The Impact of Higher-Order State and Control Effects on Local Relational Reasoning

Technical Appendix

Derek Dreyer
dreyer@mpi-sws.org

Georg Neis
neis@mpi-sws.org

Lars Birkedal
birkedal@itu.dk

August 2010

Contents

1 Languages

1.1 HOS

1.1.1 Syntax & Dynamic Semantics

$$\tau \;::=\; \alpha \mid b \mid \tau_1 \times \tau_2 \mid \tau_1 \to \tau_2 \mid \forall\alpha.\,\tau \mid \exists\alpha.\,\tau \mid \mu\alpha.\,\tau \mid \mathsf{ref}\,\tau$$

$$\begin{array}{rcl} e & ::= & x \mid l \mid \langle e_1, e_2\rangle \mid e.1 \mid e.2 \mid \lambda x{:}\tau.\,e \mid e_1\;e_2 \mid \Lambda\alpha.e \mid e\;\tau \mid \\ & & \mathsf{pack}\,\langle\tau_1, e\rangle\,\mathsf{as}\,\tau_2 \mid \mathsf{unpack}\,e_1\,\mathsf{as}\,\langle\alpha, x\rangle\,\mathsf{in}\,e_2 \mid \\ & & \mathsf{roll}_\tau\,e \mid \mathsf{unroll}\,e \mid \mathsf{ref}\,e \mid e_1 := e_2 \mid\; !e \mid e_1 == e_2 \mid \ldots \end{array}$$

$$v \;::=\; l \mid c \mid \langle v_1, v_2\rangle \mid \lambda x{:}\tau.\,e \mid \Lambda\alpha.e \mid \mathsf{pack}\,\langle\tau_1, v\rangle\,\mathsf{as}\,\tau_2 \mid \mathsf{roll}_\tau\,v \mid \ldots$$

$$\begin{array}{rcl} C & ::= & \bullet \mid \langle C, e_2\rangle \mid \langle e_1, C\rangle \mid C.1 \mid C.2 \mid \lambda x{:}\tau.\,C \mid C\;e_2 \mid e_1\;C \mid \Lambda\alpha.C \mid C\;\tau \mid \\ & & \mathsf{pack}\,\langle\tau_1, C\rangle\,\mathsf{as}\,\tau_2 \mid \mathsf{unpack}\,C\,\mathsf{as}\,\langle\alpha, x\rangle\,\mathsf{in}\,e_2 \mid \mathsf{unpack}\,e_1\,\mathsf{as}\,\langle\alpha, x\rangle\,\mathsf{in}\,C \mid \\ & & \mathsf{roll}_\tau\,C \mid \mathsf{unroll}\,C \mid \mathsf{ref}\,C \mid C := e_2 \mid e_1 := C \mid\; !C \mid C == e_2 \mid e_1 == C \mid \ldots \end{array}$$

$$\begin{array}{rcl} K & ::= & \bullet \mid \langle K, e_2\rangle \mid \langle v_1, K\rangle \mid K.1 \mid K.2 \mid K\;e_2 \mid v_1\;K \mid K\;\tau \mid \\ & & \mathsf{pack}\,\langle\tau_1, K\rangle\,\mathsf{as}\,\tau_2 \mid \mathsf{unpack}\,K\,\mathsf{as}\,\langle\alpha, x\rangle\,\mathsf{in}\,e_2 \mid \\ & & \mathsf{roll}_\tau\,K \mid \mathsf{unroll}\,K \mid \mathsf{ref}\,K \mid K := e_2 \mid v_1 := K \mid\; !K \mid K == e_2 \mid v_1 == K \mid \ldots \end{array}$$

$$\begin{array}{lcll}
\langle h; K[\langle v_1, v_2\rangle.1]\rangle & \hookrightarrow & \langle h; K[v_1]\rangle & \\
\langle h; K[\langle v_1, v_2\rangle.2]\rangle & \hookrightarrow & \langle h; K[v_2]\rangle & \\
\langle h; K[(\lambda x{:}\tau.\,e)\;v]\rangle & \hookrightarrow & \langle h; K[e[v/x]]\rangle & \\
\langle h; K[(\Lambda\alpha.e)\;\tau]\rangle & \hookrightarrow & \langle h; K[e[\tau/\alpha]]\rangle & \\
\langle h; K[\mathsf{unpack}\,(\mathsf{pack}\,\langle\tau_1, v\rangle\,\mathsf{as}\,\tau_2)\,\mathsf{as}\,\langle\alpha, x\rangle\,\mathsf{in}\,e]\rangle & \hookrightarrow & \langle h; K[e[\tau_1/\alpha][v/x]]\rangle & \\
\langle h; K[\mathsf{unroll}\,(\mathsf{roll}_\tau\,v)]\rangle & \hookrightarrow & \langle h; K[v]\rangle & \\
\langle h; K[\mathsf{ref}\,v]\rangle & \hookrightarrow & \langle h \uplus \{l{\mapsto}v\}; K[l]\rangle & (l \notin \mathrm{dom}(h)) \\
\langle h; K[l := v]\rangle & \hookrightarrow & \langle h[l{\mapsto}v]; K[\langle\rangle]\rangle & (l \in \mathrm{dom}(h)) \\
\langle h; K[!l]\rangle & \hookrightarrow & \langle h; K[v]\rangle & (h(l) = v) \\
\langle h; K[l_1 == l_2]\rangle & \hookrightarrow & \langle h; K[\mathsf{tt}]\rangle & (l_1 = l_2) \\
\langle h; K[l_1 == l_2]\rangle & \hookrightarrow & \langle h; K[\mathsf{ff}]\rangle & (l_1 \neq l_2)
\end{array}$$

$$\begin{array}{lcl}
\langle h; e\rangle \hookrightarrow^k \langle h'; e'\rangle & \stackrel{\mathrm{def}}{\Longleftrightarrow} & \exists h_0, \ldots, h_k, e_0, \ldots, e_k.\ \langle h_0; e_0\rangle = \langle h; e\rangle \wedge \langle h_k; e_k\rangle = \langle h'; e'\rangle \wedge \\
 & & \forall i \in \{0, \ldots, k-1\}.\ \langle h_i; e_i\rangle \hookrightarrow \langle h_{i+1}; e_{i+1}\rangle \\
\langle h; e\rangle \downarrow^{<k} & \stackrel{\mathrm{def}}{\Longleftrightarrow} & \exists k', h', v.\ k' < k \wedge \langle h; e\rangle \hookrightarrow^{k'} \langle h'; v\rangle \\
\langle h; e\rangle \downarrow & \stackrel{\mathrm{def}}{\Longleftrightarrow} & \exists k.\ \langle h; e\rangle \downarrow^{<k}
\end{array}$$

1.1.2 Static Semantics

$$\begin{array}{lcll}
\text{Heap typings} & \Sigma & ::= & \cdot \mid \Sigma, l{:}\tau \qquad \text{where } \mathrm{fv}(\tau) = \emptyset \\
\text{Type environments} & \Delta & ::= & \cdot \mid \Delta, \alpha \\
\text{Term environments} & \Gamma & ::= & \cdot \mid \Gamma, x{:}\tau
\end{array}$$

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

$$\frac{\mathrm{fv}(\tau) \subseteq \Delta}{\Delta \vdash \tau}$$

$\boxed{\Sigma; \Delta; \Gamma \vdash K \div \tau}$

$$\frac{\vdash K : (\Sigma; \Delta; \Gamma; \tau) \rightsquigarrow (\Sigma; \Delta; \Gamma; \tau')}{\Sigma; \Delta; \Gamma \vdash K \div \tau}$$

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

$$\frac{x{:}\tau \in \Gamma}{\Sigma; \Delta; \Gamma \vdash x : \tau} \qquad \frac{l{:}\tau \in \Sigma}{\Sigma; \Delta; \Gamma \vdash l : \mathsf{ref}\ \tau} \qquad \frac{}{\Sigma; \Delta; \Gamma \vdash c : b}$$

$$\frac{\Sigma; \Delta; \Gamma \vdash e_1 : \tau_1 \quad \Sigma; \Delta; \Gamma \vdash e_2 : \tau_2}{\Sigma; \Delta; \Gamma \vdash \langle e_1, e_2 \rangle : \tau_1 \times \tau_2} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e : \tau_1 \times \tau_2}{\Sigma; \Delta; \Gamma \vdash e.1 : \tau_1} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e : \tau_1 \times \tau_2}{\Sigma; \Delta; \Gamma \vdash e.2 : \tau_2}$$

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

$$\frac{\Sigma; \Delta, \alpha; \Gamma \vdash e : \tau}{\Sigma; \Delta; \Gamma \vdash \Lambda\alpha.e : \forall\alpha.\, \tau} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e : \forall\alpha.\, \tau_1}{\Sigma; \Delta; \Gamma \vdash e\ \tau_2 : \tau_1[\tau_2/\alpha]}$$

$$\frac{\Sigma; \Delta; \Gamma \vdash e : \tau_2[\tau_1/\alpha]}{\Sigma; \Delta; \Gamma \vdash \mathsf{pack}\ \langle \tau_1, e \rangle\ \mathsf{as}\ \exists\alpha.\, \tau_2 : \exists\alpha.\, \tau_2} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e_1 : \exists\alpha.\, \tau_1 \quad \Sigma; \Delta, \alpha; \Gamma, x{:}\tau_1 \vdash e_2 : \tau_2 \quad \Delta \vdash \tau_2}{\Sigma; \Delta; \Gamma \vdash \mathsf{unpack}\ e_1\ \mathsf{as}\ \langle \alpha, x \rangle\ \mathsf{in}\ e_2 : \tau_2}$$

$$\frac{\Sigma; \Delta; \Gamma \vdash e : \tau[\mu\alpha.\, \tau/\alpha]}{\Sigma; \Delta; \Gamma \vdash \mathsf{roll}_{\mu\alpha.\, \tau}\ e : \mu\alpha.\, \tau} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e : \mu\alpha.\, \tau}{\Sigma; \Delta; \Gamma \vdash \mathsf{unroll}\ e : \tau[\mu\alpha.\, \tau/\alpha]}$$

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

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

$\cdots$

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

$$\frac{\Sigma \subseteq \Sigma' \quad \Delta \subseteq \Delta' \quad \Gamma \subseteq \Gamma'}{\vdash \bullet : (\Sigma; \Delta; \Gamma; \tau) \rightsquigarrow (\Sigma'; \Delta'; \Gamma'; \tau')}$$

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

$$\frac{\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_1 \times \tau_2)}{\vdash C.1 : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma;\tau_1)} \qquad \frac{\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_1 \times \tau_2)}{\vdash C.2 : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma;\tau_2)}$$

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

$$\frac{\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_1 \to \tau_2) \quad \Sigma';\Delta';\Gamma' \vdash e_2 : \tau_1}{\vdash C\ e_2 : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_2)}$$

$$\frac{\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_1) \quad \Sigma';\Delta';\Gamma' \vdash e_2 : \tau_1 \to \tau_2}{\vdash e_1\ C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_2)}$$

$$\frac{\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta', \alpha;\Gamma';\tau_1)}{\vdash \Lambda\alpha.C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\forall\alpha.\,\tau_1)} \qquad \frac{\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\forall\alpha.\,\tau_1)}{\vdash C\ \tau_2 : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_1[\tau_2/\alpha])}$$

$$\frac{\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_2[\tau_1/\alpha])}{\vdash \mathsf{pack}\ \langle \tau_1, C\rangle\ \mathsf{as}\ \exists\alpha.\,\tau_2 : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\exists\alpha.\,\tau_2)}$$

$$\frac{\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\exists\alpha.\,\tau_1) \quad \Sigma';\Delta', \alpha;\Gamma', x{:}\tau_1 \vdash e_2 : \tau_2 \quad \Delta' \vdash \tau_2}{\vdash \mathsf{unpack}\ C\ \mathsf{as}\ \langle \alpha, x\rangle\ \mathsf{in}\ e_2 : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_2)}$$

$$\frac{\Sigma';\Delta';\Gamma' \vdash e_1 : \exists\alpha.\,\tau_1 \quad \vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta', \alpha;\Gamma', x{:}\tau_1;\tau_2) \quad \Delta' \vdash \tau_2}{\vdash \mathsf{unpack}\ e_1\ \mathsf{as}\ \langle \alpha, x\rangle\ \mathsf{in}\ C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_2)}$$

$$\frac{\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_1[\mu\alpha.\,\tau_1/\alpha])}{\vdash \mathsf{roll}_{\mu\alpha.\,\tau_1}\ C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\mu\alpha.\,\tau_1)}$$

$$\frac{\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\mu\alpha.\,\tau_1)}{\vdash \mathsf{unroll}\ C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_1[\mu\alpha.\,\tau_1/\alpha])}$$

$$\frac{\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_1)}{\vdash \mathsf{ref}\ C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\mathsf{ref}\ \tau_1)}$$

$$\frac{\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\mathsf{ref}\ \tau_1) \quad \Sigma';\Delta';\Gamma' \vdash e_2 : \tau_1}{\vdash C := e_2 : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\mathsf{unit})}$$

$$\frac{\Sigma';\Delta';\Gamma' \vdash e_1 : \mathsf{ref}\ \tau_1 \quad \vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_1)}{\vdash e_1 := C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\mathsf{unit})}$$

$$\frac{\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\mathsf{ref}\,\tau_1)}{\vdash !C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau_1)}$$

$$\frac{\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\mathsf{ref}\,\tau_1) \quad \Sigma';\Delta';\Gamma' \vdash e_2 : \mathsf{ref}\,\tau_1}{\vdash C == e_2 : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\mathsf{bool})}$$

$$\frac{\Sigma';\Delta';\Gamma' \vdash e_1 : \mathsf{ref}\,\tau_1 \quad \vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\mathsf{ref}\,\tau_1)}{\vdash e_1 == C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\mathsf{bool})}$$

$$\ldots$$

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

$$\frac{\forall l{:}\tau \in \Sigma.\ \Sigma;\cdot;\cdot \vdash h(l) : \tau}{\vdash h : \Sigma}$$

$\boxed{\Sigma;\Delta;\Gamma \vdash \gamma : \Gamma}$

$$\frac{}{\Sigma;\Delta;\Gamma \vdash \emptyset : \cdot} \qquad \frac{\Sigma;\Delta;\Gamma \vdash \gamma : \Gamma' \quad \Sigma;\Delta;\Gamma \vdash v : \tau}{\Sigma;\Delta;\Gamma \vdash \gamma, x{\mapsto}v : \Gamma', x{:}\tau}$$

1.1.3 Contextual and CIU Approximation

$$\begin{aligned}\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\mathrm{ctx}} e_2 : \tau \stackrel{\mathrm{def}}{=}\ & \Sigma;\Delta;\Gamma \vdash e_1 : \tau \wedge \Sigma;\Delta;\Gamma \vdash e_2 : \tau \wedge \forall C, \Sigma', \tau', h. \\ & \vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\cdot;\cdot;\tau') \wedge \vdash h : \Sigma' \wedge \\ & \langle h; C[e_1]\rangle\downarrow \implies \langle h; C[e_2]\rangle\downarrow\end{aligned}$$

$$\begin{aligned}\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\mathrm{ciu}} e_2 : \tau \stackrel{\mathrm{def}}{=}\ & \Sigma;\Delta;\Gamma \vdash e_1 : \tau \wedge \Sigma;\Delta;\Gamma \vdash e_2 : \tau \wedge \forall \delta, \gamma, K, \Sigma', h. \\ & \cdot \vdash \delta : \Delta \wedge \Sigma';\cdot;\cdot \vdash \gamma : \delta\Gamma \wedge \Sigma';\cdot;\cdot \vdash K \div \delta\tau \wedge \Sigma \subseteq \Sigma' \wedge \vdash h : \Sigma' \wedge \\ & \langle h; K[\delta\gamma e_1]\rangle\downarrow \implies \langle h; K[\delta\gamma e_2]\rangle\downarrow\end{aligned}$$

1.1.4 Random Lemmas

Lemma 1. If $\Sigma;\Delta;\Gamma \vdash K \div \tau$, then $\Sigma;\Delta;\Gamma, x{:}\tau \vdash K[x] : \tau'$, for some τ'.

Proof. By an easy induction on K. □

Lemma 2. If $\vdash C_1 : (\Sigma_1;\Delta_1;\Gamma_1;\tau_1) \rightsquigarrow (\Sigma_2;\Delta_2;\Gamma_2;\tau_2)$ and $\vdash C_2 : (\Sigma_2;\Delta_2;\Gamma_2;\tau_2) \rightsquigarrow (\Sigma_3;\Delta_3;\Gamma_3;\tau_3)$, then $\vdash C_2[C_1] : (\Sigma_1;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma_3;\Delta_3;\Gamma_3;\tau_3)$.

Lemma 3. If $\Sigma_1 \subseteq \Sigma_2$ and $\vdash C : (\Sigma_2;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau')$, then $\vdash C : (\Sigma_1;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau')$.

1.2 HOSE

HOSE is obtained from **HOS** by making the following extensions.

1.2.1 Syntax & Dynamic Semantics

$$
\begin{array}{rcl}
\tau & ::= & \ldots \mid \mathsf{exn} \\
e & ::= & \ldots \mid c_{\mathsf{exn}} \mid \mathsf{raise}\ e \mid \mathsf{try}\ e_1\ \mathsf{with}\ x.e_2 \\
v & ::= & \ldots \mid c_{\mathsf{exn}} \\
C & ::= & \ldots \mid \mathsf{raise}\ C \mid \mathsf{try}\ C\ \mathsf{with}\ x.e_2 \mid \mathsf{try}\ e_1\ \mathsf{with}\ x.C \\
K & ::= & \ldots \mid \mathsf{raise}\ K \mid \mathsf{try}\ K\ \mathsf{with}\ x.e_2
\end{array}
$$

$$
\begin{array}{lcll}
\ldots & & & \\
\langle h; K[\mathsf{raise}\ v]\rangle & \hookrightarrow & \langle h; \mathsf{raise}\ v\rangle & (K \neq \bullet \text{ and } K \text{ does not try}) \\
\langle h; K_1[\mathsf{try}\ K_2[\mathsf{raise}\ v]\ \mathsf{with}\ x.e_2]\rangle & \hookrightarrow & \langle h; K_1[e_2[v/x]]\rangle & (K_2 \text{ does not try}) \\
\langle h; K_1[\mathsf{try}\ v\ \mathsf{with}\ x.e_2]\rangle & \hookrightarrow & \langle h; K_1[v]\rangle &
\end{array}
$$

1.2.2 Static Semantics

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

$$\ldots \qquad \frac{}{\Sigma; \Delta; \Gamma \vdash c_{\mathsf{exn}} : \mathsf{exn}}$$

$$\frac{\Sigma; \Delta; \Gamma \vdash e : \mathsf{exn}}{\Sigma; \Delta; \Gamma \vdash \mathsf{raise}\ e : \tau} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e_1 : \tau \quad \Sigma; \Delta; \Gamma, x{:}\mathsf{exn} \vdash e_2 : \tau}{\Sigma; \Delta; \Gamma \vdash \mathsf{try}\ e_1\ \mathsf{with}\ x.e_2 : \tau}$$

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

$$\ldots$$

$$\frac{\vdash C : (\Sigma; \Delta; \Gamma; \tau) \rightsquigarrow (\Sigma'; \Delta'; \Gamma'; \mathsf{exn})}{\vdash \mathsf{raise}\ C : (\Sigma; \Delta; \Gamma; \tau) \rightsquigarrow (\Sigma'; \Delta'; \Gamma'; \tau_1)}$$

$$\frac{\vdash C : (\Sigma; \Delta; \Gamma; \tau) \rightsquigarrow (\Sigma'; \Delta'; \Gamma'; \tau_1) \quad \Sigma'; \Delta'; \Gamma', x{:}\mathsf{exn} \vdash e_2 : \tau_1}{\vdash \mathsf{try}\ C\ \mathsf{with}\ x.e_2 : (\Sigma; \Delta; \Gamma; \tau) \rightsquigarrow (\Sigma'; \Delta'; \Gamma'; \tau_1)}$$

$$\frac{\Sigma'; \Delta'; \Gamma' \vdash e_1 : \tau_1 \quad \vdash C : (\Sigma; \Delta; \Gamma; \tau) \rightsquigarrow (\Sigma'; \Delta'; \Gamma', x{:}\mathsf{exn}; \tau_1)}{\vdash \mathsf{try}\ e_1\ \mathsf{with}\ x.C : (\Sigma; \Delta; \Gamma; \tau) \rightsquigarrow (\Sigma'; \Delta'; \Gamma'; \tau_1)}$$

1.3 HOSC

HOSC is obtained from **HOS** by making the following extensions.

1.3.1 Syntax & Dynamic Semantics

$$
\begin{array}{rcl}
\tau & ::= & \ldots \mid \mathsf{cont}\,\tau \\
e & ::= & \ldots \mid \mathsf{cont}_\tau\ K \mid \mathsf{call/cc}_\tau\,(x.\ e) \mid \mathsf{throw}_\tau\ e_1\ \mathsf{to}\ e_2 \\
v & ::= & \ldots \mid \mathsf{cont}_\tau\ K \\
C & ::= & \ldots \mid \mathsf{call/cc}_\tau\,(x.\ C) \mid \mathsf{throw}_\tau\ C\ \mathsf{to}\ e_2 \mid \mathsf{throw}_\tau\ e_1\ \mathsf{to}\ C \\
K & ::= & \ldots \mid \mathsf{call/cc}_\tau\,(x.\ K) \mid \mathsf{throw}_\tau\ K\ \mathsf{to}\ e_2 \mid \mathsf{throw}_\tau\ v_1\ \mathsf{to}\ K
\end{array}
$$

$$
\begin{array}{lcl}
\ldots & & \\
\langle h; K[\mathsf{call/cc}_\tau\,(x.\ e)]\rangle & \hookrightarrow & \langle h; K[e[\mathsf{cont}_\tau\ K/x]]\rangle \\
\langle h; K[\mathsf{throw}_\tau\ v\ \mathsf{to}\ \mathsf{cont}_{\tau'}\ K']\rangle & \hookrightarrow & \langle h; K'[v]\rangle
\end{array}
$$

1.3.2 Static Semantics

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

$$\ldots$$

$$\frac{\Sigma; \Delta; \Gamma \vdash K \div \tau}{\Sigma; \Delta; \Gamma \vdash \mathsf{cont}_\tau\ K : \mathsf{cont}\,\tau}$$

$$\frac{\Sigma; \Delta; \Gamma, x{:}\mathsf{cont}\,\tau \vdash e : \tau}{\Sigma; \Delta; \Gamma \vdash \mathsf{call/cc}_\tau\,(x.\ e) : \tau} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e' : \tau' \quad \Sigma; \Delta; \Gamma \vdash e : \mathsf{cont}\,\tau'}{\Sigma; \Delta; \Gamma \vdash \mathsf{throw}_\tau\ e'\ \mathsf{to}\ e : \tau}$$

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

$$\ldots$$

$$\frac{\vdash C : (\Sigma; \Delta; \Gamma; \tau) \rightsquigarrow (\Sigma'; \Delta'; \Gamma', x{:}\mathsf{cont}\,\tau_1; \tau_1)}{\vdash \mathsf{call/cc}_{\tau_1}\,(x.\ C) : (\Sigma; \Delta; \Gamma; \tau) \rightsquigarrow (\Sigma'; \Delta'; \Gamma'; \tau_1)}$$

$$\frac{\vdash C : (\Sigma; \Delta; \Gamma; \tau) \rightsquigarrow (\Sigma'; \Delta'; \Gamma'; \tau_2) \quad \Sigma'; \Delta'; \Gamma' \vdash e_2 : \mathsf{cont}\,\tau_2}{\vdash \mathsf{throw}_{\tau_1}\ C\ \mathsf{to}\ e_2 : (\Sigma; \Delta; \Gamma; \tau) \rightsquigarrow (\Sigma'; \Delta'; \Gamma'; \tau_1)}$$

$$\frac{\Sigma'; \Delta'; \Gamma' \vdash e_1 : \tau_2 \quad \vdash C : (\Sigma; \Delta; \Gamma; \tau) \rightsquigarrow (\Sigma'; \Delta'; \Gamma'; \mathsf{cont}\,\tau_2)}{\vdash \mathsf{throw}_{\tau_1}\ e_1\ \mathsf{to}\ C : (\Sigma; \Delta; \Gamma; \tau) \rightsquigarrow (\Sigma'; \Delta'; \Gamma'; \tau_1)}$$

1.4 FOS

FOS is obtained from **HOS** by making the following changes to the syntax.

$$\tau ::= \ldots \mid \mathsf{ref}\, b \mid \ldots$$

$$\Sigma ::= \cdot \mid \Sigma, l{:}b$$

1.5 FOSE

FOSE is obtained by adding exceptions as in **HOSE** but at the same time restricting to first-order state as in **FOS**.

1.6 FOSC

FOSC is obtained by adding call/cc as in **HOSC** but at the same time restricting to first-order state as in **FOS**.

2 Logical Relations

2.1 HOS

$$
\begin{aligned}
\mathrm{HeapAtom}_n &\stackrel{\text{def}}{=} \{(W, h_1, h_2) \mid W \in \mathrm{World}_n\} \\
\mathrm{HeapRel}_n &\stackrel{\text{def}}{=} \{\psi \subseteq \mathrm{HeapAtom}_n \mid \forall (W, h_1, h_2) \in \psi.\ \forall W' \sqsupseteq W.\ (W', h_1, h_2) \in \psi\} \\
\mathrm{Island}_n &\stackrel{\text{def}}{=} \{\iota = (s, \delta, \varphi, \lightning, H) \mid s \in \mathrm{State} \wedge \delta \subseteq \mathrm{State}^2 \wedge \varphi \subseteq \delta \wedge \delta, \varphi \text{ reflexive} \wedge \\
&\qquad\qquad \delta, \varphi \text{ transitive} \wedge \lightning \subseteq \mathrm{State} \wedge H \in \mathrm{State} \to \mathrm{HeapRel}_n\} \\
\mathrm{World}_n &\stackrel{\text{def}}{=} \{W = (k, \Sigma_1, \Sigma_2, \omega) \mid k < n \wedge \exists m.\ \omega \in \mathrm{Island}_k^m\} \\
\mathrm{ContAtom}_n[\tau_1, \tau_2] &\stackrel{\text{def}}{=} \{(W, K_1, K_2) \mid W \in \mathrm{World}_n \wedge W.\Sigma_1; \cdot; \cdot \vdash K_1 \div \tau_1 \wedge W.\Sigma_2; \cdot; \cdot \vdash K_2 \div \tau_2\} \\
\mathrm{TermAtom}_n[\tau_1, \tau_2] &\stackrel{\text{def}}{=} \{(W, e_1, e_2) \mid W \in \mathrm{World}_n \wedge W.\Sigma_1; \cdot; \cdot \vdash e_1 : \tau_1 \wedge W.\Sigma_2; \cdot; \cdot \vdash e_2 : \tau_2\} \\
\mathrm{ValRel}[\tau_1, \tau_2] &\stackrel{\text{def}}{=} \{r \subseteq \mathrm{TermAtom}^{\mathsf{val}}[\tau_1, \tau_2] \mid \forall (W, v_1, v_2) \in r.\ \forall W' \sqsupseteq W.\ (W', v_1, v_2) \in r\} \\
\mathrm{SomeValRel} &\stackrel{\text{def}}{=} \{R = (\tau_1, \tau_2, r) \mid r \in \mathrm{ValRel}[\tau_1, \tau_2]\}
\end{aligned}
$$

$$
\begin{aligned}
\lfloor (\iota_1, \ldots, \iota_m) \rfloor_k &\stackrel{\text{def}}{=} (\lfloor \iota_1 \rfloor_k, \ldots, \lfloor \iota_m \rfloor_k) \\
\lfloor (s, \delta, \varphi, \lightning, H) \rfloor_k &\stackrel{\text{def}}{=} (s, \delta, \varphi, \lightning, \lfloor H \rfloor_k) \\
\lfloor H \rfloor_k &\stackrel{\text{def}}{=} \lambda s. \lfloor H(s) \rfloor_k \\
\lfloor \psi \rfloor_k &\stackrel{\text{def}}{=} \{(W, h_1, h_2) \in r \mid W.k < k\}
\end{aligned}
$$

$$
\begin{aligned}
\triangleright (k+1, \Sigma_1, \Sigma_2, \omega) &\stackrel{\text{def}}{=} (k, \Sigma_1, \Sigma_2, \lfloor \omega \rfloor_k) \\
\triangleright r &\stackrel{\text{def}}{=} \{(W, e_1, e_2) \mid W.k > 0 \implies (\triangleright W, e_1, e_2) \in r\}
\end{aligned}
$$

$$
\begin{aligned}
(k', \Sigma_1', \Sigma_2', \omega') \sqsupseteq (k, \Sigma_1, \Sigma_2, \omega) &\stackrel{\text{def}}{=} k' \le k \wedge \Sigma_1' \supseteq \Sigma_1 \wedge \Sigma_2' \supseteq \Sigma_2 \wedge \omega' \sqsupseteq \lfloor \omega \rfloor_{k'} \\
(\iota_1', \ldots, \iota_{m'}') \sqsupseteq (\iota_1, \ldots, \iota_m) &\stackrel{\text{def}}{=} m' \ge m \wedge \forall j \in \{1, \ldots, m\}.\ \iota_j' \sqsupseteq \iota_j \\
(s', \delta', \varphi', \lightning', H') \sqsupseteq (s, \delta, \varphi, \lightning, H) &\stackrel{\text{def}}{=} (\delta', \varphi', \lightning', H') = (\delta, \varphi, \lightning, H) \wedge (s, s') \in \delta
\end{aligned}
$$

$$
\begin{aligned}
(k', \Sigma_1', \Sigma_2', \omega') \sqsupseteq^{\mathsf{pub}} (k, \Sigma_1, \Sigma_2, \omega) &\stackrel{\text{def}}{=} k' \le k \wedge \Sigma_1' \supseteq \Sigma_1 \wedge \Sigma_2' \supseteq \Sigma_2 \wedge \omega' \sqsupseteq^{\mathsf{pub}} \lfloor \omega \rfloor_{k'} \\
(\iota_1', \ldots, \iota_{m'}') \sqsupseteq^{\mathsf{pub}} (\iota_1, \ldots, \iota_m) &\stackrel{\text{def}}{=} m' \ge m \wedge \forall j \in \{1, \ldots, m\}.\ \iota_j' \sqsupseteq^{\mathsf{pub}} \iota_j \wedge \\
&\qquad \forall j \in \{m+1, \ldots, m'\}.\ \mathrm{safe}(\iota_j') \\
(s', \delta', \varphi', \lightning', H') \sqsupseteq^{\mathsf{pub}} (s, \delta, \varphi, \lightning, H) &\stackrel{\text{def}}{=} (\delta', \varphi', \lightning', H') = (\delta, \varphi, \lightning, H) \wedge (s, s') \in \varphi
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{safe}(W) &\stackrel{\text{def}}{=} \forall \iota \in W.\omega.\ \mathrm{safe}(\iota) \\
\mathrm{safe}(\iota) &\stackrel{\text{def}}{=} \forall s'.\ (\iota.s, s') \in \iota.\varphi \implies s' \notin \iota.\lightning \\
\mathrm{consistent}(W) &\stackrel{\text{def}}{=} \nexists \iota \in W.\omega.\ \iota.s \in \iota.\lightning
\end{aligned}
$$

$$
\psi \otimes \psi' \stackrel{\text{def}}{=} \{(W, h_1 \uplus h_1', h_2 \uplus h_2') \mid (W, h_1, h_2) \in \psi \wedge (W, h_1', h_2') \in \psi'\}
$$

