

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

Technical Appendix

Technical Report MPI-SWS-2012-001

Derek Dreyer
dreyer@mpi-sws.org

Georg Neis
neis@mpi-sws.org

Lars Birkedal
birkedal@itu.dk

April 2012

Contents

1	Languages	4
1.1	HOS	4
1.1.1	Syntax & Dynamic Semantics	4
1.1.2	Static Semantics	4
1.1.3	Contextual and CIU Approximation	7
1.1.4	Random Lemmas	7
1.2	HOSE	8
1.2.1	Syntax & Dynamic Semantics	8
1.2.2	Static Semantics	8
1.3	HOSC	9
1.3.1	Syntax & Dynamic Semantics	9
1.3.2	Static Semantics	9
1.4	FOS	10
1.5	FOSE	10
1.6	FOSC	10
2	Logical Relations	11
2.1	HOS	11
2.2	HOSE	13
2.3	HOSC	13
2.4	FOS	13
2.5	FOSE	14
2.6	FOSC	14
3	Properties	15
3.1	HOS	15
3.1.1	Basic Properties	15
3.1.2	Soundness	18
3.1.3	Completeness	27
3.2	HOSE	29
3.2.1	Soundness	29
3.3	HOSC	31
3.3.1	Basic Properties	31
3.3.2	Soundness	31
3.4	FOS	33
3.5	FOSE	33
3.6	FOSC	33
4	Examples	34
4.1	HOS	34
4.1.1	Deferred Divergence 1	34
4.1.2	Well-Bracketed State Changes	37
4.1.3	Local State Release 1	40
4.2	HOSE	44
4.2.1	Deferred Divergence 2	44

4.2.2	Callback With Lock	48
4.2.3	Higher-Order Profiling	51
4.2.4	Single Return	54
4.3	HOSC	56
4.3.1	One-Shot Continuations	56
4.3.2	Local State Release 2	57
4.3.3	Twin Abstraction	60
4.4	FOS	62
4.4.1	Deferred Divergence 3	62
4.5	FOSC	64
4.5.1	Callback With Lock	64
4.5.2	Higher-Order Profiling	66
4.5.3	Irreversible State Change	69

1 Languages

1.1 HOS

1.1.1 Syntax & Dynamic Semantics

$$\tau ::= \alpha \mid b \mid \tau_1 \times \tau_2 \mid \tau_1 \rightarrow \tau_2 \mid \forall \alpha. \tau \mid \exists \alpha. \tau \mid \mu \alpha. \tau \mid \text{ref } \tau$$

$$e ::= x \mid l \mid \langle e_1, e_2 \rangle \mid e.1 \mid e.2 \mid \lambda x:\tau. e \mid e_1 e_2 \mid \Lambda \alpha. e \mid e \tau \mid \\ \text{pack } \langle \tau_1, e \rangle \text{ as } \tau_2 \mid \text{unpack } e_1 \text{ as } \langle \alpha, x \rangle \text{ in } e_2 \mid \\ \text{roll}_\tau e \mid \text{unroll } e \mid \text{ref } e \mid e_1 := e_2 \mid !e \mid e_1 == e_2 \mid \dots$$

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

$$C ::= \bullet \mid \langle C, e_2 \rangle \mid \langle e_1, C \rangle \mid C.1 \mid C.2 \mid \lambda x:\tau. C \mid C e_2 \mid e_1 C \mid \Lambda \alpha. C \mid C \tau \mid \\ \text{pack } \langle \tau_1, C \rangle \text{ as } \tau_2 \mid \text{unpack } C \text{ as } \langle \alpha, x \rangle \text{ in } e_2 \mid \text{unpack } e_1 \text{ as } \langle \alpha, x \rangle \text{ in } C \mid \\ \text{roll}_\tau C \mid \text{unroll } C \mid \text{ref } C \mid C := e_2 \mid e_1 := C \mid !C \mid C == e_2 \mid e_1 == C \mid \dots$$

$$K ::= \bullet \mid \langle K, e_2 \rangle \mid \langle v_1, K \rangle \mid K.1 \mid K.2 \mid K e_2 \mid v_1 K \mid K \tau \mid \\ \text{pack } \langle \tau_1, K \rangle \text{ as } \tau_2 \mid \text{unpack } K \text{ as } \langle \alpha, x \rangle \text{ in } e_2 \mid \\ \text{roll}_\tau K \mid \text{unroll } K \mid \text{ref } K \mid K := e_2 \mid v_1 := K \mid !K \mid K == e_2 \mid v_1 == K \mid \dots$$

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

$$\langle h; e \rangle \hookrightarrow^k \langle h'; e' \rangle \stackrel{\text{def}}{\iff} \exists h_0, \dots, h_k, e_0, \dots, e_k. \langle h_0; e_0 \rangle = \langle h; e \rangle \wedge \langle h_k; e_k \rangle = \langle h'; e' \rangle \wedge \\ \forall i \in \{0, \dots, k-1\}. \langle h_i; e_i \rangle \hookrightarrow \langle h_{i+1}; e_{i+1} \rangle$$

$$\langle h; e \rangle \downarrow^{<k} \stackrel{\text{def}}{\iff} \exists k', h', v. k' < k \wedge \langle h; e \rangle \hookrightarrow^{k'} \langle h'; v \rangle$$

$$\langle h; e \rangle \downarrow \stackrel{\text{def}}{\iff} \exists k. \langle h; e \rangle \downarrow^{<k}$$

1.1.2 Static Semantics

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

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

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

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

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

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

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

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

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

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

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

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

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

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

...

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

...

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

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

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

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

1.1.3 Contextual and CIU Approximation

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

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

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

$$\begin{array}{l}
\tau ::= \dots \mid \text{exn} \\
e ::= \dots \mid c_{\text{exn}} \mid \text{raise}_{\tau} e \mid \text{try } e_1 \text{ with } x.e_2 \\
v ::= \dots \mid c_{\text{exn}} \\
C ::= \dots \mid \text{raise}_{\tau} C \mid \text{try } C \text{ with } x.e_2 \mid \text{try } e_1 \text{ with } x.C \\
K ::= \dots \mid \text{raise}_{\tau} K \mid \text{try } K \text{ with } x.e_2
\end{array}$$

$$\begin{array}{l}
\dots \\
\langle h; K[\text{raise}_{\tau} v] \rangle \quad \hookrightarrow \langle h; \text{raise}_{\tau} v \rangle \quad (K \neq \bullet \text{ and } K \text{ does not try}) \\
\langle h; K_1[\text{try } K_2[\text{raise}_{\tau} v] \text{ with } x.e_2] \rangle \hookrightarrow \langle h; K_1[e_2[v/x]] \rangle \quad (K_2 \text{ does not try}) \\
\langle h; K_1[\text{try } v \text{ with } x.e_2] \rangle \quad \hookrightarrow \langle h; K_1[v] \rangle
\end{array}$$

1.2.2 Static Semantics

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

$$\dots \quad \frac{}{\Sigma; \Delta; \Gamma \vdash c_{\text{exn}} : \text{exn}}$$

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

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

...

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

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

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

1.3 HOSC

HOSC is obtained from HOS by making the following extensions.

1.3.1 Syntax & Dynamic Semantics

$$\begin{aligned}
\tau & ::= \dots \mid \text{cont } \tau \\
e & ::= \dots \mid \text{cont}_\tau K \mid \text{call/cc}_\tau(x. e) \mid \text{throw}_\tau e_1 \text{ to } e_2 \\
v & ::= \dots \mid \text{cont}_\tau K \\
C & ::= \dots \mid \text{call/cc}_\tau(x. C) \mid \text{throw}_\tau C \text{ to } e_2 \mid \text{throw}_\tau e_1 \text{ to } C \\
K & ::= \dots \mid \text{call/cc}_\tau(x. K) \mid \text{throw}_\tau K \text{ to } e_2 \mid \text{throw}_\tau v_1 \text{ to } K
\end{aligned}$$

$$\begin{aligned}
& \dots \\
\langle h; K[\text{call/cc}_\tau(x. e)] \rangle & \hookrightarrow \langle h; K[e[\text{cont}_\tau K/x]] \rangle \\
\langle h; K[\text{throw}_\tau v \text{ to } \text{cont}_{\tau'} K'] \rangle & \hookrightarrow \langle h; K'[v] \rangle
\end{aligned}$$

1.3.2 Static Semantics

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

...

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

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

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

...

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

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

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

1.4 FOS

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

$$\tau ::= \dots \mid \text{ref } b \mid \dots$$

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

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

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

$$\begin{aligned}
[\iota_1, \dots, \iota_m]_k &\stackrel{\text{def}}{=} ([\iota_1]_k, \dots, [\iota_m]_k) \\
[(s, \delta, \varphi, \zeta, H)]_k &\stackrel{\text{def}}{=} (s, \delta, \varphi, \zeta, [H]_k) \\
[H]_k &\stackrel{\text{def}}{=} \lambda s. [H(s)]_k \\
[\psi]_k &\stackrel{\text{def}}{=} \{(W, h_1, h_2) \in r \mid W.k < k\}
\end{aligned}$$

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

$$\begin{aligned}
(k', \Sigma'_1, \Sigma'_2, \omega') \sqsupseteq (k, \Sigma_1, \Sigma_2, \omega) &\stackrel{\text{def}}{=} k' \leq k \wedge \Sigma'_1 \supseteq \Sigma_1 \wedge \Sigma'_2 \supseteq \Sigma_2 \wedge \omega' \sqsupseteq [\omega]_{k'} \\
(\iota'_1, \dots, \iota'_{m'}) \sqsupseteq (\iota_1, \dots, \iota_m) &\stackrel{\text{def}}{=} m' \geq m \wedge \forall j \in \{1, \dots, m\}. \iota'_j \sqsupseteq \iota_j \\
(s', \delta', \varphi', \zeta', H') \sqsupseteq (s, \delta, \varphi, \zeta, H) &\stackrel{\text{def}}{=} (\delta', \varphi', \zeta', H') = (\delta, \varphi, \zeta, H) \wedge (s, s') \in \delta \\
(k', \Sigma'_1, \Sigma'_2, \omega') \sqsupseteq^{\text{pub}} (k, \Sigma_1, \Sigma_2, \omega) &\stackrel{\text{def}}{=} k' \leq k \wedge \Sigma'_1 \supseteq \Sigma_1 \wedge \Sigma'_2 \supseteq \Sigma_2 \wedge \omega' \sqsupseteq^{\text{pub}} [\omega]_{k'} \\
(\iota'_1, \dots, \iota'_{m'}) \sqsupseteq^{\text{pub}} (\iota_1, \dots, \iota_m) &\stackrel{\text{def}}{=} m' \geq m \wedge \forall j \in \{1, \dots, m\}. \iota'_j \sqsupseteq^{\text{pub}} \iota_j \wedge \\
&\quad \forall j \in \{m+1, \dots, m'\}. \text{safe}(\iota'_j) \\
(s', \delta', \varphi', \zeta', H') \sqsupseteq^{\text{pub}} (s, \delta, \varphi, \zeta, H) &\stackrel{\text{def}}{=} (\delta', \varphi', \zeta', H') = (\delta, \varphi, \zeta, H) \wedge (s, s') \in \varphi
\end{aligned}$$

