_2 - j_1, k_2 - j_1 - j_2 - 1, m)}$.
  - Furthermore, we know already that $\psi_{k_2 - j_1}^{(k_2 - j_1, k_2 - j_1 - j_2 - 1, m)}$ is downward closed.

  Now, obviously,

$$(k_2 - j_1, W_2', (), ()) \in \mathcal{V}\,[\![\mathsf{unit}]\!]\,\emptyset$$

Because $(k_2, W_2, v_2, v_2') \in \mathcal{V}\,[\![\mathsf{unit} \to \mathsf{unit}]\!]\,\emptyset$ and $(k_2 - j_1, W_2') \sqsupset (k_2, W_2)$, by definition of $\mathcal{V}\,[\![\tau \to \tau']\!]$ we can conclude that $v_2 = \lambda z : \tau.\, e_3$ and $v_2' = \lambda z : \tau.\, e_3'$, and:

$$(k_2 - j_1, W_2', [()/z]e_3, [()/z]e_3') \in \mathcal{E}\,[\![\mathsf{unit}]\!]\,\emptyset$$

Because $[()/z]e_3$ terminates, from the definition of $\mathcal{E}\,[\![\tau]\!]$ we know that

$$\begin{array}{lll} \exists s_{22}', v_{22}', W_3, & s_{21}', [()/z]e_3' \longmapsto^* s_{22}', v_{22}' & \wedge \quad s_{22}, s_{22}' :_{k_2 - j_1 - j_2} W_3 \\ & (k_2 - j_1 - j_2, W_3) \sqsupseteq (k_2 - j_1, W_2') & \wedge \quad (k_2 - j_1 - j_2, W_3, v_{22}, v_{22}') \in \mathcal{V}\,[\![\mathsf{unit}]\!]\,\emptyset \end{array}$$

By definition of the reduction rules, this implies that there is a reduction sequence

$$\begin{array}{rcl} s_2', P''[l_b', l_x', (\texttt{let}\, n = !\, l_x'\, \texttt{in}\, v_2'\, (); l_x' := n + 1)] & \longmapsto^* & s_{22}', (v_{22}'; l_x' := m + 1; l_1 := \texttt{true}) \\ & \longmapsto^* & s_{22}'[l_b' \mapsto \texttt{true}, l_x' \mapsto m + 1], () \end{array}$$

Now for the crucial step: we show that $s_{22}(l_x) = s_{22}'(l_x') = m$:

- Because $(k_2 - j_1 - j_2, W_3) \sqsupseteq (k_2 - j_1, W_2')$, it must hold that $W_3 \sqsupseteq \lfloor W_2' \rfloor_{k_2-j_1-j_2}$ and $W_3 \in \mathit{World}_{k_2-j_1-j_2}$.
- From the former we know $W_3[p+1] \sqsupseteq \lfloor w'_{p+1} \rfloor_{k_2-j_1-j_2}$.
- That means that $W_3[p+1].V \supseteq V \cup \{(k_2-j_1, k_2-j_1-j_2-1, m)\}$ and $W_3[p+1].\mathcal{L} = \lfloor \mathcal{L}_{k_2-j_1} \rfloor_{k_2-j_1-j_2} = \mathcal{L}_{k_2-j_1-j_2}$.
- Hence, because $W_3 \in \mathit{World}_{k_2-j_1-j_2}$, we have $(k_2 - j_1 - j_2, W_3[p+1].\eta) \in \mathcal{L}_{k_2-j_1-j_2}$.
- That is, $W_3[p+1].\eta = \eta^{W_3[p+1].V}_{k_2-j_1-j_2}$.
- Thus, $W_3[p+1].\psi = \psi^{\min(W_3[p+1].V)}_{k_2-j_1-j_2}$.
- From $s_{22}, s'_{22} :_{k_1-j_1-j_2} W_3$ and $k_2-j_1-j_2 > k_2-k_3 > 0$, it follows that $(k_2-j_1-j_2-1, \lfloor W_3 \rfloor_{k_2-j_1-j_2-1}, s_{22}, s'_{22}) \in \psi^{\min(W_3[p+1].V)}_{k_2-j_1-j_2}$.
- From that we see that, by the definition of ψ^V_k, $\min(W_3[p+1].V) = (k, k', v')$, such that $k \geq k_2 - j_1 - j_2 - 1$.
- The side condition of $\mathcal{L}_k$ guarantees that no overlapping triple has been added to $V \cup \{(k_2 - j_1, k_2 - j_1 - j_2 - 1, m)\}$, i.e., either $k = k_2 - j_1$ or $k < k_2 - j_1 - j_2 - 1$.
- Together with the previous point, it follows that $k = k_2 - j_1$, and consequently, $(k, k', v') = (k_2 - j_1, k_2 - j_1 - j_2 - 1, m)$, the window we entered earlier.
- Because $(k_2 - j_1 - j_2 - 1, \lfloor W_3 \rfloor_{k_2-j_1-j_2-1}, s_{22}, s'_{22}) \in \psi^{(k_2-j_1, k_2-j_1-j_2-1, m)}_{k_2-j_1-j_2}$, by the definition of ψ^V_k, we can conclude
$$s_{22}(l_b) = s'_{22}(l'_b) = \texttt{false} \quad \wedge \quad s_{22}(l_x) = s'_{22}(l'_x) = m$$