$$
\begin{aligned}
(h_1, h_2) : W \stackrel{\text{def}}{=}\ & \vdash h_1 : W.\Sigma_1 \wedge \vdash h_2 : W.\Sigma_2 \wedge \\
& (W.k > 0 \implies (\triangleright W, h_1, h_2) \in \textstyle\bigotimes_{i=1}^{|W.\omega|} W.\omega(i).H(W.\omega(i).s))
\end{aligned}
$$

$$
\begin{array}{rcl}
\mathcal{V}[\![\alpha]\!]\rho & \stackrel{\text{def}}{=} & \rho(\alpha).r \\
\mathcal{V}[\![b]\!]\rho & \stackrel{\text{def}}{=} & \{(W,v,v) \in \text{TermAtom}[b,b]\} \\
\mathcal{V}[\![\tau \times \tau']\!]\rho & \stackrel{\text{def}}{=} & \{(W, \langle v_1, v_1'\rangle, \langle v_2, v_2'\rangle) \in \text{TermAtom}[\rho_1(\tau\times\tau'), \rho_2(\tau\times\tau')] \mid \\
& & \quad (W,v_1,v_2) \in \mathcal{V}[\![\tau]\!]\rho \wedge (W,v_1',v_2') \in \mathcal{V}[\![\tau']\!]\rho\} \\
\mathcal{V}[\![\tau' \to \tau]\!]\rho & \stackrel{\text{def}}{=} & \{(W, \lambda x{:}\tau_1.\, e_1, \lambda x{:}\tau_2.\, e_2) \in \text{TermAtom}[\rho_1(\tau'\to\tau), \rho_2(\tau'\to\tau)] \mid \\
& & \quad \forall W', v_1, v_2.\ W' \sqsupseteq W \wedge (W', v_1, v_2) \in \mathcal{V}[\![\tau']\!]\rho \implies \\
& & \quad (W', e_1[v_1/x], e_2[v_2/x]) \in \mathcal{E}[\![\tau]\!]\rho\} \\
\mathcal{V}[\![\forall\alpha.\,\tau]\!]\rho & \stackrel{\text{def}}{=} & \{(W, \Lambda\alpha.e_1, \Lambda\alpha.e_2) \in \text{TermAtom}[\rho_1(\forall\alpha.\,\tau), \rho_2(\forall\alpha.\,\tau)] \mid \\
& & \quad \forall W' \sqsupseteq W.\ \forall(\tau_1,\tau_2,r) \in \text{SomeValRel}. \\
& & \quad (W', e_1[\tau_1/\alpha], e_2[\tau_2/\alpha]) \in \mathcal{E}[\![\tau]\!]\rho, \alpha{\mapsto}(\tau_1,\tau_2,r)\} \\
\mathcal{V}[\![\exists\alpha.\,\tau]\!]\rho & \stackrel{\text{def}}{=} & \{(W, \mathsf{pack}\ \langle\tau_1, v_1\rangle\ \mathsf{as}\ \tau_1', \mathsf{pack}\ \langle\tau_2, v_2\rangle\ \mathsf{as}\ \tau_2') \in \text{TermAtom}[\rho_1(\exists\alpha.\,\tau), \rho_2(\exists\alpha.\,\tau)] \mid \\
& & \quad \exists r.\ (\tau_1,\tau_2,r) \in \text{SomeValRel} \wedge (W,v_1,v_2) \in \mathcal{V}[\![\tau]\!]\rho, \alpha{\mapsto}(\tau_1,\tau_2,r)\} \\
\mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho & \stackrel{\text{def}}{=} & \{(W, \mathsf{roll}_{\tau_1}\ v_1, \mathsf{roll}_{\tau_2}\ v_2) \in \text{TermAtom}[\rho_1(\mu\alpha.\,\tau), \rho_2(\mu\alpha.\,\tau)] \mid \\
& & \quad (W,v_1,v_2) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho\} \\
\mathcal{V}[\![\mathsf{ref}\,\tau]\!]\rho & \stackrel{\text{def}}{=} & \{(W, l_1, l_2) \in \text{TermAtom}[\rho_1(\mathsf{ref}\,\tau), \rho_2(\mathsf{ref}\,\tau)] \mid \\
& & \quad \exists i.\ \forall W' \sqsupseteq W.\ (l_1,l_2) \in \text{bij}(W'.\omega(i).s) \wedge \\
& & \quad \exists\psi.\ W'.\omega(i).H(W'.\omega(i).s) = \psi \otimes \\
& & \quad \{(\widetilde{W}, \{l_1{\mapsto}v_1\}, \{l_2{\mapsto}v_2\}) \in \text{HeapAtom} \mid (\widetilde{W}, v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho\}\} \\
\\
\mathcal{O} & \stackrel{\text{def}}{=} & \{(W, e_1, e_2) \mid \forall h_1, h_2.\ (h_1,h_2) : W \wedge \langle h_1; e_1\rangle{\downarrow^{<W.k}} \implies \\
& & \quad \text{consistent}(W) \wedge \langle h_2; e_2\rangle{\downarrow}\} \\
\\
\mathcal{K}[\![\tau]\!]\rho & \stackrel{\text{def}}{=} & \{(W, K_1, K_2) \in \text{ContAtom}[\rho_1(\tau), \rho_2(\tau)] \mid \\
& & \quad \forall W', v_1, v_2.\ W' \sqsupseteq^{\mathsf{pub}} W \wedge (W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho \implies \\
& & \quad (W', K_1[v_1], K_2[v_2]) \in \mathcal{O}\} \\
\\
\mathcal{E}[\![\tau]\!]\rho & \stackrel{\text{def}}{=} & \{(W, e_1, e_2) \in \text{TermAtom}[\rho_1(\tau), \rho_2(\tau)] \mid \\
& & \quad \forall K_1, K_2.\ (W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho \implies (W, K_1[e_1], K_2[e_2]) \in \mathcal{O}\} \\
\\
\mathcal{G}[\![\cdot]\!]\rho & \stackrel{\text{def}}{=} & \{(W, \emptyset) \mid W \in \text{World}\} \\
\mathcal{G}[\![\Gamma, x{:}\tau]\!]\rho & \stackrel{\text{def}}{=} & \{(W, (\gamma, x{\mapsto}(v_1,v_2))) \mid (W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho \wedge (W,v_1,v_2) \in \mathcal{V}[\![\tau]\!]\rho\} \\
\\
\mathcal{D}[\![\cdot]\!] & \stackrel{\text{def}}{=} & \{\emptyset\} \\
\mathcal{D}[\![\Delta, \alpha]\!] & \stackrel{\text{def}}{=} & \{\rho, \alpha{\mapsto}R \mid \rho \in \mathcal{D}[\![\Delta]\!] \wedge R \in \text{SomeValRel}\} \\
\\
\mathcal{S}[\![\cdot]\!] & \stackrel{\text{def}}{=} & \text{World} \\
\mathcal{S}[\![\Sigma, l{:}\tau]\!] & \stackrel{\text{def}}{=} & \mathcal{S}[\![\Sigma]\!] \cap \{W \in \text{World} \mid (W,l,l) \in \mathcal{V}[\![\mathsf{ref}\,\tau]\!]\emptyset\}
\end{array}
$$

$$
\begin{array}{rcl}
\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\log} e_2 : \tau & \stackrel{\text{def}}{=} & \Sigma;\Delta;\Gamma \vdash e_1 : \tau \wedge \Sigma;\Delta;\Gamma \vdash e_2 : \tau \wedge \\
& & \forall W, \rho, \gamma.\ W \in \mathcal{S}[\![\Sigma]\!] \wedge \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho \implies \\
& & (W, \rho_1\gamma_1 e_1, \rho_2\gamma_2 e_2) \in \mathcal{E}[\![\tau]\!]\rho
\end{array}
$$

The bij() function (for extracting the bijection encoded in a state) can be defined as follows for our examples (assuming State contains sets of language values):

$$\mathrm{bij}(s) \stackrel{\text{def}}{=} \begin{cases} \{(l_1, l_2) \mid \langle l_1, l_2 \rangle \in s\} & \text{if that is a partial bijection} \\ \emptyset & \text{otherwise} \end{cases}$$

2.2 HOSE

One addition and one change:

$$\mathcal{V}[\![\mathsf{exn}]\!]\rho \stackrel{\text{def}}{=} \{(W, v, v) \in \mathrm{TermAtom}[\mathsf{exn}, \mathsf{exn}]\}$$

$$\begin{aligned} \mathcal{K}[\![\tau]\!]\rho \stackrel{\text{def}}{=} \{&(W, K_1, K_2) \in \mathrm{ContAtom}[\rho_1(\tau), \rho_2(\tau)] \mid \\ &\forall W', v_1, v_2.\ W' \sqsupseteq^{\mathsf{pub}} W \implies \\ &((W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho \implies (W', K_1[v_1], K_2[v_2]) \in \mathcal{O}) \wedge \\ &((W', v_1, v_2) \in \mathcal{V}[\![\mathsf{exn}]\!]\rho \implies (W', K_1[\mathsf{raise}\ v_1], K_2[\mathsf{raise}\ v_2]) \in \mathcal{O})\} \end{aligned}$$

2.3 HOSC

One addition and one change:

$$\mathcal{V}[\![\mathsf{cont}\ \tau]\!]\rho \stackrel{\text{def}}{=} \{(W, \mathsf{cont}\ K_1, \mathsf{cont}\ K_2) \mid (W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho\}$$

$$\mathrm{Island}'_n \stackrel{\text{def}}{=} \{\iota \in \mathrm{Island}_n \mid \iota.\varphi = \iota.\delta \wedge \iota.\lightning = \emptyset\}$$

2.4 FOS

A few simple changes:

$$\begin{aligned} \mathrm{HeapAtom}_n &\stackrel{\text{def}}{=} \mathrm{Heap} \times \mathrm{Heap} \\ \mathrm{HeapRel}_n &\stackrel{\text{def}}{=} \{\psi \subseteq \mathrm{HeapAtom}_n\} \end{aligned}$$

$$\begin{aligned} (h_1, h_2) : W \stackrel{\text{def}}{=}\ & \vdash h_1 : W.\Sigma_1 \wedge \vdash h_2 : W.\Sigma_2 \wedge (W.k > 0 \implies \exists h_1^1, \ldots, h_1^{|W.\omega|}, h_2^1, \ldots, h_2^{|W.\omega|}. \\ & h_1 = h_1^1 \uplus \cdots \uplus h_1^{|W.\omega|} \wedge h_2 = h_2^1 \uplus \cdots \uplus h_2^{|W.\omega|} \wedge \forall j \in \{1, \ldots, |W.\omega|\}. \\ & (h_1^j, h_2^j) \in W.\omega(j).H(W.\omega(j).s)) \end{aligned}$$

$$\psi \otimes \psi' \stackrel{\text{def}}{=} \{(h_1 \uplus h_1', h_2 \uplus h_2') \mid (h_1, h_2) \in \psi \wedge (h_1', h_2') \in \psi'\}$$

$$\begin{aligned} \mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho \stackrel{\text{def}}{=} \{&(W, l_1, l_2) \in \mathrm{TermAtom}[\rho_1(\mathsf{ref}\ \tau), \rho_2(\mathsf{ref}\ \tau)] \mid \\ &\exists i.\ \forall W' \sqsupseteq W.\ (l_1, l_2) \in \mathrm{bij}(W'.\omega(i).s) \wedge \\ &\exists \psi.\ W'.\omega(i).H(W'.\omega(i).s) = \psi \otimes \\ &\{(\{l_1 \mapsto v_1\}, \{l_2 \mapsto v_2\}) \in \mathrm{HeapAtom} \mid (v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho\}\} \end{aligned}$$

2.5 FOSE

Combine the corresponding adaptations.

2.6 FOSC

Combine the corresponding adaptations.

3 Properties

3.1 HOS

3.1.1 Basic Properties

Lemma 4.

1. $\triangleright W \sqsupseteq^{\mathsf{pub}} W$
2. $\sqsupseteq^{\mathsf{pub}} \subseteq \sqsupseteq$
3. If $W' \sqsupseteq W$, then $\triangleright W' \sqsupseteq \triangleright W$.
4. If $W' \sqsupseteq^{\mathsf{pub}} W$, then $\triangleright W' \sqsupseteq^{\mathsf{pub}} \triangleright W$.

Lemma 5. $\mathcal{V}[\![\tau]\!]\rho \subseteq \mathcal{E}[\![\tau]\!]\rho$

Proof.

- Suppose $(W, v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$, $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$, $(h_1, h_2) : W$, and $\langle h_1; K_1[v_1]\rangle\downarrow^{<W.k}$.
- We need to show consistent(W) and $\langle h_2; K_2[v_2]\rangle\downarrow$, which follow from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$ with $W \sqsupseteq^{\mathsf{pub}} W$.

□

Lemma 6 (Irrelevance)**.** If $\mathrm{fv}(\tau) \subseteq \mathrm{dom}(\rho)$ and $\rho(\alpha) = \rho'(\alpha)$ for all $\alpha \in \mathrm{dom}(\rho)$, then

1. $\mathcal{V}[\![\tau]\!]\rho = \mathcal{V}[\![\tau]\!]\rho'$,
2. $\mathcal{K}[\![\tau]\!]\rho = \mathcal{K}[\![\tau]\!]\rho'$,
3. $\mathcal{E}[\![\tau]\!]\rho = \mathcal{E}[\![\tau]\!]\rho'$, and
4. $\mathcal{G}[\![\tau]\!]\rho = \mathcal{G}[\![\tau]\!]\rho'$.

Lemma 7.

1. If $W \in \mathcal{S}[\![\Sigma]\!]$, then $\Sigma \subseteq W.\Sigma_1$ and $\Sigma \subseteq W.\Sigma_2$.
2. If $\rho \in \mathcal{D}[\![\Delta]\!]$, then $\cdot \vdash \rho_1 : \Delta$ and $\cdot \vdash \rho_2 : \Delta$.
3. If $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$, then $W.\Sigma_1; \cdot; \cdot \vdash \gamma_1 : \rho_1\Gamma$ and $W.\Sigma_2; \cdot; \cdot \vdash \gamma_2 : \rho_2\Gamma$.

Lemma 8.

1. If safe(W), then consistent(W).
2. If $W' \sqsupseteq^{\mathsf{pub}} W$ and safe(W), then safe(W').

Proof.

1. Obvious from the definitions (state transitions are reflexive).
2. - Suppose there is $W.\omega(j).s \in W.\omega(j).\not\downarrow$ for some $j \in \{1, \ldots, |W.\omega|\}$.

- By definition of $W' \sqsupseteq^{\mathsf{pub}} W$ we then have $W.\omega(j).s \in W'.\omega(j).\lightning$ and $(W.\omega(j).s, W'.\omega(j).s) \in W'.\omega(j).\varphi$.
- Hence the definition of Island implies $W'.\omega(j).s \in W.\omega'(j).\lightning$, which is in contradiction with consistent(W').

3. - Say $W'.\omega = (\iota'_1, \ldots, \iota'_{m'})$ and $W.\omega = (\iota_1, \ldots, \iota_m)$.
   - Suppose $j \in \{1, \ldots, m'\}$ and $(\iota'_j.s, s) \in \iota'_j.\varphi$.
   - To show: $s \notin \iota'_j.\lightning$
   - We distinguish whether or not the island in question was already present in W.
     (a) Case $j \in \{m+1, \ldots, m'\}$:
       – Then safe(ι'_j) by definition of $\sqsupseteq^{\mathsf{pub}}$.
       – Instantiating this yields the claim.
     (b) Case $j \in \{1, \ldots, m\}$:
       – Then $(\iota_j.s, \iota'_j.s) \in \iota_j.\varphi$ and $\iota_j.\varphi = \iota'_j.\varphi$.
       – Due to transitivity we have $(\iota_j.s, s) \in \iota_j.\varphi$.
       – By assumption we know safe(ι_j).
       – Instantiating this yields $s \notin \iota_j.\lightning$.
       – Since $\iota_j.\lightning = \iota'_j.\lightning$, we are done.

□

Lemma 9 (Transitivity and Reflexivity of $\sqsupseteq$ and $\sqsupseteq^{\mathsf{pub}}$)**.**

1. $\sqsupseteq$ is transitive and reflexive.
2. $\sqsupseteq^{\mathsf{pub}}$ is transitive and reflexive.

Proof. Follows easily from the definitions (using the fact that state transitions are transitive and reflexive). □

Lemma 10 (Monotonicity)**.**

1. If $W' \sqsupseteq W$ and $(W, v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$, then $(W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$.
2. If $W' \sqsupseteq W$ and $W \in \mathcal{S}[\![\Sigma]\!]$, then $W' \in \mathcal{S}[\![\Sigma]\!]$.
3. If $W' \sqsupseteq W$ and $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$, then $(W', \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.
4. If $W' \sqsupseteq^{\mathsf{pub}} W$ and $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$, then $(W', K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$.
5. If $W' \sqsupseteq W$ and $(W, h_1, h_2) \in \psi \in \mathrm{HeapRel}$, then $(W', h_1, h_2) \in \psi$.
6. If $(h_1, h_2) : W$ and $W.k > 0$, then $(h_1, h_2) : \triangleright W$.

Proof.

1. By induction on n and τ. Easy to verify.
2. Follows from (1).

3. Follows from (1).
4. By definition.
5. By definition of HeapRel.
6. Follows from (5).

□

Lemma 11 (Substitution)**.**

1. $\mathcal{V}[\![\tau]\!](\rho, \alpha{\mapsto}(\rho_1\tau', \rho_2\tau', \mathcal{V}[\![\tau']\!]\rho)) = \mathcal{V}[\![\tau[\tau'/\alpha]]\!]\rho$
2. $\mathcal{K}[\![\tau]\!](\rho, \alpha{\mapsto}(\rho_1\tau', \rho_2\tau', \mathcal{V}[\![\tau']\!]\rho)) = \mathcal{K}[\![\tau[\tau'/\alpha]]\!]\rho$
3. $\mathcal{E}[\![\tau]\!](\rho, \alpha{\mapsto}(\rho_1\tau', \rho_2\tau', \mathcal{V}[\![\tau']\!]\rho)) = \mathcal{E}[\![\tau[\tau'/\alpha]]\!]\rho$

Lemma 12. If $\langle h; e_1\rangle \downarrow^{<W.k}$ implies $\langle h; e_1'\rangle \downarrow^{<W.k}$ and $\langle h; e_2'\rangle \downarrow$ implies $\langle h; e_2\rangle \downarrow$ for any h, then $(W, e_1', e_2') \in \mathcal{O}$ implies $(W, e_1, e_2) \in \mathcal{O}$.

3.1.2 Soundness

Lemma 13 (Compatibility: Var)**.** If $x{:}\tau \in \Gamma$, then $\Sigma; \Delta; \Gamma \vdash x \precsim_{\log} x : \tau$.

Proof.

- Suppose $W \in \mathcal{S}[\![\Sigma]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.
- It suffices to show $(W, \rho_1\gamma_1 x, \rho_2\gamma_2 x) \in \mathcal{V}[\![\tau]\!]\rho$.
- We know $(W, \gamma_1 x, \gamma_2 x) \in \mathcal{V}[\![\tau]\!]\rho$.
- By definition of TermAtom, $\gamma_1 x$ and $\gamma_2 x$ contain no free type variables, so $\gamma_1 x = \rho_1\gamma_1 x$ and $\gamma_2 x = \rho_2\gamma_2 x$.

□

Lemma 14 (Compatibility: Pair)**.** If $\Sigma; \Delta; \Gamma \vdash e_1 \precsim_{\log} e_2 : \tau$ and $\Sigma; \Delta; \Gamma \vdash e_3 \precsim_{\log} e_4 : \tau'$, then $\Sigma; \Delta; \Gamma \vdash \langle e_1, e_3\rangle \precsim_{\log} \langle e_2, e_4\rangle : \tau \times \tau'$.

Proof.

- This reduces to showing $(W, K_1[\langle v_1, \bullet\rangle], K_2[\langle v_2, \bullet\rangle]) \in \mathcal{K}[\![\tau']\!]\rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\tau \times \tau']\!]\rho$ and $(W, v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W$ and $(W', v_3, v_4) \in \mathcal{V}[\![\tau']\!]\rho$.
- To show: $(W', K_1[\langle v_1, v_3\rangle], K_2[\langle v_2, v_4\rangle]) \in \mathcal{O}$
- This follows from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\tau \times \tau']\!]\rho$, if we can show $(W', \langle v_1, v_3\rangle, \langle v_2, v_4\rangle) \in \mathcal{V}[\![\tau \times \tau']\!]\rho$.
- The latter follows from $(W, v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$ and $(W', v_3, v_4) \in \mathcal{V}[\![\tau']\!]\rho$ with the help of monotonicity (Lemma 10).

□

Lemma 15 (Compatibility: Fst (Snd analogously))**.** If $\Sigma; \Delta; \Gamma \vdash e_1 \precsim_{\log} e_2 : \tau \times \tau'$, then $\Sigma; \Delta; \Gamma \vdash e_1.1 \precsim_{\log} e_2.1 : \tau$.

Proof.

- This reduces to showing $(W, K_1[\bullet.1], K_2[\bullet.1]) \in \mathcal{K}[\![\tau \times \tau']\!]\rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W$ and $(W', \langle v_1, v_3\rangle, \langle v_2, v_4\rangle) \in \mathcal{V}[\![\tau \times \tau']\!]\rho$.
- To show: $(W', K_1[\langle v_1, v_3\rangle.1], K_2[\langle v_2, v_4\rangle.1]) \in \mathcal{O}$
- By Lemma 12 it suffices to show $(W', K_1[v_1], K_2[v_2]) \in \mathcal{O}$.
- Since $(W', \langle v_1, v_3\rangle, \langle v_2, v_4\rangle) \in \mathcal{V}[\![\tau \times \tau']\!]\rho$ implies $(W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$, this follows from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$.

□

Lemma 16 (Compatibility: Abs)**.** If $\Sigma;\Delta;\Gamma,x{:}\tau' \vdash e_1 \precsim_{\log} e_2 : \tau$, then $\Sigma;\Delta;\Gamma \vdash \lambda x{:}\tau'.\, e_1 \precsim_{\log} \lambda x{:}\tau'.\, e_2 : \tau' \to \tau$.

Proof.

- Suppose $W \in \mathcal{S}[\![\Sigma]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.
- It suffices to show $(W, \lambda x{:}\rho_1\tau'.\, \rho_1\gamma_1 e_1, \lambda x{:}\rho_2\tau'.\, \rho_2\gamma_2 e_2) \in \mathcal{V}[\![\tau' \to \tau]\!]\rho$.
- So suppose $W' \sqsupseteq W$, $(W', v_1, v_2) \in \mathcal{V}[\![\tau']\!]\rho$ and $(W', K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$.
- To show: $(W', K_1[(\rho_1\gamma_1 e_1)[v_1/x]], K_2[(\rho_2\gamma_2 e_2)[v_2/x]]) \in \mathcal{O}$
- By definition of TermAtom, v_1 and v_2 contain no free type variables, so $K_1[(\rho_1\gamma_1 e_1)[v_1/x]] = K_1[\rho_1\gamma_1' e_1]$ and $K_2[(\rho_2\gamma_2 e_2)[v_2/x]] = K_2[\rho_2\gamma_2' e_2]$ for $\gamma' := \gamma, x{\mapsto}(v_1, v_2)$.
- By monotonicity (Lemma 10) we have $W' \in \mathcal{S}[\![\Sigma]\!]$ and $(W', \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.
- Consequently, $(W', \gamma') \in \mathcal{G}[\![\Gamma, x{:}\tau']\!]\rho$.
- Instantiating the assumption then yields $(W', \rho_1\gamma_1' e_1, \rho_2\gamma_2' e_2) \in \mathcal{E}[\![\tau]\!]\rho$, which in turn yields the claim.

□

Lemma 17 (Compatibility: App)**.** If $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\log} e_2 : \tau' \to \tau$ and $\Sigma;\Delta;\Gamma \vdash e_3 \precsim_{\log} e_4 : \tau'$, then $\Sigma;\Delta;\Gamma \vdash e_1\ e_3 \precsim_{\log} e_2\ e_4 : \tau$.

Proof.

- This reduces to showing $(W, K_1[v_1\ \bullet], K_2[v_2\ \bullet]) \in \mathcal{K}[\![\tau']\!]\rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$ and $(W, v_1, v_2) \in \mathcal{V}[\![\tau' \to \tau]\!]\rho$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W$ and $(W', v_3, v_4) \in \mathcal{V}[\![\tau']\!]\rho$.
- To show: $(W', K_1[v_1\ v_3], K_2[v_2\ v_4]) \in \mathcal{O}$
- We know $v_1 = \lambda x{:}\tau_1.\, e_1'$ and $v_2 = \lambda x{:}\tau_2.\, e_2'$.
- By Lemma 12 it thus suffices to show $(W', K_1[e_1'[v_3/x]], K_2[e_2'[v_4/x]]) \in \mathcal{O}$.
- Instantiating $(W, v_1, v_2) \in \mathcal{V}[\![\tau' \to \tau]\!]\rho$ yields $(W', e_1'[v_3/x], e_2'[v_4/x]) \in \mathcal{E}[\![\tau]\!]\rho$.
- It remains to show $(W', K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$, which follows by monotonicity (Lemma 10) from the assumption.

□

Lemma 18 (Compatibility: Gen)**.** If $\Sigma;\Delta,\alpha;\Gamma \vdash e_1 \precsim_{\log} e_2 : \tau$, then $\Sigma;\Delta;\Gamma \vdash \Lambda\alpha.e_1 \precsim_{\log} \Lambda\alpha.e_2 : \forall\alpha.\,\tau$.

Proof.

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

- It suffices to show $(W, \Lambda\alpha.\rho_1\gamma_1 e_1, \Lambda\alpha.\rho_2\gamma_2 e_2) \in \mathcal{V}[\![\forall\alpha.\,\tau]\!]\rho$.
- So suppose $W' \sqsupseteq W$, $(\tau_1, \tau_2, r) \in \text{SomeValRel}$, and $(W', K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho'$, where $\rho' := \rho, \alpha{\mapsto}(\tau_1, \tau_2, r)$.
- To show: $(W', K_1[(\rho_1\gamma_1 e_1)[\tau_1/\alpha]], K_2[(\rho_2\gamma_2 e_2)[\tau_2/\alpha]]) \in \mathcal{O}$
- Note that
  - $K_1[(\rho_1\gamma_1 e_1)[\tau_1/\alpha]] = K_1[\rho_1'\gamma_1 e_1]$ and
  - $K_2[(\rho_2\gamma_2 e_2)[\tau_2/\alpha]] = K_2[\rho_2'\gamma_2 e_2]$.
- It is easy to see that $\rho' \in \mathcal{D}[\![\Delta, \alpha]\!]$.
- By monotonicity (Lemma 10) we have $W' \in \mathcal{S}[\![\Sigma]\!]$ and $(W', \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho'$.
- Instantiating the assumption then yields $(W', \rho_1'\gamma_1 e_1, \rho_2'\gamma_2 e_2) \in \mathcal{E}[\![\tau]\!]\rho'$.
- Instantiating this with $(W', K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho'$ yields the claim.

□

Lemma 19 (Compatibility: Inst)**.** If $\Sigma; \Delta; \Gamma \vdash e_1 \precsim_{\log} e_2 : \forall\alpha.\,\tau$ and $\Delta \vdash \tau'$, then $\Sigma; \Delta; \Gamma \vdash e_1\ \tau' \precsim_{\log} e_2\ \tau' : \tau[\tau'/\alpha]$.

Proof.

- This reduces to showing $(W, K_1[\bullet\ \rho_1\tau'], K_2[\bullet\ \rho_2\tau']) \in \mathcal{K}[\![\forall\alpha.\,\tau]\!]\rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\tau[\tau'/\alpha]]\!]\rho$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W$ and $(W', v_1, v_2) \in \mathcal{V}[\![\forall\alpha.\,\tau]\!]\rho$.
- To show: $(W', K_1[v_1\ \rho_1\tau'], K_2[v_2\ \rho_2\tau']) \in \mathcal{O}$
- We know $v_1 = \Lambda\alpha.e_1'$ and $v_2 = \Lambda\alpha.e_2'$.
- By Lemma 12 it thus suffices to show $(W', K_1[e_1'[\rho_1\tau'/\alpha]], K_2[e_2'[\rho_2\tau'/\alpha]]) \in \mathcal{O}$.
- Instantiating $(W, v_1, v_2) \in \mathcal{V}[\![\forall\alpha.\,\tau]\!]\rho$ with $R := (\rho_1\tau', \rho_2\tau', \mathcal{V}[\![\tau']\!]\rho)$ yields $(W', e_1'[\rho_1\tau'/\alpha], e_2'[\rho_2\tau'/\alpha]) \in \mathcal{E}[\![\tau]\!](\rho, \alpha{\mapsto}R)$.
- By substitution (Lemma 11), $(W', e_1'[\rho_1\tau'/\alpha], e_2'[\rho_2\tau'/\alpha]) \in \mathcal{E}[\![\tau[\tau'/\alpha]]\!]\rho$.
- By monotonicity (Lemma 10), $(W', K_1, K_2) \in \mathcal{K}[\![\tau[\tau'/\alpha]]\!]\rho$.
- Instantiating $(W', e_1'[\rho_1\tau'/\alpha], e_2'[\rho_2\tau'/\alpha]) \in \mathcal{E}[\![\tau[\tau'/\alpha]]\!]\rho$ then yields the claim.

□

Lemma 20 (Compatibility: Pack)**.** If $\Sigma; \Delta; \Gamma \vdash e_1 \precsim_{\log} e_2 : \tau[\tau'/\alpha]$, then $\Sigma; \Delta; \Gamma \vdash \mathsf{pack}\ \langle\tau', e_1\rangle\ \mathsf{as}\ \exists\alpha.\,\tau \precsim_{\log} \mathsf{pack}\ \langle\tau', e_2\rangle\ \mathsf{as}\ \exists\alpha.\,\tau : \exists\alpha.\,\tau$.

Proof.

- This reduces to showing $(W, K_1[\mathsf{pack}\ \langle \rho_1\tau', \bullet\rangle\ \mathsf{as}\ \exists\alpha.\,\rho_1\tau], K_2[\mathsf{pack}\ \langle \rho_2\tau', \bullet\rangle\ \mathsf{as}\ \exists\alpha.\,\rho_2\tau]) \in \mathcal{K}[\![\tau[\tau'/\alpha]]\!]\rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\exists\alpha.\,\tau]\!]\rho$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W$ and $(W', v_1, v_2) \in \mathcal{V}[\![\tau[\tau'/\alpha]]\!]\rho$.
- To show: $(W', K_1[\mathsf{pack}\ \langle \rho_1\tau', v_1\rangle\ \mathsf{as}\ \exists\alpha.\,\rho_1\tau], K_2[\mathsf{pack}\ \langle \rho_2\tau', v_2\rangle\ \mathsf{as}\ \exists\alpha.\,\rho_2\tau]) \in \mathcal{O}$
- This follows from $(W, K_1, K_2) \in \mathcal{K}[\![\exists\alpha.\,\tau]\!]\rho$, if we can show $(W', \mathsf{pack}\ \langle \rho_1\tau', v_1\rangle\ \mathsf{as}\ \exists\alpha.\,\rho_1\tau, \mathsf{pack}\ \langle \rho_2\tau', v_2\rangle\ \mathsf{as}\ \exists\alpha.\,\rho_2\tau) \in \mathcal{V}[\![\exists\alpha.\,\tau]\!]\rho$.
- By monotonicity (Lemma 10) we know $(W', v_1, v_2) \in \mathcal{V}[\![\tau[\tau'/\alpha]]\!]\rho$.
- By substitution (Lemma 11), $(W', v_1, v_2) \in \mathcal{V}[\![\tau]\!](\rho, \alpha{\mapsto}(\rho_1\tau', \rho_2\tau', \mathcal{V}[\![\tau']\!]\rho))$.
- This implies the claim.