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

$$\begin{aligned}
\psi \otimes \psi' &\stackrel{\text{def}}{=} \{(W, h_1 \uplus h'_1, h_2 \uplus h'_2) \mid (W, h_1, h_2) \in \psi \wedge (W, h'_1, h'_2) \in \psi'\} \\
(h_1, h_2) : W &\stackrel{\text{def}}{=} \vdash h_1 : W.\Sigma_1 \wedge \vdash h_2 : W.\Sigma_2 \wedge \\
&\quad (W.k > 0 \implies (\triangleright W, h_1, h_2) \in \bigotimes_{i=1}^{|W.\omega|} W.\omega(i).H(W.\omega(i).s))
\end{aligned}$$

$$\begin{aligned}
\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' \rightarrow \tau]\rho &\stackrel{\text{def}}{=} \{(W, \lambda x:\tau_1. e_1, \lambda x:\tau_2. e_2) \in \text{TermAtom}[\rho_1(\tau' \rightarrow \tau), \rho_2(\tau' \rightarrow \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, \text{pack } \langle \tau_1, v_1 \rangle \text{ as } \tau'_1, \text{pack } \langle \tau_2, v_2 \rangle \text{ 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, \text{roll}_{\tau_1} v_1, \text{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}[\text{ref } \tau]\rho &\stackrel{\text{def}}{=} \{(W, l_1, l_2) \in \text{TermAtom}[\rho_1(\text{ref } \tau), \rho_2(\text{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^{\text{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}[\text{ref } \tau]\emptyset\} \\
\Sigma; \Delta; \Gamma \vdash e_1 \lesssim_{\log} e_2 : \tau &\stackrel{\text{def}}{=} \Sigma; \Delta; \Gamma \vdash e_1 : \tau \wedge \Sigma; \Delta; \Gamma \vdash e_2 : \tau \wedge \\
&\quad \forall W, \rho, \gamma. W \in \mathcal{S}[\Sigma] \wedge \rho \in \mathcal{D}[\Delta] \wedge (W, \gamma) \in \mathcal{G}[\Gamma]\rho \implies \\
&\quad (W, \rho_1 \gamma_1 e_1, \rho_2 \gamma_2 e_2) \in \mathcal{E}[\tau]\rho
\end{aligned}$$

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

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

2.2 HOSE

One addition and one change:

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

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

2.3 HOSC

One addition and one change:

$$\mathcal{V}[\llbracket \text{cont } \tau \rrbracket \rho] \stackrel{\text{def}}{=} \{(W, \text{cont}_{\rho_1 \tau} K_1, \text{cont}_{\rho_2 \tau} K_2) \mid (W, K_1, K_2) \in \mathcal{K}[\llbracket \tau \rrbracket \rho]\}$$

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

2.4 FOS

A few simple changes:

$$\text{HeapAtom}_n \stackrel{\text{def}}{=} \text{Heap} \times \text{Heap}$$

$$\text{HeapRel}_n \stackrel{\text{def}}{=} \{\psi \subseteq \text{HeapAtom}_n\}$$

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

$$\psi \otimes \psi' \stackrel{\text{def}}{=} \{(h_1 \uplus h'_1, h_2 \uplus h'_2) \mid (h_1, h_2) \in \psi \wedge (h'_1, h'_2) \in \psi'\}$$

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

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

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 $\text{consistent}(W)$ 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 $W \sqsupseteq^{\text{pub}} W$.

□

Lemma 6 (Irrelevance). If $\text{fv}(\tau) \subseteq \text{dom}(\rho)$ and $\rho(\alpha) = \rho'(\alpha)$ for all $\alpha \in \text{dom}(\rho)$, 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 $W.\Sigma_1; \cdot \vdash \gamma_1 : \rho_1 \Gamma$ and $W.\Sigma_2; \cdot \vdash \gamma_2 : \rho_2 \Gamma$.

Lemma 8.

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

Proof.

1. Obvious from the definitions (state transitions are reflexive).
2. • Suppose there is $W.\omega(j).s \in W.\omega(j).\dot{\downarrow}$ for some $j \in \{1, \dots, |W.\omega|\}$.

- By definition of $W' \sqsupseteq^{\text{pub}} W$ we then have $W.\omega(j).s \in W'.\omega(j).\dot{s}$ and $(W.\omega(j).s, W'.\omega(j).s) \in W'.\omega(j).\varphi$.
 - Hence the definition of Island implies $W'.\omega(j).s \in W.\omega'(j).\dot{s}$, which is in contradiction with $\text{consistent}(W')$.
3. • Say $W'.\omega = (\iota'_1, \dots, \iota'_{m'})$ and $W.\omega = (\iota_1, \dots, \iota_m)$.
- Suppose $j \in \{1, \dots, m'\}$ and $(\iota'_j.s, s) \in \iota'_j.\varphi$.
 - To show: $s \notin \iota'_j.\dot{s}$
 - We distinguish whether or not the island in question was already present in W .
 - (a) Case $j \in \{m+1, \dots, m'\}$:
 - Then $\text{safe}(\iota'_j)$ by definition of \sqsupseteq^{pub} .
 - Instantiating this yields the claim.
 - (b) Case $j \in \{1, \dots, m\}$:
 - 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 $\text{safe}(\iota_j)$.
 - Instantiating this yields $s \notin \iota_j.\dot{s}$.
 - Since $\iota_j.\dot{s} = \iota'_j.\dot{s}$, we are done.

□

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

1. \sqsupseteq is transitive and reflexive.
2. \sqsupseteq^{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 $W' \sqsupseteq^{\text{pub}} W$ 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 $(W, h_1, h_2) \in \psi \in \text{HeapRel}$, 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 $\Sigma; \Delta; \Gamma \vdash x \lesssim_{\log} x : \tau$.

Proof.

- Suppose $W \in \mathcal{S}[\Sigma]$, $\rho \in \mathcal{D}[\Delta]$, and $(W, \gamma) \in \mathcal{G}[\Gamma]\rho$.
- It suffices to show $(W, \rho_1\gamma_1x, \rho_2\gamma_2x) \in \mathcal{V}[\tau]\rho$.
- We know $(W, \gamma_1x, \gamma_2x) \in \mathcal{V}[\tau]\rho$.
- By definition of TermAtom, γ_1x and γ_2x contain no free type variables, so $\gamma_1x = \rho_1\gamma_1x$ and $\gamma_2x = \rho_2\gamma_2x$.

□

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

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 $W' \sqsupseteq^{\text{pub}} W$ 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 $\Sigma; \Delta; \Gamma \vdash e_1 \lesssim_{\log} e_2 : \tau \times \tau'$, then $\Sigma; \Delta; \Gamma \vdash e_{1.1} \lesssim_{\log} e_{2.1} : \tau$.

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 $W' \sqsupseteq^{\text{pub}} W$ 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 $\Sigma; \Delta; \Gamma, x:\tau' \vdash e_1 \lesssim_{\log} e_2 : \tau$, then $\Sigma; \Delta; \Gamma \vdash \lambda x:\tau'. e_1 \lesssim_{\log} \lambda x:\tau'. e_2 : \tau' \rightarrow \tau$.

Proof.

- Suppose $W \in \mathcal{S}[\Sigma]$, $\rho \in \mathcal{D}[\Delta]$, and $(W, \gamma) \in \mathcal{G}[\Gamma]\rho$.
- It suffices to show $(W, \lambda x:\rho_1\tau'. \rho_1\gamma_1e_1, \lambda x:\rho_2\tau'. \rho_2\gamma_2e_2) \in \mathcal{V}[\tau' \rightarrow \tau]\rho$.
- 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: $(W', K_1[(\rho_1\gamma_1e_1)[v_1/x]], K_2[(\rho_2\gamma_2e_2)[v_2/x]]) \in \mathcal{O}$
- By definition of TermAtom, v_1 and v_2 contain no free type variables, so $K_1[(\rho_1\gamma_1e_1)[v_1/x]] = K_1[\rho_1\gamma'_1e_1]$ and $K_2[(\rho_2\gamma_2e_2)[v_2/x]] = K_2[\rho_2\gamma'_2e_2]$ 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 $(W', \rho_1\gamma'_1e_1, \rho_2\gamma'_2e_2) \in \mathcal{E}[\tau]\rho$, which in turn yields the claim.

□

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

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 $(W, v_1, v_2) \in \mathcal{V}[\tau' \rightarrow \tau]\rho$.
- So suppose $W' \sqsupseteq^{\text{pub}} W$ 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 $(W, v_1, v_2) \in \mathcal{V}[\tau' \rightarrow \tau]\rho$ 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 $\Sigma; \Delta, \alpha; \Gamma \vdash e_1 \lesssim_{\log} e_2 : \tau$, then $\Sigma; \Delta; \Gamma \vdash \Lambda\alpha.e_1 \lesssim_{\log} \Lambda\alpha.e_2 : \forall\alpha.\tau$.

Proof.

- Suppose $W \in \mathcal{S}[\Sigma]$, $\rho \in \mathcal{D}[\Delta]$, and $(W, \gamma) \in \mathcal{G}[\Gamma]\rho$.
- It suffices to show $(W, \Lambda\alpha.\rho_1\gamma_1e_1, \Lambda\alpha.\rho_2\gamma_2e_2) \in \mathcal{V}[\forall\alpha.\tau]\rho$.
- 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: $(W', K_1[(\rho_1\gamma_1e_1)[\tau_1/\alpha]], K_2[(\rho_2\gamma_2e_2)[\tau_2/\alpha]]) \in \mathcal{O}$
- Note that
 - $K_1[(\rho_1\gamma_1e_1)[\tau_1/\alpha]] = K_1[\rho'_1\gamma_1e_1]$ and
 - $K_2[(\rho_2\gamma_2e_2)[\tau_2/\alpha]] = K_2[\rho'_2\gamma_2e_2]$.
- 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 $(W', \rho'_1\gamma_1e_1, \rho'_2\gamma_2e_2) \in \mathcal{E}[\tau]\rho'$.
- Instantiating this with $(W', K_1, K_2) \in \mathcal{K}[\tau]\rho'$ yields the claim.

□

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

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 $W' \sqsupseteq^{\text{pub}} W$ 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 $\Sigma; \Delta; \Gamma \vdash e_1 \lesssim_{\log} e_2 : \tau[\tau'/\alpha]$, then $\Sigma; \Delta; \Gamma \vdash \text{pack } \langle \tau', e_1 \rangle \text{ as } \exists \alpha. \tau \lesssim_{\log} \text{pack } \langle \tau', e_2 \rangle \text{ as } \exists \alpha. \tau : \exists \alpha. \tau$.

Proof.

- This reduces to showing $(W, K_1[\text{pack } \langle \rho_1 \tau', \bullet \rangle \text{ as } \exists \alpha. \rho_1 \tau], K_2[\text{pack } \langle \rho_2 \tau', \bullet \rangle \text{ as } \exists \alpha. \rho_2 \tau]) \in \mathcal{K}[\tau[\tau'/\alpha]]\rho$ for $(W, K_1, K_2) \in \mathcal{K}[\exists \alpha. \tau]\rho$.
- So suppose $W' \sqsupseteq^{\text{pub}} W$ and $(W', v_1, v_2) \in \mathcal{V}[\tau[\tau'/\alpha]]\rho$.
- To show: $(W', K_1[\text{pack } \langle \rho_1 \tau', v_1 \rangle \text{ as } \exists \alpha. \rho_1 \tau], K_2[\text{pack } \langle \rho_2 \tau', v_2 \rangle \text{ as } \exists \alpha. \rho_2 \tau]) \in \mathcal{O}$
- This follows from $(W, K_1, K_2) \in \mathcal{K}[\exists \alpha. \tau]\rho$, if we can show $(W', \text{pack } \langle \rho_1 \tau', v_1 \rangle \text{ as } \exists \alpha. \rho_1 \tau, \text{pack } \langle \rho_2 \tau', v_2 \rangle \text{ as } \exists \alpha. \rho_2 \tau) \in \mathcal{V}[\exists \alpha. \tau]\rho$.
- 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 $\Sigma; \Delta; \Gamma \vdash e_1 \lesssim_{\log} e_2 : \exists \alpha. \tau$ and $\Sigma; \Delta, \alpha; \Gamma, x:\tau \vdash e_3 \lesssim_{\log} e_4 : \tau'$ and $\Delta \vdash \tau'$, then $\Sigma; \Delta; \Gamma \vdash \text{unpack } e_1 \text{ as } \langle \alpha, x \rangle \text{ in } e_3 \lesssim_{\log} \text{unpack } e_2 \text{ as } \langle \alpha, x \rangle \text{ in } e_4 : \tau'$.