Now let
$$s'_3 = s'_{22}[l_b \mapsto \texttt{true}, l_x \mapsto m+1]$$
Because $k_3 < k_2$, by downward closure $(k_2 - k_3 - 1, \lfloor W_3 \rfloor_{k_2-k_3-1}, s_3, s'_3) \in \psi^{(k_2-j_1, k_2-j_1-j_2-1, m)}_{k_2-j_1-j_2}$, so we have
$$s_3, s'_3 :_{k_2-k_3} W_3$$
It remains to be shown that
$$(k_2 - k_3, W_3, (), ()) \in \mathcal{V}\,[\![\mathsf{unit}]\!]\,\emptyset$$
which is trivially true.

Now consider (2). By definition of $\mathcal{V}\,[\![\tau \to \tau']\!]$, we have to show that:
$$\begin{array}{ll} \forall (k_2, W_2) \sqsupset (k_0 - k_1, W_1), v_2, v'_2, & (k_2, W_2, v_2, v'_2) \in \mathcal{V}\,[\![\mathsf{unit}]\!]\,\emptyset \implies \\ & (k_2, W_2, \lambda z : \mathsf{unit}.\ !\, l_x, \lambda z : \mathsf{unit}.\ !\, l'_x) \in \mathcal{E}\,[\![\mathsf{int}]\!]\,\emptyset \end{array}$$
Assume $(k_2, W_2) \sqsupset (k_0 - k_1, W_1)$. By definition of $\mathcal{E}\,[\![\tau]\!]$, we are required to show:
$$\begin{array}{rlll} \forall k_3 < k_2, s_2, s'_2, s_2, v_3, & s_2, s'_2 :_{k_2} W_2 & \wedge \quad s_2, !\, l_x \longmapsto^{k_3} s_3, v_3 & \implies \\ \exists s'_3, v'_3, W_3, & s_3, s'_3 :_{k_2-k_3} W_3 & \wedge \quad s'_2, !\, l'_x \longmapsto^{*} s'_3, v'_3 & \wedge \\ & (k_2 - k_3, W_3) \sqsupseteq (k_2, W_2) & \wedge \quad (k_2 - k_3, W_3, v_3, v'_3) \in \mathcal{V}\,[\![\mathsf{int}]\!]\,\emptyset & \end{array}$$
Assume $s_2, s'_2 :_{k_2} W_2$ and $s_2, !\, l_x \longmapsto^{k_3} s_3, v_3$. As for (1), we can derive, for some b and m:
$$\begin{array}{rcccl} s_2(l_b) & = & s'_2(l'_b) & = & b \\ s_2(l_x) & = & s'_2(l'_x) & = & m \end{array}$$

Hence, by definition of the reduction relation:

$$\begin{array}{lcllcl} s_3 & = & s_2, & v_3 & = & m \\ s_3' & = & s_2', & v_3' & = & m \end{array}$$

Let $W_3 = W_2$, which trivially is valid and extends W_2. Likewise, $s_3, s_3' :_{k_2 - k_3} W_3$ is immediate. It remains to be shown that

$$(k_2 - k_3, W_3, m, m) \in \mathcal{V}\,[\![\mathsf{int}]\!]\,\emptyset$$

which obviously is the case. □

References

[1] Amal Ahmed. Step-indexed syntactic logical relations for recursive and quantified types (extended). Technical Report TR-01-06, Harvard University, 2006. Available at: `http://ttic.uchicago.edu/~amal/papers/lr-recquant-techrpt.pdf`.

[2] Anindya Banerjee and David A. Naumann. State based ownership, reentrance, and encapsulation. In *ECOOP*, 2005.

[3] Nick Benton and Benjamin Leperchey. Relational reasoning in a nominal semantics for storage. In *TLCA*, 2005.

[4] Nina Bohr and Lars Birkedal. Relational reasoning for recursive types and references. In *APLAS*, 2006.

[5] Vasileios Koutavas and Mitchell Wand. Small bisimulations for reasoning about higher-order imperative programs. In *POPL*, 2006.

[6] Albert R. Meyer and Kurt Sieber. Towards fully abstract semantics for local variables. In *POPL*, 1988.

[7] Andrew Pitts. Typed operational reasoning. In B. C. Pierce, editor, *Advanced Topics in Types and Programming Languages*, pages 245–289. The MIT Press, 2005.