□

Lemma 21 (Compatibility: Unpack)**.** If $\Sigma; \Delta; \Gamma \vdash e_1 \precsim_{\log} e_2 : \exists\alpha.\,\tau$ and $\Sigma; \Delta, \alpha; \Gamma, x{:}\tau \vdash e_3 \precsim_{\log} e_4 : \tau'$ and $\Delta \vdash \tau'$, then $\Sigma; \Delta; \Gamma \vdash \mathsf{unpack}\ e_1\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ e_3 \precsim_{\log} \mathsf{unpack}\ e_2\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ e_4 : \tau'$.

Proof.

- Suppose $W \in \mathcal{S}[\![\Sigma]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$, and $(W, K_1, K_2) \in \mathcal{K}[\![\tau']\!]\rho$.
- To show: $(W, K_1[\mathsf{unpack}\ \rho_1\gamma_1 e_1\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ \rho_1\gamma_1 e_3], K_2[\mathsf{unpack}\ \rho_2\gamma_2 e_2\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ \rho_2\gamma_2 e_4]) \in \mathcal{O}$
- This follows from instantiating the first premise if we can show $(W, K_1[\mathsf{unpack}\ \bullet\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ \rho_1\gamma_1 e_3], K_2[\mathsf{unpack}\ \bullet\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ \rho_2\gamma_2 e_4]) \in \mathcal{K}[\![\exists\alpha.\,\tau]\!]\rho$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W$ and $(W', v_1, v_2) \in \mathcal{V}[\![\exists\alpha.\,\tau]\!]\rho$.
- To show: $(W', K_1[\mathsf{unpack}\ v_1\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ \rho_1\gamma_1 e_3], K_2[\mathsf{unpack}\ v_2\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ \rho_2\gamma_2 e_4]) \in \mathcal{O}$
- We know $v_1 = \mathsf{pack}\ \langle\tau_1, v_1'\rangle\ \mathsf{as}\ \tau_1'$ and $v_2 = \mathsf{pack}\ \langle\tau_2, v_2'\rangle\ \mathsf{as}\ \tau_2'$ with $(W', v_1', v_2') \in \mathcal{V}[\![\tau]\!]\rho'$, where $\rho' := \rho, \alpha{\mapsto}(\tau_1, \tau_2, r)$ (and thus $\rho' \in \mathcal{D}[\![\Delta, \alpha]\!]$) and $r \in \mathrm{ValRel}$.
- By Lemma 12 it thus suffices to show $(W', K_1[(\rho_1\gamma_1 e_3)[\tau_1/\alpha][v_1'/x]], K_2[(\rho_2\gamma_2 e_4)[\tau_2/\alpha][v_2'/x]]) \in \mathcal{O}$.
- Let $\gamma' := \gamma, x{\mapsto}(v_1', v_2')$.
- By monotonicity (Lemma 10), $(W', \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho'$, so $(W', \gamma') \in \mathcal{G}[\![\Gamma, x{:}\tau]\!]\rho'$.
- Also by monotonicity (Lemma 10), $W' \in \mathcal{S}[\![\Sigma]\!]$.
- By definition of TermAtom, v_1' and v_2' contain no free type variables and hence $(\rho_1\gamma_1 e_3)[\tau_1/\alpha][v_1'/x] = \rho_1'\gamma_1' e_3$ as well as $(\rho_2\gamma_2 e_4)[\tau_2/\alpha][v_2'/x] = \rho_2'\gamma_2' e_4$.
- Instantiating the second premise yields $(W', \rho_1'\gamma_1' e_3, \rho_2'\gamma_2' e_4) \in \mathcal{E}[\![\tau']\!]\rho'$.

- Since $(W', K_1, K_2) \in \mathcal{K}[\![\tau']\!]\rho$ by monotonicity (Lemma 10) and $\alpha \notin \mathrm{fv}(\tau')$, instantiating $(W', \rho_1'\gamma_1' e_3, \rho_2'\gamma_2' e_4) \in \mathcal{E}[\![\tau']\!]\rho'$ yields the claim.

□

Lemma 22 (Compatibility: Roll)**.** If $\Sigma; \Delta; \Gamma \vdash e_1 \precsim_{\log} e_2 : \tau[\mu\alpha.\,\tau/\alpha]$, then $\Sigma; \Delta; \Gamma \vdash \mathsf{roll}_{\mu\alpha.\,\tau}\ e_1 \precsim_{\log} \mathsf{roll}_{\mu\alpha.\,\tau}\ e_2 : \mu\alpha.\,\tau$.

Proof.

- This reduces to showing $(W, K_1[\mathsf{roll}_{\mu\alpha.\,\rho_1\tau}\ \bullet], K_2[\mathsf{roll}_{\mu\alpha.\,\rho_2\tau}\ \bullet]) \in \mathcal{K}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\mu\alpha.\,\tau]\!]\rho$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W$ and $(W', v_1, v_2) \in \mathcal{V}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho$.
- To show: $(W', K_1[\mathsf{roll}_{\mu\alpha.\,\rho_1\tau}\ v_1], K_2[\mathsf{roll}_{\mu\alpha.\,\rho_2\tau}\ v_2]) \in \mathcal{O}$
- This follows from $(W, K_1, K_2) \in \mathcal{K}[\![\mu\alpha.\,\tau]\!]\rho$, if we can show $(W', \mathsf{roll}_{\mu\alpha.\,\rho_1\tau}\ v_1, \mathsf{roll}_{\mu\alpha.\,\rho_2\tau}\ v_2) \in \mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho$.
- By monotonicity (Lemma 10) we know $(\triangleright W', v_1, v_2) \in \mathcal{V}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho$.
- Hence $(W', v_1, v_2) \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho$, which implies the claim.

□

Lemma 23 (Compatibility: Unroll)**.** If $\Sigma; \Delta; \Gamma \vdash e_1 \precsim_{\log} e_2 : \mu\alpha.\,\tau$, then $\Sigma; \Delta; \Gamma \vdash \mathsf{unroll}\ e_1 \precsim_{\log} \mathsf{unroll}\ e_2 : \tau[\mu\alpha.\,\tau/\alpha]$.

Proof.

- This reduces to showing $(W, K_1[\mathsf{unroll}\ \bullet], K_2[\mathsf{unroll}\ \bullet]) \in \mathcal{K}[\![\mu\alpha.\,\tau]\!]\rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W$, $(W', v_1, v_2) \in \mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho$, $(h_1, h_2) : W'$, and $\langle h_1; K_1[\mathsf{unroll}\ v_1]\rangle\downarrow^{<W'.k}$.
- To show: consistent(W') and $\langle h_2; K_2[\mathsf{unroll}\ v_2]\rangle\downarrow$.
- We know $v_1 = \mathsf{roll}_{\tau_1}\ v_1'$ and $v_2 = \mathsf{roll}_{\tau_2}\ v_2'$ with $(W', v_1', v_2') \in \triangleright\mathcal{V}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho$.
- Note that
  - $\langle h_1; K_1[\mathsf{unroll}\ v_1]\rangle\downarrow^{<W'.k} \iff \langle h_1; K_1[v_1']\rangle\downarrow^{<W'.k-1}$ and
  - $\langle h_2; K_2[\mathsf{unroll}\ v_2]\rangle\downarrow \iff \langle h_2; K_2[v_2']\rangle\downarrow$.
- By monotonicity (Lemma 10), $(\triangleright W', K_1, K_2) \in \mathcal{K}[\![\tau[\mu\alpha.\,\tau/\alpha]]\!]\rho$.
- Instantiating this yields the claims.

□

Lemma 24 (Compatibility: New)**.** If $\Sigma; \Delta; \Gamma \vdash e_1 \precsim_{\log} e_2 : \tau$, then $\Sigma; \Delta; \Gamma \vdash \mathsf{ref}\ e_1 \precsim_{\log} \mathsf{ref}\ e_2 : \mathsf{ref}\ \tau$.

Proof.

- This reduces to showing $(W, K_1[\mathsf{ref}\ \bullet], K_2[\mathsf{ref}\ \bullet]) \in \mathcal{K}[\![\tau]\!]\rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{ref}\ \tau]\!]\rho$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W$, $(W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$, $(h_1, h_2) : W'$, and $\langle h_1; K_1[\mathsf{ref}\ v_1]\rangle\downarrow^{<W'.k}$.
- To show: consistent(W') and $\langle h_2; K_2[\mathsf{ref}\ v_2]\rangle\downarrow$
- Note that
  - $\langle h_1; K_1[\mathsf{ref}\ v_1]\rangle\downarrow^{<W'.k} \iff \langle h_1 \uplus \{l_1 \mapsto v_1\}; K_1[l_1]\rangle\downarrow^{<W'.k-1}$ (where l_1 fresh) and
  - $\langle h_2; K_2[\mathsf{ref}\ v_2]\rangle\downarrow \iff \langle h_2 \uplus \{l_2 \mapsto v_2\}; K_2[l_2]\rangle\downarrow$ (where l_2 fresh).
- Let $\iota := (\{\langle l_1, l_2\rangle\}, \emptyset^*, \emptyset^*, \emptyset, H)$, where $H(\{\langle l_1, l_2\rangle\}) := \{(W'', h_1', h_2') \mid (W'', h_1'(l_1), h_2'(l_2)) \in \mathcal{V}[\![\tau]\!]\rho\}$.
- Now let $W'' := (W'.k, (W'.\Sigma_1, l_1{:}\rho_1\tau), (W'.\Sigma_2, l_2{:}\rho_2\tau), (\omega, \iota))$, so $W'' \sqsupseteq^{\mathsf{pub}} W' \sqsupseteq^{\mathsf{pub}} W$.
- Due to $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$ it suffices to show $(h_1 \uplus \{l_1 \mapsto v_1\}, h_2 \uplus \{l_2 \mapsto v_2\}) : W''$ and $(W'', l_1, l_2) \in \mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho$.
- The latter holds by construction.
- For the former note that from $(h_1, h_2) : W'$ we know $h_1 = h_1^1 \uplus \cdots \uplus h_1^{|W'.\omega|}$ and $h_2 = h_2^1 \uplus \cdots \uplus h_2^{|W'.\omega|}$ with $(\triangleright W', h_1^j, h_2^j) \in W'.\omega(j).H(W'.\omega(j).s)$ for all $j \in \{1, \ldots, |W'.\omega|\}$.
- By monotonicity (Lemma 10), this implies $(\triangleright W'', h_1^j, h_2^j) \in W'.\omega(j).H(W'.\omega(j).s)$ for all $j \in \{1, \ldots, |W'.\omega|\}$.
- And since $W'' = W' \uplus \iota$, this in turn implies $(\triangleright W'', h_1^j, h_2^j) \in W''.\omega(j).H(W''.\omega(j).s)$ for all $j \in \{1, \ldots, |W'.\omega|\}$.
- It thus suffices to show $(\triangleright W'', \{l_1 \mapsto v_1\}, \{l_2 \mapsto v_2\}) \in H(\{\langle l_1, l_2\rangle\})$, *i.e.,* $(\triangleright W'', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$.
- This follows from $(W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$ by monotonicity (Lemma 10).

□

Lemma 25 (Compatibility: Assign)**.** If $\Sigma; \Delta; \Gamma \vdash e_1 \precsim_{\log} e_2 : \mathsf{ref}\ \tau$ and $\Sigma; \Delta; \Gamma \vdash e_3 \precsim_{\log} e_4 : \tau$, then $\Sigma; \Delta; \Gamma \vdash e_1 := e_3 \precsim_{\log} e_2 := e_4 : \mathsf{unit}$.

Proof.

- Suppose $W \in \mathcal{S}[\![\Sigma]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.
- To show: $(W, \rho_1\gamma_1 e_1 := \rho_1\gamma_1 e_3, \rho_2\gamma_2 e_2 := \rho_2\gamma_2 e_4) \in \mathcal{E}[\![\mathsf{unit}]\!]\rho$
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{unit}]\!]\rho$, $(h_1, h_2) : W$, and $\langle h_1; K_1[\rho_1\gamma_1 e_1 := \rho_1\gamma_1 e_3]\rangle\downarrow^{<W.k}$.
- Since instantiating the first assumption yields $(W, \rho_1\gamma_1 e_1, \rho_2\gamma_2 e_2) \in \mathcal{E}[\![\mathsf{ref}\ \tau]\!]\rho$, it suffices to show $(W, K_1[\bullet := \rho_1\gamma_1 e_3], K_2[\bullet := \rho_2\gamma_2 e_4]) \in \mathcal{K}[\![\mathsf{ref}\ \tau]\!]\rho$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W$, $(W', v_1, v_2) \in \mathcal{V}[\![\mathsf{ref}\ \tau]\!]\rho$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1[v_1 := \rho_1\gamma_1 e_3]\rangle\downarrow^{<W'.k}$.

- To show: consistent(W') and $\langle h_2'; K_2[v_2 := \rho_2\gamma_2 e_4]\rangle\downarrow$
- Using monotonicity (Lemma 10) and the second assumption, we get $(W', \rho_1\gamma_1 e_3, \rho_2\gamma_2 e_4) \in \mathcal{E}[\![\tau]\!]\rho$.
- Hence it suffices to show $(W', K_1[v_1 := \bullet], K_2[v_2 := \bullet]) \in \mathcal{K}[\![\tau]\!]\rho$.
- So suppose $W'' \sqsupseteq^{\mathsf{pub}} W'$, $(W'', v_3, v_4) \in \mathcal{V}[\![\tau]\!]\rho$, $(h_1'', h_2'') : W''$, and $\langle h_1''; K_1[v_1 := v_3]\rangle\downarrow^{<W''.k}$.
- To show: consistent(W'') and $\langle h_2''; K_2[v_2 := v_4]\rangle\downarrow$
- From $(W', v_1, v_2) \in \mathcal{V}[\![\mathsf{ref}\,\tau]\!]\rho$, $W'' \sqsupseteq^{\mathsf{pub}} W'$ and $(h_1'', h_2'') : W''$ we know $v_1 \in \mathrm{dom}(h_1'')$ and $v_2 \in \mathrm{dom}(h_2'')$.
- Consequently,
  - $\langle h_1''; K_1[v_1 := v_3]\rangle\downarrow^{<W''.k} \iff \langle h_1''[v_1 \mapsto v_3]; K_1[\langle\rangle]\rangle\downarrow^{<W''.k-1}$ and
  - $\langle h_2''; K_2[v_2 := v_4]\rangle\downarrow \iff \langle h_2''[v_2 \mapsto v_4]; K_2[\langle\rangle]\rangle\downarrow$.
- We know $(W'', K_1, K_2) \in \mathcal{K}[\![\mathsf{unit}]\!]\rho$ by monotonicity (Lemma 10).
- We show $(h_1''[v_1 \mapsto v_3], h_2''[v_2 \mapsto v_4]) : W''$:
  - Due to $(W', v_1, v_2) \in \mathcal{V}[\![\mathsf{ref}\,\tau]\!]\rho$, $W'' \sqsupseteq^{\mathsf{pub}} W'$ and $(h_1'', h_2'') : W''$, this boils down to showing $(\triangleright W'', v_3, v_4) \in \mathcal{V}[\![\tau]\!]\rho$.
  - This follows from $(W'', v_3, v_4) \in \mathcal{V}[\![\tau]\!]\rho$ by monotonicity (Lemma 10).
- Since $(W'', \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\rho$, instantiating $(W'', K_1, K_2) \in \mathcal{K}[\![\mathsf{unit}]\!]\rho$ yields consistent(W'') and $\langle h_2''[v_2 \mapsto v_4]; K_2[\langle\rangle]\rangle\downarrow$.

□

Lemma 26 (Compatibility: Deref)**.** If $\Sigma; \Delta; \Gamma \vdash e_1 \precsim_{\log} e_2 : \mathsf{ref}\,\tau$, then $\Sigma; \Delta; \Gamma \vdash\, !e_1 \precsim_{\log} !e_2 : \tau$.

Proof.

- This reduces to showing $(W, K_1[!\bullet], K_2[!\bullet]) \in \mathcal{K}[\![\mathsf{ref}\,\tau]\!]\rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W$, $(W', v_1, v_2) \in \mathcal{V}[\![\mathsf{ref}\,\tau]\!]\rho$, $(h_1, h_2) : W'$, and $\langle h_1; K_1[!v_1]\rangle\downarrow^{<W'.k}$.
- To show: consistent(W') and $\langle h_2; K_2[!v_2]\rangle\downarrow$
- From $(W', v_1, v_2) \in \mathcal{V}[\![\mathsf{ref}\,\tau]\!]\rho$ and $(h_1, h_2) : W'$ we know $v_1 \in \mathrm{dom}(h_1)$ and $v_2 \in \mathrm{dom}(h_2)$.
- Consequently,
  - $\langle h_1; K_1[!v_1]\rangle\downarrow^{<W'.k} \iff \langle h_1; K_1[h_1(v_1)]\rangle\downarrow^{<W'.k-1}$ and
  - $\langle h_2; K_2[!v_2]\rangle\downarrow \iff \langle h_2; K_2[h_2(v_2)]\rangle\downarrow$.
- By monotonicity (Lemma 10), $(h_1, h_2) : \triangleright W'$.
- Due to $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$ it suffices to show $(\triangleright W', h_1(v_1), h_2(v_2)) \in \mathcal{V}[\![\tau]\!]\rho$.
- This follows from $(W', v_1, v_2) \in \mathcal{V}[\![\mathsf{ref}\,\tau]\!]\rho$ and $(h_1, h_2) : W'$.

□

Lemma 27 (Compatibility: Refeq)**.** If $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\log} e_2 : \mathsf{ref}\,\tau$ and $\Sigma;\Delta;\Gamma \vdash e_3 \precsim_{\log} e_4 : \mathsf{ref}\,\tau'$, then $\Sigma;\Delta;\Gamma \vdash e_1 == e_3 \precsim_{\log} e_2 == e_4 : \mathsf{bool}$.

Proof.

- This reduces to showing $(W, K_1[l_1 == \bullet], K_2[l_2 == \bullet]) \in \mathcal{K}[\![\mathsf{ref}\,\tau']\!]\rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{bool}]\!]\rho$ and $(W, l_1, l_2) \in \mathcal{V}[\![\mathsf{ref}\,\tau]\!]\rho$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W$, $(W', l_3, l_4) \in \mathcal{V}[\![\mathsf{ref}\,\tau']\!]\rho$, $(h_1, h_2) : W'$, and $\langle h_1; K_1[l_1 == l_3]\rangle\downarrow^{<W'.k}$.
- To show: consistent(W') and $\langle h_2; K_2[l_2 == l_4]\rangle\downarrow$
- Assume $l_1 = l_3$ (the other case is analogous):
- Then $\langle h_1; K_1[\mathsf{tt}]\rangle\downarrow^{<W'.k-1}$.
- By monotonicity (Lemma 10) we know $(W', l_1, l_2) \in \mathcal{V}[\![\mathsf{ref}\,\tau]\!]\rho$.
- Consequently there are i, j such that:
  1. $(l_1, l_2) \in \mathrm{bij}(W'.\omega(i).s)$ and
     $\exists\psi.\ W'.\omega(i).H(W'.\omega(i).s) = \psi \otimes \{(\widetilde{W}, \{l_1{\mapsto}v_1\}, \{l_2{\mapsto}v_2\}) \mid (\widetilde{W}, v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho\}$
  2. $(l_3, l_4) \in \mathrm{bij}(W'.\omega(j).s)$ and
     $\exists\psi.\ W'.\omega(j).H(W'.\omega(j).s) = \psi \otimes \{(\widetilde{W}, \{l_3{\mapsto}v_3\}, \{l_4{\mapsto}v_4\}) \mid (\widetilde{W}, v_3, v_4) \in \mathcal{V}[\![\tau]\!]\rho\}$
- Case $i \neq j$:
  - Since $(h_1, h_2) : W'$, this implies that $\{l_1{\mapsto}v_1\}$ and $\{l_3{\mapsto}v_3\}$ are disjoint and that $\{l_2{\mapsto}v_2\}$ and $\{l_4{\mapsto}v_4\}$ are disjoint.
  - Consequently, $l_1 \neq l_3$ and $l_2 \neq l_4$.
  - Therefore $\langle h_1; K_1[l_1 == l_3]\rangle\downarrow^{<W'.k}$ implies $\langle h_1; K_1[\mathsf{ff}]\rangle\downarrow^{<W'.k}$ and $\langle h_2; K_2[l_2 == l_4]\rangle\downarrow$ would be implied by $\langle h_2; K_2[\mathsf{ff}]\rangle\downarrow$.
  - The claims then follow from $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{bool}]\!]\rho$ and $(W', \mathsf{ff}, \mathsf{ff}) \in \mathcal{V}[\![\mathsf{bool}]\!]\rho$.
- Case $i = j$:
  - Then $(l_1, l_2) \in \mathrm{bij}(W'.\omega(i).s)$ and $(l_3, l_4) \in \mathrm{bij}(W'.\omega(j).s)$ imply that either $l_1 = l_3$ and $l_2 = l_4$, or $l_1 \neq l_3$ and $l_2 \neq l_4$.
  - In the latter case we proceed as above.
  - In the former case we proceed analogously, using $(W', \mathsf{tt}, \mathsf{tt}) \in \mathcal{V}[\![\mathsf{bool}]\!]\rho$.

□

Theorem 1 (Fundamental Property)**.** If $\Sigma;\Delta;\Gamma \vdash e : \tau$, then $\Sigma;\Delta;\Gamma \vdash e \precsim_{\log} e : \tau$.

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

Lemma 28 (Weakening)**.** If $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\log} e_2 : \tau$ and $\Sigma \subseteq \Sigma'$, $\Delta \subseteq \Delta'$, $\Gamma \subseteq \Gamma'$, $\Delta' \vdash \Gamma'$, then $\Sigma';\Delta';\Gamma' \vdash e_1 \precsim_{\log} e_2 : \tau$.

Lemma 29 (Congruency)**.** If $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\log} e_2 : \tau$ and $\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\Delta';\Gamma';\tau')$, then $\Sigma';\Delta';\Gamma' \vdash C[e_1] \precsim_{\log} C[e_2] : \tau'$.

Proof. By induction on the structure of C, in each case using the corresponding compatibility lemma. The case $C = \bullet$ requires Lemma 28. □

In order to prove Lemma 31, we need to show a variant of the fundamental property that is restricted to values, for which we define:

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

Notice the use of the value relation $\mathcal{V}[\![\tau]\!]\rho$ rather than the term relation $\mathcal{E}[\![\tau]\!]\rho$.

Lemma 30 (Fundamental Property for Values)**.** If $\Sigma;\Delta;\Gamma \vdash v : \tau$, then $\Sigma;\Delta;\Gamma \vdash v \precsim^{\text{val}}_{\log} v : \tau$.

Proof. By induction on the typing derivation, in each case using an easy-to-show variant of the appropriate compatibility lemma. □

Lemma 31 (Wundertüte)**.** If $\vdash h : \Sigma$, then for any k there is $W \in \mathcal{S}[\![k+1]\!]\,\Sigma$ such that $W.k = k$ and $(h,h) : W$ and safe(W).

Proof. Say $\Sigma = l_1{:}\tau_1, \ldots, l_n{:}\tau_n$. Construct W as follows:

- $W := (k, \Sigma, \Sigma, \omega)$
- $\omega := \iota_0, \iota_1, \ldots, \iota_n$
- $\iota_0 := (\langle\rangle, \emptyset, \emptyset, \emptyset, \lambda s.\ \text{HeapAtom}_k)$
- $\iota_j := (\{\langle l_j, l_j\rangle\}, \emptyset, \emptyset, \emptyset, H_j)$ for $j \in \{1,\ldots,n\}$
- $H_j(\{\langle l_j, l_j\rangle\}) := \{(W', h_1, h_2) \in \text{HeapAtom}_k \mid (W', h_1(l_j), h_2(l_j)) \in \mathcal{V}[\![\tau_j]\!]\emptyset\}$ for $j \in \{1,\ldots,n\}$

Showing $(h,h) : W$ reduces to showing $(\triangleright W, h|_{\{l_j\}}, h|_{\{l_j\}}) \in H_j(\{\langle l_j, l_j\rangle\})$, *i.e.,* $(\triangleright W, h|_{\{l_j\}}, h|_{\{l_j\}}) \in \mathcal{V}[\![\tau_j]\!]\emptyset$. This follows from the fundamental property for values (Lemma 30). □

Lemma 32 (Adequacy)**.** If $\Sigma;\cdot;\cdot \vdash e_1 \precsim_{\log} e_2 : \tau$ and $\vdash h : \Sigma$ and $\langle h; e_1\rangle\downarrow$, then $\langle h; e_2\rangle\downarrow$.

Proof.

- Say $\langle h; e_1\rangle\downarrow^j$.
- By Lemma 31 there is $W \in \mathcal{S}[\![\Sigma]\!]$ with $W.k = j+1$, $(h,h) : W$, and safe(W).
- Instantiating $\Sigma;\cdot;\cdot \vdash e_1 \precsim_{\log} e_2 : \tau$ yields $(W, e_1, e_2) \in \mathcal{E}[\![\tau]\!]\emptyset$.
- It thus suffices to show $(W, \bullet, \bullet) \in \mathcal{K}[\![\tau]\!]\emptyset$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W$, $(W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\emptyset$, $(h_1, h_2) : W'$ and $\langle h_1; v_1\rangle\downarrow^{<W'.k}$.

- We need to show consistent(W') and $\langle h_2; v_2\rangle\downarrow$.
- The former follows from safe(W) by Lemma 8 and the latter is immediate.

□

Theorem 2 (Soundness)**.** If $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\log} e_2 : \tau$, then $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\text{ctx}} e_2 : \tau$.

Proof.

- Suppose $\Sigma;\Delta;\Gamma \vdash e_1 : \tau$, $\Sigma;\Delta;\Gamma \vdash e_2 : \tau$, $\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\cdot;\cdot;\tau')$, $\vdash h : \Sigma'$, and $\langle h; C[e_1]\rangle\downarrow$.
- By congruency (Lemma 29), $\Sigma';\cdot;\cdot \vdash C[e_1] \precsim_{\log} C[e_2] : \tau'$.
- By adequacy (Lemma 32), $\langle h; C[e_2]\rangle\downarrow$.

□

3.1.3 Completeness

Lemma 33. If $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\text{ctx}} e_2 : \tau$, then $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\text{ciu}} e_2 : \tau$.

Proof.

- Suppose
  - $\Sigma;\Delta;\Gamma \vdash e_1 : \tau$,
  - $\Sigma;\Delta;\Gamma \vdash e_2 : \tau$,
  - $\vdash \delta : \Delta$,
  - $\Sigma';\cdot;\cdot \vdash \gamma : \delta\Gamma$,
  - $\Sigma';\cdot;\cdot \vdash K \div \delta\tau$,
  - $\Sigma \subseteq \Sigma'$,
  - $\vdash h : \Sigma'$, and
  - $\langle h; K[\delta\gamma e_1]\rangle\downarrow$.
- To show: $\langle h; K[\delta\gamma e_2]\rangle\downarrow$
- Say $\Delta = \alpha_1,\ldots,\alpha_m$ and $\delta(\alpha_i) = \sigma_i$ as well as $\Gamma = x_1{:}\tau_1,\ldots,x_n{:}\tau_n$ and $\gamma(x_i) = v_i$.
- Let $C' := (\Lambda\alpha_1.\ldots\Lambda\alpha_m.\lambda x_1{:}\tau_1.\ldots\lambda x_n{:}\tau_n.\bullet)\ \sigma_1\ \ldots\ \sigma_m\ v_1\ \ldots\ v_n$ and $C := K[C']$.
- It is easy to see that $\vdash C' : (\Sigma';\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\cdot;\cdot;\delta\tau)$.
- By Lemma 2 then $\vdash C : (\Sigma';\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\cdot;\cdot;\tau')$ for some τ'.
- Hence $\vdash C : (\Sigma;\Delta;\Gamma;\tau) \rightsquigarrow (\Sigma';\cdot;\cdot;\tau')$ by Lemma 3.
- Note that
  - $\langle h; K[\delta\gamma e_1]\rangle\downarrow \iff \langle h; C[e_1]\rangle\downarrow$ and

– $\langle h; K[\delta\gamma e_2]\rangle\downarrow \iff \langle h; C[e_2]\rangle\downarrow$.

- Consequently, the claim follows from $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\text{ctx}} e_2 : \tau$.

□

Lemma 34. If $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\text{ciu}} e_2 : \tau$, then $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\text{log}} e_2 : \tau$.

Proof.

- Suppose $W \in \mathcal{S}[\![\Sigma]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.
- To show: $(W, \rho_1\gamma_1 e_1, \rho_2\gamma_2 e_2) \in \mathcal{E}[\![\tau]\!]\rho$
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$, $(h_1, h_2) : W$, and $\langle h_1; K_1[\rho_1\gamma_1 e_1]\rangle\downarrow^{<W.k}$.
- To show: consistent(W) and $\langle h_2; K_2[\rho_2\gamma_2 e_2]\rangle\downarrow$
- By Theorem 1 we know $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\text{log}} e_1 : \tau$.
- Instantiating this yields consistent(W) and $\langle h_2; K_2[\rho_2\gamma_2 e_1]\rangle\downarrow$.
- Using our assumption, it suffices to show
  1. $\cdot \vdash \rho_2 : \Delta$ and $W.\Sigma_2;\cdot;\cdot \vdash \gamma_2 : \rho_2\Gamma$, which follow by Lemma 7;
  2. $W.\Sigma_2;\cdot;\cdot \vdash K_2 \div \rho_2\tau$, which holds by definition of ContAtom;
  3. $\Sigma \subseteq W.\Sigma_2$, which follows by Lemma 7; and
  4. $\vdash h_2 : W.\Sigma_2$, which holds by definition of HeapAtom.

□

Corollary 1 (Completeness)**.** If $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\text{ctx}} e_2 : \tau$, then $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\text{log}} e_2 : \tau$.

3.2 HOSE

Like for **HOS**, except for the following adaptations and additions:

3.2.1 Soundness

In each of the previous compatibility proofs and in the proof of the adequacy theorem, we need to make the following extension: whenever we show that some tuple is in the continuation relation $\mathcal{K}[\![\tau]\!]\rho$, we now—as dictated by its new definition—also have to deal with exceptions. In each case, this is easily done since the code in question doesn't catch them.

The additional compatibilty lemmas are:

Lemma 35 (Compatibility: Raise)**.** If $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\log} e_2 : \mathsf{exn}$, then $\Sigma;\Delta;\Gamma \vdash \mathsf{raise}\ e_1 \precsim_{\log} \mathsf{raise}\ e_2 : \tau$.

Proof.

- Suppose $W \in \mathcal{S}[\![\Sigma]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.
- To show: $(W, \mathsf{raise}\ \rho_1\gamma_1 e_1, \mathsf{raise}\ \rho_2\gamma_2 e_2) \in \mathcal{E}[\![\tau]\!]\rho$
- So suppse $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$.
- To show: $(W, K_1[\mathsf{raise}\ \rho_1\gamma_1 e_1], K_2[\mathsf{raise}\ \rho_2\gamma_2 e_2]) \in \mathcal{O}$
- After instantiating the premise it suffices to show $(W, K_1[\mathsf{raise}\ \bullet], K_2[\mathsf{raise}\ \bullet]) \in \mathcal{K}[\![\mathsf{exn}]\!]\rho$.
- So suppose $(W', v_1, v_2) \in \mathcal{V}[\![\mathsf{exn}]\!]\rho$ for $W' \sqsupseteq^{\mathsf{pub}} W$.
- To show: $(W', K_1[\mathsf{raise}\ v_1], K_2[\mathsf{raise}\ v_2]) \in \mathcal{O}$ and $(W', K_1[\mathsf{raise}\ (\mathsf{raise}\ v_1)], K_2[\mathsf{raise}\ (\mathsf{raise}\ v_2)]) \in \mathcal{O}$
- The former follows immediately from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$.
- The second part reduces by Lemma 12 to showing $(W', K_1[\mathsf{raise}\ v_1], K_2[\mathsf{raise}\ v_2]) \in \mathcal{O}$, which we just did.