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: $(W, K_1[\text{unpack } \rho_1 \gamma_1 e_1 \text{ as } \langle \alpha, x \rangle \text{ in } \rho_1 \gamma_1 e_3], K_2[\text{unpack } \rho_2 \gamma_2 e_2 \text{ as } \langle \alpha, x \rangle \text{ in } \rho_2 \gamma_2 e_4]) \in \mathcal{O}$
- This follows from instantiating the first premise if we can show $(W, K_1[\text{unpack } \bullet \text{ as } \langle \alpha, x \rangle \text{ in } \rho_1 \gamma_1 e_3], K_2[\text{unpack } \bullet \text{ as } \langle \alpha, x \rangle \text{ in } \rho_2 \gamma_2 e_4]) \in \mathcal{K}[\exists \alpha. \tau]\rho$.
- So suppose $W' \sqsupseteq^{\text{pub}} W$ and $(W', v_1, v_2) \in \mathcal{V}[\exists \alpha. \tau]\rho$.
- To show: $(W', K_1[\text{unpack } v_1 \text{ as } \langle \alpha, x \rangle \text{ in } \rho_1 \gamma_1 e_3], K_2[\text{unpack } v_2 \text{ as } \langle \alpha, x \rangle \text{ in } \rho_2 \gamma_2 e_4]) \in \mathcal{O}$
- We know $v_1 = \text{pack } \langle \tau_1, v'_1 \rangle \text{ as } \tau'_1$ and $v_2 = \text{pack } \langle \tau_2, v'_2 \rangle \text{ as } \tau'_2$ 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 $r \in \text{ValRel}$.
- 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 $(\rho_1\gamma_1e_3)[\tau_1/\alpha][v'_1/x] = \rho'_1\gamma'_1e_3$ as well as $(\rho_2\gamma_2e_4)[\tau_2/\alpha][v'_2/x] = \rho'_2\gamma'_2e_4$.
- Instantiating the second premise yields $(W', \rho'_1\gamma'_1e_3, \rho'_2\gamma'_2e_4) \in \mathcal{E}[\![\tau']\!] \rho'$.
- Since $(W', K_1, K_2) \in \mathcal{K}[\![\tau']\!] \rho$ by monotonicity (Lemma 10) and $\alpha \notin \text{fv}(\tau')$, instantiating $(W', \rho'_1\gamma'_1e_3, \rho'_2\gamma'_2e_4) \in \mathcal{E}[\![\tau']\!] \rho'$ yields the claim.

□

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

Proof.

- This reduces to showing $(W, K_1[\text{roll}_{\mu\alpha. \rho_1\tau} \bullet], K_2[\text{roll}_{\mu\alpha. \rho_2\tau} \bullet]) \in \mathcal{K}[\![\tau[\mu\alpha. \tau/\alpha]]\!] \rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\mu\alpha. \tau]\!] \rho$.
- So suppose $W' \sqsupseteq^{\text{pub}} W$ and $(W', v_1, v_2) \in \mathcal{V}[\![\tau[\mu\alpha. \tau/\alpha]]\!] \rho$.
- To show: $(W', K_1[\text{roll}_{\mu\alpha. \rho_1\tau} v_1], K_2[\text{roll}_{\mu\alpha. \rho_2\tau} v_2]) \in \mathcal{O}$
- This follows from $(W, K_1, K_2) \in \mathcal{K}[\![\mu\alpha. \tau]\!] \rho$, if we can show $(W', \text{roll}_{\mu\alpha. \rho_1\tau} v_1, \text{roll}_{\mu\alpha. \rho_2\tau} v_2) \in \mathcal{V}[\![\mu\alpha. \tau]\!] \rho$.
- If $W'.k > 0$, then by monotonicity (Lemma 10) $(\triangleright W', v_1, v_2) \in \mathcal{V}[\![\tau[\mu\alpha. \tau/\alpha]]\!] \rho$.
- 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 $\Sigma; \Delta; \Gamma \vdash e_1 \lesssim_{\log} e_2 : \mu\alpha. \tau$, then $\Sigma; \Delta; \Gamma \vdash \text{unroll} e_1 \lesssim_{\log} \text{unroll} e_2 : \tau[\mu\alpha. \tau/\alpha]$.

Proof.

- This reduces to showing $(W, K_1[\text{unroll} \bullet], K_2[\text{unroll} \bullet]) \in \mathcal{K}[\![\mu\alpha. \tau]\!] \rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\tau[\mu\alpha. \tau/\alpha]]\!] \rho$.
- So suppose $W' \sqsupseteq^{\text{pub}} W$, $(W', v_1, v_2) \in \mathcal{V}[\![\mu\alpha. \tau]\!] \rho$, $(h_1, h_2) : W'$, and $\langle h_1; K_1[\text{unroll} v_1] \rangle \downarrow^{<W'.k}$.
- To show: $\text{consistent}(W')$ and $\langle h_2; K_2[\text{unroll} v_2] \rangle \downarrow$.
- We know $v_1 = \text{roll}_{\tau_1} v'_1$ and $v_2 = \text{roll}_{\tau_2} v'_2$ with $(W', v'_1, v'_2) \in \triangleright \mathcal{V}[\![\tau[\mu\alpha. \tau/\alpha]]\!] \rho$.
- Note that
 - $\langle h_1; K_1[\text{unroll} v_1] \rangle \downarrow^{<W'.k} \iff \langle h_1; K_1[v'_1] \rangle \downarrow^{<W'.k-1}$ and
 - $\langle h_2; K_2[\text{unroll} v_2] \rangle \downarrow \iff \langle h_2; K_2[v'_2] \rangle \downarrow$.
- 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 $\Sigma; \Delta; \Gamma \vdash e_1 \lesssim_{\log} e_2 : \tau$, then $\Sigma; \Delta; \Gamma \vdash \text{ref } e_1 \lesssim_{\log} \text{ref } e_2 : \text{ref } \tau$.

Proof.

- This reduces to showing $(W, K_1[\text{ref } \bullet], K_2[\text{ref } \bullet]) \in \mathcal{K}[\tau]\rho$ for $(W, K_1, K_2) \in \mathcal{K}[\text{ref } \tau]\rho$.
- So suppose $W' \sqsupseteq^{\text{pub}} W$, $(W', v_1, v_2) \in \mathcal{V}[\tau]\rho$, $(h_1, h_2) : W'$, and $\langle h_1; K_1[\text{ref } v_1] \rangle \downarrow^{<W'.k}$.
- To show: $\text{consistent}(W')$ and $\langle h_2; K_2[\text{ref } v_2] \rangle \downarrow$.
- Note that
 - $\langle h_1; K_1[\text{ref } v_1] \rangle \downarrow^{<W'.k} \iff \langle h_1 \uplus \{l_1 \mapsto v_1\}; K_1[l_1] \rangle \downarrow^{<W'.k-1}$ (where l_1 fresh) and
 - $\langle h_2; K_2[\text{ref } v_2] \rangle \downarrow \iff \langle h_2 \uplus \{l_2 \mapsto v_2\}; K_2[l_2] \rangle \downarrow$ (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 $W'' \sqsupseteq^{\text{pub}} W' \sqsupseteq^{\text{pub}} W$.
- 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 $(W'', l_1, l_2) \in \mathcal{V}[\text{ref } \tau]\rho$.
- The latter holds by construction.
- For the former note that from $(h_1, h_2) : W'$ we know $h_1 = h_1^1 \uplus \dots \uplus h_1^{|W'.\omega|}$ and $h_2 = h_2^1 \uplus \dots \uplus h_2^{|W'.\omega|}$ with $(\triangleright W', h_1^j, h_2^j) \in W'.\omega(j).H(W'.\omega(j).s)$ for all $j \in \{1, \dots, |W'.\omega|\}$.
- 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 $j \in \{1, \dots, |W'.\omega|\}$.
- 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 $j \in \{1, \dots, |W'.\omega|\}$.
- 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 $\Sigma; \Delta; \Gamma \vdash e_1 \lesssim_{\log} e_2 : \text{ref } \tau$ and $\Sigma; \Delta; \Gamma \vdash e_3 \lesssim_{\log} e_4 : \tau$, then $\Sigma; \Delta; \Gamma \vdash e_1 := e_3 \lesssim_{\log} e_2 := e_4 : \text{unit}$.

Proof.

- Suppose $W \in \mathcal{S}[\Sigma]$, $\rho \in \mathcal{D}[\Delta]$, and $(W, \gamma) \in \mathcal{G}[\Gamma]\rho$.
- To show: $(W, \rho_1 \gamma_1 e_1 := \rho_1 \gamma_1 e_3, \rho_2 \gamma_2 e_2 := \rho_2 \gamma_2 e_4) \in \mathcal{E}[\text{unit}]\rho$
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\text{unit}]\rho$, $(h_1, h_2) : W$, 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 $(W, \rho_1 \gamma_1 e_1, \rho_2 \gamma_2 e_2) \in \mathcal{E}[\![\text{ref } \tau]\!] \rho$, it suffices to show $(W, K_1[\bullet := \rho_1 \gamma_1 e_3], K_2[\bullet := \rho_2 \gamma_2 e_4]) \in \mathcal{K}[\![\text{ref } \tau]\!] \rho$.
- So suppose $W' \sqsupseteq^{\text{pub}} W$, $(W', v_1, v_2) \in \mathcal{V}[\![\text{ref } \tau]\!] \rho$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K_1[v_1 := \rho_1 \gamma_1 e_3] \rangle \downarrow^{<W'.k}$.
- To show: $\text{consistent}(W')$ 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 $W'' \sqsupseteq^{\text{pub}} W'$, $(W'', v_3, v_4) \in \mathcal{V}[\![\tau]\!] \rho$, $(h''_1, h''_2) : W''$, and $\langle h''_1; K_1[v_1 := v_3] \rangle \downarrow^{<W''.k}$.
- To show: $\text{consistent}(W'')$ and $\langle h''_2; K_2[v_2 := v_4] \rangle \downarrow$
- From $(W', v_1, v_2) \in \mathcal{V}[\![\text{ref } \tau]\!] \rho$, $W'' \sqsupseteq^{\text{pub}} W'$ and $(h''_1, h''_2) : W''$ we know $v_1 \in \text{dom}(h''_1)$ and $v_2 \in \text{dom}(h''_2)$.
- 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 $(W'', K_1, K_2) \in \mathcal{K}[\![\text{unit}]\!] \rho$ by monotonicity (Lemma 10).
- We show $(h''_1[v_1 \mapsto v_3], h''_2[v_2 \mapsto v_4]) : W''$:
 - Due to $(W', v_1, v_2) \in \mathcal{V}[\![\text{ref } \tau]\!] \rho$, $W'' \sqsupseteq^{\text{pub}} W'$ 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 $(W'', \langle \rangle, \langle \rangle) \in \mathcal{V}[\![\text{unit}]\!] \rho$, instantiating $(W'', K_1, K_2) \in \mathcal{K}[\![\text{unit}]\!] \rho$ yields $\text{consistent}(W'')$ and $\langle h''_2[v_2 \mapsto v_4]; K_2[\langle \rangle] \rangle \downarrow$.

□

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

Proof.

- This reduces to showing $(W, K_1[! \bullet], K_2[! \bullet]) \in \mathcal{K}[\![\text{ref } \tau]\!] \rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\tau]\!] \rho$.
- So suppose $W' \sqsupseteq^{\text{pub}} W$, $(W', v_1, v_2) \in \mathcal{V}[\![\text{ref } \tau]\!] \rho$, $(h_1, h_2) : W'$, and $\langle h_1; K_1[!v_1] \rangle \downarrow^{<W'.k}$.
- To show: $\text{consistent}(W')$ and $\langle h_2; K_2[!v_2] \rangle \downarrow$
- From $(W', v_1, v_2) \in \mathcal{V}[\![\text{ref } \tau]\!] \rho$ and $(h_1, h_2) : W'$ we know $v_1 \in \text{dom}(h_1)$ and $v_2 \in \text{dom}(h_2)$.
- 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 $(W', v_1, v_2) \in \mathcal{V}[\![\text{ref } \tau]\!] \rho$ and $(h_1, h_2) : W'$.

□

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

Proof.