□

Lemma 36 (Compatibility: Try)**.** If $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\log} e_2 : \tau$ and $\Sigma;\Delta;\Gamma, x{:}\mathsf{exn} \vdash e_3 \precsim_{\log} e_4 : \tau$, then $\Sigma;\Delta;\Gamma \vdash \mathsf{try}\ e_1\ \mathsf{with}\ x.e_3 \precsim_{\log} \mathsf{try}\ e_2\ \mathsf{with}\ x.e_4 : \tau$.

Proof.

- Suppose $W \in \mathcal{S}[\![\Sigma]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.
- To show: $(W, \mathsf{try}\ \rho_1\gamma_1 e_1\ \mathsf{with}\ x.\rho_1\gamma_1 e_3, \mathsf{try}\ \rho_2\gamma_2 e_2\ \mathsf{with}\ x.\rho_2\gamma_2 e_4) \in \mathcal{E}[\![\tau]\!]\rho$
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$.
- To show: $(W, K_1[\mathsf{try}\ \rho_1\gamma_1 e_1\ \mathsf{with}\ x.\rho_1\gamma_1 e_3], K_2[\mathsf{try}\ \rho_2\gamma_2 e_2\ \mathsf{with}\ x.\rho_2\gamma_2 e_4]) \in \mathcal{O}$
- After instantiating the first premise it suffices to show $(W, K_1[\mathsf{try}\ \bullet\ \mathsf{with}\ x.\rho_1\gamma_1 e_3], K_2[\mathsf{try}\ \bullet\ \mathsf{with}\ x.\rho_2\gamma_2 e_4]) \in \mathcal{K}[\![\tau]\!]\rho$.

1. – First suppose $(W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$ for $W' \sqsupseteq^{\mathsf{pub}} W$.
   – To show: $(W', K_1[\mathsf{try}\ v_1\ \mathsf{with}\ x.\rho_1\gamma_1 e_3], K_2[\mathsf{try}\ v_2\ \mathsf{with}\ x.\rho_2\gamma_2 e_4]) \in \mathcal{O}$
   – By Lemma 12 it suffices to show $(W', K_1[v_1], K_2[v_2]) \in \mathcal{O}$, which follows from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$.
2. – Now suppose $(W', v_1, v_2) \in \mathcal{V}[\![\mathsf{exn}]\!]\rho$ for $W' \sqsupseteq^{\mathsf{pub}} W$.
   – To show: $(W', K_1[\mathsf{try\ raise}\ v_1\ \mathsf{with}\ x.\rho_1\gamma_1 e_3], K_2[\mathsf{try\ raise}\ v_2\ \mathsf{with}\ x.\rho_2\gamma_2 e_4]) \in \mathcal{O}$
   – This reduces to showing $(W', K_1[(\rho_1\gamma_1 e_3)[v_1/x]], K_2[(\rho_2\gamma_2 e_4)[v_2/x]]) \in \mathcal{O}$
   – By definition of TermAtom, v_1 and v_2 contain no free type variables and hence $K_1[(\rho_1\gamma_1 e_3)[v_1/x]] = K_1[\rho_1\gamma_1' e_3]$ and $K_2[(\rho_2\gamma_2 e_4)[v_2/x]] = K_2[\rho_2\gamma_2' e_4]$ for $\gamma' := \gamma, x{\mapsto}(v_1, v_2)$.
   – By monotonicity (Lemma 10) we have $W' \in \mathcal{S}[\![\Sigma]\!]$ and $(W', \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.
   – Consequently, $(W', \gamma') \in \mathcal{G}[\![\Gamma, x{:}\mathsf{exn}]\!]\rho$.
   – Instantiating the second premise then yields $(W', \rho_1\gamma_1' e_3, \rho_2\gamma_2' e_4) \in \mathcal{E}[\![\tau]\!]\rho$.
   – Since $W' \sqsupseteq^{\mathsf{pub}} W$, $(W', K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$ by monotonicity (Lemma 10).
   – Instantiating $(W', \rho_1\gamma_1' e_3, \rho_2\gamma_2' e_4) \in \mathcal{E}[\![\tau]\!]\rho$ then yields the claim.

□

3.3 HOSC

Like for **HOS**, but with the following additions and adaptations.

3.3.1 Basic Properties

Lemma 37. $\sqsupseteq = \sqsupseteq^{\mathsf{pub}}$

Lemma 38. For any $W \in \text{World}$, $\text{safe}(W)$.

3.3.2 Soundness

Definition 1.

$$\Sigma;\Delta;\Gamma \vdash K_1 \precsim_{\log} K_2 \div \tau \stackrel{\text{def}}{=} \begin{array}{l} \Sigma;\Delta;\Gamma \vdash K_1 \div \tau \wedge \Sigma;\Delta;\Gamma \vdash K_2 \div \tau \wedge \forall W,\rho,\gamma. \\ W \in \mathcal{S}[\![\Sigma]\!] \wedge \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho \implies \\ (W, \rho_1\gamma_1 K_1, \rho_2\gamma_2 K_2) \in \mathcal{K}[\![\tau]\!]\rho \end{array}$$

Lemma 39 (Compatibility: Cont)**.** If $\Sigma;\Delta;\Gamma \vdash K_1 \precsim_{\log} K_2 \div \tau$, then $\Sigma;\Delta;\Gamma \vdash \mathsf{cont}_\tau\ K_1 \precsim_{\log} \mathsf{cont}_\tau\ K_2 : \mathsf{cont}\,\tau$.

Proof.

- Suppose $W \in \mathcal{S}[\![\Sigma]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.
- To show: $(W, \mathsf{cont}_{\rho_1\tau}\ \rho_1\gamma_1 K_1, \mathsf{cont}_{\rho_2\tau}\ \rho_2\gamma_2 K_2) \in \mathcal{V}[\![\mathsf{cont}\,\tau]\!]\rho$
- It suffices to show $(W, \rho_1\gamma_1 K_1, \rho_2\gamma_2 K_2) \in \mathcal{K}[\![\tau]\!]\rho$.
- This follows immediately from instantiating the assumption.

□

Lemma 40 (Compatibility: Call/cc)**.** If $\Sigma;\Delta;\Gamma, x{:}\mathsf{cont}\,\tau \vdash e_1 \precsim_{\log} e_2 : \tau$, then $\Sigma;\Delta;\Gamma \vdash \mathsf{call/cc}_\tau\,(x.\ e_1) \precsim_{\log} \mathsf{call/cc}_\tau\,(x.\ e_2) : \tau$.

Proof.

- Suppose $W \in \mathcal{S}[\![\Sigma]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, $(W,\gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$, and $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$.
- To show: $(W, K_1[\mathsf{call/cc}_{\rho_1\tau}\,(x.\ \rho_1\gamma_1 e_1)], K_2[\mathsf{call/cc}_{\rho_2\tau}\,(x.\ \rho_2\gamma_2 e_2)]) \in \mathcal{O}$
- By Lemma 12 it suffices to show $(W, K_1[(\rho_1\gamma_1 e_1)[K_1/x]], K_2[(\rho_2\gamma_2 e_2)[K_2/x]]) \in \mathcal{O}$.
- By definition of ContAtom, K_1 and K_2 contain no free type variables, so $K_1[(\rho_1\gamma_1 e_1)[K_1/x]] = K_1[\rho_1\gamma_1' e_1]$ and $K_2[(\rho_2\gamma_2 e_2)[K_2/x]] = K_2[\rho_2\gamma_2' e_2]$ for $\gamma' := \gamma, x{\mapsto}(K_1, K_2)$.
- Note that we have $(W,\gamma') \in \mathcal{G}[\![\Gamma, x{:}\mathsf{cont}\,\tau]\!]\rho$.
- Instantiating the assumption now yields $(W, \rho_1\gamma_1' e_1, \rho_2\gamma_2' e_2) \in \mathcal{E}[\![\tau]\!]\rho$, from which the claim follows.

□

Lemma 41 (Compatibility: Throw)**.** If $\Sigma;\Delta;\Gamma \vdash e_1 \precsim_{\log} e_2 : \tau'$ and $\Sigma;\Delta;\Gamma \vdash e_3 \precsim_{\log} e_4 : \mathsf{cont}\,\tau'$, then $\Sigma;\Delta;\Gamma \vdash \mathsf{throw}_\tau\ e_1\ \mathsf{to}\ e_3 \precsim_{\log} \mathsf{throw}_\tau\ e_2\ \mathsf{to}\ e_4 : \tau$.

Proof.

- This reduces to showing $(W, K_1[\mathsf{throw}_{\rho_1\tau}\ v_1\ \mathsf{to}\ \bullet], K_2[\mathsf{throw}_{\rho_2\tau}\ v_2\ \mathsf{to}\ \bullet]) \in \mathcal{K}[\![\mathsf{cont}\,\tau']\!]\rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\rho$ and $(W, v_1, v_2) \in \mathcal{V}[\![\tau']\!]\rho$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W$ and $(W', K_3, K_4) \in \mathcal{K}[\![\tau']\!]\rho$.
- To show: $(W', K_1[\mathsf{throw}_{\rho_1\tau}\ v_1\ \mathsf{to\ cont}\ K_3], K_2[\mathsf{throw}_{\rho_2\tau}\ v_2\ \mathsf{to\ cont}\ K_4]) \in \mathcal{O}$
- By Lemma 12 it suffices to show $(W', K_3[v_1], K_4[v_2]) \in \mathcal{O}$.
- By monotonicity (Lemma 10) we know $(W', v_1, v_2) \in \mathcal{V}[\![\tau']\!]\rho$.
- Hence instantiating $(W', K_3, K_4) \in \mathcal{K}[\![\tau']\!]\rho$ yields the claim.

□

Theorem 3 (Fundamental Property)**.**

1. If $\Sigma;\Delta;\Gamma \vdash e : \tau$, then $\Sigma;\Delta;\Gamma \vdash e \precsim_{\log} e : \tau$.
2. If $\Sigma;\Delta;\Gamma \vdash K \div \tau$, then $\Sigma;\Delta;\Gamma \vdash K \precsim_{\log} K \div \tau$.

Proof. By mutual induction on $|e|$ and $|K|$, where these size functions are defined in a straightforward way such that $|K| = |K[x]|$ and $K < |\mathsf{cont}_\tau\ K|$.

1. In each case we use the appropriate compatibility lemma. The induction hypothesis is needed for $e = \mathsf{cont}\ K$:
   - By inversion we know $\tau = \mathsf{cont}\,\tau'$ and $\Sigma;\Delta;\Gamma \vdash K \div \tau'$.
   - Since $|K| < |\mathsf{cont}\ K|$, part (2) of the induction hypothesis yields $\Sigma;\Delta;\Gamma \vdash K \precsim_{\log} K \div \tau'$.
   - The claim then follows by the compatibility lemma for cont.
2. - Suppose $W \in \mathcal{S}[\![\Sigma]\!]$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $(W, \gamma) \in \mathcal{G}[\![\Gamma]\!]\rho$.
   - To show: $(W, \rho_1\gamma_1 K, \rho_2\gamma_2 K) \in \mathcal{K}[\![\tau]\!]\rho$
   - So suppose $W' \sqsupseteq^{\mathsf{pub}} W$, $(W', v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$, $(h_1, h_2) : W'$, and $\langle h_1; \rho_1\gamma_1 K[v_1]\rangle\downarrow^{<W'.k}$.
   - To show: $\langle h_2; \rho_2\gamma_2 K[v_2]\rangle\downarrow$
   - By Lemma 1, there is τ' such that $\Sigma;\Delta;\Gamma, x{:}\tau \vdash K[x] : \tau'$.
   - Since $|K[x]| = |K|$, we have $\Sigma;\Delta;\Gamma, x{:}\tau \vdash K[x] \precsim_{\log} K[x] : \tau'$ by part (1).
   - Using monotonicity (Lemma 10), it is easy to see that $W' \in \mathcal{S}[\![\Sigma]\!]$ and $(W', \gamma') \in \mathcal{G}[\![\Gamma, x{:}\tau]\!]\rho$ for $\gamma' := \gamma, x{\mapsto}(v_1, v_2)$.
   - Instantiating $\Sigma;\Delta;\Gamma, x{:}\tau \vdash K[x] \precsim_{\log} K[x] : \tau'$ thus yields $(W', \rho_1\gamma_1' K[x], \rho_2\gamma_2' K[x]) \in \mathcal{E}[\![\tau']\!]\rho$.
   - Note that $\gamma_1' K[x] = \gamma_1 K[v_1]$ and $\gamma_2' K[x] = \gamma_2 K[v_2]$.
   - It is easy to see that $(W', \bullet, \bullet) \in \mathcal{K}[\![\tau']\!]\rho$.
   - Instantiating $(W', \rho_1\gamma_1' K[x], \rho_2\gamma_2' K[x]) \in \mathcal{E}[\![\tau']\!]\rho$ then yields the claim.

□

3.4 FOS

Like for **HOS** except that the compatibility lemmas for reference constructs and the construction of a canonical safe world become simpler, because heap relations are no longer world-indexed.

3.5 FOSE

The above adaptations for first-order state and exceptions are orthogonal and can easily be combined.

3.6 FOSC

The above adaptations for first-order state and continuations are orthogonal and can easily be combined.

4 Examples

Note: for convenience we often write HeapAtom when we actually mean HeapAtom_n, for an n that is clear from context.

4.1 HOS

4.1.1 Deferred Divergence 1

$$\begin{array}{lcl}
\tau & = & ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit} \\
e_1 & = & \mathsf{let}\ x = \mathsf{ref}\ \mathsf{ff}\ \mathsf{in}\ \mathsf{let}\ y = \mathsf{ref}\ \mathsf{ff}\ \mathsf{in} \\
 & & \lambda f{:}(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}.\ f\ (\lambda z{:}\mathsf{unit}.\ \mathsf{if}\ !x = \mathsf{ff}\ \mathsf{then}\ y := \mathsf{tt}\ \mathsf{else}\ \bot); \\
 & & \qquad\qquad \mathsf{if}\ !y = \mathsf{ff}\ \mathsf{then}\ x := \mathsf{tt}\ \mathsf{else}\ \bot \\
e_2 & = & \lambda f{:}(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}.\ f\ (\lambda z{:}\mathsf{unit}.\ \bot)
\end{array}$$

This equivalence does not hold in the presence of call/cc. Here is a distinguishing context C:

$$\mathsf{call/cc}\,(k.\ \bullet\ (\lambda g.\,\mathsf{throw}\ g\ \langle\rangle\ \mathsf{to}\ k))$$

It is easy to verify that $C[e_1]$ terminates, while $C[e_2]$ doesn't.

Furthermore, e_1 and e_2 are not equivalent in **HOSE** (or even **FOSE**). Here is a distinguishing context C:

$$\begin{array}{l}
\mathsf{let}\ g = \bullet\ \mathsf{in} \\
\mathsf{let}\ f = (\lambda g'.\, g'\ \langle\rangle; \mathsf{raise}\ c)\ \mathsf{in} \\
\mathsf{try}\ g\ f\ \mathsf{with}\ _.\langle\rangle
\end{array}$$

It is easy to verify that $C[e_1]$ yields $\langle\rangle$, while $C[e_2]$ diverges.

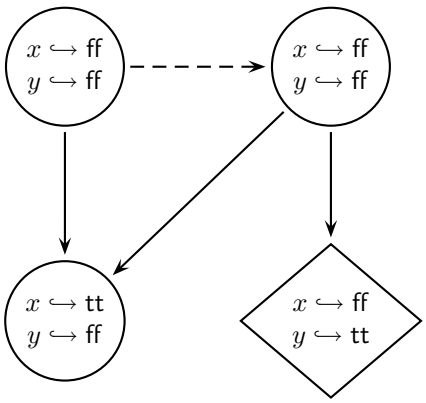
The programes are, however, equivalent in **HOS**, which we prove by showing that each logically approximates the other.

We first show $\cdot;\cdot;\cdot \vdash e_1 \precsim_{\log} e_2 : ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit}$:

- This reduces to showing $(W, e_1, e_2) \in \mathcal{E}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, where $W \in \mathcal{S}[\![\cdot]\!]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_1]\rangle\downarrow^{<W.k}$.
- To show: consistent(W) and $\langle h_2; K_2[e_2]\rangle\downarrow$
- $\langle h_1; K_1[e_1]\rangle\downarrow^{<W.k}$ implies $\langle h_1 \uplus \{l_x{\mapsto}\mathsf{ff}\} \uplus \{l_y{\mapsto}\mathsf{ff}\}; K_1[v_1[l_x/x][l_y/y]]\rangle\downarrow^{<W.k}$, where v_1 is the function value in e_1 and l_x, l_y are distinct and fresh.
- Let
  - $H(\langle i, j\rangle) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \text{HeapAtom} \mid \widetilde{h_1}(l_x) = i \wedge \widetilde{h_1}(l_y) = j\}$
  - $H(\langle i, j, \_\rangle) := H(\langle i, j\rangle)$
  - $\varphi := \{(\langle \mathsf{ff}, \mathsf{ff}, 0\rangle, \langle \mathsf{tt}, \mathsf{ff}\rangle), (\langle \mathsf{ff}, \mathsf{ff}, 1\rangle, \langle \mathsf{tt}, \mathsf{ff}\rangle), (\langle \mathsf{ff}, \mathsf{ff}, 1\rangle, \langle \mathsf{ff}, \mathsf{tt}\rangle)\}^*$
  - $\delta := (\varphi \uplus \{(\langle \mathsf{ff}, \mathsf{ff}, 0\rangle, \langle \mathsf{ff}, \mathsf{ff}, 1\rangle)\})^*$
  - $\iota_s := (s, \delta, \varphi, \{\langle \mathsf{ff}, \mathsf{tt}\rangle\}, H)$

– $W_s := W[\Sigma_1 := W.\Sigma_1, l_x{:}\mathsf{bool}, l_y{:}\mathsf{bool}][\omega := W.\omega, \iota_s]$

The island represents the following STS:



- Note that $\mathrm{safe}(\iota_{\langle \mathsf{ff},\mathsf{ff},0\rangle})$ and thus $W_{\langle \mathsf{ff},\mathsf{ff},0\rangle} \sqsupseteq^{\mathsf{pub}} W$.
- Furthermore, using monotonicity (Lemma 10), it is easy to see that $(h_1 \uplus \{l_x \mapsto \mathsf{ff}\} \uplus \{l_y \mapsto \mathsf{ff}\}, h_2) : W_{\langle \mathsf{ff},\mathsf{ff},0\rangle}$.
- Consequently, if we can show $(W_{\langle \mathsf{ff},\mathsf{ff},0\rangle}, v_1[l_x/x][l_y/y], e_2) \in \mathcal{V}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, then the claims follow from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$.
- So suppose $W' \sqsupseteq W_{\langle \mathsf{ff},\mathsf{ff},0\rangle}$ and $(W', \lambda g.\, e_1', \lambda g.\, e_2') \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1'[\widehat{e_1}[l_x/x][l_y/y][\lambda g.\, e_1'/f]]\rangle \downarrow^{<W'.k}$, where $\widehat{e_1}$ is the body of v_1.
- To show: consistent(W') and $\langle h_2'; K_2'[(\lambda g.\, e_2')\ (\lambda z.\, \bot)]\rangle \downarrow$
- $\langle h_1'; K_1'[\widehat{e_1}[l_x/x][l_y/y][\lambda g.\, e_1'/f]]\rangle \downarrow^{<W'.k}$ implies $\langle h_1'; K_1'[e_1'']\rangle \downarrow^{<W'.k}$, where $e_1'' = (e_1'[\lambda z.\, \mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot/g]; \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot)$.
- Notation: we write W_s' to mean the world obtained from W' by setting our island's current state to s.
- If $W' = W'_{\langle \mathsf{ff},\mathsf{ff},0\rangle}$, then let $\widehat{W'} := W'_{\langle \mathsf{ff},\mathsf{ff},1\rangle}$; otherwise let $\widehat{W'} := W'$.
- It is easy to see that $\widehat{W'} \sqsupseteq W'$.
- We now show $(\widehat{W'}, e_1'[\lambda z.\, \mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot/g], e_2'[\lambda z.\, \bot/g]) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$:
  - Since $(W', \lambda g.\, e_1', \lambda g.\, e_2') \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, it suffices to show $(\widehat{W'}, \lambda z.\, \mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot, \lambda z.\, \bot) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$.
  - So suppose $W'' \sqsupseteq \widehat{W'}$, $(W'', K_1'', K_2'') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$, and $(h_1'', h_2'') : W''$.
  - We show that $\langle h_1''; K_1''[\mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle \downarrow^{<W''.k}$ is impossible.
  - Case $W'' \in \{W''_{\langle \mathsf{ff},\mathsf{ff},1\rangle}, W''_{\langle \mathsf{ff},\mathsf{tt}\rangle}\}$:

* Then $(h_1'', h_2'') : W''$ implies $h_1''(l_x) = \mathsf{ff}$.
* Consequently, $\langle h_1''; K_1''[\mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle\downarrow^{<W''.k}$ would imply $\langle h_1''[l_y{\mapsto}\mathsf{tt}]; K_1''[\langle\rangle]\rangle\downarrow^{<W''.k}$.
* It is easy to see that $W''_{\langle \mathsf{ff},\mathsf{tt}\rangle} \sqsupseteq^{\mathsf{pub}} W''$ and, using monotonicity (Lemma 10), that $(h_1''[l_y{\mapsto}\mathsf{tt}], h_2'') : W''_{\langle \mathsf{ff},\mathsf{tt}\rangle}$.
* Since also $(W''_{\langle \mathsf{ff},\mathsf{tt}\rangle}, \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$, instantiating $(W'', K_1'', K_2'') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$ then yields consistent$(W''_{\langle \mathsf{ff},\mathsf{tt}\rangle})$.

– Case $W'' = W''_{\langle \mathsf{tt},\mathsf{ff}\rangle}$:
* Then $(h_1'', h_2'') : W''$ implies $h_1''(l_x) = \mathsf{tt}$.
* Consequently, $\langle h_1''; K_1''[\mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle\uparrow$.

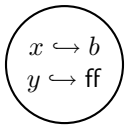
- We now show $(\widehat{W'}, K_1'[\bullet; \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot], K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$:
  – Suppose $W'' \sqsupseteq^{\mathsf{pub}} \widehat{W'}$, $(h_1'', h_2'') : W''$, and $\langle h_1''; K_1'[\langle\rangle; \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle\downarrow^{<W''.k}$.
  – To show: consistent(W'') and $\langle h_2''; K_2'[\langle\rangle]\rangle\downarrow$
  – Observe that $h_1''(l_y)$ must be ff and therefore $W'' \in \{W''_{\langle \mathsf{ff},\mathsf{ff},1\rangle}, W''_{\langle \mathsf{tt},\mathsf{ff}\rangle}\}$.
  – Also, this means that $\langle h_1''[l_x{\mapsto}\mathsf{tt}]; K_1'[\langle\rangle]\rangle\downarrow^{<W''.k}$.
  – It is easy to see that $(h_1''[l_x{\mapsto}\mathsf{tt}], h_2'') : W''_{\langle \mathsf{tt},\mathsf{ff}\rangle}$ and that $W''_{\langle \mathsf{tt},\mathsf{ff}\rangle} \sqsupseteq^{\mathsf{pub}} W'_{\langle \mathsf{tt},\mathsf{ff}\rangle} \sqsupseteq^{\mathsf{pub}} W'$.
  – Also, $(W''_{\langle \mathsf{tt},\mathsf{ff}\rangle}, \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$.
  – Hence, instantiating $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$ yields consistent$(W''_{\langle \mathsf{tt},\mathsf{ff}\rangle})$ and $\langle h_2''; K_2'[\langle\rangle]\rangle\downarrow$.
  – The former implies consistent(W'').
- Using monotonicity (Lemma 10), we easily get $(h_1', h_2') : W''$.
- Instantiating $(W'', e_1'[\lambda z.\, \mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot/g], e_2'[\lambda z.\, \bot/g]) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$ thus yields consistent(W'') and $\langle h_2'; K_2'[e_2'[\lambda z.\, \bot/g]]\rangle\downarrow$.
- The former implies consistent(W') and the latter implies $\langle h_2'; K_2'[(\lambda g.\, e_2')\ (\lambda z.\, \bot)]\rangle\downarrow$.

We show $\cdot; \cdot; \cdot \vdash e_2 \precsim_{\log} e_1 : \tau$.

- This reduces to showing $(W, e_2, e_1) \in \mathcal{E}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, where $W \in \mathcal{S}[\![\cdot]\!]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_2]\rangle\downarrow^{<W.k}$.
- To show: consistent(W) and $\langle h_2; K_2[e_1]\rangle\downarrow$
- Observe that $\langle h_2; K_2[e_1]\rangle\downarrow$ if $\langle h_2 \uplus \{l_x{\mapsto}\mathsf{ff}\} \uplus \{l_y{\mapsto}\mathsf{ff}\}; K_2[\widehat{e_1}[l_x/x][l_y/y]]\rangle\downarrow$, where $\widehat{e_1}$ is the function value in e_1 and l_y any free location.
- Let
  – $H(\langle\rangle) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \mathrm{HeapAtom} \mid \widetilde{h_2}(l_y) = \mathsf{ff} \wedge l_x \in \mathrm{dom}(h_2)\}$
  – $\iota := (\langle\rangle, \emptyset^*, \emptyset^*, \emptyset, H)$

– $\widehat{W} := W[\Sigma_2 := W.\Sigma_2, l_x{:}\mathsf{bool}, l_y{:}\mathsf{bool}][\omega := W.\omega, \iota]$

The island represents the following STS:



- Note that $\widehat{W} \sqsupseteq^{\mathsf{pub}} W$ and $(h_1, h_2 \uplus \{l_x \mapsto \mathsf{ff}\} \uplus \{l_y \mapsto \mathsf{ff}\}) : \widehat{W}$.
- Because of $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\emptyset$ it thus suffices to show $(\widehat{W}, e_2, \widehat{e_1}[l_x/x][l_y/y]) \in \mathcal{V}[\![\tau]\!]\emptyset$.
- So suppose $W' \sqsupseteq W$, $(W', f_1, f_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1'[f_1\ (\lambda\_.\, \bot)]\rangle\downarrow^{<W'.k}$.
- To show: $\langle h_2'; K_2'[f_2\ (\lambda\_.\, \mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot); \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle\downarrow$ and consistent(W')
- We show $(W', f_1\ (\lambda\_.\, \bot), f_2\ (\lambda\_.\, \mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot)) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$:
  - Since $(W', f_1, f_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, it suffices to show $(W', (\lambda\_.\, \bot), (\lambda\_.\, \mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot)) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$.
  - This holds trivially, because $\langle h_1''; K_1''[\bot]\rangle$ diverges for any h_1'' and K_1''.
- We show $(W', K_1', K_2'[\bullet; \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$:
  - So suppose $W'' \sqsupseteq^{\mathsf{pub}} W'$, $(h_1'', h_2'') : W''$, and $\langle h_1''; K_1'[\langle\rangle]\rangle\downarrow^{<W''.k}$.
  - To show: consistent(W'') and $\langle h_2''; K_2'[\mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle\downarrow$
  - From $(h_1'', h_2'') : W''$ we know $h_2''(l_y) = \mathsf{ff}$.
  - Therefore, $\langle h_2''; K_2'[\mathsf{if}\ !l_y\ \mathsf{then}\ \bot\ \mathsf{else}\ \langle\rangle]\rangle\downarrow$ if $\langle h_2''[l_x \mapsto \mathsf{tt}]; K_2'[\langle\rangle]\rangle\downarrow$.
  - Note that $(h_1'', h_2'') : W''$ implies $(h_1'', h_2''[l_x \mapsto \mathsf{tt}]) : W''$.
  - The claims thus follow from instantiating $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$ with $(W'', \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$.
- Combining these yields the claims.

4.1.2 Well-Bracketed State Changes

$$\begin{array}{lcl} e_1 & = & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in} \\ & & \lambda f{:}\mathsf{unit} \to \mathsf{unit}.\ (x := 0; f\ \langle\rangle; x := 1; f\ \langle\rangle; !x) \\ e_2 & = & \lambda f{:}\mathsf{unit} \to \mathsf{unit}.\ (f\ \langle\rangle; f\ \langle\rangle; 1) \end{array}$$

It is easy to see that e_1 and e_2 are not equivalent in **HOSC** (or even **FOSC**). In particular, here is a distinguishing context C:

$$\begin{array}{l} \mathsf{let}\ g = \bullet\ \mathsf{in}\ \mathsf{let}\ b = \mathsf{ref}\ \mathsf{ff}\ \mathsf{in} \\ \mathsf{let}\ f = (\lambda\_.\, \mathsf{if}\ !b\ \mathsf{then}\ \mathsf{call/cc}\,(k.\ g\ (\lambda\_.\, \mathsf{throw}\ \langle\rangle\ \mathsf{to}\ k)) \\ \qquad\qquad\qquad \mathsf{else}\ b := \mathsf{tt})\ \mathsf{in} \\ g\ f \end{array}$$

Exploiting its ability to capture the continuation K of the second call to f, the context C is able to set x back to 0 and then immediately throw control back to K. It is easy to verify that $C[e_1]$ yields 0, while $C[e_2]$ yields 1.

It is also easy to see that e_1 and e_2 are not equivalent in **HOSE** (or even **FOSE**). In particular, here is a distinguishing context C:

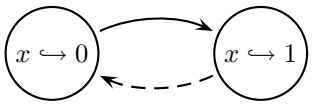
$$\begin{array}{l}\mathsf{let}\ g = \bullet\ \mathsf{in}\\ \mathsf{let}\ f_2 = (\lambda\_.\ \mathsf{raise}\ c)\ \mathsf{in}\\ \mathsf{let}\ x = \mathsf{ref}\ \mathsf{tt}\ \mathsf{in}\\ \mathsf{let}\ f_1 = (\lambda\_.\ \mathsf{if}\ !x\ \mathsf{then}\ x := \mathsf{ff}\ \mathsf{else}\ \mathsf{try}\ g\ f_2\ \mathsf{with}\ \_.\langle\rangle)\ \mathsf{in}\\ g\ f\end{array}$$

It is easy to verify that $C[e_1]$ yields 0, while $C[e_2]$ yields 1.