- This reduces to showing $(W, K_1[l_1 == \bullet], K_2[l_2 == \bullet]) \in \mathcal{K}[\![\text{ref } \tau']\!] \rho$ for $(W, K_1, K_2) \in \mathcal{K}[\![\text{bool}]\!] \rho$ and $(W, l_1, l_2) \in \mathcal{V}[\![\text{ref } \tau]\!] \rho$.
- So suppose $W' \sqsupseteq^{\text{pub}} W$, $(W', l_3, l_4) \in \mathcal{V}[\![\text{ref } \tau']\!] \rho$, $(h_1, h_2) : W'$, and $\langle h_1; K_1[l_1 == l_3] \rangle \downarrow^{<W'.k}$.
- To show: $\text{consistent}(W')$ and $\langle h_2; K_2[l_2 == l_4] \rangle \downarrow$.
- Assume $l_1 = l_3$ (the other case is analogous):
- Then $\langle h_1; K_1[\text{tt}] \rangle \downarrow^{<W'.k-1}$.
- By monotonicity (Lemma 10) we know $(W', l_1, l_2) \in \mathcal{V}[\![\text{ref } \tau]\!] \rho$.
- Consequently there are i, j such that:
 1. $(l_1, l_2) \in \text{bij}(W'.\omega(i).s)$ 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. $(l_3, l_4) \in \text{bij}(W'.\omega(j).s)$ 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 $\langle h_1; K_1[\text{ff}] \rangle \downarrow^{<W'.k}$ and $\langle h_2; K_2[l_2 == l_4] \rangle \downarrow$ would be implied by $\langle h_2; K_2[\text{ff}] \rangle \downarrow$.
 - The claims then follow from $(W, K_1, K_2) \in \mathcal{K}[\![\text{bool}]\!] \rho$ and $(W', \text{ff}, \text{ff}) \in \mathcal{V}[\![\text{bool}]\!] \rho$.
- Case $i = j$:
 - Then $(l_1, l_2) \in \text{bij}(W'.\omega(i).s)$ and $(l_3, l_4) \in \text{bij}(W'.\omega(j).s)$ 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 $(W', \text{tt}, \text{tt}) \in \mathcal{V}[\![\text{bool}]\!] \rho$.

□

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

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

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

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

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

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:

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

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 $\Sigma; \Delta; \Gamma \vdash v \lesssim_{\log}^{\text{val}} v : \tau$.

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

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

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

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

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). \square

Lemma 32 (Adequacy). If $\Sigma; \cdot; \cdot \vdash e_1 \lesssim_{\log} e_2 : \tau$ 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 $\text{safe}(W)$.

- Instantiating $\Sigma; \cdot; \cdot \vdash e_1 \lesssim_{\log} e_2 : \tau$ 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 $W' \sqsupseteq^{\text{pub}} W$, $(W', v_1, v_2) \in \mathcal{V}[\tau]\emptyset$, $(h_1, h_2) : W'$ and $\langle h_1; v_1 \rangle \downarrow^{<W'.k}$.
- We need to show $\text{consistent}(W')$ and $\langle h_2; v_2 \rangle \downarrow$.
- The former follows from $\text{safe}(W)$ by Lemma 8 and the latter is immediate.

□

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

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), $\Sigma'; \cdot; \cdot \vdash C[e_1] \lesssim_{\log} C[e_2] : \tau'$.
- By adequacy (Lemma 32), $\langle h; C[e_2] \rangle \downarrow$.

□

3.1.3 Completeness

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

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 $\Delta = \alpha_1, \dots, \alpha_m$ and $\delta(\alpha_i) = \sigma_i$ as well as $\Gamma = x_1:\tau_1, \dots, x_n:\tau_n$ and $\gamma(x_i) = v_i$.
- Let $C' := (\Lambda\alpha_1 \dots \Lambda\alpha_m. \lambda x_1:\tau_1. \dots \lambda x_n:\tau_n. \bullet) \sigma_1 \dots \sigma_m v_1 \dots v_n$ 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 $\Sigma; \Delta; \Gamma \vdash e_1 \lesssim_{\text{ctx}} e_2 : \tau$.

□

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

Proof.

- Suppose $W \in \mathcal{S}[\Sigma]$, $\rho \in \mathcal{D}[\Delta]$, and $(W, \gamma) \in \mathcal{G}[\Gamma]\rho$.
- To show: $(W, \rho_1\gamma_1e_1, \rho_2\gamma_2e_2) \in \mathcal{E}[\tau]\rho$
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\tau]\rho$, $(h_1, h_2) : W$, and $\langle h_1; K_1[\rho_1\gamma_1e_1] \rangle \downarrow^{<W.k}$.
- To show: $\text{consistent}(W)$ and $\langle h_2; K_2[\rho_2\gamma_2e_2] \rangle \downarrow$
- By Theorem 1 we know $\Sigma; \Delta; \Gamma \vdash e_1 \lesssim_{\text{log}} e_1 : \tau$.
- Instantiating this yields $\text{consistent}(W)$ and $\langle h_2; K_2[\rho_2\gamma_2e_1] \rangle \downarrow$.
- 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 $\Sigma; \Delta; \Gamma \vdash e_1 \lesssim_{\text{ctx}} e_2 : \tau$, then $\Sigma; \Delta; \Gamma \vdash e_1 \lesssim_{\text{log}} e_2 : \tau$.

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 compatibility lemmas are:

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

Proof.

- Suppose $W \in \mathcal{S}[\Sigma]$, $\rho \in \mathcal{D}[\Delta]$, and $(W, \gamma) \in \mathcal{G}[\Gamma]\rho$.
- To show: $(W, \text{raise } \rho_1 \gamma_1 e_1, \text{raise } \rho_2 \gamma_2 e_2) \in \mathcal{E}[\tau]\rho$
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\tau]\rho$.
- To show: $(W, K_1[\text{raise } \rho_1 \gamma_1 e_1], K_2[\text{raise } \rho_2 \gamma_2 e_2]) \in \mathcal{O}$
- After instantiating the premise it suffices to show $(W, K_1[\text{raise } \bullet], K_2[\text{raise } \bullet]) \in \mathcal{K}[\text{exn}]\rho$.
- So suppose $(W', v_1, v_2) \in \mathcal{V}[\text{exn}]\rho$ for $W' \sqsupseteq^{\text{pub}} W$.
- To show: $(W', K_1[\text{raise } v_1], K_2[\text{raise } v_2]) \in \mathcal{O}$ and $(W', K_1[\text{raise } (\text{raise } v_1)], K_2[\text{raise } (\text{raise } v_2)]) \in \mathcal{O}$
- 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 $(W', K_1[\text{raise } v_1], K_2[\text{raise } v_2]) \in \mathcal{O}$, which we just did.

□

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

Proof.

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

1. – First suppose $(W', v_1, v_2) \in \mathcal{V}[\![\tau]\!] \rho$ for $W' \sqsupseteq^{\text{pub}} W$.
 - To show: $(W', K_1[\text{try } v_1 \text{ with } x.\rho_1\gamma_1e_3], K_2[\text{try } v_2 \text{ with } x.\rho_2\gamma_2e_4]) \in \mathcal{O}$
 - 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 $(W', v_1, v_2) \in \mathcal{V}[\![\text{exn}]\!] \rho$ for $W' \sqsupseteq^{\text{pub}} W$.
 - To show: $(W', K_1[\text{try raise } v_1 \text{ with } x.\rho_1\gamma_1e_3], K_2[\text{try raise } v_2 \text{ with } x.\rho_2\gamma_2e_4]) \in \mathcal{O}$
 - This reduces to showing $(W', K_1[(\rho_1\gamma_1e_3)[v_1/x]], K_2[(\rho_2\gamma_2e_4)[v_2/x]]) \in \mathcal{O}$
 - By definition of TermAtom, v_1 and v_2 contain no free type variables and hence $K_1[(\rho_1\gamma_1e_3)[v_1/x]] = K_1[\rho_1\gamma'_1e_3]$ and $K_2[(\rho_2\gamma_2e_4)[v_2/x]] = K_2[\rho_2\gamma'_2e_4]$ 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, $(W', \gamma') \in \mathcal{G}[\![\Gamma, x:\text{exn}]\!] \rho$.
 - Instantiating the second premise then yields $(W', \rho_1\gamma'_1e_3, \rho_2\gamma'_2e_4) \in \mathcal{E}[\![\tau]\!] \rho$.
 - Since $W' \sqsupseteq^{\text{pub}} W$, $(W', K_1, K_2) \in \mathcal{K}[\![\tau]\!] \rho$ by monotonicity (Lemma 10).
 - Instantiating $(W', \rho_1\gamma'_1e_3, \rho_2\gamma'_2e_4) \in \mathcal{E}[\![\tau]\!] \rho$ then yields the claim.

□

3.3 HOSC

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

3.3.1 Basic Properties

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

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

3.3.2 Soundness

Definition 1.

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

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

Proof.

- Suppose $W \in \mathcal{S}[\Sigma]$, $\rho \in \mathcal{D}[\Delta]$, and $(W, \gamma) \in \mathcal{G}[\Gamma]\rho$.
- To show: $(W, \text{cont}_{\rho_1 \tau} \rho_1 \gamma_1 K_1, \text{cont}_{\rho_2 \tau} \rho_2 \gamma_2 K_2) \in \mathcal{V}[\text{cont } \tau]\rho$
- 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 $\Sigma; \Delta; \Gamma, x:\text{cont } \tau \vdash e_1 \lesssim_{\log} e_2 : \tau$, then $\Sigma; \Delta; \Gamma \vdash \text{call/cc}_{\tau}(x. e_1) \lesssim_{\log} \text{call/cc}_{\tau}(x. e_2) : \tau$.

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: $(W, K_1[\text{call/cc}_{\rho_1 \tau}(x. \rho_1 \gamma_1 e_1)], K_2[\text{call/cc}_{\rho_2 \tau}(x. \rho_2 \gamma_2 e_2)]) \in \mathcal{O}$
- By Lemma 12 it suffices to show $(W, K_1[(\rho_1 \gamma_1 e_1)[K_1/x]], K_2[(\rho_2 \gamma_2 e_2)[K_2/x]]) \in \mathcal{O}$.
- Since $(W, K_1, K_2) \in \mathcal{K}[\tau]\rho$ implies $(W, \text{cont } K_1, \text{cont } K_2) \in \mathcal{V}[\text{cont } \tau]\rho$, we get $(W, \gamma') \in \mathcal{G}[\Gamma, x:\text{cont } \tau]\rho$ for $\gamma' = \gamma, x \mapsto (\text{cont } K_1, \text{cont } K_2)$.
- Instantiating the assumption now yields $(W, \rho_1 \gamma'_1 e_1, \rho_2 \gamma'_2 e_2) \in \mathcal{E}[\tau]\rho$
- Hence $(W, K_1[\rho_1 \gamma'_1 e_1], K_2[\rho_2 \gamma'_2 e_2]) \in \mathcal{O}$.
- By definition of ContAtom, K_1 and K_2 contain no free type variables. Consequently, $\rho_1 \gamma'_1 e_1 = (\rho_1 \gamma_1 e_1)[K_1/x]$ and $\rho_2 \gamma'_2 e_2 = (\rho_2 \gamma_2 e_2)[K_2/x]$.

□

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

Proof.

- This reduces to showing $(W, K_1[\text{throw}_{\rho_1 \tau} v_1 \text{ to } \bullet], K_2[\text{throw}_{\rho_2 \tau} v_2 \text{ to } \bullet]) \in \mathcal{K}[\llbracket \text{cont } \tau' \rrbracket] \rho$ for $(W, K_1, K_2) \in \mathcal{K}[\llbracket \tau \rrbracket] \rho$ and $(W, v_1, v_2) \in \mathcal{V}[\llbracket \tau' \rrbracket] \rho$.
- So suppose $W' \sqsupseteq^{\text{pub}} W$ and $(W', K_3, K_4) \in \mathcal{K}[\llbracket \tau' \rrbracket] \rho$.
- To show: $(W', K_1[\text{throw}_{\rho_1 \tau} v_1 \text{ to cont } K_3], K_2[\text{throw}_{\rho_2 \tau} v_2 \text{ to cont } K_4]) \in \mathcal{O}$
- 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 $(W', v_1, v_2) \in \mathcal{V}[\llbracket \tau' \rrbracket] \rho$.
- Hence instantiating $(W', K_3, K_4) \in \mathcal{K}[\llbracket \tau' \rrbracket] \rho$ yields the claim.

□

Theorem 3 (Fundamental Property).