The programes are, however, equivalent in **HOS**, which we prove by showing that each logically approximates the other.
We show $\cdot;\cdot;\cdot \vdash e_1 \precsim_{\log} e_2 : (\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}$:

- This reduces to showing $(W, e_1, e_2) \in \mathcal{E}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}]\!]\emptyset$, where $W \in \mathcal{S}[\![\cdot]\!]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}]\!]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_1]\rangle\downarrow^{<W.k}$.
- To show: consistent(W) and $\langle h_2; K_2[e_2]\rangle\downarrow$
- $\langle h_1; K_1[e_1]\rangle\downarrow^{<W.k}$ implies $\langle h_1 \uplus \{l_x \mapsto 0\}; K_1[\widehat{e_1}]\rangle\downarrow^{<W.k}$, where l_x is fresh and $\widehat{e_1} := \lambda f.\,(l_x := 0; f\ \langle\rangle; l_x := 1; f\ \langle\rangle; !l_x)$.
- Let
  - $H(i) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \mathrm{HeapAtom} \mid \widetilde{h_1}(l_x) = i\}$
  - $\varphi := \{(0,1)\}^*$
  - $\delta := (\varphi \uplus \{(1,0)\})^*$
  - $\iota_s := (s, \delta, \varphi, \emptyset, H)$
  - $W_s := W[W.\Sigma_1 := W.\Sigma_1, l_x{:}\mathsf{int}][W.\omega := W.\omega, \iota_s]$

  The island represents the following STS:



- It is easy to see that $W_0 \sqsupseteq^{\mathsf{pub}} W$ and, using monotonicity (Lemma 10), that $(h_1 \uplus \{l_x \mapsto 0\}, h_2) : W_0$.
- Hence by instantiating $(W, K_1, K_2) \in \mathcal{K}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}]\!]\emptyset$, it suffices to show $(W_0, \widehat{e_1}, e_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}]\!]\emptyset$.
- So suppose $W' \sqsupseteq W_0$ and $(W', \lambda z.\,e_1', \lambda z.\,e_2') \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$, $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{int}]\!]\emptyset$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1'[\widehat{e_1}'[\lambda z.\,e_1'/f]]\rangle\downarrow^{<W'.k}$, where $\widehat{e_1}'$ is the body of $\widehat{e_1}$.

- To show: consistent(W') and $\langle h_2'; K_2'[\widehat{e_2}'[\lambda z.\, e_2'/f]]\rangle\downarrow$, where $\widehat{e_2}'$ is the body of e_2
- $\langle h_1'; K_1'[\widehat{e_1}'[\lambda z.\, e_1'/f]]\rangle\downarrow^{<W'.k}$ implies $\langle h_1'[l_x{\mapsto}0]; K_1'[(e_1'[\langle\rangle/z]; l_x := 1; (\lambda z.\, e_1')\ \langle\rangle; !l_x)]\rangle\downarrow^{<W'.k}$.
- Notation: we write W_s' to mean the world obtained from W' by setting our island's current state to s.
- It is easy to see that $W_0' \sqsupseteq W'$ and that consistent(W_0') would imply consistent(W').
- Since $(W_0', \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$, instantiating $(W', \lambda g.\, e_1', \lambda z.\, e_2') \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$ yields $(W_0', e_1'[\langle\rangle/z], e_2'[\langle\rangle/z]) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$.
- It is easy to see, using monotonicity (Lemma 10), that $(h_1'[l_x{\mapsto}0], h_2') : W_0'$.
- Since $\langle h_2'; K_2'[\widehat{e_2}'[\lambda z.\, e_2'/f]]\rangle\downarrow$ would follow from $\langle h_2'; K_2'[(e_2'[\langle\rangle/z]; (\lambda z.\, e_2')\ \langle\rangle; 1)]\rangle\downarrow$, it therefore suffices to show $(W_0', K_1'[(\bullet; l_x := 1; (\lambda z.\, e_1')\ \langle\rangle; !l_x)], K_2'[(\bullet; (\lambda z.\, e_2')\ \langle\rangle; 1)]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
- So suppose $W'' \sqsupseteq^{\mathsf{pub}} W_0'$, $(h_1'', h_2'') : W''$, and $\langle h_1''; K_1'[(\langle\rangle; l_x := 1; (\lambda z.\, e_1')\ \langle\rangle; !l_x)]\rangle\downarrow^{<W''.k}$.
- To show: consistent(W'') and $\langle h_2''; K_2'[(\langle\rangle; (\lambda z.\, e_2')\ \langle\rangle; 1)]\rangle\downarrow$
- $\langle h_1''; K_1'[(\langle\rangle; l_x := 1; (\lambda z.\, e_1')\ \langle\rangle; !l_x)]\rangle\downarrow^{<W''.k}$ implies $\langle h_1''[l_x{\mapsto}1]; K_1'[(e_1'[\langle\rangle/z]; !l_x)]\rangle\downarrow^{<W''.k}$
- It is easy to see that $W_1'' \sqsupseteq^{\mathsf{pub}} W'$.
- Since $(W_1'', \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$, instantiating $(W', \lambda z.\, e_1', \lambda z.\, e_2') \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$ yields $(W_1'', e_1'[\langle\rangle/z], e_2'[\langle\rangle/z]) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$.
- It is easy to see, using monotonicity (Lemma 10), that $(h_1''[l_x{\mapsto}1], h_2'') : W_1''$.
- Also, consistent(W_1'') would imply consistent(W'').
- Since $\langle h_2''; K_2'[(\langle\rangle; (\lambda z.\, e_2')\ \langle\rangle; 1)]\rangle\downarrow$ would be implied by $\langle h_2''; K_2'[(e_2'[\langle\rangle/z]; 1)]\rangle\downarrow$, it therefore suffices to show $(W_1'', K_1'[(\bullet; !l_x)], K_2'[(\bullet; 1)]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
- So suppose $W''' \sqsupseteq^{\mathsf{pub}} W_1''$, $(h_1''', h_2''') : W'''$, and $\langle h_1'''; K_1'[(\langle\rangle; !l_x)]\rangle\downarrow^{<W'''.k}$.
- To show: consistent(W''') and $\langle h_2'''; K_2'[(\langle\rangle; 1)]\rangle\downarrow$
- Note that $W''' \sqsupseteq^{\mathsf{pub}} W_1''$ and $(h_1''', h_2''') : W'''$ imply $h_1'''(l_x) = 1$.
- Hence $\langle h_1'''; K_1'[(\langle\rangle; !l_x)]\rangle\downarrow^{<W'''.k}$ implies $\langle h_1'''; K_1'[1]\rangle\downarrow^{<W'''.k}$.
- We know $W''' \sqsupseteq^{\mathsf{pub}} W_1'' \sqsupseteq^{\mathsf{pub}} W'$ and $(W''', 1, 1) \in \mathcal{V}[\![\mathsf{int}]\!]\emptyset$.
- Therefore, instantiating $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{int}]\!]\emptyset$ yields consistent(W''') and $\langle h_2'''; K_2'[1]\rangle\downarrow$.
- The latter implies $\langle h_2'''; K_2'[(\langle\rangle; 1)]\rangle\downarrow$.

Here is a higher-level explanation of the proof:

To show e_1 and e_2 related, suppose given some world and a pair of heaps h_1 and h_2 satisfying this world. Then e_1 allocates a new location l_x extending h_1 to h_1'. We extend our world with a new island, as in the picture, and it is clear that the resulting world $W_0 \sqsupseteq^{\mathsf{pub}}$-extends the old world, and that h_1' and h_2 satisfy W_0. Thus it suffices to show that the functions returned by e_1 and e_2 are related in this new world W_0. To this end, suppose we are given any world W' that $\sqsupseteq$-extends W_0, heaps h_1'' and h_2'' satisfying W', and functions f_1 and f_2 related in W'. Notice that in W' our island can be in either the left or the right state and we do not know which! We then have to show that $e_1' = (x := 0; f_1\ \langle\rangle; x := 1; f_1\ \langle\rangle; !x)$ and $e_2' = (f_2\ \langle\rangle; f_2\ \langle\rangle; 1)$ are related computations in world W'. Let us write W_s' to mean the world obtained from W' by setting our island's current state to s (i.e., 0 if the left state, 1 is the right state). Notice that W_0' is a $\sqsupseteq$-extension of W' — here we crucially use that we have edges both from the left to the right and vice versa. Now, since e_1' assign 0 to x, it means that we get heaps $h_1''[l_x \mapsto 0]$ and h_2'' which are related in W_0'. Moreover, since f_1 and f_2 are functions related in W' and $W_0' \sqsupseteq W'$, we also have that there exists a future world $W'' \sqsupseteq^{\mathsf{pub}} W_0'$ such that f_1 and f_2 take arguments and heaps related in W_0' to values and heaps related in W''. Now we then have to show that $e_1'' = (x := 1; f_1\ \langle\rangle; !x)$ and $e_2'' = (f_2\ \langle\rangle; 1)$ are related computations in world W''. We proceed as above, and get, after the assignment $x := 1$ in e_1'' that the resulting heaps are related in W_1'' (i.e., the world obtained from W'' by setting our island's current state to 1). Then we call f_1 and f_2 respectively, and we get that there exists a future world $W''' \sqsupseteq^{\mathsf{pub}} W_1''$ (note the $\sqsupseteq^{\mathsf{pub}}$, not $\sqsupseteq$). Since it is an extension via public edges only, we know that our island is still in state 1 (the state on the right) and thus we find that e_1'' returns 1 when looking up the value of x, just as e_2'', and hence they are related, as required.

4.1.3 Local State Release 1

$$
\begin{array}{lcl}
\tau & = & ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{ref\ int} \\
e_1 & = & \lambda f{:}(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}.\ \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in} \\
 & & \qquad \mathsf{let}\ y = \mathsf{ref}\ 0\ \mathsf{in} \\
 & & \qquad \mathsf{let}\ z = \mathsf{ref}\ 0\ \mathsf{in} \\
 & & \qquad f\ (\lambda\_{:}\mathsf{unit}.\ \mathsf{if}\ !x = 0\ \mathsf{then}\ y := 1\ \mathsf{else}\ z := 1); \\
 & & \qquad \mathsf{if}\ !y = 0\ \mathsf{then}\ x := 1\ \mathsf{else}\ (z := 1; x := 1); \\
 & & \qquad z \\
 & & \\
e_2 & = & \lambda f{:}(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}.\ \mathsf{let}\ z = \mathsf{ref}\ 0\ \mathsf{in} \\
 & & \qquad f\ (\lambda\_{:}\mathsf{unit}.\ z := 1); \\
 & & \qquad z
\end{array}
$$

We show $\cdot;\cdot;\cdot \vdash e_1 \precsim_{\log} e_2 : \tau$.

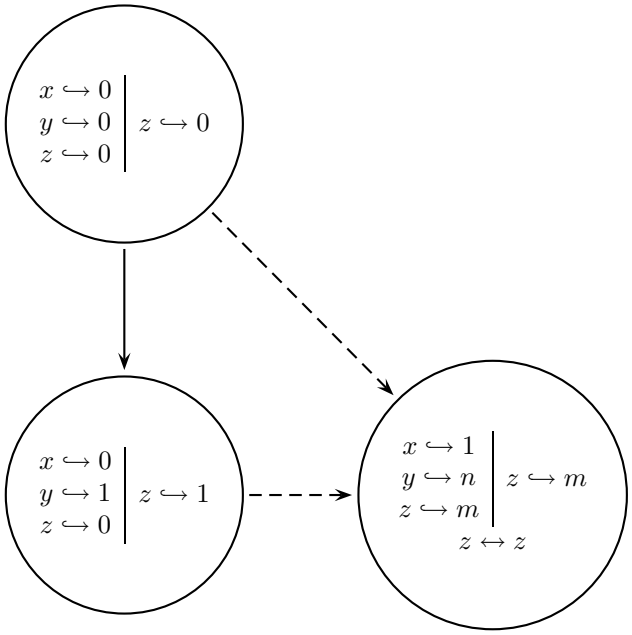
- This reduces to showing $(W_0, e_1, e_2) \in \mathcal{V}[\![\tau]\!]\emptyset$, where $W_0 \in \mathcal{S}[\![\cdot]\!]$.
- So suppose $W \sqsupseteq W_0$, $(W, f_1, f_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{ref\ int}]\!]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[\widehat{e_1}[f_1/f]]\rangle\downarrow^{<W.k}$, where $\widehat{e_1}$ is the body of e_1.
- To show: consistent(W) and $\langle h_2; K_2[\widehat{e_2}[f_2/f]]\rangle\downarrow$, where $\widehat{e_2}$ is the body of e_2
- $\langle h_1; K_1[\widehat{e_1}[f_1/f]]\rangle\downarrow^{<W.k}$ implies $\langle \widetilde{h_1}; K_1[\widetilde{e_1}]\rangle\downarrow^{<W.k}$, where:

- $\widetilde{h_1} := h_1 \uplus \{l_x \mapsto 0\} \uplus \{l_y \mapsto 0\} \uplus \{l_z^1 \mapsto 0\}$
- $\widetilde{e_1} := f_1\ (\lambda\_.\ \mathsf{if}\ !l_x = 0\ \mathsf{then}\ l_y := 1\ \mathsf{else}\ l_z^1 := 1);$
  $\mathsf{if}\ !l_y = 0\ \mathsf{then}\ l_x := 1\ \mathsf{else}\ (l_z^1 := 1; l_x := 1);$
  l_z^1
- l_x, l_y, l_z^1 are distinct and fresh

- Similarly, $\langle h_2; K_2[\widehat{e_2}[f_2/f]]\rangle\downarrow$ if $\langle \widetilde{h_2}; K_2[\widetilde{e_2}]\rangle\downarrow$, where:
  - $\widetilde{h_2} := h_2[l_z^2 \mapsto 0]$
  - $\widetilde{e_2} := f_2\ (\lambda\_.\ l_z^2 := 1);$
    l_z^2
  - l_z^2 is fresh

- Let
  - $H(1) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \mathrm{HeapAtom} \mid \widetilde{h_1}(l_x) = \widetilde{h_1}(l_y) = \widetilde{h_1}(l_z^1) = \widetilde{h_2}(l_z^2) = 0\}$
  - $H(2) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \mathrm{HeapAtom} \mid \widetilde{h_1}(l_x) = \widetilde{h_1}(l_z^1) = 0 \wedge \widetilde{h_1}(l_y) = \widetilde{h_2}(l_z^2) = 1\}$
  - $\mathfrak{z} := \{\langle l_z^1, l_z^2\rangle\}$
  - $H(\mathfrak{z}) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \mathrm{HeapAtom} \mid \widetilde{h_1}(l_x) = 1 \wedge \widetilde{h_1}(l_y) = n \wedge \widetilde{h_1}(l_z^1) = \widetilde{h_2}(l_z^2) = m\}$
  - $\varphi := \{(1, 2)\}$
  - $\delta := (\varphi \uplus \{(1, \mathfrak{z}), (2, \mathfrak{z})\})^*$
  - $\iota_s := (s, \delta, \varphi, \emptyset, H)$
  - $W_s := W[\Sigma_1 := W.\Sigma_1, l_x{:}\mathsf{int}, l_y{:}\mathsf{int}, l_z^1{:}\mathsf{int}][\Sigma_2 := W.\Sigma_2, l_z^2{:}\mathsf{int}][\omega := W.\omega, \iota_s]$

  The island represents the following STS:



- It is easy to see that $W_1 \sqsupseteq W$ and, using monotonicity (Lemma 10), that $(\widetilde{h_1}, \widetilde{h_2}) : W_1$.
- We show $(W_1, f_1\ (\lambda\_.\ \mathsf{if}\ !l_x = 0\ \mathsf{then}\ l_y := 1\ \mathsf{else}\ l_z^1 := 1), f_2\ (\lambda\_.\ l_z^2 := 1)) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$:
  - Since $(W, f_1, f_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, it suffices to show $(W_1, (\lambda\_.\ \mathsf{if}\ !l_x = 0\ \mathsf{then}\ (l_z^1 := 0; l_y := 1)\ \mathsf{else}\ l_z^1 := 1), (\lambda\_.\ l_z^2 := 1)) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$.
  - So suppose $W' \sqsupseteq W_1$, $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1'[\mathsf{if}\ !l_x = 0\ \mathsf{then}\ l_y := 1\ \mathsf{else}\ l_z^1 := 1]\rangle \downarrow^{<W'.k}$.
  - To show: consistent(W') and $\langle h_2'; K_2'[l_z^2 := 1]\rangle \downarrow$, *i.e.,* $\langle h_2'[l_z^2 \mapsto 1]; K_2'[\langle\rangle]\rangle \downarrow$
  - Case $W' \in \{W_1', W_2'\}$:
    - Then $(h_1', h_2') : W'$ implies $h_1'(l_x) = 0$ and thus $\langle h_1'[l_y \mapsto 1]; K_1'[\langle\rangle]\rangle \downarrow^{<W.k}$.
    - It is easy to see that $W_2' \sqsupseteq^{\mathsf{pub}} W'$ and, using monotonicity (Lemma 10), that $(h_1'[l_y \mapsto 1], h_2'[l_z^2 \mapsto 1]) : W_2'$.
    - Also, consistent(W_2') would imply consistent(W').
    - Since $(W_2', \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$, the claims then follow from instantiating $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
  - Case $W' = W_3'$:
    - Then $(h_1', h_2') : W'$ implies $h_1'(l_x) = 1$ and thus $\langle h_1'[l_z^1 \mapsto 1]; K_1'[\langle\rangle]\rangle \downarrow^{<W.k}$.
    - It is easy to see that $(h_1'[l_z^1 \mapsto 1], h_2'[l_z^2 \mapsto 1]) : W'$.
    - Since $(W', \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$, the claims then follow from instantiating $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
- It is obvious that consistent(W_1) would imply consistent(W).
- Hence it suffices to show $(W_1, K_1[\bullet; \mathsf{if}\ !l_y = 0\ \mathsf{then}\ l_x := 1\ \mathsf{else}\ (l_z^1 := 1; l_x := 1); l_z^1], K_2[\bullet; l_z^2]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W_1$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1[\langle\rangle; \mathsf{if}\ !l_y = 0\ \mathsf{then}\ l_x := 1\ \mathsf{else}\ (l_z^1 := 1; l_x := 1); l_z^1]\rangle \downarrow^{<W'.k}$.
- To show: consistent(W') and $\langle h_2'; K_2[\langle\rangle; l_z^2]\rangle \downarrow$, *i.e.,* $\langle h_2'; K_2[l_z^2]\rangle \downarrow$
- Case $W' = W_1'$:
  - Then $(h_1', h_2') : W'$ implies $h_1'(l_y) = 0$ and thus $\langle h_1'[l_x \mapsto 1]; K_1[l_z^1]\rangle \downarrow^{<W'.k}$.
  - It is easy to see that $W_3' \sqsupseteq W'$ and, using monotonicity (Lemma 10), that $(h_1'[l_x \mapsto 1], h_2') : W_3'$.
  - Is is also easy to see that $W_3' \sqsupseteq^{\mathsf{pub}} W_3 \sqsupseteq^{\mathsf{pub}} W$ and that consistent(W_3') would imply consistent(W').
  - The claims then follow from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{ref\ int}]\!]\emptyset$, if we can show $(W_3', l_z^1, l_z^2) \in \mathcal{V}[\![\mathsf{ref\ int}]\!]\emptyset$.
  - The latter is easy to verify, because $\mathsf{bij}(3) = \{(l_z^1, l_z^2)\}$.
- Case $W' = W_2'$:
  - Then $(h_1', h_2') : W'$ implies $h_1'(l_y) = 1$ and thus $\langle h_1'[l_z^1 \mapsto 1][l_x \mapsto 1]; K_1[l_z^1]\rangle \downarrow^{<W'.k}$.

- It is easy to see that $W'_3 \sqsupseteq W'$ and, using monotonicity (Lemma 10), that $(h'_1[l^1_z \mapsto 1][l_x \mapsto 1], h'_2) : W'_3$.
- Is is also easy to see that $W'_3 \sqsupseteq^{\mathsf{pub}} W_3 \sqsupseteq^{\mathsf{pub}} W$ and that consistent(W'_3) would imply consistent(W').
- The claims then follow from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{ref\ int}]\!]\emptyset$, if we can show $(W'_3, l^1_z, l^2_z) \in \mathcal{V}[\![\mathsf{ref\ int}]\!]\emptyset$.
- The latter is easy to verify, because bij$(3) = \{(l^1_z, l^2_z)\}$.

- Case $W' = W'_3$: impossible, because there is no public transition from states 1 to 3

4.2 HOSE

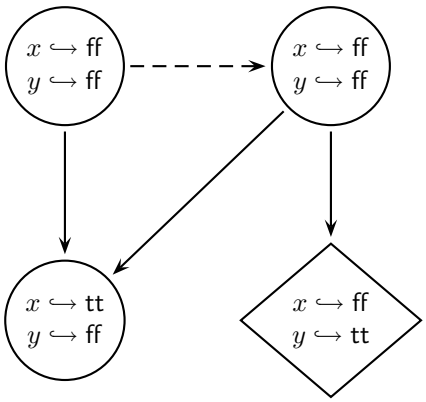
4.2.1 Deferred Divergence 2

$$
\begin{array}{lcl}
\tau & = & ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit} \\
e_1 & = & \mathsf{let}\ x = \mathsf{ref}\ \mathsf{ff}\ \mathsf{in}\ \mathsf{let}\ y = \mathsf{ref}\ \mathsf{ff}\ \mathsf{in} \\
 & & \lambda f{:}(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}.\ \mathsf{try}\ f\ (\lambda z{:}\mathsf{unit}.\ \mathsf{if}\ !x = \mathsf{ff}\ \mathsf{then}\ y := \mathsf{tt}\ \mathsf{else}\ \bot) \\
 & & \qquad\qquad \mathsf{with}\ z.(\mathsf{if}\ !y = \mathsf{ff}\ \mathsf{then}\ x := \mathsf{tt}\ \mathsf{else}\ \bot; \mathsf{raise}\ z); \\
 & & \qquad \mathsf{if}\ !y = \mathsf{ff}\ \mathsf{then}\ x := \mathsf{tt}\ \mathsf{else}\ \bot \\
e_2 & = & \lambda f{:}(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}.\ f\ (\lambda z{:}\mathsf{unit}.\ \bot)
\end{array}
$$

The programes are equivalent in **HOSE**, which we prove by showing that each logically approximates the other.
We first show $\cdot;\cdot;\cdot \vdash e_1 \precsim_{\log} e_2 : ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit}$:

- This reduces to showing $(W, e_1, e_2) \in \mathcal{E}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, where $W \in \mathcal{S}[\![\cdot]\!]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_1]\rangle\downarrow^{<W.k}$.
- To show: consistent(W) and $\langle h_2; K_2[e_2]\rangle\downarrow$
- $\langle h_1; K_1[e_1]\rangle\downarrow^{<W.k}$ implies $\langle h_1 \uplus \{l_x{\mapsto}\mathsf{ff}\} \uplus \{l_y{\mapsto}\mathsf{ff}\}; K_1[v_1[l_x/x][l_y/y]]\rangle\downarrow^{<W.k}$, where v_1 is the function value in e_1 and l_x, l_y are distinct and fresh.
- Let
  - $H(\langle i, j\rangle) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \text{HeapAtom} \mid \widetilde{h_1}(l_x) = i \wedge \widetilde{h_1}(l_y) = j\}$
  - $H(\langle i, j, \_\rangle) := H(\langle i, j\rangle)$
  - $\varphi := \{(\langle \mathsf{ff}, \mathsf{ff}, 0\rangle, \langle \mathsf{tt}, \mathsf{ff}\rangle), (\langle \mathsf{ff}, \mathsf{ff}, 1\rangle, \langle \mathsf{tt}, \mathsf{ff}\rangle), (\langle \mathsf{ff}, \mathsf{ff}, 1\rangle, \langle \mathsf{ff}, \mathsf{tt}\rangle)\}^*$
  - $\delta := (\varphi \uplus \{(\langle \mathsf{ff}, \mathsf{ff}, 0\rangle, \langle \mathsf{ff}, \mathsf{ff}, 1\rangle)\})^*$
  - $\iota_s := (s, \delta, \varphi, \{\langle \mathsf{ff}, \mathsf{tt}\rangle\}, H)$
  - $W_s := W[\Sigma_1 := W.\Sigma_1, l_x{:}\mathsf{bool}, l_y{:}\mathsf{bool}][\omega := W.\omega, \iota_s]$

  The island represents the following STS:



- Note that $\mathrm{safe}(\iota_{\langle \mathsf{ff},\mathsf{ff},0\rangle})$ and thus $W_{\langle \mathsf{ff},\mathsf{ff},0\rangle} \sqsupseteq^{\mathsf{pub}} W$.
- Furthermore, using monotonicity (Lemma 10), it is easy to see that $(h_1 \uplus \{l_x \mapsto \mathsf{ff}\} \uplus \{l_y \mapsto \mathsf{ff}\}, h_2) : W_{\langle \mathsf{ff},\mathsf{ff},0\rangle}$.
- Consequently, if we can show $(W_{\langle \mathsf{ff},\mathsf{ff},0\rangle}, v_1[l_x/x][l_y/y], e_2) \in \mathcal{V}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, then the claims follow from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$.
- So suppose $W' \sqsupseteq W_{\langle \mathsf{ff},\mathsf{ff},0\rangle}$ and $(W', \lambda g.\, e_1', \lambda g.\, e_2') \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1'[\widehat{e_1}[l_x/x][l_y/y][\lambda g.\, e_1'/f]]\rangle \downarrow^{<W'.k}$, where $\widehat{e_1}$ is the body of v_1.
- To show: consistent(W') and $\langle h_2'; K_2'[(\lambda g.\, e_2')\ (\lambda z.\, \bot)]\rangle \downarrow$
- $\langle h_1'; K_1'[\widehat{e_1}[l_x/x][l_y/y][\lambda g.\, e_1'/f]]\rangle \downarrow^{<W'.k}$ implies $\langle h_1'; K_1'[e_1'']\rangle \downarrow^{<W'.k}$, where $e_1'' = (e_1'[\lambda z.\, \mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot/g]; \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot)$.
- Notation: we write W_s' to mean the world obtained from W' by setting our island's current state to s.
- If $W' = W'_{\langle \mathsf{ff},\mathsf{ff},0\rangle}$, then let $\widehat{W'} := W'_{\langle \mathsf{ff},\mathsf{ff},1\rangle}$; otherwise let $\widehat{W'} := W'$.
- It is easy to see that $\widehat{W'} \sqsupseteq W'$.
- We now show $(\widehat{W'}, e_1'[\lambda z.\, \mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot/g], e_2'[\lambda z.\, \bot/g]) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$:
  - Since $(W', \lambda g.\, e_1', \lambda g.\, e_2') \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, it suffices to show $(\widehat{W'}, \lambda z.\, \mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot, \lambda z.\, \bot) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$.
  - So suppose $W'' \sqsupseteq \widehat{W'}$, $(W'', K_1'', K_2'') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$, and $(h_1'', h_2'') : W''$.
  - We show that $\langle h_1''; K_1''[\mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle \downarrow^{<W''.k}$ is impossible.
  - Case $W'' \in \{W''_{\langle \mathsf{ff},\mathsf{ff},1\rangle}, W''_{\langle \mathsf{ff},\mathsf{tt}\rangle}\}$:
    - Then $(h_1'', h_2'') : W''$ implies $h_1''(l_x) = \mathsf{ff}$.
    - Consequently, $\langle h_1''; K_1''[\mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle \downarrow^{<W''.k}$ would imply $\langle h_1''[l_y \mapsto \mathsf{tt}]; K_1''[\langle\rangle]\rangle \downarrow^{<W''.k}$.
    - It is easy to see that $W''_{\langle \mathsf{ff},\mathsf{tt}\rangle} \sqsupseteq^{\mathsf{pub}} W''$ and, using monotonicity (Lemma 10), that $(h_1''[l_y \mapsto \mathsf{tt}], h_2'') : W''_{\langle \mathsf{ff},\mathsf{tt}\rangle}$.
    - Since also $(W''_{\langle \mathsf{ff},\mathsf{tt}\rangle}, \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$, instantiating $(W'', K_1'', K_2'') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$ then yields consistent($W''_{\langle \mathsf{ff},\mathsf{tt}\rangle}$).
  - Case $W'' = W''_{\langle \mathsf{tt},\mathsf{ff}\rangle}$:
    - Then $(h_1'', h_2'') : W''$ implies $h_1''(l_x) = \mathsf{tt}$.
    - Consequently, $\langle h_1''; K_1''[\mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle \uparrow$.
- We now show $(\widehat{W'}, K_1'[\mathsf{try}\ \bullet\ \mathsf{with}\ z.(\mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot; \mathsf{raise}\ z); \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot], K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$:
  1. – First suppose $W'' \sqsupseteq^{\mathsf{pub}} \widehat{W'}$, $(h_1'', h_2'') : W''$, and $\langle h_1''; K_1'[\mathsf{try}\ \langle\rangle\ \mathsf{with}\ z.(\mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot; \mathsf{raise}\ z); \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle \downarrow^{<W''.k}$.

- To show: consistent(W'') and $\langle h_2''; K_2'[\langle\rangle]\rangle\downarrow$
- Note that $\langle h_1''; K_1'[\mathsf{try}\ \langle\rangle\ \mathsf{with}\ z.(\mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot; \mathsf{raise}\ z); \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle\downarrow^{<W''.k}$ implies $\langle h_1''; K_1'[\mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle\downarrow^{<W''.k}$.
- Observe that $h_1''(l_y)$ must be ff and therefore $W'' \in \{W''_{\langle \mathsf{ff},\mathsf{ff},1\rangle}, W''_{\langle \mathsf{tt},\mathsf{ff}\rangle}\}$.
- Also, this means that $\langle h_1''[l_x{\mapsto}\mathsf{tt}]; K_1'[\langle\rangle]\rangle\downarrow^{<W''.k}$.
- It is easy to see that $(h_1''[l_x{\mapsto}\mathsf{tt}], h_2'') : W''_{\langle \mathsf{tt},\mathsf{ff}\rangle}$ and that $W''_{\langle \mathsf{tt},\mathsf{ff}\rangle} \sqsupseteq^{\mathsf{pub}} W'_{\langle \mathsf{tt},\mathsf{ff}\rangle} \sqsupseteq^{\mathsf{pub}} W'$.
- Also, $(W''_{\langle \mathsf{tt},\mathsf{ff}\rangle}, \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$.
- Hence, instantiating $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$ yields both consistent($W''_{\langle \mathsf{tt},\mathsf{ff}\rangle}$) and $\langle h_2''; K_2'[\langle\rangle]\rangle\downarrow$.
- The former implies consistent(W'').

2. - Now suppose $W'' \sqsupseteq^{\mathsf{pub}} \widehat{W'}$, $(W'', v_1, v_2) \in \mathcal{V}[\![\mathsf{exn}]\!]\emptyset$, $(h_1'', h_2'') : W''$ and $\langle h_1''; K_1'[\mathsf{try}\ \mathsf{raise}\ v_1\ \mathsf{with}\ z.(\mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot; \mathsf{raise}\ z); \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle\downarrow^{<W''.k}$.
   - To show: consistent(W'') and $\langle h_2''; \mathsf{raise}\ v_2\rangle\downarrow$
   - Note that $\langle h_1''; K_1'[(\mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot; \mathsf{raise}\ v_1); \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle\downarrow^{<W''.k}$ implies $\langle h_1''[l_x{\mapsto}\mathsf{tt}]; K_1'[\mathsf{raise}\ v_1]\rangle\downarrow^{<W''.k}$ and $h_1''(l_y) = \mathsf{ff}$.
   - The latter means $W'' = W''_{\langle \mathsf{tt},\mathsf{ff}\rangle}$ or $W'' = W''_{\langle \mathsf{ff},\mathsf{ff}\rangle}$.
   - In any case it is easy to see that $W''_{\langle \mathsf{tt},\mathsf{ff}\rangle} \sqsupseteq^{\mathsf{pub}} W'$.
   - Also, $(h_1''[l_x{\mapsto}\mathsf{tt}], h_2'') : W''_{\langle \mathsf{tt},\mathsf{ff}\rangle}$.
   - By monotonicity (Lemma 10), $(W''_{\langle \mathsf{tt},\mathsf{ff}\rangle}, v_1, v_2) \in \mathcal{V}[\![\mathsf{exn}]\!]\emptyset$.
   - Finally, consistent($W''_{\langle \mathsf{tt},\mathsf{ff}\rangle}$) would imply consistent(W'').
   - The claims then follow from instantiating $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.

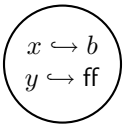
- Using monotonicity (Lemma 10), we easily get $(h_1', h_2') : W''$.
- Instantiating $(W'', e_1'[\lambda z.\, \mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot/g], e_2'[\lambda z.\, \bot/g]) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$ thus yields consistent(W'') and $\langle h_2'; K_2'[e_2'[\lambda z.\, \bot/g]]\rangle\downarrow$.
- The former implies consistent(W') and the latter implies $\langle h_2'; K_2'[(\lambda g.\, e_2')\ (\lambda z.\, \bot)]\rangle\downarrow$.

We show $\cdot;\cdot;\cdot \vdash e_2 \precsim_{\log} e_1 : \tau$.

- This reduces to showing $(W, e_2, e_1) \in \mathcal{E}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, where $W \in \mathcal{S}[\![\cdot]\!]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_2]\rangle\downarrow^{<W.k}$.
- To show: consistent(W) and $\langle h_2; K_2[e_1]\rangle\downarrow$
- Observe that $\langle h_2; K_2[e_1]\rangle\downarrow$ if $\langle h_2 \uplus \{l_x{\mapsto}\mathsf{ff}\} \uplus \{l_y{\mapsto}\mathsf{ff}\}; K_2[\widehat{e_1}[l_x/x][l_y/y]]\rangle\downarrow$, where $\widehat{e_1}$ is the function value in e_1 and l_y any free location.
- Let
  - $H(\langle\rangle) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \mathrm{HeapAtom} \mid \widetilde{h_2}(l_y) = \mathsf{ff} \wedge l_x \in \mathrm{dom}(h_2)\}$

– $\iota := (\langle\rangle, \emptyset^*, \emptyset^*, \emptyset, H)$
– $\widehat{W} := W[\Sigma_2 := W.\Sigma_2, l_x{:}\mathsf{bool}, l_y{:}\mathsf{bool}][\omega := W.\omega, \iota]$

The island represents the following STS:



- Note that $\widehat{W} \sqsupseteq^{\mathsf{pub}} W$ and $(h_1, h_2 \uplus \{l_x{\mapsto}\mathsf{ff}\} \uplus \{l_y{\mapsto}\mathsf{ff}\}) : \widehat{W}$.
- Because of $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\emptyset$ it thus suffices to show $(\widehat{W}, e_2, \widehat{e_1}[l_x/x][l_y/y]) \in \mathcal{V}[\![\tau]\!]\emptyset$.
- So suppose $W' \sqsupseteq W$, $(W', f_1, f_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1'[f_1\ (\lambda\_.\ \bot)]\rangle\downarrow^{<W'.k}$.
- To show: consistent(W') and $\langle h_2'; K_2'[\mathsf{try}\ f_2\ (\lambda z.\ \mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot)\ \mathsf{with}\ z.(\mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot; \mathsf{raise}\ z); \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle\downarrow$
- We show $(W', f_1\ (\lambda\_.\ \bot), f_2\ (\lambda\_.\ \mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot)) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$:
  – Since $(W', f_1, f_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, it suffices to show $(W', (\lambda\_.\ \bot), (\lambda\_.\ \mathsf{if}\ !l_x = \mathsf{ff}\ \mathsf{then}\ l_y := \mathsf{tt}\ \mathsf{else}\ \bot)) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$.
  – This holds trivially, because $\langle h_1''; K_1''[\bot]\rangle$ diverges for any h_1'' and K_1''.
- We show $(W', K_1', K_2'[\mathsf{try}\ \bullet\ \mathsf{with}\ z.(\mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot; \mathsf{raise}\ z); \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$:
  1. – So first suppose $W'' \sqsupseteq^{\mathsf{pub}} W'$, $(h_1'', h_2'') : W''$, and $\langle h_1''; K_1'[\langle\rangle]\rangle\downarrow^{<W''.k}$.
     – To show: consistent(W'') and $\langle h_2''; K_2'[\mathsf{try}\ \langle\rangle\ \mathsf{with}\ z.(\mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot; \mathsf{raise}\ z); \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle\downarrow$
     – From $(h_1'', h_2'') : W''$ we know $h_2''(l_y) = \mathsf{ff}$.
     – Therefore, $\langle h_2''; K_2'[\mathsf{try}\ \langle\rangle\ \mathsf{with}\ z.(\mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot; \mathsf{raise}\ z); \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle\downarrow$ if $\langle h_2''[l_x{\mapsto}\mathsf{tt}]; K_2'[\langle\rangle]\rangle\downarrow$.
     – Note that $(h_1'', h_2'') : W''$ implies $(h_1'', h_2''[l_x{\mapsto}\mathsf{tt}]) : W''$.
     – The claims thus follow from instantiating $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$ with $(W'', \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$.
  2. – Now suppose $W'' \sqsupseteq^{\mathsf{pub}} W'$, $(W'', v_1, v_2) \in \mathcal{V}[\![\mathsf{exn}]\!]\emptyset$, $(h_1'', h_2'') : W''$ and $\langle h_1''; K_1'[\mathsf{raise}\ v_1]\rangle\downarrow^{<W''}$.
     – To show: consistent(W'') and $\langle h_2''; K_2'[\mathsf{try}\ \mathsf{raise}\ v_2\ \mathsf{with}\ z.(\mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot; \mathsf{raise}\ z); \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle\downarrow < W''.k$.
     – From $(h_1'', h_2'') : W''$ we know $h_2''(l_y) = \mathsf{ff}$.
     – Hence, $\langle h_2''; K_2'[(\mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot; \mathsf{raise}\ v_2); \mathsf{if}\ !l_y = \mathsf{ff}\ \mathsf{then}\ l_x := \mathsf{tt}\ \mathsf{else}\ \bot]\rangle\downarrow^{<W''.k}$ if $\langle h_2''[l_x{\mapsto}\mathsf{tt}]; K_2'[\mathsf{raise}\ v_2]\rangle\downarrow^{<W''.k}$.
     – Note that $(h_1'', h_2'') : W''$ implies $(h_1'', h_2''[l_x{\mapsto}\mathsf{tt}]) : W''$.
     – The claims thus follow from instantiating $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
- Combining these yields the claims.

4.2.2 Callback With Lock

$$
\begin{array}{lcl}
C & = & \mathsf{let}\ b = \mathsf{ref}\ \mathsf{tt}\ \mathsf{in} \\
 & & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in} \\
 & & \langle \lambda f{:}\mathsf{unit} \to \mathsf{unit}.\ \mathsf{if}\ !b\ \mathsf{then}\ (b := \mathsf{ff}; \bullet; b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle, \\
 & & \ \lambda z{:}\mathsf{unit}.\ !x\rangle \\
e_1 & = & C[f\ \langle\rangle; x := !x + 1] \\
e_2 & = & C[\mathsf{let}\ n = !x\ \mathsf{in}\ f\ \langle\rangle; x := n + 1]
\end{array}
$$

Here is a context that is able to distinguish e_1 and e_2 using call/cc:

$$
\begin{array}{l}
\mathsf{let}\ \langle inc, poll\rangle = \bullet\ \mathsf{in} \\
\mathsf{call/cc}\,(k_0.\ \mathsf{let}\ r = \mathsf{ref}\ k_0\ \mathsf{in} \\
\qquad\qquad \mathsf{let}\ b = \mathsf{ref}\ \mathsf{tt}\ \mathsf{in} \\
\qquad\qquad \mathsf{let}\ g = (\lambda\_.\,\mathsf{call/cc}\,(k.\ r := k))\ \mathsf{in} \\
\qquad\qquad \mathsf{let}\ h = (\lambda\_.\,b := \mathsf{ff}; \mathsf{throw}\ \langle\rangle\ \mathsf{to}\ !r)\ \mathsf{in} \\
\qquad\qquad inc\ g; (\mathsf{if}\ !b\ \mathsf{then}\ inc\ h\ \mathsf{else}\ \langle\rangle); \mathsf{if}\ poll\ \langle\rangle = 2\ \mathsf{then}\ \langle\rangle\ \mathsf{else}\ \bot)
\end{array}
$$

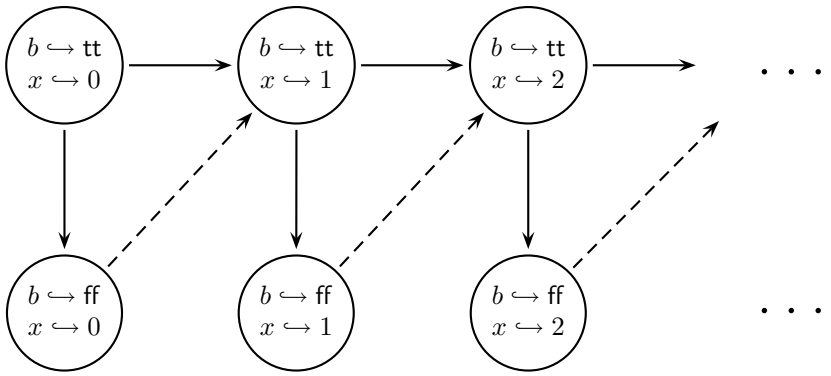
When it calls the increment method f the second time, the callback jumps back to its continuation during f's first run. In that continuation, n (on the right) is still bound to 0, although x points to 1 now. It is easy to verify that $C'[e_1]$ terminates, but $C'[e_2]$ does not.

In the absence of call/cc but presence of exceptions, the programs are equivalent.
We show $\cdot;\cdot;\cdot \vdash e_1 \precsim_{\log} e_2 : ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \times (\mathsf{unit} \to \mathsf{int})$:

- This reduces to showing $(W, e_1, e_2) \in \mathcal{E}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \times (\mathsf{unit} \to \mathsf{int})]\!]\emptyset$, where $W \in \mathcal{S}[\![\cdot]\!]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \times (\mathsf{unit} \to \mathsf{int})]\!]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_1]\rangle\downarrow^{<W.k}$.
- To show: consistent(W) and $\langle h_2; K_2[e_2]\rangle\downarrow$
- $\langle h_1; K_1[e_1]\rangle\downarrow^{<W.k}$ implies $\langle \widehat{h_1}; K_1[v_1]\rangle\downarrow^{<W.k}$, where
  - $v_1 := \langle v_1^1, v_1^2\rangle$,
  - $v_1^1 := \lambda f.\ \mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; f\ \langle\rangle; l_x := !l_x + 1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle$,
  - $v_1^2 := \lambda z.\ !l_x$,
  - $\widehat{h_1} := h_1 \uplus \{l_b \mapsto \mathsf{tt}\} \uplus \{l_x \mapsto 0\}$, and
  - l_b, l_x are fresh and distinct.
- Similarly, $\langle h_2; K_2[e_2]\rangle\downarrow$ if $\langle \widehat{h_2}; K_2[v_2]\rangle\downarrow$, where
  - $v_2 := \langle v_2^1, v_2^2\rangle$,
  - $v_2^1 := \lambda f.\ \mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; \mathsf{let}\ n = !l_x\ \mathsf{in}\ f\ \langle\rangle; l_x := n + 1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle$,
  - $v_2^2 := \lambda z.\ !l_x$, and
  - $h_2' := h_2 \uplus \{l_b \mapsto \mathsf{tt}\} \uplus \{l_x \mapsto 0\}$.

- Let
  - $H(\langle o, i\rangle) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \text{HeapAtom} \mid \widetilde{h_1}(l_b) = \widetilde{h_2}(l_b) = o \wedge \widetilde{h_1}(l_x) = \widetilde{h_2}(l_x) = i\}$
  - $\varphi := \{(\langle \mathsf{tt}, i\rangle, \langle \mathsf{tt}, i+1\rangle) \mid i \in \mathbb{N}\}^*$
  - $\delta := (\varphi \uplus \{(\langle \mathsf{tt}, i\rangle, \langle \mathsf{ff}, i\rangle) \mid i \in \mathbb{N}\} \uplus \{(\langle \mathsf{ff}, i\rangle, \langle \mathsf{tt}, i+1\rangle) \mid i \in \mathbb{N}\})^*$
  - $\iota_s := (s, \delta, \varphi, \emptyset, H)$
  - $W_s := W[\Sigma_1 := W.\Sigma_1, l_b{:}\mathsf{unit}, l_x{:}\mathsf{int}][\omega := W.\omega, \iota_s]$

  The island represents the following STS:



- It is easy to see that $W_{\langle \mathsf{tt},0\rangle} \sqsupseteq^{\mathsf{pub}} W$ and, using monotonicity (Lemma 10), that $(\widehat{h_1}, \widehat{h_2}) : W_{\langle \mathsf{tt},0\rangle}$.
- It thus suffices to show $(W_{\langle \mathsf{tt},0\rangle}, v_1, v_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \times (\mathsf{unit} \to \mathsf{int})]\!]\emptyset$, which splits into two parts.
- We show $(W_{\langle \mathsf{tt},0\rangle}, v_1^1, v_2^1) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$:
  - Suppose $W' \sqsupseteq W_{\langle \mathsf{tt},0\rangle}$, $(W', \lambda y.\, e_3, \lambda y.\, e_4) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$, $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1'[\mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; (\lambda y.\, e_3)\ \langle\rangle; l_x := !l_x{+}1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle]\rangle \downarrow^{<W'.k}$.
  - To show: consistent(W') and $\langle h_2'; K_2'[\mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; \mathsf{let}\ n = !l_x\ \mathsf{in}\ (\lambda y.\, e_4)\ \langle\rangle; l_x := n{+}1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle]\rangle \downarrow$
  - Notation: we write W_s' to denote the world obtained from W' by setting our island's current state to s.
  - Case $W' = W'_{\langle \mathsf{tt},i\rangle}$ for some i:
    - Then $(h_1', h_2') : W'$ implies $h_1'(l_b) = h_2'(l_b) = \mathsf{tt}$ and $h_1'(l_x) = h_2'(l_x) = i$.
    - Hence $\langle h_1'; K_1'[\mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; (\lambda y.\, e_3)\ \langle\rangle; l_x := !l_x + 1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle]\rangle \downarrow^{<W'.k}$ implies $\langle h_1'[l_b{\mapsto}\mathsf{ff}]; K_1'[e_3[\langle\rangle/y]; (\lambda y.\, e_3)\ \langle\rangle; l_x := !l_x + 1; l_b := \mathsf{tt})\rangle\langle\rangle \downarrow^{<W'.k}$.
    - Similarly,
      $\langle h_2'; K_2'[\mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; \mathsf{let}\ n = !l_x\ \mathsf{in}\ (\lambda y.\, e_4)\ \langle\rangle; l_x := n + 1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle]\rangle \downarrow$ if $\langle h_2'[l_b{\mapsto}\mathsf{ff}]; K_2'[e_4[\langle\rangle/y]; l_x := i + 1; l_b := \mathsf{tt})\rangle \downarrow$.

* It is easy to see that $W'_{\langle \mathsf{ff},i\rangle} \sqsupseteq^{\mathsf{pub}} W'$ and, using monotonicity (Lemma 10), that $(h'_1[l_b{\mapsto}\mathsf{ff}], h'_2[l_b{\mapsto}\mathsf{ff}]) : W'_{\langle \mathsf{ff},i\rangle}$.
* Also, consistent($W'_{\langle \mathsf{ff},i\rangle}$) would imply consistent(W').
* Since $(W'_{\langle \mathsf{ff},i\rangle}, \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$ and thus $(W'_{\langle \mathsf{ff},i\rangle}, e_3[\langle\rangle/y], e_4[\langle\rangle/y]) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$, it suffices to show $(W'_{\langle \mathsf{ff},i\rangle}, K'_1[\bullet; l_x := !l_x + 1; l_b := \mathsf{tt}], K'_2[\bullet; l_x := i + 1; l_b := \mathsf{tt}]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
* First suppose $W'' \sqsupseteq^{\mathsf{pub}} W'_{\langle \mathsf{ff},i\rangle}$, $(h''_1, h''_2) : W''$, and $\langle h''_1; K'_1[\langle\rangle; l_x := !l_x{+}1; l_b := \mathsf{tt}]\rangle \downarrow^{<W''.k}$.
* To show: consistent(W'') and $\langle h''_2; K'_2[\langle\rangle; l_x := i + 1; l_b := \mathsf{tt}]\rangle \downarrow$
* Note that the only public successor of $\langle \mathsf{ff}, i\rangle$ is $\langle \mathsf{ff}, i\rangle$ itself and therefore $W'' = W''_{\langle \mathsf{ff},i\rangle}$.
* Hence $(h''_1, h''_2) : W''$ implies $h''_1(l_x) = i$ and thus $\langle h''_1[l_x{\mapsto}(i{+}1)][l_b{\mapsto}\mathsf{tt}]; K'_1[\langle\rangle]\rangle \downarrow^{<W''.k}$.
* Note that $\langle h''_2; K'_2[\langle\rangle; l_x := i + 1; l_b := \mathsf{tt}]\rangle \downarrow$ if $\langle h''_2[l_x{\mapsto}(i + 1)][l_b{\mapsto}\mathsf{tt}]; K'_2[\langle\rangle]\rangle \downarrow$.
* It is easy to see, using monotonicity (Lemma 10), that $W''_{\langle \mathsf{tt},i+1\rangle} \sqsupseteq^{\mathsf{pub}} W'_{\langle \mathsf{tt},i+1\rangle} \sqsupseteq^{\mathsf{pub}} W'$.
* Furthermore, using $(h''_1, h''_2) : W''$, $W''_{\langle \mathsf{tt},i+1\rangle} \sqsupseteq W''$, and monotonicity (Lemma 10) it is easy to see that $(h''_1[l_x{\mapsto}(i + 1)][l_b{\mapsto}\mathsf{tt}], h''_2[l_x{\mapsto}(i + 1)][l_b{\mapsto}\mathsf{tt}]) : W''_{\langle \mathsf{tt},i+1\rangle}$.
* Also, consistent($W''_{\langle \mathsf{tt},i+1\rangle}$) would imply consistent(W'').
* Since $(W''_{\langle \mathsf{tt},i+1\rangle}, \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$, the claims therefore follow from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
* Now suppose $W'' \sqsupseteq^{\mathsf{pub}} W'_{\langle \mathsf{ff},i\rangle}$ and $(W'', v'_1, v'_2) \in \mathcal{V}[\![\mathsf{exn}]\!]\emptyset$.
* To show: $(W'', K'_1[\mathsf{raise}\ v'_1; l_x := !l_x{+}1; l_b := \mathsf{tt}], K'_2[\mathsf{raise}\ v'_2; l_x := i{+}1; l_b := \mathsf{tt}]) \in \mathcal{O}$
* By Lemma 12 it suffices to show $(W'', K'_1[\mathsf{raise}\ v'_1], K'_2[\mathsf{raise}\ v'_2]) \in \mathcal{O}$, which follows from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.

– Case $W' = W'_{\langle \mathsf{ff},i\rangle}$ for some i:

* Then $(h'_1, h'_2) : W'$ implies $h'_1(l_b) = h'_2(l_b) = \mathsf{ff}$ and $h'_1(l_x) = h'_2(l_x) = i$.
* Hence $\langle h'_1; K'_1[\mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; (\lambda y.\, e_3)\ \langle\rangle; l_x := !l_x + 1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle]\rangle \downarrow^{<W'.k}$ implies $\langle h'_1; K'_1[\langle\rangle]\rangle \downarrow^{<W'.k}$.
* Similarly, $\langle h'_2; K'_2[\mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; \mathsf{let}\ n = !l_x\ \mathsf{in}\ (\lambda y.\, e_4)\ \langle\rangle; l_x := n{+}1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle]\rangle \downarrow$ if $\langle h'_2; K'_2[\langle\rangle]\rangle \downarrow$.
* Since $(W', \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$ the claims then follow from $(W', K'_1, K'_2) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.

• We show $(W_{\langle \mathsf{tt},0\rangle}, v^2_1, v^2_2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{int}]\!]\emptyset$:

– Suppose $W' \sqsupseteq W_{\langle \mathsf{tt},0\rangle}$, $(W', K'_1, K'_2) \in \mathcal{K}[\![\mathsf{int}]\!]\emptyset$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K'_1[!l_x]\rangle \downarrow^{<W'.k}$.

– To show: consistent(W') and $\langle h'_2; K'_2[!l_x]\rangle \downarrow$

– From $(h'_1, h'_2) : W'$ and the way we constructed our island we know $h'_1(l_x) = h'_2(l_x) = i$, for some i.

– Hence $\langle h'_1; K'_1[!l_x]\rangle \downarrow^{<W'.k}$ implies $\langle h'_1; K'_1[i]\rangle \downarrow^{<W'.k}$.

– Similarly, $\langle h'_2; K'_2[!l_x]\rangle \downarrow$ if $\langle h'_2; K'_2[i]\rangle \downarrow$.

– Since $(W', i, i) \in \mathcal{V}[\![\mathsf{int}]\!]\emptyset$ the claims then follow from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\![\mathsf{int}]\!]\emptyset$.

4.2.3 Higher-Order Profiling

$$p \quad = \quad \lambda f.\, \mathsf{let}\ c = \mathsf{ref}\ 0\ \mathsf{in}\ \langle \lambda x.\, (c := !c + 1; f\ x), \lambda\_.\, !c \rangle$$

p is a higher-order function that takes a function f and returns a tracked version of it, i.e., a function that behaves like f except that each time it is called a local counter is incremented by 1. f also returns a function for reading the current value of that counter.

Establishing the equivalence of the following two programs can be seen as a partial correctness proof of the profiling operation:

$$\begin{array}{lcl} e_1 & = & \lambda f.\, \lambda g.\, \lambda a.\, \mathsf{let}\ \langle g', g'' \rangle = p\ g\ \mathsf{in}\ (f\ g'; g'\ \langle\rangle; a\ g'; g''\ \langle\rangle) \\ e_2 & = & \lambda f.\, \lambda g.\, \lambda a.\, \mathsf{let}\ \langle g', g'' \rangle = p\ g\ \mathsf{in}\ (f\ g'; g\ \langle\rangle; a\ g'; g''\ \langle\rangle + 1) \end{array}$$

The proof goes as follows. We construct an island consisting of two states. The first one, asserting that the counter has the same value on both sides, has a private transition to the second. The second asserts that the value of the counter is larger by 1 on the left side than on the right side.

Initially, we are in the first state (c points to 0 on both sides). When f returns, we know that we are still in that state, because there is no public transition leading anywhere else. (Of course c might have increased by now, but if so, then by the same amount on both sides: the only way f can touch the counter is by running its argument.) Now we call the tracked version of g on the left side and the original g on the right side, thus incrementing the counter only on the left side. Accordingly, we have to move along the private transition to the second state. Then a is called and, since there is no other state reachable from here, c will still point to a number larger by one on the left than on the right side when a returns. Consequently, $g''\ \langle\rangle$ on the left will yield the same value as $g''\ \langle\rangle + 1$ on the right.

Formally, we show
$\cdot; \cdot; \cdot \vdash e_1 \precsim_{\log} e_2 : ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to (\mathsf{unit} \to \mathsf{unit}) \to ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{int}$.

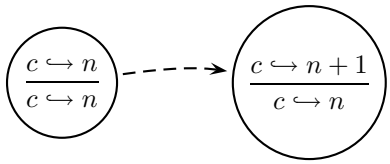
- This reduces to showing
  $(\widetilde{W}, e_1, e_2) \in \mathcal{V}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to (\mathsf{unit} \to \mathsf{unit}) \to ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{int}]\!]\emptyset$,
  where $\widetilde{W} \in \mathcal{S}[\![\cdot]\!]$.
- This boils down to showing $(W, e_1', e_2') \in \mathcal{E}[\![\mathsf{int}]\!]\emptyset$, where
  - $W \sqsupseteq \widetilde{W}$,
  - $e_1' := \mathsf{let}\ \langle g', g'' \rangle = p\ g_1\ \mathsf{in}\ (f_1\ g'; g'\ \langle\rangle; a_1\ g'; g''\ \langle\rangle)$,
  - $e_2' := \mathsf{let}\ \langle g', g'' \rangle = p\ g_2\ \mathsf{in}\ (f_2\ g'; g_2\ \langle\rangle; a_2\ g'; g''\ \langle\rangle + 1)$,
  - $(W, f_1, f_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$,
  - $(W, g_1, g_2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$, and
  - $(W, a_1, a_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{int}]\!]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_1'] \rangle \downarrow^{<W.k}$.
- To show: consistent(W) and $\langle h_2; K_2[e_2'] \rangle \downarrow$
- $\langle h_1; K_1[e_1'] \rangle \downarrow^{<W.k}$ implies $\langle \widehat{h_1}; K_1[f_1\ g_1'; g_1'\ \langle\rangle; a_1\ g_1'; (\lambda\_.\, !l_1)\ \langle\rangle] \rangle \downarrow^{<W.k}$, where

- $\widehat{h_1} := h_1 \uplus \{l_1 \mapsto 0\}$,
- $g_1' := \lambda x.\, (l_1 := !l_1 + 1; g_1\ x)$, and
- l_1 is fresh.

- Similarly, $\langle h_2; K_2[e_2']\rangle\downarrow$ if $\langle \widehat{h_2}; K_2[f_2\ g_2'; g_2\ \langle\rangle; a_2\ g_2'; (\lambda\_.\, !l_2)\ \langle\rangle + 1]\rangle\downarrow$, where
  - $\widehat{h_2} := h_2 \uplus \{l_2 \mapsto 0\}$,
  - $g_2' := \lambda x.\, (l_2 := !l_2 + 1; g_2\ x)$, and
  - l_2 is fresh.

- Let
  - $H(n) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \text{HeapAtom} \mid \widetilde{h_1}(l_1) = \widetilde{h_2}(l_2) + n\}$
  - $\iota_s := (s, \{(0,1)\}^*, \emptyset^*, \emptyset, H)$
  - $W_s := W[\Sigma_1 := W.\Sigma_1, l_1{:}\mathsf{int}][\Sigma_2 := W.\Sigma_2, l_2{:}\mathsf{int}][\omega := W.\omega, \iota_s]$

  The island represents the following STS:



- It is easy to see that $W_0 \sqsupseteq^{\mathsf{pub}} W$ and, using monotonicity (Lemma 10), that $(\widehat{h_1}, \widehat{h_2}) : W_0$.
- We show $(W_0, f_1\ g_1', f_2\ g_2') \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$:
  - Since $(W, f_1, f_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, it suffices to show $(W_0, g_1', g_2') \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$.
  - So suppose $W' \sqsupseteq W_0$, $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1'[l_1 := !l_1 + 1; g_1\ \langle\rangle]\rangle\downarrow^{<W'.k}$.
  - To show: consistent(W') and $\langle h_2'; K_2'[l_2 := !l_2 + 1; g_2\ \langle\rangle]\rangle\downarrow$
  - $\langle h_1'; K_1'[l_1 := !l_1 + 1; g_1\ \langle\rangle]\rangle\downarrow^{<W'.k}$ implies $\langle h_1'[l_1 \mapsto h_1'(l_1) + 1]; K_1'[g_1\ \langle\rangle]\rangle\downarrow^{<W'.k}$.
  - Similarly, $\langle h_2'; K_2'[l_2 := !l_2 + 1; g_2\ \langle\rangle]\rangle\downarrow$ if $\langle h_2'[l_2 \mapsto h_2'(l_2) + 1]; K_2'[g_2\ \langle\rangle]\rangle\downarrow$.
  - Incrementing both counters by one preserves either invariant and hence it is easy to see that $(h_1'[l_1 \mapsto h_1'(l_1) + 1], h_2'[l_2 \mapsto h_2'(l_2) + 1]) : W'$.
  - It therefore suffices to show $(W', g_1\ \langle\rangle, g_2\ \langle\rangle) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$, which follows from $(W, g_1, g_2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$ and $(W', \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$.
- It thus suffices to show $(W_0, K_1[\bullet; g_1'\ \langle\rangle; a_1\ g_1'; (\lambda\_.\, !l_1)\ \langle\rangle], K_2[\bullet; g_2\ \langle\rangle; a_2\ g_2'; (\lambda\_.\, !l_2)\ \langle\rangle + 1]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
- So first suppose $W' \sqsupseteq^{\mathsf{pub}} W_0$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1[\langle\rangle; g_1'\ \langle\rangle; a_1\ g_1'; (\lambda\_.\, !l_1)\ \langle\rangle]\rangle\downarrow^{<W'.k}$, which implies $\langle \widehat{h_1'}; K_1[g_1\ \langle\rangle; a_1\ g_1'; (\lambda\_.\, !l_1)\ \langle\rangle]\rangle\downarrow^{<W'.k}$, where $\widehat{h_1'} := h_1'[l_1 \mapsto h_1'(l_1) + 1]$.

- To show: consistent(W') and $\langle h_2'; K_2[\langle\rangle; g_2\ \langle\rangle; a_2\ g_2'; (\lambda\_.\, !l_2)\ \langle\rangle + 1]\rangle\downarrow$, *i.e.,* $\langle h_2'; K_2[g_2\ \langle\rangle; a_2\ g_2'; (\lambda\_.\, !l_2)\ \langle\rangle + 1]\rangle\downarrow$
- Notation: we write W_s' for the world obtained from W' by setting the current state of our island to s.
- Note that $W_1' \sqsupseteq W'$.
- Using $(h_1', h_2') : W'$ and monotonicity (Lemma 10), it is then easy to see that $(\widehat{h_1'}, h_2') : W_1'$.
- From $(W, g_1, g_2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$ and $(W_1', \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$ we get $(W_1', g_1\ \langle\rangle, g_2\ \langle\rangle) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$.
- Furthermore, it is obvious that consistent(W_1') would imply consistent(W').
- It thus suffices to show $(W_1', K_1[\bullet; a_1\ g_1'; (\lambda\_.\, !l_1)\ \langle\rangle], K_2[\bullet; a_2\ g_2'; (\lambda\_.\, !l_2)\ \langle\rangle + 1]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
- So first suppose $W'' \sqsupseteq^{\mathsf{pub}} W_1'$, $(h_1'', h_2'') : W''$, and $\langle h_1''; K_1[\langle\rangle; a_1\ g_1'; (\lambda\_.\, !l_1)\ \langle\rangle]\rangle\downarrow^{<W''.k}$, *i.e.,* $\langle h_1''; K_1[a_1\ g_1'; (\lambda\_.\, !l_1)\ \langle\rangle]\rangle\downarrow^{<W''.k}$.
  - To show: consistent(W'') and $\langle h_2''; K_2[\langle\rangle; a_2\ g_2'; (\lambda\_.\, !l_2)\ \langle\rangle + 1]\rangle\downarrow$, *i.e.,* $\langle h_2''; K_2[a_2\ g_2'; (\lambda\_.\, !l_2)\ \langle\rangle + 1]\rangle\downarrow$.
  - Following the proof of $(W_0, f_1\ g_1', f_2\ g_2') \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$ above, we can easily show $(W'', a_1\ g_1', a_2\ g_2') \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$.
  - It thus suffices to show $(W'', K_1[\bullet; (\lambda\_.\, !l_1)\ \langle\rangle], K_2[\bullet; (\lambda\_.\, !l_2)\ \langle\rangle + 1]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
  - So first suppose $W''' \sqsupseteq^{\mathsf{pub}} W''$, $(h_1''', h_2''') : W'''$, and $\langle h_1'''; K_1[\langle\rangle; (\lambda\_.\, !l_1)\ \langle\rangle]\rangle\downarrow^{<W'''.k}$.
    - To show: consistent(W''') and $\langle h_2'''; K_2[\langle\rangle; (\lambda\_.\, !l_2)\ \langle\rangle + 1]\rangle\downarrow$
    - From $(h_1''', h_2''') : W'''$ and $W''' \sqsupseteq^{\mathsf{pub}} W''$ we know $h_1'''(l_1) = n+1$ and $h_2'''(l_2) = n$, for some n.
    - Hence $\langle h_1'''; K_1[\langle\rangle; (\lambda\_.\, !l_1)\ \langle\rangle]\rangle\downarrow^{<W'''.k}$ implies $\langle h_1'''; K_1[n+1]\rangle\downarrow^{<W'''.k}$.
    - Similarly $\langle h_2'''; K_2[\langle\rangle; (\lambda\_.\, !l_2)\ \langle\rangle + 1]\rangle\downarrow$ if $\langle h_2'''; K_2[n+1]\rangle\downarrow$.
    - It is easy to see that $W''' = W_1''' \sqsupseteq^{\mathsf{pub}} W_1'' \sqsupseteq^{\mathsf{pub}} W_1' \sqsupseteq^{\mathsf{pub}} W$.
    - Since $(W''', n+1, n+1) \in \mathcal{V}[\![\mathsf{int}]\!]\emptyset$, the claims then follow from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{int}]\!]\emptyset$.
  - Now suppose $W''' \sqsupseteq^{\mathsf{pub}} W''$ and $(W''', v_1, v_2) \in \mathcal{V}[\![\mathsf{exn}]\!]\emptyset$.
    - To show: $(W''', K_1[\mathsf{raise}\ v_1; (\lambda\_.\, !l_1)\ \langle\rangle], K_2[\mathsf{raise}\ v_2; (\lambda\_.\, !l_2)\ \langle\rangle + 1]) \in \mathcal{O}$
    - By Lemma 12 it suffices to show $(W''', K_1[\mathsf{raise}\ v_1], K_2[\mathsf{raise}\ v_2]) \in \mathcal{O}$.
    - Since $W' \sqsupseteq^{\mathsf{pub}} W$ we know $W_1' \sqsupseteq^{\mathsf{pub}} W$ and thus $W''' \sqsupseteq^{\mathsf{pub}} W$.
    - The claim then follows from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{int}]\!]\emptyset$.
- Now suppose $W'' \sqsupseteq^{\mathsf{pub}} W_1'$ and $(W'', v_1, v_2) \in \mathcal{V}[\![\mathsf{exn}]\!]\emptyset$.
  - To show: $(W'', K_1[\mathsf{raise}\ v_1; a_1\ g_1'; (\lambda\_.\, !l_1)\ \langle\rangle], K_2[\mathsf{raise}\ v_2; a_2\ g_2'; (\lambda\_.\, !l_2)\ \langle\rangle + 1]) \in \mathcal{O}$
  - By Lemma 12 it suffices to show $(W'', K_1[\mathsf{raise}\ v_1], K_2[\mathsf{raise}\ v_2]) \in \mathcal{O}$.
  - Since $W' \sqsupseteq^{\mathsf{pub}} W$ we know $W_1' \sqsupseteq^{\mathsf{pub}} W$ and thus $W'' \sqsupseteq^{\mathsf{pub}} W$.
  - The claim then follows from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{int}]\!]\emptyset$.