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

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

1. In each case we use the appropriate compatibility lemma. The induction hypothesis is needed for $e = \text{cont } K$:
 - By inversion we know $\tau = \text{cont } \tau'$ and $\Sigma; \Delta; \Gamma \vdash K \div \tau'$.
 - Since $|K| < |\text{cont } K|$, part (2) of the induction hypothesis yields $\Sigma; \Delta; \Gamma \vdash K \lesssim_{\log} K \div \tau'$.
 - The claim then follows by the compatibility lemma for cont .
2.
 - Suppose $W \in \mathcal{S}[\llbracket \Sigma \rrbracket]$, $\rho \in \mathcal{D}[\llbracket \Delta \rrbracket]$, and $(W, \gamma) \in \mathcal{G}[\llbracket \Gamma \rrbracket] \rho$.
 - To show: $(W, \rho_1 \gamma_1 K, \rho_2 \gamma_2 K) \in \mathcal{K}[\llbracket \tau \rrbracket] \rho$
 - So suppose $W' \sqsupseteq^{\text{pub}} W$, $(W', v_1, v_2) \in \mathcal{V}[\llbracket \tau \rrbracket] \rho$, $(h_1, h_2) : W'$, 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 $\Sigma; \Delta; \Gamma, x:\tau \vdash K[x] \lesssim_{\log} K[x] : \tau'$ by part (1).
 - Using monotonicity (Lemma 10), it is easy to see that $W' \in \mathcal{S}[\llbracket \Sigma \rrbracket]$ and $(W', \gamma') \in \mathcal{G}[\llbracket \Gamma, x:\tau \rrbracket] \rho$ for $\gamma' := \gamma, x \mapsto (v_1, v_2)$.
 - Instantiating $\Sigma; \Delta; \Gamma, x:\tau \vdash K[x] \lesssim_{\log} K[x] : \tau'$ thus yields $(W', \rho_1 \gamma'_1 K[x], \rho_2 \gamma'_2 K[x]) \in \mathcal{E}[\llbracket \tau' \rrbracket] \rho$.
 - 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 $(W', \bullet, \bullet) \in \mathcal{K}[\llbracket \tau' \rrbracket] \rho$.
 - Instantiating $(W', \rho_1 \gamma'_1 K[x], \rho_2 \gamma'_2 K[x]) \in \mathcal{E}[\llbracket \tau' \rrbracket] \rho$ 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 `HeapAtomn`, for an n that is clear from context.

4.1 HOS

4.1.1 Deferred Divergence 1

$$\begin{aligned}
\tau &= ((\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}) \rightarrow \text{unit} \\
e_1 &= \text{let } x = \text{ref ff} \text{ in let } y = \text{ref ff} \text{ in} \\
&\quad \lambda f: (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}. f (\lambda z: \text{unit}. \text{if } !x = \text{ff} \text{ then } y := \text{tt} \text{ else } \perp); \\
&\quad \quad \quad \text{if } !y = \text{ff} \text{ then } x := \text{tt} \text{ else } \perp \\
e_2 &= \lambda f: (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}. f (\lambda z: \text{unit}. \perp)
\end{aligned}$$

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

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

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 :

$$\begin{aligned}
&\text{let } g = \bullet \text{ in} \\
&\text{let } f = (\lambda g'. g' \langle \rangle; \text{raise } c) \text{ in} \\
&\text{try } g \text{ } f \text{ with } _ \langle \rangle
\end{aligned}$$

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

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

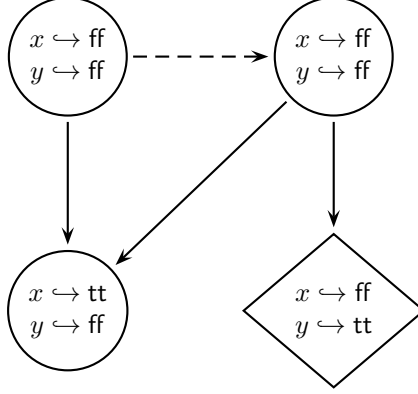
We first show $\cdot; \cdot; \cdot \vdash e_1 \lesssim_{\log} e_2 : ((\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}) \rightarrow \text{unit}$:

- This reduces to showing $(W, e_1, e_2) \in \mathcal{E}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$, where $W \in \mathcal{S}[\cdot]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_1] \rangle \downarrow^{<W.k}$.
- To show: $\text{consistent}(W)$ and $\langle h_2; K_2[e_2] \rangle \downarrow$
- $\langle h_1; K_1[e_1] \rangle \downarrow^{<W.k}$ implies $\langle h_1 \uplus \{l_x \mapsto \text{ff}\} \uplus \{l_y \mapsto \text{ff}\}; K_1[v_1[l_x/x][l_y/y]] \rangle \downarrow^{<W.k}$, where v_1 is the function value in e_1 and l_x, l_y are distinct and fresh.
- Let

$$\begin{aligned}
- & H(\langle i, j \rangle) := \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_x) = i \wedge \widetilde{h}_1(l_y) = j\} \\
- & H(\langle i, j, - \rangle) := H(\langle i, j \rangle) \\
- & \varphi := \{(\langle \text{ff}, \text{ff}, 0 \rangle, \langle \text{tt}, \text{ff} \rangle), (\langle \text{ff}, \text{ff}, 1 \rangle, \langle \text{tt}, \text{ff} \rangle), (\langle \text{ff}, \text{ff}, 1 \rangle, \langle \text{ff}, \text{tt} \rangle)\}^* \\
- & \delta := (\varphi \uplus \{(\langle \text{ff}, \text{ff}, 0 \rangle, \langle \text{ff}, \text{ff}, 1 \rangle)\})^* \\
- & \iota_s := (s, \delta, \varphi, \{\langle \text{ff}, \text{tt} \rangle\}, H)
\end{aligned}$$

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

The island represents the following STS:



- Note that $\text{safe}(\iota_{\langle \text{ff}, \text{ff}, 0 \rangle})$ and thus $W_{\langle \text{ff}, \text{ff}, 0 \rangle} \sqsupseteq^{\text{pub}} W$.
- Furthermore, using monotonicity (Lemma 10), it is easy to see that $(h_1 \uplus \{l_x \mapsto \text{ff}\} \uplus \{l_y \mapsto \text{ff}\}, h_2) : W_{\langle \text{ff}, \text{ff}, 0 \rangle}$.
- Consequently, if we can show $(W_{\langle \text{ff}, \text{ff}, 0 \rangle}, v_1[l_x/x][l_y/y], e_2) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$, then the claims follow from instantiating $(W, K_1, K_2) \in \mathcal{K}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$.
- So suppose $W' \sqsupseteq W_{\langle \text{ff}, \text{ff}, 0 \rangle}$ and $(W', \lambda g. e'_1, \lambda g. e'_2) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$, $(W', K'_1, K'_2) \in \mathcal{K}[\langle \text{unit} \rangle \emptyset]$, $(h'_1, h'_2) : W'$, 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: $\text{consistent}(W')$ and $\langle h'_2; K'_2[(\lambda g. e'_2) (\lambda z. \perp)] \rangle \downarrow$
- $\langle h'_1; K'_1[\widehat{e}_1[l_x/x][l_y/y][\lambda g. e'_1/f]] \rangle \downarrow^{<W'.k}$ implies $\langle h'_1; K'_1[e'_1] \rangle \downarrow^{<W'.k}$, where $e'_1 = (e'_1[\lambda z. \text{if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp/g]; \text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp)$.
- Notation: we write W'_s to mean the world obtained from W' by setting our island's current state to s .
- If $W' = W'_{\langle \text{ff}, \text{ff}, 0 \rangle}$, then let $\widehat{W}' := W'_{\langle \text{ff}, \text{ff}, 1 \rangle}$; otherwise let $\widehat{W}' := W'$.
- It is easy to see that $\widehat{W}' \sqsupseteq W'$.
- We now show $(\widehat{W}', e'_1[\lambda z. \text{if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp/g], e'_2[\lambda z. \perp/g]) \in \mathcal{E}[\langle \text{unit} \rangle \emptyset]$:
 - Since $(W', \lambda g. e'_1, \lambda g. e'_2) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$, it suffices to show $(\widehat{W}', \lambda z. \text{if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp, \lambda z. \perp) \in \mathcal{V}[\langle \text{unit} \rightarrow \text{unit} \rangle \emptyset]$.
 - So suppose $W'' \sqsupseteq \widehat{W}'$, $(W'', K''_1, K''_2) \in \mathcal{K}[\langle \text{unit} \rangle \emptyset]$, and $(h''_1, h''_2) : W''$.
 - We show that $\langle h''_1; K''_1[\text{if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp] \rangle \downarrow^{<W''.k}$ is impossible.
 - Case $W'' \in \{W''_{\langle \text{ff}, \text{ff}, 1 \rangle}, W''_{\langle \text{ff}, \text{tt} \rangle}\}$:

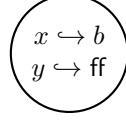
- * Then $(h''_1, h''_2) : W''$ implies $h''_1(l_x) = \text{ff}$.
- * Consequently, $\langle h''_1; K''_1[\text{if } !l_x = \text{ff then } l_y := \text{tt else } \perp] \rangle \downarrow^{<W'' \cdot k}$ would imply $\langle h''_1[l_y \mapsto \text{tt}]; K''_1[\langle \rangle] \rangle \downarrow^{<W'' \cdot k}$.
- * It is easy to see that $W''_{\langle \text{ff}, \text{tt} \rangle} \sqsupseteq^{\text{pub}} W''$ and, using monotonicity (Lemma 10), that $(h''_1[l_y \mapsto \text{tt}], h''_2) : W''_{\langle \text{ff}, \text{tt} \rangle}$.
- * Since also $(W''_{\langle \text{ff}, \text{tt} \rangle}, \langle \rangle, \langle \rangle) \in \mathcal{V}[\llbracket \text{unit} \rrbracket \emptyset]$, instantiating $(W'', K''_1, K''_2) \in \mathcal{K}[\llbracket \text{unit} \rrbracket \emptyset]$ then yields $\text{consistent}(W''_{\langle \text{ff}, \text{tt} \rangle})$.
- Case $W'' = W''_{\langle \text{tt}, \text{ff} \rangle}$:
 - * Then $(h''_1, h''_2) : W''$ implies $h''_1(l_x) = \text{tt}$.
 - * Consequently, $\langle h''_1; K''_1[\text{if } !l_x = \text{ff then } l_y := \text{tt else } \perp] \rangle \uparrow$.
- We now show $(\widehat{W}', K'_1[\bullet; \text{if } !l_y = \text{ff then } l_x := \text{tt else } \perp], K'_2) \in \mathcal{K}[\llbracket \text{unit} \rrbracket \emptyset]$:
 - Suppose $W'' \sqsupseteq^{\text{pub}} \widehat{W}'$, $(h''_1, h''_2) : W''$, and $\langle h''_1; K'_1[\langle \rangle; \text{if } !l_y = \text{ff then } l_x := \text{tt else } \perp] \rangle \downarrow^{<W'' \cdot k}$.
 - To show: $\text{consistent}(W'')$ and $\langle h''_2; K'_2[\langle \rangle] \rangle \downarrow$
 - Observe that $h''_1(l_y)$ must be ff and therefore $W'' \in \{W''_{\langle \text{ff}, \text{ff}, 1 \rangle}, W''_{\langle \text{tt}, \text{ff} \rangle}\}$.
 - Also, this means that $\langle h''_1[l_x \mapsto \text{tt}]; K'_1[\langle \rangle] \rangle \downarrow^{<W'' \cdot k}$.
 - It is easy to see that $(h''_1[l_x \mapsto \text{tt}], h''_2) : W''_{\langle \text{tt}, \text{ff} \rangle}$ and that $W''_{\langle \text{tt}, \text{ff} \rangle} \sqsupseteq^{\text{pub}} W'_{\langle \text{tt}, \text{ff} \rangle} \sqsupseteq^{\text{pub}} W'$.
 - Also, $(W''_{\langle \text{tt}, \text{ff} \rangle}, \langle \rangle, \langle \rangle) \in \mathcal{V}[\llbracket \text{unit} \rrbracket \emptyset]$.
 - Hence, instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\llbracket \text{unit} \rrbracket \emptyset]$ yields $\text{consistent}(W''_{\langle \text{tt}, \text{ff} \rangle})$ and $\langle h''_2; K'_2[\langle \rangle] \rangle \downarrow$.
 - The former implies $\text{consistent}(W'')$.
- Using monotonicity (Lemma 10), we easily get $(h'_1, h'_2) : W''$.
- Instantiating $(W'', e'_1[\lambda z. \text{if } !l_x = \text{ff then } l_y := \text{tt else } \perp / g], e'_2[\lambda z. \perp / g]) \in \mathcal{E}[\llbracket \text{unit} \rrbracket \emptyset]$ thus yields $\text{consistent}(W'')$ and $\langle h'_2; K'_2[e'_2[\lambda z. \perp / g]] \rangle \downarrow$.
- The former implies $\text{consistent}(W')$ and the latter implies $\langle h'_2; K'_2[(\lambda g. e'_2)(\lambda z. \perp)] \rangle \downarrow$.