- Now suppose $W' \sqsupseteq^{\mathsf{pub}} W_0$ and $(W', v_1, v_2) \in \mathcal{V}[\![\mathsf{exn}]\!]\emptyset$.

– To show: $(W', K_1[\mathsf{raise}\ v_1; g_1'\ \langle\rangle; a_1\ g_1'; (\lambda\_.\, !l_1)\ \langle\rangle], K_2[\mathsf{raise}\ v_2; g_2\ \langle\rangle; a_2\ g_2'; (\lambda\_.\, !l_2)\ \langle\rangle + 1]) \in \mathcal{O}$

– By Lemma 12 it suffices to show $(W', K_1[\mathsf{raise}\ v_1], K_2[\mathsf{raise}\ v_2]) \in \mathcal{O}$.

– Since $W' \sqsupseteq^{\mathsf{pub}} W$, this follows from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{int}]\!]\emptyset$.

4.3 HOSC

4.3.1 One-Shot Continuations

$$\begin{array}{lcl}
\tau_\alpha & := & \mathsf{cont}\,\alpha \to \alpha \\[2ex]
\mathsf{callcc1} & := & \Lambda\alpha.\lambda f{:}\tau_\alpha.\,\mathsf{let}\ b = \mathsf{ref}\ \mathsf{tt}\ \mathsf{in} \\
& & \qquad \mathsf{call/cc}_\alpha\,(x. \\
& & \qquad f\ (\mathsf{cont}_\alpha\ (\mathsf{let}\ y = \bullet\ \mathsf{in}\ \mathsf{if}\ !b\ \mathsf{then}\ (b := \mathsf{ff}; \mathsf{throw}_{\mathsf{unit}}\ y\ \mathsf{to}\ x)\ \mathsf{else}\ \bot_{\mathsf{unit}}))) \\[2ex]
\mathsf{fix}\ f(x).\ e & := & \lambda y.\,(\mathsf{unroll}\ v)\ v\ y \quad \text{where } v = \mathsf{roll}\ (\lambda z.\,(\lambda f.\,\lambda x.\,e)\ (\lambda y.\,\mathsf{unroll}\ z\ z\ y)) \text{ for } y, z \notin \mathrm{fv}(e) \\[2ex]
G_r^\alpha & := & \mathsf{fix}\ g(f).\ \mathsf{let}\ x = \mathsf{callcc1}\ \alpha\ (\lambda z{:}\mathsf{cont}\,\alpha.\,(r := z; f\ (\mathsf{cont}_\alpha\ (\mathsf{throw}_{\mathsf{unit}}\ \bullet\ \mathsf{to}\ !r)))) \\
& & \qquad \mathsf{callcc1}\ \alpha\ (\lambda z{:}\mathsf{cont}\,\alpha.\,g\ (\lambda_{:}\mathsf{cont}\,\alpha.\,\mathsf{throw}_{\mathsf{unit}}\ x\ \mathsf{to}\ z)) \\[2ex]
\mathsf{callcc}' & := & \Lambda\alpha.\lambda f{:}\tau_\alpha.\,\mathsf{let}\ r = \mathsf{ref}\ (\mathsf{cont}_\alpha\ \bullet)\ \mathsf{in}\ G_r^\alpha\ f \\[2ex]
\mathsf{callcc} & := & \Lambda\alpha.\lambda f{:}\tau_\alpha.\,\mathsf{call/cc}_\alpha\,(x.\ f\ x)
\end{array}$$

We show $\cdot;\cdot;\cdot \vdash \mathsf{callcc} \precsim_{\log} \mathsf{callcc}' : \forall\alpha.\,\tau_\alpha \to \alpha$.

- This reduces to showing $(W_0, \mathsf{callcc}, \mathsf{callcc}') \in \mathcal{V}[\![\forall\alpha.\,\tau_\alpha \to \alpha]\!]\emptyset$, where $W_0 \in \mathcal{S}[\![\cdot]\!]$.
- So suppose $W_1 \sqsupseteq W_0$ and $(\tau_1, \tau_2, r) \in \mathrm{SomeValRel}$.
- To show: $(W_1, \lambda f.\,\mathsf{call/cc}\ (x.\ f\ x), \lambda f.\,\mathsf{let}\ r = \mathsf{ref}\ (\mathsf{cont}\ \bullet)\ \mathsf{in}\ G_r^{\tau_2}\ f) \in \mathcal{V}[\![\tau_\alpha \to \alpha]\!]\rho$, where $\rho := \alpha{\mapsto}(\tau_1, \tau_2, r)$
- So suppose $W \sqsupseteq W_1$, $(W, f_1, f_2) \in \mathcal{V}[\![\tau_\alpha]\!]\rho$, $(W, K_1, K_2) \in \mathcal{K}[\![\alpha]\!]\rho$, $(h_1, h_2) : W$, and $\langle h_1; K_1[\mathsf{call/cc}\,(x.\ f_1\ x)]\rangle \downarrow^{<W.k}$.
- To show: $\langle h_2; K_2[\mathsf{let}\ r = \mathsf{ref}\ (\mathsf{cont}\ \bullet)\ \mathsf{in}\ G_r^{\tau_2}\ f_2]\rangle \downarrow$
- $\langle h_1; K_1[\mathsf{call/cc}\,(x.\ f_1\ x)]\rangle \downarrow^{<W.k}$ implies $\langle h_1; K_1[f_1\ (\mathsf{cont}\ K_1)]\rangle \downarrow^{<W.k}$.
- Similarly, $\langle h_2; K_2[\mathsf{let}\ r = \mathsf{ref}\ (\mathsf{cont}\ \bullet)\ \mathsf{in}\ G_r^{\tau_2}\ f_2]\rangle \downarrow$ if $\langle \widehat{h_2}; K_2[f_2\ (\mathsf{cont}\ (\mathsf{throw}\ \bullet\ \mathsf{to}\ !l_r))]\rangle \downarrow$, where
  - $K := K_2[\mathsf{let}\ x = \bullet\ \mathsf{in}\ \mathsf{callcc1}\ \tau_2\ (\lambda z.\,G_{l_r}^{\tau_2}\ (\lambda\_.\,\mathsf{throw}\ x\ \mathsf{to}\ z))]$
  - $e_l := \mathsf{cont}\ (\mathsf{let}\ y = \bullet\ \mathsf{in}\ \mathsf{if}\ !l\ \mathsf{then}\ (l := \mathsf{ff}; \mathsf{throw}\ y\ \mathsf{to}\ \mathsf{cont}\ K)\ \mathsf{else}\ \bot)$
  - $\widehat{h_2} := h_2 \uplus \{l_r{\mapsto}e_{l_b}\} \uplus \{l_b{\mapsto}\mathsf{tt}\}$
  - and l_r, l_b are distinct and fresh.
- Let
  - $H(\langle\rangle) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \mathrm{HeapAtom} \mid \exists l \in \mathrm{dom}(h_2).\ \widetilde{h_2}(l_r) = e_l \wedge \widetilde{h_2}(l) = \mathsf{tt}\}$
  - $\iota := (\langle\rangle, \emptyset^*, \emptyset^*, \emptyset, H)$
  - $\widehat{W} := W[\Sigma_2 := W.\Sigma_2, l_r{:}\mathsf{cont}\,\tau_2, l_b{:}\mathsf{bool}][\omega := (W.\omega, \iota)]$

- It is easy to see that $\widehat{W} \sqsupseteq^{\mathsf{pub}} W$ and, using monotonicity (Lemma 10), that $(h_1, \widehat{h_2}) : \widehat{W}$.
- Since $(\widehat{W}, K_1, K_2) \in \mathcal{K}[\![\alpha]\!]\rho$ by monotonicity (Lemma 10), it then suffices to show $(\widehat{W}, f_1\ (\mathsf{cont}\ K_1), f_2\ (\mathsf{cont}\ (\mathsf{throw}\ \bullet\ \mathsf{to}\ !l_r))) \in \mathcal{E}[\![\alpha]\!]\rho$.
- Since $(W, f_1, f_2) \in \mathcal{V}[\![\tau_\alpha]\!]\rho$, this reduces to showing $(\widehat{W}, \mathsf{cont}\ K_1, \mathsf{cont}\ (\mathsf{throw}\ \bullet\ \mathsf{to}\ !l_r)) \in \mathcal{V}[\![\mathsf{cont}\,\alpha]\!]\rho$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} \widehat{W}$, $(W', v_1', v_2') \in \mathcal{V}[\![\alpha]\!]\rho$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1[v_1']\rangle\downarrow^{<W'.k}$.
- To show: $\langle h_2'; \mathsf{throw}\ v_2'\ \mathsf{to}\ !l_r\rangle\downarrow$
- From $(h_1', h_2') : W'$ we know that $h_2'(l_r) = e_l$ and $h_2'(l) = \mathsf{tt}$, for some l.
- Hence $\langle h_2'; \mathsf{throw}\ v_2'\ \mathsf{to}\ !l_r\rangle \downarrow$ if $\langle h_2'[l{\mapsto}\mathsf{ff}]; K_2[\mathsf{callcc1}\ \tau_2\ (\lambda z.\, G_{l_r}^{\tau_2}\ (\lambda\_.\, \mathsf{throw}\ v_2'\ \mathsf{to}\ z))]\rangle \downarrow$ if $\langle h_2'[l{\mapsto}\mathsf{ff}][l_r{\mapsto}e_{l'}] \uplus \{l'{\mapsto}\mathsf{tt}\}; K_2[v_2']\rangle\downarrow$, where l' is fresh.
- Let $W'' := W'[\Sigma_2 := W'.\Sigma_2, l'{:}\mathsf{bool}]$.
- It is easy to see that $W'' \sqsupseteq^{\mathsf{pub}} W'$ and, using monotonicity (Lemma 10), that $(h_1', h_2'[l{\mapsto}\mathsf{ff}][l_r{\mapsto}e_{l'}] \uplus \{l'{\mapsto}\mathsf{tt}\}) : W''$.
- Also by monotonicity (Lemma 10) we know $(W'', v_1', v_2') \in \mathcal{V}[\![\alpha]\!]\rho$.
- Hence, using $W'' \sqsupseteq^{\mathsf{pub}} W$ and instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\alpha]\!]\rho$ yields the claim.

4.3.2 Local State Release 2

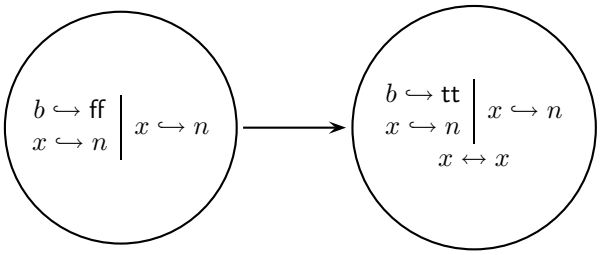
$$
\begin{array}{rcl}
e_1 & = & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in} \\
 & & \mathsf{let}\ b = \mathsf{ff}\ \mathsf{in} \\
 & & \langle(\lambda\_.\, b := \mathsf{tt}; x), (\lambda y.\, y == x\ \mathsf{andalso}\ !b)\rangle \\
e_2 & = & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in} \\
 & & \langle(\lambda\_.\, x), (\lambda y.\, y == x)\rangle
\end{array}
$$

We show $\cdot;\cdot;\cdot \vdash e_1 \precsim_{\log} e_2 : (\mathsf{unit} \to \mathsf{ref\ int}) \times (\mathsf{ref\ int} \to \mathsf{bool})$:

- This reduces to showing $(W, e_1, e_2) \in \mathcal{E}[\![(\mathsf{unit} \to \mathsf{ref\ int}) \times (\mathsf{ref\ int} \to \mathsf{bool})]\!]\emptyset$, where $W \in \mathcal{S}[\![\cdot]\!]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\![(\mathsf{unit} \to \mathsf{ref\ int}) \times (\mathsf{ref\ int} \to \mathsf{bool})]\!]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_1]\rangle\downarrow^{<W.k}$.
- To show: consistent(W) and $\langle h_2; K_2[e_2]\rangle\downarrow$
- $\langle h_1; K_1[e_1]\rangle\downarrow^{<W.k}$ implies $\langle\widehat{h_1}; K_1[\langle v_1, v_3\rangle]\rangle\downarrow^{<W.k}$, where
  - $\widehat{h_1} := h_1 \uplus \{l_x^1{\mapsto}0\} \uplus \{l_b{\mapsto}\mathsf{ff}\}$,
  - $v_1 := (\lambda\_.\, l_b := \mathsf{tt}; l_x^1)$,
  - $v_3 := (\lambda y.\, y == l_x^1\ \mathsf{andalso}\ !l_b)$, and
  - l_x^1, l_b are fresh and distinct.

- Similarly, $\langle h_2; K_2[e_2]\rangle\downarrow$ if $\langle\widehat{h_2}; K_2[\langle v_2, v_4\rangle]\rangle\downarrow$, where
  - $\widehat{h_2} := h_2 \uplus \{l_x^2 \mapsto 0\}$,
  - $v_2 := (\lambda\_.\, l_x^2)$,
  - $v_4 := (\lambda y.\, y == l_x^2)$, and
  - l_x^2 is fresh.
- Let
  - $H(1) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \text{HeapAtom} \mid \widetilde{h_1}(l_b) = \mathsf{ff} \wedge \exists n.\ \widetilde{h_1}(l_x^1) = n = \widetilde{h_2}(l_x^2)\}$
  - $2 := \{\langle l_x^1, l_x^2\rangle\}$
  - $H(2) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \text{HeapAtom} \mid \widetilde{h_1}(l_b) = \mathsf{tt} \wedge \exists n.\ \widetilde{h_1}(l_x^1) = n = \widetilde{h_2}(l_x^2)\}$
  - $\varphi := \{(1, 2)\}^*$
  - $\delta := \varphi$
  - $\iota_s := (s, \delta, \varphi, \emptyset, H)$
  - $W_s := W[\Sigma_1 := W.\Sigma_1, l_x^1{:}\mathsf{int}, l_b{:}\mathsf{bool}][\Sigma_2 := W.\Sigma_2, l_x^2{:}\mathsf{int}][\omega := W.\omega, \iota_s]$

  The island represents the following STS:



- It is easy to see that $W_1 \sqsupseteq^{\mathsf{pub}} W$ and, using monotonicity (Lemma 10), that $(\widehat{h_1}, \widehat{h_2}) : W_1$.
- Also, consistent(W_1) would imply consistent(W).
- It thus suffices to show $(W_1, \langle v_1, v_3\rangle, \langle v_2, v_4\rangle) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{ref\ int}) \times (\mathsf{ref\ int} \to \mathsf{bool})]\!]\emptyset$, which splits into two parts.
- We show $(W_1, v_1, v_2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{ref\ int}]\!]\emptyset$:
  - Suppose $W' \sqsupseteq W_1$, $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{ref\ int}]\!]\emptyset$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1'[l_b := \mathsf{tt}; l_x^1]\rangle\downarrow^{<W'.k}$.
  - To show: consistent(W') and $\langle h_2'; K_2'[l_x^2]\rangle\downarrow$
  - $\langle h_1'; K_1'[l_b := \mathsf{tt}; l_x^1]\rangle\downarrow^{<W'.k}$ implies $\langle h_1'[l_b \mapsto \mathsf{tt}]; K_1'[l_x^1]\rangle\downarrow^{<W'.k}$.
  - Let $\widehat{W'}$ be the world obtained from W' by setting our island's current state to 2.
  - It is easy to see that $\widehat{W'} \sqsupseteq^{\mathsf{pub}} W'$ and, using monotonicity (Lemma 10), that $(h_1'[l_b \mapsto \mathsf{tt}], h_2') : \widehat{W'}$.

– Also, consistent($\widehat{W'}$) would imply consistent(W').

– Since $(\widehat{W'}, K_1', K_2') \in \mathcal{K}[\![\mathsf{ref\ int}]\!]\emptyset$, it therefore remains to show $(\widehat{W'}, l_x^1, l_x^2) \in \mathcal{V}[\![\mathsf{ref\ int}]\!]\emptyset$.

– So suppose $W'' \sqsupseteq \widehat{W'}$.

– Notice that $\mathrm{bij}(W''.\omega(p).s) = \mathrm{bij}(\widehat{W'}.\omega(p).s) = \mathrm{bij}(2) = \mathrm{bij}(\{\langle l_x^1, l_x^2\rangle\}) = \{(l_x^1, l_x^2)\}$.

– Furthermore:

$$
\begin{aligned}
& W''.\omega(p).H(W''.\omega(p).s) \\
=& \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \mathrm{HeapAtom} \mid \widetilde{h_1}(l_b) = b \wedge \exists n.\ \widetilde{h_1}(l_x^1) = n = \widetilde{h_2}(l_x^2)\} \\
=& \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \mathrm{HeapAtom} \mid \widetilde{h_1}(l_b) = b \wedge l_x^1 \notin \mathrm{dom}(\widetilde{h_1}) \wedge l_x^2 \notin \mathrm{dom}(\widetilde{h_2})\} \\
\otimes& \{(\widetilde{W}, \{l_x^1 \mapsto n_1\}, \{l_x^2 \mapsto n_2\}) \in \mathrm{HeapAtom} \mid n_1 = n_2\} \\
=& \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \mathrm{HeapAtom} \mid \widetilde{h_1}(l_b) = b \wedge l_x^1 \notin \mathrm{dom}(\widetilde{h_1}) \wedge l_x^2 \notin \mathrm{dom}(\widetilde{h_2})\} \\
\otimes& \{(\widetilde{W}, \{l_x^1 \mapsto v_1\}, \{l_x^2 \mapsto v_2\}) \in \mathrm{HeapAtom} \mid (\widetilde{W}, v_1, v_2) \in \mathcal{V}[\![\mathsf{int}]\!]\emptyset\}
\end{aligned}
$$

- We show $(W_1, v_3, v_4) \in \mathcal{V}[\![\mathsf{ref\ int} \to \mathsf{bool}]\!]\emptyset$:

  – Suppose $W' \sqsupseteq W_1$, $(W', l_1, l_2) \in \mathcal{V}[\![\mathsf{ref\ int}]\!]\emptyset$, $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{ref\ int}]\!]\emptyset$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1'[l_1 == l_x^1\ \mathsf{andalso}\ !l_b]\rangle\downarrow^{<W'.k}$.

  – To show: consistent(W') and $\langle h_2'; K_2'[l_2 == l_x^2]\rangle\downarrow$

  – We know $(l_1, l_2) \in \mathrm{bij}(W'.\omega(i).s)$ for some i such that $W'.\omega(i).H(W'.\omega(i).s)$ "talks about" l_1.

  – Case $l_1 = l_x^1$ or $l_2 = l_x^2$:

    * Since $(h_1', h_2') : W'$, i must be p and $W'.\omega(p).s$ must be 2.
    * Hence $l_1 = l_x^1$ and $l_2 = l_x^2$ and $h_1'(l_b) = \mathsf{tt}$.
    * Consequently, $\langle h_1'; K_1'[l_1 == l_x^1\ \mathsf{andalso}\ !l_b]\rangle\downarrow^{<W'.k}$ implies $\langle h_1'; K_1'[\mathsf{tt}]\rangle\downarrow^{<W'.k}$.
    * Similarly, $\langle h_2'; K_2'[l_2 == l_x^2]\rangle\downarrow$ if $\langle h_2'; K_2'[\mathsf{tt}]\rangle\downarrow$.
    * Since $(W', \mathsf{tt}, \mathsf{tt}) \in \mathcal{V}[\![\mathsf{bool}]\!]\emptyset$, the claims now follow from instantiating $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{ref\ int}]\!]\emptyset$.

  – Case $l_1 \neq l_x^1$ and $l_2 \neq l_x^2$:

    * Then $\langle h_1'; K_1'[l_1 == l_x^1\ \mathsf{andalso}\ !l_b]\rangle\downarrow^{<W'.k}$ implies $\langle h_1'; K_1'[\mathsf{ff}]\rangle\downarrow^{<W'.k}$.
    * Similarly, $\langle h_2'; K_2'[l_2 == l_x^2]\rangle\downarrow$ if $\langle h_2'; K_2'[\mathsf{ff}]\rangle\downarrow$.
    * Since $(W', \mathsf{ff}, \mathsf{ff}) \in \mathcal{V}[\![\mathsf{bool}]\!]\emptyset$, the claims now follow from instantiating $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{ref\ int}]\!]\emptyset$.

A higher-level explanation:

To show e_1 and e_2 related, we observe that after the allocations of local references b, x_1, and x_2, the expressions e_1 and e_2 return a pair of functions. We install an island describing how the local state evolves in the two expressions; as shown in the picture above. Intuitively, the left state describes the local state before the context calls the function of type unit to ref int, whereas the state on the right describes the local state after the context has called that function. In both states,

the n is existentially quantified; i.e., there should exists an n such that x_1 on the left stores n and x_2 on the right stores n. Finally, the arrow connecting x_1 and x_2 in the state on the right depicts the bijection between locations on the left and the right in this state, capturing the intuition that in this state (after having called the function of type unit to ref int) the context may know the location x_1, respectively x_2, (since they are returned by the function of type unit to ref int).

Then we have to show that the pair of functions returned by e_1 and e_2 are related. Since functions should work in all future worlds, we have to consider both states for both of the functions.

For the functions of type unit to ref int, in the left hand state: Given related values and related heaps, we immediately see that we end up with heaps and values that are related in the future world given by the state on the right (so there does indeed exist a future world in which the values and heaps returned by the functions are related). In particular, we use the fact that the functions return x_1 and x_2 which are indeed in bijective correspondence in the state on the right, as required for relatedness at the reference type ref int.

For the functions of type unit to ref int, in the right hand state: Given related values and heaps, it is clear that we also get related values heaps satisfying the same state.

For the functions of type ref int to bool, in either the left hand state or the right hand side state: Given related values l_1 and l_2 and heaps, we case analyze on the related values. Observe first, that since l_1 and l_2 are related there must be some island at which l_1 and l_2 are in bijective correspondence. Now, if $l_1 = x_1$ or $l_2 = x_2$: Then the island must the one depicted in the picture, in the right hand state, and hence we have both $l_1 = x_1$ and $l_2 = x_2$ and thus both functions will return true. Finally, if $l_1 \neq x_1$ and $l_2 \neq x_2$, then both functions return false.

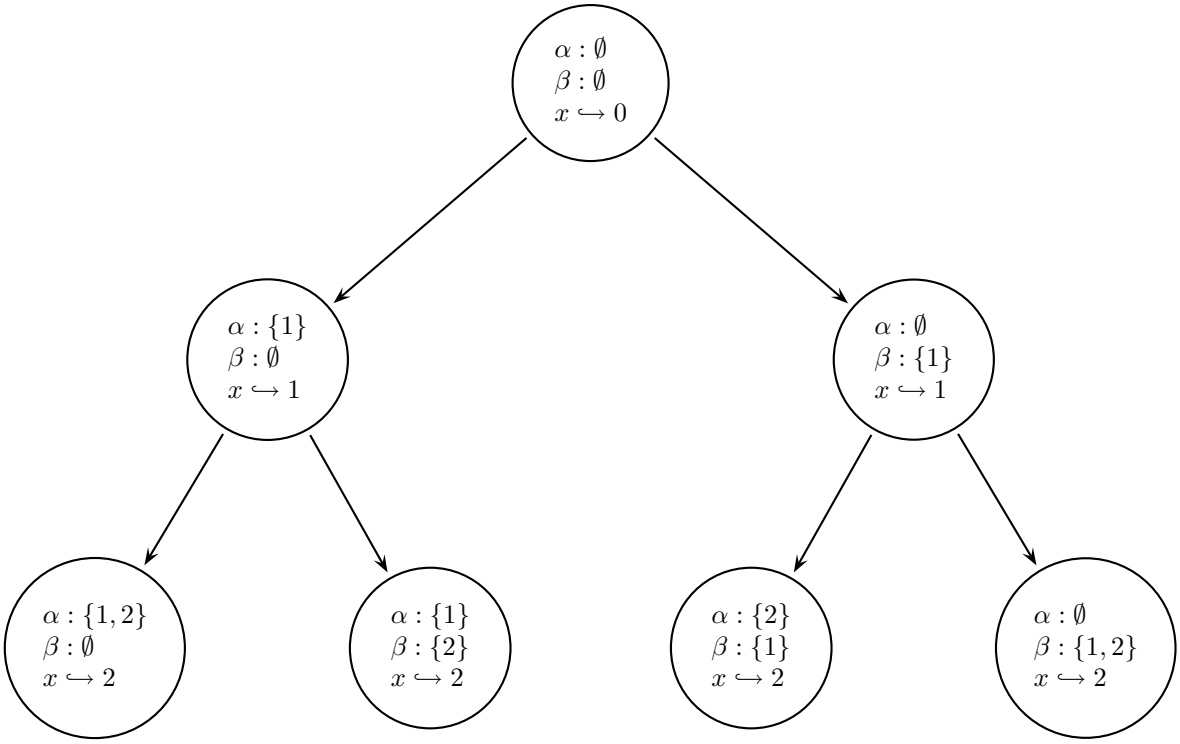
4.3.3 Twin Abstraction

$$
\begin{array}{rcl}
\tau & = & \exists\alpha.\,\exists\beta.\,(\mathsf{unit} \to \alpha) \times (\mathsf{unit} \to \beta) \times (\alpha \times \beta \to \mathsf{bool}) \\
e_1 & = & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in}\ \mathsf{pack}\ \langle \mathsf{int}, \mathsf{pack}\ \langle \mathsf{int}, \langle \lambda\_.\, x := !x + 1; !x, \\
 & & \qquad\qquad\qquad\qquad \lambda\_.\, x := !x + 1; !x, \\
 & & \qquad\qquad\qquad\qquad \lambda p.\, p.1 = p.2 \rangle\rangle\rangle \\
e_2 & = & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in}\ \mathsf{pack}\ \langle \mathsf{int}, \mathsf{pack}\ \langle \mathsf{int}, \langle \lambda\_.\, x := !x + 1; !x, \\
 & & \qquad\qquad\qquad\qquad \lambda\_.\, x := !x + 1; !x, \\
 & & \qquad\qquad\qquad\qquad \lambda p.\, \mathsf{ff} \rangle\rangle\rangle
\end{array}
$$

The proof is analogous to ADR's. We only show the construction of the island.

$$
\begin{array}{rcl}
\iota_s & = & (s, \delta, \varphi, \emptyset, H) \\
\delta & = & \{(s, s') \mid \exists m.\ m = \max\left(\{0\} \uplus \{n \mid \exists i \in \{1,2\}.\ \langle i, n\rangle \in s\}\right) \wedge \\
 & & \qquad\qquad \exists j \in \{1,2\}.\ s' = s \uplus \{\langle j, m+1\rangle\}\} \\
\varphi & = & \delta \\
H(s) & = & \{(W, h_1, h_2) \in \mathrm{HeapAtom} \mid \exists m.\ m = \max\left(\{0\} \uplus \{n \mid \exists i \in \{1,2\}.\ \langle i, n\rangle \in s\}\right) \wedge \\
 & & \qquad\qquad\qquad\qquad h_1(l_x) = m = h_2(l_x)\}
\end{array}
$$

The island represents the following infinite STS (here only showing the first three levels):



4.4 FOS

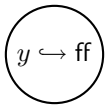
4.4.1 Deferred Divergence 3

$$\begin{array}{lcl}\tau & = & ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{unit} \\ e_1 & = & \mathsf{let}\ y = \mathsf{ref}\ \mathsf{ff}\ \mathsf{in} \\ & & \lambda f{:}(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}.\ f\ (\lambda z{:}\mathsf{unit}.\ y := \mathsf{tt}); \\ & & \qquad\qquad\qquad\qquad \mathsf{if}\ !y\ \mathsf{then}\ \bot\ \mathsf{else}\ \langle\rangle \\ e_2 & = & \lambda f{:}(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}.\ f\ (\lambda z{:}\mathsf{unit}.\ \bot)\end{array}$$

We show $\cdot;\cdot;\cdot \vdash e_2 \precsim_{\log} e_1 : \tau$ (the other, more difficult direction is presented in the paper).

- This reduces to showing $(W, e_2, e_1) \in \mathcal{E}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, where $W \in \mathcal{S}[\![\cdot]\!]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_2]\rangle\downarrow^{<W.k}$.
- To show: consistent(W) and $\langle h_2; K_2[e_1]\rangle\downarrow$
- Observe that $\langle h_2; K_2[e_1]\rangle\downarrow$ if $\langle h_2 \uplus \{l_y \mapsto \mathsf{ff}\}; K_2[\widehat{e_1}[l_y/y]]\rangle\downarrow$, where $\widehat{e_1}$ is the body of e_1 and l_y any free location.
- Let
  - $H(\langle\rangle) := \{(\widetilde{h_1}, \widetilde{h_2}) \in \mathrm{HeapAtom} \mid \widetilde{h_2}(l_y) = \mathsf{ff}\}$
  - $\iota := (\langle\rangle, \emptyset^*, \emptyset^*, \emptyset, H)$
  - $\widehat{W} := W[\Sigma_2 := W.\Sigma_2, l_y{:}\mathsf{bool}][\omega := W.\omega, \iota]$

  The island represents the following STS:



- Note that $\widehat{W} \sqsupseteq^{\mathsf{pub}} W$ and $(h_1, h_2 \uplus \{l_y \mapsto \mathsf{ff}\}) : \widehat{W}$.
- Because of $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!]\emptyset$ it thus suffices to show $(\widehat{W}, e_2, \widehat{e_1}[l_y/y]) \in \mathcal{V}[\![\tau]\!]\emptyset$.
- So suppose $W' \sqsupseteq W$, $(W', f_1, f_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1'[f_1\ (\lambda\_.\ \bot)]\rangle\downarrow^{<W'.k}$.
- To show: consistent(W') and $\langle h_2'; K_2'[f_2\ (\lambda\_.\ l_y := \mathsf{tt}); \mathsf{if}\ !l_y\ \mathsf{then}\ \bot\ \mathsf{else}\ \langle\rangle]\rangle\downarrow$
- We show $(W', f_1\ (\lambda\_.\ \bot), f_2\ (\lambda\_.\ l_y := \mathsf{tt})) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$:
  - Since $(W', f_1, f_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, it suffices to show $(W', (\lambda\_.\ \bot), (\lambda\_.\ l_y := \mathsf{tt})) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$.
  - This holds trivially, because $\langle h_1''; K_1''[\bot]\rangle$ diverges for any h_1'' and K_1''.
- We show $(W', K_1', K_2'[\bullet; \mathsf{if}\ !l_y\ \mathsf{then}\ \bot\ \mathsf{else}\ \langle\rangle]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$:
  - So suppose $W'' \sqsupseteq^{\mathsf{pub}} W'$, $(h_1'', h_2'') : W''$, and $\langle h_1''; K_1'[\langle\rangle]\rangle\downarrow^{<W''.k}$.

- To show: consistent(W'') and $\langle h_2''; K_2'[\mathsf{if}\ !l_y\ \mathsf{then}\ \bot\ \mathsf{else}\ \langle\rangle]\rangle\downarrow$
- From $(h_1'', h_2'') : W''$ we know $h_2''(l_y) = \mathsf{ff}$.
- Therefore, $\langle h_2''; K_2'[\mathsf{if}\ !l_y\ \mathsf{then}\ \bot\ \mathsf{else}\ \langle\rangle]\rangle\downarrow$ if $\langle h_2''; K_2'[\langle\rangle]\rangle\downarrow$.
- The claims thus follow from instantiating $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$ with $(W'', \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$.

- Combining these yields the claims.

4.5 FOSC

4.5.1 Callback With Lock

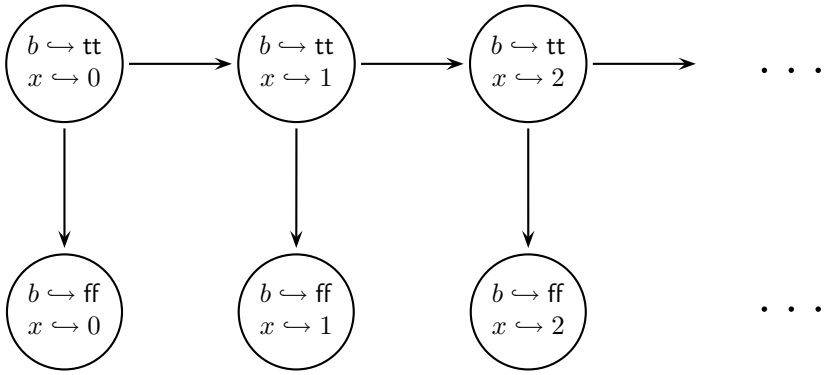
$$
\begin{array}{lcl}
C & = & \mathsf{let}\ b = \mathsf{ref}\ \mathsf{tt}\ \mathsf{in} \\
 & & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in} \\
 & & \langle \lambda f{:}\mathsf{unit} \to \mathsf{unit}.\ \mathsf{if}\ !b\ \mathsf{then}\ (b := \mathsf{ff}; \bullet; b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle, \\
 & & \ \lambda z{:}\mathsf{unit}.\ !x\rangle \\
e_1 & = & C[f\ \langle\rangle; x := !x + 1] \\
e_2 & = & C[\mathsf{let}\ n = !x\ \mathsf{in}\ f\ \langle\rangle; x := n + 1]
\end{array}
$$

We already showed that e_1 approximates e_2 in the higher-order-state setting without control. This proof had to use private transitions, because the approximation does not hold in the presence of control. In the first-order-state setting, however, the approximation *does* hold in the presence of control—see the following proof, which does not make use of private transitions.
We show $\cdot;\cdot;\cdot \vdash e_1 \precsim_{\log} e_2 : ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \times (\mathsf{unit} \to \mathsf{int})$:

- This reduces to showing $(W, e_1, e_2) \in \mathcal{E}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \times (\mathsf{unit} \to \mathsf{int})]\!]\emptyset$, where $W \in \mathcal{S}[\![\cdot]\!]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \times (\mathsf{unit} \to \mathsf{int})]\!]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_1]\rangle\downarrow^{<W.k}$.
- To show: consistent(W) and $\langle h_2; K_2[e_2]\rangle\downarrow$
- $\langle h_1; K_1[e_1]\rangle\downarrow^{<W.k}$ implies $\langle \widehat{h_1}; K_1[v_1]\rangle\downarrow^{<W.k}$, where
  - $v_1 := \langle v_1^1, v_1^2\rangle$,
  - $v_1^1 := \lambda f.\ \mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; f\ \langle\rangle; l_x := !l_x + 1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle$,
  - $v_1^2 := \lambda z.\ !l_x$,
  - $\widehat{h_1} := h_1 \uplus \{l_b \mapsto \mathsf{tt}\} \uplus \{l_x \mapsto 0\}$, and
  - l_b, l_x are fresh and distinct.
- Similarly, $\langle h_2; K_2[e_2]\rangle\downarrow$ if $\langle \widehat{h_2}; K_2[v_2]\rangle\downarrow$, where
  - $v_2 := \langle v_2^1, v_2^2\rangle$,
  - $v_2^1 := \lambda f.\ \mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; \mathsf{let}\ n = !l_x\ \mathsf{in}\ f\ \langle\rangle; l_x := n + 1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle$,
  - $v_2^2 := \lambda z.\ !l_x$, and
  - $h_2' := h_2 \uplus \{l_b \mapsto \mathsf{tt}\} \uplus \{l_x \mapsto 0\}$.
- Let
  - $H(\langle o, i\rangle) := \{(\widetilde{h_1}, \widetilde{h_2}) \in \text{HeapAtom} \mid \widetilde{h_1}(l_b) = \widetilde{h_2}(l_b) = o \wedge \widetilde{h_1}(l_x) = \widetilde{h_2}(l_x) = i\}$
  - $\varphi := \{(\langle \mathsf{tt}, i\rangle, \langle \mathsf{tt}, i+1\rangle) \mid i \in \mathbb{N}\}^*$
  - $\delta := (\varphi \uplus \{(\langle \mathsf{tt}, i\rangle, \langle \mathsf{ff}, i\rangle) \mid i \in \mathbb{N}\} \uplus \{(\langle \mathsf{ff}, i\rangle, \langle \mathsf{tt}, i+1\rangle) \mid i \in \mathbb{N}\})^*$
  - $\iota_s := (s, \delta, \varphi, \emptyset, H)$

– $W_s := W[W.\Sigma_1 := W.\Sigma_1, l_b{:}\mathsf{unit}, l_x{:}\mathsf{int}][W.\omega := W.\omega, \iota_s]$

The island represents the following STS:



- It is easy to see that $W_{\langle \mathsf{tt},0\rangle} \sqsupseteq^{\mathsf{pub}} W$ and $(\widehat{h_1}, \widehat{h_2}) : W_{\langle \mathsf{tt},0\rangle}$.
- It thus suffices to show $(W_{\langle \mathsf{tt},0\rangle}, v_1, v_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \times (\mathsf{unit} \to \mathsf{int})]\!]\emptyset$, which splits into two parts.
- We show $(W_{\langle \mathsf{tt},0\rangle}, v_1^1, v_2^1) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$:
  - Suppose $W' \sqsupseteq W_{\langle \mathsf{tt},0\rangle}$, $(W', \lambda y.\, e_3, \lambda y.\, e_4) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$, $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1'[\mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; (\lambda y.\, e_3)\ \langle\rangle; l_x := !l_x{+}1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle]\rangle \downarrow^{<W'.k}$.
  - To show: consistent(W') and $\langle h_2'; K_2'[\mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; \mathsf{let}\ n = !l_x\ \mathsf{in}\ (\lambda y.\, e_4)\ \langle\rangle; l_x := n{+}1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle]\rangle \downarrow$
  - Notation: we write W_s' to denote the world obtained from W' by setting our island's current state to s.
  - Case $W' = W'_{\langle \mathsf{tt},i\rangle}$ for some i:
    - Then $(h_1', h_2') : W'$ implies $h_1'(l_b) = h_2'(l_b) = \mathsf{tt}$ and $h_1'(l_x) = h_2'(l_x) = i$.
    - Hence $\langle h_1'; K_1'[\mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; (\lambda y.\, e_3)\ \langle\rangle; l_x := !l_x + 1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle]\rangle \downarrow^{<W'.k}$ implies $\langle h_1'[l_b{\mapsto}\mathsf{ff}]; K_1'[e_3[\langle\rangle/y]; (\lambda y.\, e_3)\ \langle\rangle; l_x := !l_x + 1; l_b := \mathsf{tt})\rangle\langle\rangle \downarrow^{<W'.k}$.
    - Similarly, $\langle h_2'; K_2'[\mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; \mathsf{let}\ n = !l_x\ \mathsf{in}\ (\lambda y.\, e_4)\ \langle\rangle; l_x := n{+}1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle]\rangle \downarrow$ if $\langle h_2'[l_b{\mapsto}\mathsf{ff}]; K_2'[e_4[\langle\rangle/y]; l_x := i + 1; l_b := \mathsf{tt})\rangle \downarrow$.
    - It is easy to see that $W'_{\langle \mathsf{ff},i\rangle} \sqsupseteq W'$ and $(h_1'[l_b{\mapsto}\mathsf{ff}], h_2'[l_b{\mapsto}\mathsf{ff}]) : W'_{\langle \mathsf{ff},i\rangle}$.
    - Also, consistent($W'_{\langle \mathsf{ff},i\rangle}$) would imply consistent(W').
    - Since $(W'_{\langle \mathsf{ff},i\rangle}, \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$ and thus $(W'_{\langle \mathsf{ff},i\rangle}, e_3[\langle\rangle/y], e_4[\langle\rangle/y]) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$, it suffices to show $(W'_{\langle \mathsf{ff},i\rangle}, K_1'[\bullet; l_x := !l_x + 1; l_b := \mathsf{tt}], K_2'[\bullet; l_x := i + 1; l_b := \mathsf{tt}]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
    - So suppose $W'' \sqsupseteq^{\mathsf{pub}} W'_{\langle \mathsf{ff},i\rangle}$, $(h_1'', h_2'') : W''$, and $\langle h_1''; K_1'[\langle\rangle; l_x := !l_x{+}1; l_b := \mathsf{tt}]\rangle \downarrow^{<W''.k}$.
    - To show: consistent(W'') and $\langle h_2''; K_2'[\langle\rangle; l_x := i + 1; l_b := \mathsf{tt}]\rangle \downarrow$
    - Note that the only public successor of $\langle \mathsf{ff}, i\rangle$ is $\langle \mathsf{ff}, i\rangle$ itself and therefore $W'' = W''_{\langle \mathsf{ff},i\rangle}$.

* Hence $(h_1'', h_2'') : W''$ implies $h_1''(l_x) = i$ and thus $\langle h_1''[l_x \mapsto (i+1)][l_b \mapsto \mathsf{tt}]; K_1'[\langle\rangle]\rangle \downarrow^{<W''.k}$.
* Note that $\langle h_2''; K_2'[\langle\rangle; l_x := i+1; l_b := \mathsf{tt}]\rangle \downarrow$ if $\langle h_2''[l_x \mapsto (i+1)][l_b \mapsto \mathsf{tt}]; K_2'[\langle\rangle]\rangle \downarrow$.
* It is easy to see that $W''_{\langle \mathsf{tt}, i+1\rangle} \sqsupseteq^{\mathsf{pub}} W'_{\langle \mathsf{tt}, i+1\rangle} \sqsupseteq^{\mathsf{pub}} W'$.
* Furthermore, using $(h_1'', h_2'') : W''$ it is easy to see that $(h_1''[l_x \mapsto (i+1)][l_b \mapsto \mathsf{tt}], h_2''[l_x \mapsto (i+1)][l_b \mapsto \mathsf{tt}]) : W''_{\langle \mathsf{tt}, i+1\rangle}$.
* Also, consistent$(W''_{\langle \mathsf{tt}, i+1\rangle})$ would imply consistent(W'').
* Since $(W''_{\langle \mathsf{tt}, i+1\rangle}, \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$, the claims therefore follow from instantiating $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.

– Case $W' = W'_{\langle \mathsf{ff}, i\rangle}$ for some i:
* Then $(h_1', h_2') : W'$ implies $h_1'(l_b) = h_2'(l_b) = \mathsf{ff}$ and $h_1'(l_x) = h_2'(l_x) = i$.
* Hence $\langle h_1'; K_1'[\mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; (\lambda y.\, e_3)\ \langle\rangle; l_x := !l_x + 1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle]\rangle \downarrow^{<W'.k}$ implies $\langle h_1'; K_1'[\langle\rangle]\rangle \downarrow^{<W'.k}$.
* Similarly, $\langle h_2'; K_2'[\mathsf{if}\ !l_b\ \mathsf{then}\ (l_b := \mathsf{ff}; \mathsf{let}\ n = !l_x\ \mathsf{in}\ (\lambda y.\, e_4)\ \langle\rangle; l_x := n+1; l_b := \mathsf{tt})\ \mathsf{else}\ \langle\rangle]\rangle \downarrow$ if $\langle h_2'; K_2'[\langle\rangle]\rangle \downarrow$.
* Since $(W', \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$ the claims then follow from $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.

- We show $(W_{\langle \mathsf{tt}, 0\rangle}, v_1^2, v_2^2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{int}]\!]\emptyset$:
  – Suppose $W' \sqsupseteq W_{\langle \mathsf{tt}, 0\rangle}$, $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{int}]\!]\emptyset$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1'[!l_x]\rangle \downarrow^{<W'.k}$.
  – To show: consistent(W') and $\langle h_2'; K_2'[!l_x]\rangle \downarrow$
  – From $(h_1', h_2') : W'$ and the way we constructed our island we know $h_1'(l_x) = h_2'(l_x) = i$, for some i.
  – Hence $\langle h_1'; K_1'[!l_x]\rangle \downarrow^{<W'.k}$ implies $\langle h_1'; K_1'[i]\rangle \downarrow^{<W'.k}$.
  – Similarly, $\langle h_2'; K_2'[!l_x]\rangle \downarrow$ if $\langle h_2'; K_2'[i]\rangle \downarrow$.
  – Since $(W', i, i) \in \mathcal{V}[\![\mathsf{int}]\!]\emptyset$ the claims then follow from instantiating $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{int}]\!]\emptyset$.

4.5.2 Higher-Order Profiling

$$p \quad = \quad \lambda f.\, \mathsf{let}\ c = \mathsf{ref}\ 0\ \mathsf{in}\ \langle \lambda x.\, (c := !c + 1; f\ x), \lambda\_.\, !c\rangle$$

$$\begin{aligned} e_1 &= \lambda f.\, \lambda g.\, \lambda a.\, \mathsf{let}\ \langle g', g''\rangle = p\ g\ \mathsf{in}\ (f\ g'; g'\ \langle\rangle; a\ g'; g''\ \langle\rangle) \\ e_2 &= \lambda f.\, \lambda g.\, \lambda a.\, \mathsf{let}\ \langle g', g''\rangle = p\ g\ \mathsf{in}\ (f\ g'; g\ \langle\rangle; a\ g'; g''\ \langle\rangle + 1) \end{aligned}$$

Formally, we show
$\cdot; \cdot; \cdot \vdash e_1 \precsim_{\log} e_2 : ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to (\mathsf{unit} \to \mathsf{unit}) \to ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{int}$.

- This reduces to showing
  $(\widetilde{W}, e_1, e_2) \in \mathcal{V}[\![((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to (\mathsf{unit} \to \mathsf{unit}) \to ((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}) \to \mathsf{int}]\!]\emptyset$,
  where $\widetilde{W} \in \mathcal{S}[\![\cdot]\!]$.
- This boils down to showing $(W, e_1', e_2') \in \mathcal{E}[\![\mathsf{int}]\!]\emptyset$, where
  – $W \sqsupseteq \widetilde{W}$,

- $e_1' := \mathsf{let}\ \langle g', g''\rangle = p\ g_1\ \mathsf{in}\ (f_1\ g'; g'\ \langle\rangle; a_1\ g'; g''\ \langle\rangle)$,
- $e_2' := \mathsf{let}\ \langle g', g''\rangle = p\ g_2\ \mathsf{in}\ (f_2\ g'; g_2\ \langle\rangle; a_2\ g'; g''\ \langle\rangle + 1)$,
- $(W, f_1, f_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$,
- $(W, g_1, g_2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$, and
- $(W, a_1, a_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$.

- So suppose $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{int}]\!]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_1']\rangle\downarrow^{<W.k}$.
- To show: $\langle h_2; K_2[e_2']\rangle\downarrow$
- $\langle h_1; K_1[e_1']\rangle\downarrow^{<W.k}$ implies $\langle \widehat{h_1}; K_1[f_1\ g_1'; g_1'\ \langle\rangle; a_1\ g_1'; (\lambda\_.\ !l_1)\ \langle\rangle]\rangle\downarrow^{<W.k}$, where
  - $\widehat{h_1} := h_1 \uplus \{l_1 \mapsto 0\}$,
  - $g_1' := \lambda x.\, (l_1 := !l_1 + 1; g_1\ x)$, and
  - l_1 is fresh.
- Similarly, $\langle h_2; K_2[e_2']\rangle\downarrow$ if $\langle \widehat{h_2}; K_2[f_2\ g_2'; g_2\ \langle\rangle; a_2\ g_2'; (\lambda\_.\ !l_2)\ \langle\rangle + 1]\rangle\downarrow$, where
  - $\widehat{h_2} := h_2 \uplus \{l_2 \mapsto 0\}$,
  - $g_2' := \lambda x.\, (l_2 := !l_2 + 1; g_2\ x)$, and
  - l_2 is fresh.
- Let
  - $H(n) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \text{HeapAtom} \mid \widetilde{h_1}(l_1) = \widetilde{h_2}(l_2) + n\}$
  - $\iota_s := (s, \emptyset^*, \emptyset^*, \emptyset, H)$
  - $W_s := W[\Sigma_1 := W.\Sigma_1, l_1{:}\mathsf{int}][\Sigma_2 := W.\Sigma_2, l_2{:}\mathsf{int}][\omega := W.\omega, \iota_s]$
- It is easy to see that $W_0 \sqsupseteq^{\mathsf{pub}} W$ and, using monotonicity (Lemma 10), that $(\widehat{h_1}, \widehat{h_2}) : W_0$.
- We show $(W_0, f_1\ g_1', f_2\ g_2') \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$:
  - Since $(W, f_1, f_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, it suffices to show $(W_0, g_1', g_2') \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$.
  - So suppose $W' \sqsupseteq W_0$, $(W', K_1', K_2') \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1'[l_1 := !l_1 + 1; g_1\ \langle\rangle]\rangle\downarrow^{<W'.k}$.
  - To show: $\langle h_2'; K_2'[l_2 := !l_2 + 1; g_2\ \langle\rangle]\rangle\downarrow$
  - $\langle h_1'; K_1'[l_1 := !l_1 + 1; g_1\ \langle\rangle]\rangle\downarrow^{<W'.k}$ implies $\langle h_1'[l_1 \mapsto h_1'(l_1) + 1]; K_1'[g_1\ \langle\rangle]\rangle\downarrow^{<W'.k}$.
  - Similarly, $\langle h_2'; K_2'[l_2 := !l_2 + 1; g_2\ \langle\rangle]\rangle\downarrow$ if $\langle h_2'[l_2 \mapsto h_2'(l_2) + 1]; K_2'[g_2\ \langle\rangle]\rangle\downarrow$.
  - Incrementing both counters by one preserves the invariant imposed by our island and hence it is easy to see that $(h_1'[l_1 \mapsto h_1'(l_1) + 1], h_2'[l_2 \mapsto h_2'(l_2) + 1]) : W'$.
  - It therefore suffices to show $(W', g_1\ \langle\rangle, g_2\ \langle\rangle) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$, which follows from $(W, g_1, g_2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$ and $(W', \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$.

- It thus suffices to show $(W_0, K_1[\bullet; g_1'\ \langle\rangle; a_1\ g_1'; (\lambda\_.\ !l_1)\ \langle\rangle], K_2[\bullet; g_2\ \langle\rangle; a_2\ g_2'; (\lambda\_.\ !l_2)\ \langle\rangle + 1]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
- So suppose $W' \sqsupseteq^{\mathsf{pub}} W_0$, $(h_1', h_2') : W'$, and $\langle h_1'; K_1[\langle\rangle; g_1'\ \langle\rangle; a_1\ g_1'; (\lambda\_.\ !l_1)\ \langle\rangle]\rangle\downarrow^{<W'.k}$, which implies $\langle\widehat{h_1'}; K_1[g_1\ \langle\rangle; a_1\ g_1'; (\lambda\_.\ !l_1)\ \langle\rangle]\rangle\downarrow^{<W'.k}$, where $\widehat{h_1'} := h_1'[l_1 \mapsto h_1'(l_1) + 1]$.
- To show: $\langle h_2'; K_2[\langle\rangle; g_2\ \langle\rangle; a_2\ g_2'; (\lambda\_.\ !l_2)\ \langle\rangle + 1]\rangle\downarrow$, *i.e.,* $\langle h_2'; K_2[g_2\ \langle\rangle; a_2\ g_2'; (\lambda\_.\ !l_2)\ \langle\rangle + 1]\rangle\downarrow$.
- Let W_1' be the world obtained from W' by replacing our island ι_0 with ι_1.
- Note that we do not have $W_1' \sqsupseteq W'$. But because we are in the first-order setting, $(h_1', h_2') : W_1'$ nevertheless follows from $(\widehat{h_1'}, h_2') : W'$.
- It is easy to see that $W_1' \sqsupseteq W$, though.
- From $(W, g_1, g_2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$ and $(W_1', \langle\rangle, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit}]\!]\emptyset$ we get $(W_1', g_1\ \langle\rangle, g_2\ \langle\rangle) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$.
- It thus suffices to show $(W_1', K_1[\bullet; a_1\ g_1'; (\lambda\_.\ !l_1)\ \langle\rangle], K_2[\bullet; a_2\ g_2'; (\lambda\_.\ !l_2)\ \langle\rangle + 1]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
- So suppose $W'' \sqsupseteq^{\mathsf{pub}} W_1'$, $(h_1'', h_2'') : W''$, and $\langle h_1''; K_1[\langle\rangle; a_1\ \ g_1'; (\lambda\_.\ !l_1)\ \langle\rangle]\rangle\downarrow^{<W''.k}$, *i.e.,* $\langle h_1''; K_1[a_1\ g_1'; (\lambda\_.\ !l_1)\ \langle\rangle]\rangle\downarrow^{<W''.k}$.
- To show: $\langle h_2''; K_2[\langle\rangle; a_2\ g_2'; (\lambda\_.\ !l_2)\ \langle\rangle + 1]\rangle\downarrow$, *i.e.,* $\langle h_2''; K_2[a_2\ g_2'; (\lambda\_.\ !l_2)\ \langle\rangle + 1]\rangle\downarrow$.
- Following the proof of $(W_0, f_1\ g_1', f_2\ g_2') \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$ above, we can easily show $(W'', a_1\ g_1', a_2\ g_2') \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$.
- It thus suffices to show $(W'', K_1[\bullet; (\lambda\_.\ !l_1)\ \langle\rangle], K_2[\bullet; (\lambda\_.\ !l_2)\ \langle\rangle + 1]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
- So suppose $W''' \sqsupseteq^{\mathsf{pub}} W''$, $(h_1''', h_2''') : W'''$, and $\langle h_1'''; K_1[\langle\rangle; (\lambda\_.\ !l_1)\ \langle\rangle]\rangle\downarrow^{<W'''.k}$.
- To show: $\langle h_2'''; K_2[\langle\rangle; (\lambda\_.\ !l_2)\ \langle\rangle + 1]\rangle\downarrow$
- From $(h_1''', h_2''') : W'''$ and $W''' \sqsupseteq^{\mathsf{pub}} W''$ we know $h_1'''(l_1) = n + 1$ and $h_2'''(l_2) = n$, for some n.
- Hence $\langle h_1'''; K_1[\langle\rangle; (\lambda\_.\ !l_1)\ \langle\rangle]\rangle\downarrow^{<W'''.k}$ implies $\langle h_1'''; K_1[n + 1]\rangle\downarrow^{<W'''.k}$.
- Similarly $\langle h_2'''; K_2[\langle\rangle; (\lambda\_.\ !l_2)\ \langle\rangle + 1]\rangle\downarrow$ if $\langle h_2'''; K_2[n + 1]\rangle\downarrow$.
- It is easy to see that $W''' = W_1''' \sqsupseteq^{\mathsf{pub}} W_1'' \sqsupseteq^{\mathsf{pub}} W_1' \sqsupseteq^{\mathsf{pub}} W$.
- Since $(W''', n + 1, n + 1) \in \mathcal{V}[\![\mathsf{int}]\!]\emptyset$, the claims then follow from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{int}]\!]\emptyset$.

4.5.3 Irreversible State Change

$$\begin{array}{lcl} e_1 & = & \lambda f.\, \mathsf{let}\ x = \mathsf{ref}\ \mathsf{tt}\ \mathsf{in}\ f\ (\lambda\_.\, x := \mathsf{ff}); x := \mathsf{tt}; \lambda\_.\, !x \\ e_2 & = & \lambda f.\, f\ (\lambda\_.\, \langle\rangle); \lambda\_.\, \mathsf{tt} \end{array}$$

The two programs are not equivalent in **HOS**, as the following context demonstrates:

$$\begin{array}{lcl} C & = & \mathsf{let}\ g = \bullet\ \mathsf{in} \\ & & \mathsf{let}\ y = \mathsf{ref}\ (\lambda\_.\, \langle\rangle)\ \mathsf{in} \\ & & \mathsf{let}\ f = (\lambda g'.\, y := g')\ \mathsf{in} \\ & & \mathsf{let}\ f' = g\ f\ \mathsf{in} \\ & & !y\ \langle\rangle; f'\ \langle\rangle \end{array}$$

It is easy to see that $C[e_1]$ yields ff, while $C[e_2]$ yields tt.

The two programs are, however, equivalent in **FOSC**. We show $\cdot;\cdot;\cdot \vdash e_1 \precsim_{\log} e_2 : (\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}$:

- This reduces to showing $(\widehat{W}, e_1, e_2) \in \mathcal{V}[\![(\mathsf{unit} \to \mathsf{unit}) \to \mathsf{unit}]\!]\emptyset$, where $\widehat{W} \in \mathcal{S}[\![\cdot]\!]$.
- So suppose $W \sqsupseteq \widehat{W}$, $(W, f_1, f_2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$, $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[\mathsf{let}\ x = \mathsf{ref}\ \mathsf{tt}\ \mathsf{in}\ f_1\ (\lambda\_.\, x := \mathsf{ff}); x := \mathsf{tt}; \lambda\_.\, !x]\rangle\downarrow^{<W.k}$.
- To show: $\langle h_2; K_2[f_2\ (\lambda\_.\, \langle\rangle); \lambda\_.\, \mathsf{tt}]\rangle\downarrow$
- $\langle h_1; K_1[\mathsf{let}\ x = \mathsf{ref}\ \mathsf{tt}\ \mathsf{in}\ f_1\ (\lambda\_.\, x := \mathsf{ff}); x := \mathsf{tt}; \lambda\_.\, !x]\rangle\downarrow^{<W.k}$ implies $\langle h_1'; K_1[f_1\ (\lambda\_.\, l_x := \mathsf{ff}); l_x := \mathsf{tt}; \lambda\_.\, !l_x]\rangle\downarrow^{<W.k}$, where $h_1' = h_1 \uplus \{l_x \mapsto \mathsf{tt}\}$.
- Let
  - $H(\langle\rangle) := \mathrm{HeapAtom}$
  - $\iota := (\langle\rangle, \emptyset^*, \emptyset^*, \emptyset, H)$
  - $W' := W[\Sigma_1 := W.\Sigma_1, l_x{:}\mathsf{unit} \to \mathsf{unit}][\omega := W.\omega, \iota]$
- It is easy to see that $W' \sqsupseteq^{\mathsf{pub}} W$ and, using monotonicity (Lemma 10), that $(h_1', h_2) : W'$.
- We show $(W', f_1\ (\lambda\_.\, l_x := \mathsf{ff}), f_2\ (\lambda\_.\, \langle\rangle)) \in \mathcal{E}[\![\mathsf{unit}]\!]\emptyset$:
  - Since $(W, f_1, f_2) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$, it suffices to show $(W', \lambda\_.\, l_x := \mathsf{ff}, \lambda\_.\, \langle\rangle) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{unit}]\!]\emptyset$.
  - Since our island does not impose any constraints on l_x, this is obvious.
- It thus suffices to show $(W', K_1[\bullet; l_x := \mathsf{tt}; \lambda\_.\, !l_x], K_2[\bullet; \lambda\_.\, \mathsf{tt}]) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$.
- So suppose $W'' \sqsupseteq^{\mathsf{pub}} W'$, $(h_1'', h_2'') : W''$, and $\langle h_1''; K_1[\langle\rangle; l_x := \mathsf{tt}; \lambda\_.\, !l_x]\rangle\downarrow^{<W''.k}$.
- To show: $\langle h_2''; K_2[\langle\rangle; \lambda\_.\, \mathsf{tt}]\rangle\downarrow$
- Note that $\langle h_1''; K_1[\langle\rangle; l_x := \mathsf{tt}; \lambda\_.\, !l_x]\rangle\downarrow^{<W''.k}$ implies $\langle h_1''[l_x \mapsto \mathsf{tt}]; K_1[\lambda\_.\, !l_x]\rangle\downarrow^{<W''.k}$.

- Furthermore, $\langle h_2''; K_2[\langle\rangle; \lambda\_.\, \mathsf{tt}]\rangle \downarrow$ if $\langle h_2''; K_2[\lambda\_.\, \mathsf{tt}]\rangle \downarrow$.
- Let
  - $H'(\langle\rangle) := \{(\widetilde{W}, \widetilde{h_1}, \widetilde{h_2}) \in \text{HeapAtom} \mid \widetilde{h_1}(l_x) = \mathsf{tt}\}$
  - $\iota' := (\langle\rangle, \emptyset^*, \emptyset^*, \emptyset, H')$
  - W''' be the world obtained from W'' by replacing our previously installed island ι with ι'.
- It is easy to see that $W''' \sqsupseteq^{\mathsf{pub}} W$ and $(h_1''[l_x \mapsto \mathsf{tt}], h_2'') : W'''$.
- Because our island ι' enforces $l_x \hookrightarrow \mathsf{tt}$, it is obvious that $(W''', \lambda\_.\, !l_x, \lambda\_.\, \mathsf{tt}) \in \mathcal{V}[\![\mathsf{unit} \to \mathsf{bool}]\!]\emptyset$.
- Instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\mathsf{unit}]\!]\emptyset$ now yields the claim.