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

- This reduces to showing $(W, e_2, e_1) \in \mathcal{E}[\llbracket (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rrbracket \emptyset]$, where $W \in \mathcal{S}[\cdot]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\llbracket \tau \rrbracket \emptyset]$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_2] \rangle \downarrow^{<W \cdot k}$.
- To show: $\text{consistent}(W)$ and $\langle h_2; K_2[e_1] \rangle \downarrow$
- Observe that $\langle h_2; K_2[e_1] \rangle \downarrow$ if $\langle h_2 \uplus \{l_x \mapsto \text{ff}\} \uplus \{l_y \mapsto \text{ff}\}; K_2[\widehat{e}_1[l_x/x][l_y/y]] \rangle \downarrow$, where \widehat{e}_1 is the function value in e_1 and l_y any free location.
- Let
 - $H(\langle \rangle) := \{\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2 \in \text{HeapAtom} \mid \widetilde{h}_2(l_y) = \text{ff} \wedge l_x \in \text{dom}(h_2)\}$
 - $\iota := (\langle \rangle, \emptyset^*, \emptyset^*, \emptyset, H)$

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

The island represents the following STS:



- Note that $\widehat{W} \sqsupseteq^{\text{pub}} W$ and $(h_1, h_2 \uplus \{l_x \mapsto \text{ff}\} \uplus \{l_y \mapsto \text{ff}\}) : \widehat{W}$.
- 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 $W' \sqsupseteq W$, $(W', f_1, f_2) \in \mathcal{V}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}]\emptyset$, $(W', K'_1, K'_2) \in \mathcal{K}[\text{unit}]\emptyset$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K'_1[f_1(\lambda_{_} \perp)] \rangle \downarrow^{<W'.k}$.
- To show: $\langle h'_2; K'_2[f_2(\lambda_{_} \text{ if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp); \text{ if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp] \rangle \downarrow$ and $\text{consistent}(W')$
- We show $(W', f_1(\lambda_{_} \perp), f_2(\lambda_{_} \text{ if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp)) \in \mathcal{E}[\text{unit}]\emptyset$:
 - Since $(W', f_1, f_2) \in \mathcal{V}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}]\emptyset$, it suffices to show $(W', (\lambda_{_} \perp), (\lambda_{_} \text{ if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp)) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset$.
 - This holds trivially, because $\langle h'_1; K'_1[\perp] \rangle$ diverges for any h'_1 and K'_1 .
- We show $(W', K'_1, K'_2[\bullet; \text{ if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp]) \in \mathcal{K}[\text{unit}]\emptyset$:
 - So suppose $W'' \sqsupseteq^{\text{pub}} W'$, $(h''_1, h''_2) : W''$, and $\langle h''_1; K'_1[\langle \rangle] \rangle \downarrow^{<W''.k}$.
 - To show: $\text{consistent}(W'')$ and $\langle h''_2; K'_2[\text{ if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp] \rangle \downarrow$
 - From $(h''_1, h''_2) : W''$ we know $h''_2(l_y) = \text{ff}$.
 - Therefore, $\langle h''_2; K'_2[\text{ if } !l_y \text{ then } \perp \text{ else } \langle \rangle] \rangle \downarrow$ if $\langle h''_2[l_x \mapsto \text{tt}]; K'_2[\langle \rangle] \rangle \downarrow$.
 - Note that $(h''_1, h''_2) : W''$ implies $(h''_1, h''_2[l_x \mapsto \text{tt}]) : W''$.
 - The claims thus follow from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\text{unit}]\emptyset$ with $(W'', \langle \rangle, \langle \rangle) \in \mathcal{V}[\text{unit}]\emptyset$.
- Combining these yields the claims.

4.1.2 Well-Bracketed State Changes

$$\begin{aligned} e_1 &= \text{let } x = \text{ref } 0 \text{ in} \\ &\quad \lambda f:\text{unit} \rightarrow \text{unit}. (x := 0; f \langle \rangle; x := 1; f \langle \rangle; !x) \\ e_2 &= \lambda f:\text{unit} \rightarrow \text{unit}. (f \langle \rangle; f \langle \rangle; 1) \end{aligned}$$

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 :

$$\begin{aligned} &\text{let } g = \bullet \text{ in let } b = \text{ref } \text{ff} \text{ in} \\ &\text{let } f = (\lambda_{_} \text{ if } !b \text{ then call/cc}(k). g(\lambda_{_} \text{ throw } \langle \rangle \text{ to } k)) \\ &\quad \text{else } b := \text{tt} \text{ in} \\ &g f \end{aligned}$$

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 :

```

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

```

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

The programs are, however, equivalent in **HOS**, which we prove by showing that each logically approximates the other (here we only give one direction, the reverse is proven analogously).

We show $\cdot; \cdot \vdash e_1 \lesssim_{\log} e_2 : (\text{unit} \rightarrow \text{unit}) \rightarrow \text{int}$:

- This reduces to showing $(W, e_1, e_2) \in \mathcal{E}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{int}] \emptyset$, where $W \in \mathcal{S}[\cdot]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{int}] \emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_1] \rangle \downarrow^{<W.k}$.
- To show: $\text{consistent}(W)$ and $\langle h_2; K_2[e_2] \rangle \downarrow$
- $\langle h_1; K_1[e_1] \rangle \downarrow^{<W.k}$ implies $\langle h_1 \uplus \{l_x \mapsto 0\}; K_1[\hat{e}_1] \rangle \downarrow^{<W.k}$, where l_x is fresh and $\hat{e}_1 := \lambda f. (l_x := 0; f \langle \rangle; l_x := 1; f \langle \rangle; !l_x)$.

- Let

- $H(i) := \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_x) = i\}$
- $\varphi := \{(0, 1)\}^*$
- $\delta := (\varphi \uplus \{(1, 0)\})^*$
- $\iota_s := (s, \delta, \varphi, \emptyset, H)$
- $W_s := W[W.\Sigma_1 := W.\Sigma_1, l_x:\text{int}][W.\omega := W.\omega, \iota_s]$

The island represents the following STS:



- It is easy to see that $W_0 \sqsupseteq^{\text{pub}} W$ and, using monotonicity (Lemma 10), that $(h_1 \uplus \{l_x \mapsto 0\}, h_2) : W_0$.
- Hence by instantiating $(W, K_1, K_2) \in \mathcal{K}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{int}] \emptyset$, it suffices to show $(W_0, \hat{e}_1, e_2) \in \mathcal{V}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{int}] \emptyset$.
- So suppose $W' \sqsupseteq W_0$ and $(W', \lambda z. e'_1, \lambda z. e'_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}] \emptyset$, $(W', K'_1, K'_2) \in \mathcal{K}[\text{int}] \emptyset$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K'_1[\hat{e}'_1[\lambda z. e'_1/f]] \rangle \downarrow^{<W'.k}$, where \hat{e}'_1 is the body of \hat{e}_1 .

- To show: $\text{consistent}(W')$ 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 $W'_0 \supseteq W'$ and that $\text{consistent}(W'_0)$ would imply $\text{consistent}(W')$.
- Since $(W'_0, \langle \rangle, \langle \rangle) \in \mathcal{V}[\text{unit}]\emptyset$, instantiating $(W', \lambda g. e'_1, \lambda z. e'_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset$ yields $(W'_0, e'_1[\langle \rangle/z], e'_2[\langle \rangle/z]) \in \mathcal{E}[\text{unit}]\emptyset$.
- 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 $(W'_0, K'_1[(\bullet; l_x := 1; (\lambda z. e'_1) \langle \rangle; !l_x)], K'_2[(\bullet; (\lambda z. e'_2) \langle \rangle; 1)]) \in \mathcal{K}[\text{unit}]\emptyset$.
- So suppose $W'' \supseteq^{\text{pub}} W'_0$, $(h''_1, h''_2) : W''$, 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: $\text{consistent}(W'')$ 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 $W''_1 \supseteq^{\text{pub}} W''$.
- Since $(W''_1, \langle \rangle, \langle \rangle) \in \mathcal{V}[\text{unit}]\emptyset$, instantiating $(W', \lambda z. e'_1, \lambda z. e'_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset$ yields $(W''_1, e'_1[\langle \rangle/z], e'_2[\langle \rangle/z]) \in \mathcal{E}[\text{unit}]\emptyset$.
- It is easy to see, using monotonicity (Lemma 10), that $(h''_1[l_{x \mapsto 1}], h''_2) : W''_1$.
- Also, $\text{consistent}(W''_1)$ would imply $\text{consistent}(W'')$.
- 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 $(W''_1, K'_1[(\bullet; !l_x)], K'_2[(\bullet; 1)]) \in \mathcal{K}[\text{unit}]\emptyset$.
- So suppose $W''' \supseteq^{\text{pub}} W''_1$, $(h'''_1, h'''_2) : W'''$, and $\langle h'''_1; K'_1[(\langle \rangle; !l_x)] \rangle \downarrow^{<W'''.k}$.
- To show: $\text{consistent}(W''')$ and $\langle h'''_2; K'_2[(\langle \rangle; 1)] \rangle \downarrow$
- Note that $W''' \supseteq^{\text{pub}} W''_1$ 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 $W''' \supseteq^{\text{pub}} W''_1 \supseteq^{\text{pub}} W''$ and $(W''', 1, 1) \in \mathcal{V}[\text{int}]\emptyset$.
- Therefore, instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\text{int}]\emptyset$ yields $\text{consistent}(W''')$ 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 $W_0 \sqsupseteq^{\text{pub}}$ -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 $W'' \sqsupseteq^{\text{pub}} W'_0$ 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 $W''' \sqsupseteq^{\text{pub}} W''_1$ (note the \sqsupseteq^{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

$$\begin{aligned}
\tau &= ((\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}) \rightarrow \text{ref int} \\
e_1 &= \lambda f: (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}. \text{let } x = \text{ref } 0 \text{ in} \\
&\quad \text{let } y = \text{ref } 0 \text{ in} \\
&\quad \text{let } z = \text{ref } 0 \text{ in} \\
&\quad f (\lambda_: \text{unit}. \text{if } !x = 0 \text{ then } y := 1 \text{ else } z := 1); \\
&\quad \text{if } !y = 0 \text{ then } x := 1 \text{ else } (z := 1; x := 1); \\
&\quad z \\
e_2 &= \lambda f: (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}. \text{let } z = \text{ref } 0 \text{ in} \\
&\quad f (\lambda_: \text{unit}. z := 1); \\
&\quad z
\end{aligned}$$

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

- This reduces to showing $(W_0, e_1, e_2) \in \mathcal{V}[\tau]\emptyset$, where $W_0 \in \mathcal{S}[\cdot]$.
- So suppose $W \sqsupseteq W_0$, $(W, f_1, f_2) \in \mathcal{V}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}]\emptyset$, $(W, K_1, K_2) \in \mathcal{K}[\text{ref int}]\emptyset$, $(h_1, h_2) : W$, 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: $\text{consistent}(W)$ 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:

- $\widetilde{h}_1 := h_1 \uplus \{l_x \mapsto 0\} \uplus \{l_y \mapsto 0\} \uplus \{l_z^1 \mapsto 0\}$
- $\widetilde{e}_1 := f_1(\lambda _ . \text{if } !l_x = 0 \text{ then } l_y := 1 \text{ else } l_z^1 := 1);$
 $\text{if } !l_y = 0 \text{ then } l_x := 1 \text{ else } (l_z^1 := 1; l_x := 1);$
 l_z^1
- l_x, l_y, l_z^1 are distinct and fresh

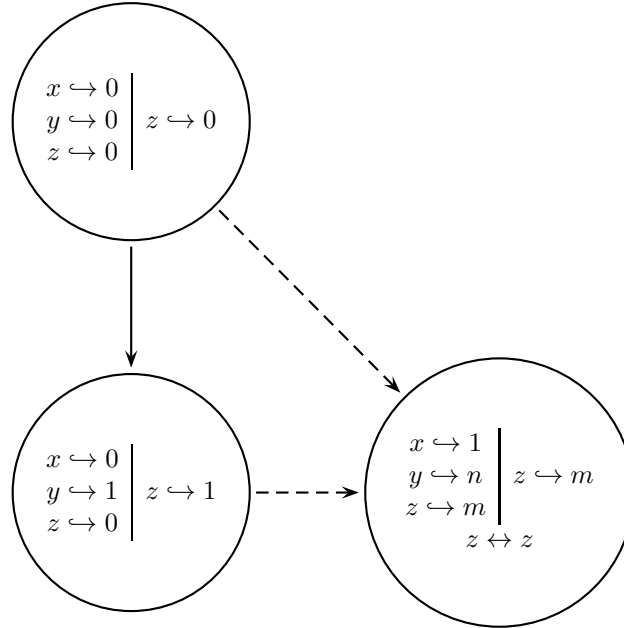
- Similarly, $\langle h_2; K_2[\widehat{e}_2[f_2/f]] \rangle \downarrow$ if $\langle \widetilde{h}_2; K_2[\widetilde{e}_2] \rangle \downarrow$, where:

- $\widetilde{h}_2 := h_2[l_z^2 \mapsto 0]$
- $\widetilde{e}_2 := f_2(\lambda _ . l_z^2 := 1);$
 l_z^2
- l_z^2 is fresh

- Let

- $H(1) := \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_x) = \widetilde{h}_1(l_y) = \widetilde{h}_1(l_z^1) = \widetilde{h}_2(l_z^2) = 0\}$
- $H(2) := \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_x) = \widetilde{h}_1(l_z^1) = 0 \wedge \widetilde{h}_1(l_y) = \widetilde{h}_2(l_z^2) = 1\}$
- $3 := \{l_z^1, l_z^2\}$
- $H(3) := \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_x) = 1 \wedge \widetilde{h}_1(l_y) = n \wedge \widetilde{h}_1(l_z^1) = \widetilde{h}_2(l_z^2) = m\}$
- $\varphi := \{(1, 2)\}$
- $\delta := (\varphi \uplus \{(1, 3), (2, 3)\})^*$
- $\iota_s := (s, \delta, \varphi, \emptyset, H)$
- $W_s := W[\Sigma_1 := W.\Sigma_1, l_x:\text{int}, l_y:\text{int}, l_z^1:\text{int}][\Sigma_2 := W.\Sigma_2, l_z^2:\text{int}][\omega := W.\omega, \iota_s]$

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 $(W_1, f_1(\lambda_{\cdot}. \text{if } !l_x = 0 \text{ then } l_y := 1 \text{ else } l_z^1 := 1), f_2(\lambda_{\cdot}. l_z^2 := 1)) \in \mathcal{E}[\![\text{unit}]\!]\emptyset$:
 - Since $(W, f_1, f_2) \in \mathcal{V}[\![\text{unit} \rightarrow \text{unit}] \rightarrow \text{unit}]\!\emptyset$, it suffices to show $(W_1, (\lambda_{\cdot}. \text{if } !l_x = 0 \text{ then } (l_z^1 := 0; l_y := 1) \text{ else } l_z^1 := 1), (\lambda_{\cdot}. l_z^2 := 1)) \in \mathcal{V}[\![\text{unit} \rightarrow \text{unit}]\!]\emptyset$.
 - So suppose $W' \sqsupseteq W_1$, $(W', K'_1, K'_2) \in \mathcal{K}[\![\text{unit}]\!]\emptyset$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K'_1[\text{if } !l_x = 0 \text{ then } l_y := 1 \text{ else } l_z^1 := 1] \rangle \downarrow^{<W'.k}$.
 - To show: $\text{consistent}(W')$ 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 $W'_2 \sqsupseteq^{\text{pub}} W'$ and, using monotonicity (Lemma 10), that $(h'_1[l_y \mapsto 1], h'_2[l_z^2 \mapsto 1]) : W'_2$.
 - * Also, $\text{consistent}(W'_2)$ would imply $\text{consistent}(W')$.
 - * Since $(W'_2, \langle \rangle, \langle \rangle) \in \mathcal{V}[\![\text{unit}]\!]\emptyset$, the claims then follow from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\![\text{unit}]\!]\emptyset$.
 - 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 $(W', \langle \rangle, \langle \rangle) \in \mathcal{V}[\![\text{unit}]\!]\emptyset$, the claims then follow from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\![\text{unit}]\!]\emptyset$.
- It is obvious that $\text{consistent}(W_1)$ would imply $\text{consistent}(W)$.
- Hence it suffices to show $(W_1, K_1[\bullet; \text{if } !l_y = 0 \text{ then } l_x := 1 \text{ else } (l_z^1 := 1; l_x := 1)]; l_z^1, K_2[\bullet; l_z^2]) \in \mathcal{K}[\![\text{unit}]\!]\emptyset$.
- So suppose $W' \sqsupseteq^{\text{pub}} W_1$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K_1[\langle \rangle; \text{if } !l_y = 0 \text{ then } l_x := 1 \text{ else } (l_z^1 := 1; l_x := 1)]; l_z^1 \rangle \downarrow^{<W'.k}$.
- To show: $\text{consistent}(W')$ 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 $(h'_1[l_x \mapsto 1], h'_2) : W'_3$.
 - It is also easy to see that $W'_3 \sqsupseteq^{\text{pub}} W_3 \sqsupseteq^{\text{pub}} W$ and that $\text{consistent}(W'_3)$ would imply $\text{consistent}(W')$.
 - The claims then follow from instantiating $(W, K_1, K_2) \in \mathcal{K}[\![\text{ref int}]\!]\emptyset$, if we can show $(W'_3, l_z^1, l_z^2) \in \mathcal{V}[\![\text{ref int}]\!]\emptyset$.
 - The latter is easy to verify, because $\text{bij}(3) = \{(l_z^1, l_z^2)\}$.
- 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 $(h'_1[l_z^1 \mapsto 1][l_x \mapsto 1], h'_2) : W'_3$.
 - It is also easy to see that $W'_3 \sqsupseteq^{\text{pub}} W_3 \sqsupseteq^{\text{pub}} W$ and that $\text{consistent}(W'_3)$ would imply $\text{consistent}(W')$.
 - The claims then follow from instantiating $(W, K_1, K_2) \in \mathcal{K}[\llbracket \text{ref int} \rrbracket \emptyset]$, if we can show $(W'_3, l_z^1, l_z^2) \in \mathcal{V}[\llbracket \text{ref int} \rrbracket \emptyset]$.
 - The latter is easy to verify, because $\text{bij}(3) = \{(l_z^1, l_z^2)\}$.
- 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

$$\begin{aligned}
\tau &= ((\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}) \rightarrow \text{unit} \\
e_1 &= \text{let } x = \text{ref ff} \text{ in let } y = \text{ref ff} \text{ in} \\
&\quad \lambda f:(\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}. \text{try } f (\lambda z:\text{unit}. \text{if } !x = \text{ff} \text{ then } y := \text{tt} \text{ else } \perp) \\
&\quad \quad \text{with } z. (\text{if } !y = \text{ff} \text{ then } x := \text{tt} \text{ else } \perp; \text{raise}_z); \\
&\quad \quad \text{if } !y = \text{ff} \text{ then } x := \text{tt} \text{ else } \perp \\
e_2 &= \lambda f:(\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}. f (\lambda z:\text{unit}. \perp)
\end{aligned}$$

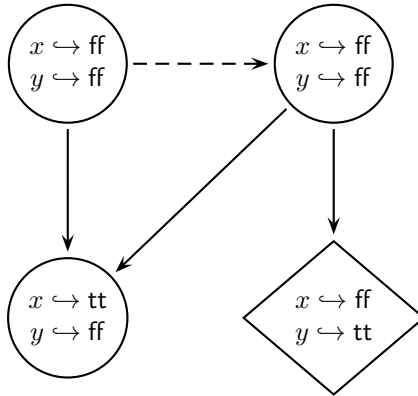
The programs are equivalent in **HOSE**, which we prove by showing that each logically approximates the other.

We first show $\cdot; \cdot; \cdot \vdash e_1 \lesssim_{\text{log}} e_2 : ((\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}) \rightarrow \text{unit}$:

- This reduces to showing $(W, e_1, e_2) \in \mathcal{E}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$, where $W \in \mathcal{S}[\cdot]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_1] \rangle \downarrow^{<W.k}$.
- To show: $\text{consistent}(W)$ and $\langle h_2; K_2[e_2] \rangle \downarrow$
- $\langle h_1; K_1[e_1] \rangle \downarrow^{<W.k}$ implies $\langle h_1 \uplus \{l_x \mapsto \text{ff}\} \uplus \{l_y \mapsto \text{ff}\}; K_1[v_1[l_x/x][l_y/y]] \rangle \downarrow^{<W.k}$, where v_1 is the function value in e_1 and l_x, l_y are distinct and fresh.
- Let

$$\begin{aligned}
- H(\langle i, j \rangle) &:= \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_x) = i \wedge \widetilde{h}_1(l_y) = j\} \\
- H(\langle i, j, _ \rangle) &:= H(\langle i, j \rangle) \\
- \varphi &:= \{(\langle \text{ff}, \text{ff}, 0 \rangle, \langle \text{tt}, \text{ff} \rangle), (\langle \text{ff}, \text{ff}, 1 \rangle, \langle \text{tt}, \text{ff} \rangle), (\langle \text{ff}, \text{ff}, 1 \rangle, \langle \text{ff}, \text{tt} \rangle)\}^* \\
- \delta &:= (\varphi \uplus \{(\langle \text{ff}, \text{ff}, 0 \rangle, \langle \text{ff}, \text{ff}, 1 \rangle)\})^* \\
- \iota_s &:= (s, \delta, \varphi, \{\langle \text{ff}, \text{tt} \rangle\}, H) \\
- W_s &:= W[\Sigma_1 := W.\Sigma_1, l_x:\text{bool}, l_y:\text{bool}][\omega := W.\omega, \iota_s]
\end{aligned}$$

The island represents the following STS:



- Note that $\text{safe}(l_{\langle \text{ff}, \text{ff}, 0 \rangle})$ and thus $W_{\langle \text{ff}, \text{ff}, 0 \rangle} \sqsupseteq^{\text{pub}} W$.
- Furthermore, using monotonicity (Lemma 10), it is easy to see that $(h_1 \uplus \{l_x \mapsto \text{ff}\} \uplus \{l_y \mapsto \text{ff}\}, h_2) : W_{\langle \text{ff}, \text{ff}, 0 \rangle}$.
- Consequently, if we can show $(W_{\langle \text{ff}, \text{ff}, 0 \rangle}, v_1[l_x/x][l_y/y], e_2) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$, then the claims follow from instantiating $(W, K_1, K_2) \in \mathcal{K}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$.
- So suppose $W' \sqsupseteq W_{\langle \text{ff}, \text{ff}, 0 \rangle}$ and $(W', \lambda g. e'_1, \lambda g. e'_2) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$, $(W', K'_1, K'_2) \in \mathcal{K}[\langle \text{unit} \rangle \emptyset]$, $(h'_1, h'_2) : W'$, 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: $\text{consistent}(W')$ and $\langle h'_2; K'_2[(\lambda z. \perp)] \rangle \downarrow$
- $\langle h'_1; K'_1[\widehat{e}_1[l_x/x][l_y/y][\lambda g. e'_1/f]] \rangle \downarrow^{<W'.k}$ implies $\langle h'_1; K'_1[e''] \rangle \downarrow^{<W'.k}$, where $e'' = (e'_1[\lambda z. \text{if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp/g]; \text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp)$.
- Notation: we write W'_s to mean the world obtained from W' by setting our island's current state to s .
- If $W' = W'_{\langle \text{ff}, \text{ff}, 0 \rangle}$, then let $\widehat{W}' := W'_{\langle \text{ff}, \text{ff}, 1 \rangle}$; otherwise let $\widehat{W}' := W'$.
- It is easy to see that $\widehat{W}' \sqsupseteq W'$.
- We now show $(\widehat{W}', e'_1[\lambda z. \text{if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp/g], e'_2[\lambda z. \perp/g]) \in \mathcal{E}[\langle \text{unit} \rangle \emptyset]$:
 - Since $(W', \lambda g. e'_1, \lambda g. e'_2) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$, it suffices to show $(\widehat{W}', \lambda z. \text{if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp, \lambda z. \perp) \in \mathcal{V}[\langle \text{unit} \rightarrow \text{unit} \rangle \emptyset]$.
 - So suppose $W'' \sqsupseteq \widehat{W}'$, $(W'', K''_1, K''_2) \in \mathcal{K}[\langle \text{unit} \rangle \emptyset]$, and $(h''_1, h''_2) : W''$.
 - We show that $\langle h''_1; K''_1[\text{if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp] \rangle \downarrow^{<W''.k}$ is impossible.
 - Case $W'' \in \{W''_{\langle \text{ff}, \text{ff}, 1 \rangle}, W''_{\langle \text{ff}, \text{tt} \rangle}\}$:
 - * Then $(h''_1, h''_2) : W''$ implies $h''_1(l_x) = \text{ff}$.
 - * Consequently, $\langle h''_1; K''_1[\text{if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp] \rangle \downarrow^{<W''.k}$ would imply $\langle h''_1[l_y \mapsto \text{tt}]; K''_1[\langle \rangle] \rangle \downarrow^{<W''.k}$.
 - * It is easy to see that $W''_{\langle \text{ff}, \text{tt} \rangle} \sqsupseteq^{\text{pub}} W''$ and, using monotonicity (Lemma 10), that $(h''_1[l_y \mapsto \text{tt}], h''_2) : W''_{\langle \text{ff}, \text{tt} \rangle}$.
 - * Since also $(W''_{\langle \text{ff}, \text{tt} \rangle}, \langle \rangle, \langle \rangle) \in \mathcal{V}[\langle \text{unit} \rangle \emptyset]$, instantiating $(W'', K''_1, K''_2) \in \mathcal{K}[\langle \text{unit} \rangle \emptyset]$ then yields $\text{consistent}(W''_{\langle \text{ff}, \text{tt} \rangle})$.
 - Case $W'' = W''_{\langle \text{tt}, \text{ff} \rangle}$:
 - * Then $(h''_1, h''_2) : W''$ implies $h''_1(l_x) = \text{tt}$.
 - * Consequently, $\langle h''_1; K''_1[\text{if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp] \rangle \uparrow$.
- We now show $(\widehat{W}', K'_1[\text{try } \bullet \text{ with } z.(\text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp; \text{raise } z); \text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp], K'_2) \in \mathcal{K}[\langle \text{unit} \rangle \emptyset]$:
 - First suppose $W'' \sqsupseteq^{\text{pub}} \widehat{W}'$, $(h''_1, h''_2) : W''$, and $\langle h''_1; K'_1[\text{try } \langle \rangle \text{ with } z.(\text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp; \text{raise } z); \text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp] \rangle \downarrow^{<W''.k}$.

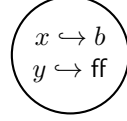
- To show: $\text{consistent}(W'')$ and $\langle h_2''; K_2'(\langle \rangle) \rangle \downarrow$
 - Note that $\langle h_1''; K_1'[\text{try } \langle \rangle \text{ with } z.(\text{if } !l_y = \text{ff then } l_x := \text{tt else } \perp; \text{raise } z); \text{if } !l_y = \text{ff then } l_x := \text{tt else } \perp] \rangle \downarrow^{<W'' \cdot k}$ implies $\langle h_1''; K_1'[\text{if } !l_y = \text{ff then } l_x := \text{tt else } \perp] \rangle \downarrow^{<W'' \cdot k}$.
 - Observe that $h_1''(l_y)$ must be ff and therefore $W'' \in \{W''_{\langle \text{ff}, \text{ff}, 1 \rangle}, W''_{\langle \text{tt}, \text{ff} \rangle}\}$.
 - Also, this means that $\langle h_1''[l_x \mapsto \text{tt}]; K_1'(\langle \rangle) \rangle \downarrow^{<W'' \cdot k}$.
 - It is easy to see that $(h_1''[l_x \mapsto \text{tt}], h_2'') : W''_{\langle \text{tt}, \text{ff} \rangle}$ and that $W''_{\langle \text{tt}, \text{ff} \rangle} \sqsupseteq^{\text{pub}} W'_{\langle \text{tt}, \text{ff} \rangle} \sqsupseteq^{\text{pub}} W'$.
 - Also, $(W''_{\langle \text{tt}, \text{ff} \rangle}, \langle \rangle, \langle \rangle) \in \mathcal{V}[\llbracket \text{unit} \rrbracket \emptyset]$.
 - Hence, instantiating $(W', K_1', K_2') \in \mathcal{K}[\llbracket \text{unit} \rrbracket \emptyset]$ yields both $\text{consistent}(W''_{\langle \text{tt}, \text{ff} \rangle})$ and $\langle h_2''; K_2'(\langle \rangle) \rangle \downarrow$.
 - The former implies $\text{consistent}(W'')$.
2. - Now suppose $W'' \sqsupseteq^{\text{pub}} \widehat{W}'$, $(W'', v_1, v_2) \in \mathcal{V}[\llbracket \text{exn} \rrbracket \emptyset]$, $(h_1'', h_2'') : W''$ and $\langle h_1''; K_1'[\text{try raise } v_1 \text{ with } z.(\text{if } !l_y = \text{ff then } l_x := \text{tt else } \perp; \text{raise } z); \text{if } !l_y = \text{ff then } l_x := \text{tt else } \perp] \rangle \downarrow^{<W'' \cdot k}$.
- To show: $\text{consistent}(W'')$ and $\langle h_2''; \text{raise } v_2 \rangle \downarrow$
 - Note that $\langle h_1''; K_1'[(\text{if } !l_y = \text{ff then } l_x := \text{tt else } \perp; \text{raise } v_1); \text{if } !l_y = \text{ff then } l_x := \text{tt else } \perp] \rangle \downarrow^{<W'' \cdot k}$ implies $\langle h_1''[l_x \mapsto \text{tt}]; K_1'[\text{raise } v_1] \rangle \downarrow^{<W'' \cdot k}$ and $h_1''(l_y) = \text{ff}$.
 - The latter means $W'' = W''_{\langle \text{tt}, \text{ff} \rangle}$ or $W'' = W''_{\langle \text{ff}, \text{ff} \rangle}$.
 - In any case it is easy to see that $W''_{\langle \text{tt}, \text{ff} \rangle} \sqsupseteq^{\text{pub}} W'$.
 - Also, $(h_1''[l_x \mapsto \text{tt}], h_2'') : W''_{\langle \text{tt}, \text{ff} \rangle}$.
 - By monotonicity (Lemma 10), $(W''_{\langle \text{tt}, \text{ff} \rangle}, v_1, v_2) \in \mathcal{V}[\llbracket \text{exn} \rrbracket \emptyset]$.
 - Finally, $\text{consistent}(W''_{\langle \text{tt}, \text{ff} \rangle})$ would imply $\text{consistent}(W'')$.
 - The claims then follow from instantiating $(W', K_1', K_2') \in \mathcal{K}[\llbracket \text{unit} \rrbracket \emptyset]$.
- Using monotonicity (Lemma 10), we easily get $(h_1', h_2') : W''$.
 - Instantiating $(W'', e_1'[\lambda z. \text{if } !l_x = \text{ff then } l_y := \text{tt else } \perp/g], e_2'[\lambda z. \perp/g]) \in \mathcal{E}[\llbracket \text{unit} \rrbracket \emptyset]$ thus yields $\text{consistent}(W'')$ and $\langle h_2''; K_2'[e_2'[\lambda z. \perp/g]] \rangle \downarrow$.
 - The former implies $\text{consistent}(W')$ and the latter implies $\langle h_2''; K_2'[(\lambda g. e_2')(\lambda z. \perp)] \rangle \downarrow$.

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

- This reduces to showing $(W, e_2, e_1) \in \mathcal{E}[\llbracket (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rrbracket \emptyset]$, where $W \in \mathcal{S}[\cdot]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\llbracket \tau \rrbracket \emptyset]$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_2] \rangle \downarrow^{<W \cdot k}$.
- To show: $\text{consistent}(W)$ and $\langle h_2; K_2[e_1] \rangle \downarrow$
- Observe that $\langle h_2; K_2[e_1] \rangle \downarrow$ if $\langle h_2 \uplus \{l_x \mapsto \text{ff}\} \uplus \{l_y \mapsto \text{ff}\}; K_2[\widehat{e}_1[l_x/x][l_y/y]] \rangle \downarrow$, where \widehat{e}_1 is the function value in e_1 and l_y any free location.
- Let
 - $H(\langle \rangle) := \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_2(l_y) = \text{ff} \wedge l_x \in \text{dom}(h_2)\}$

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

The island represents the following STS:



- Note that $\widehat{W} \sqsupseteq^{\text{pub}} W$ and $(h_1, h_2 \uplus \{l_x \mapsto \text{ff}\} \uplus \{l_y \mapsto \text{ff}\}) : \widehat{W}$.
- 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 $W' \sqsupseteq W$, $(W', f_1, f_2) \in \mathcal{V}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}]\emptyset$, $(W', K'_1, K'_2) \in \mathcal{K}[\text{unit}]\emptyset$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K'_1[f_1(\lambda_{_} \perp)] \rangle \downarrow^{<W'.k}$.
- To show: $\text{consistent}(W')$ and $\langle h'_2; K'_2[\text{try } f_2(\lambda z. \text{if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp) \text{ with } z.(\text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp; \text{raise } z); \text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp] \rangle \downarrow$
- We show $(W', f_1(\lambda_{_} \perp), f_2(\lambda_{_} \text{if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp)) \in \mathcal{E}[\text{unit}]\emptyset$:
 - Since $(W', f_1, f_2) \in \mathcal{V}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}]\emptyset$, it suffices to show $(W', (\lambda_{_} \perp), (\lambda_{_} \text{if } !l_x = \text{ff} \text{ then } l_y := \text{tt} \text{ else } \perp)) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset$.
 - This holds trivially, because $\langle h'_1; K'_1[\perp] \rangle$ diverges for any h''_1 and K''_1 .
- We show $(W', K'_1, K'_2[\text{try } \bullet \text{ with } z.(\text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp; \text{raise } z); \text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp]) \in \mathcal{K}[\text{unit}]\emptyset$:
 - So first suppose $W'' \sqsupseteq^{\text{pub}} W'$, $(h''_1, h''_2) : W''$, and $\langle h''_1; K'_1[\langle \rangle] \rangle \downarrow^{<W''.k}$.
 - To show: $\text{consistent}(W'')$ and $\langle h''_2; K'_2[\text{try } \langle \rangle \text{ with } z.(\text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp; \text{raise } z); \text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp] \rangle \downarrow$
 - From $(h''_1, h''_2) : W''$ we know $h''_2(l_y) = \text{ff}$.
 - Therefore, $\langle h''_2; K'_2[\text{try } \langle \rangle \text{ with } z.(\text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp; \text{raise } z); \text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp] \rangle \downarrow$ if $\langle h''_2[l_x \mapsto \text{tt}]; K'_2[\langle \rangle] \rangle \downarrow$.
 - Note that $(h''_1, h''_2) : W''$ implies $(h''_1, h''_2[l_x \mapsto \text{tt}]) : W''$.
 - The claims thus follow from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\text{unit}]\emptyset$ with $(W'', \langle \rangle, \langle \rangle) \in \mathcal{V}[\text{unit}]\emptyset$.
 - Now suppose $W'' \sqsupseteq^{\text{pub}} W'$, $(W'', v_1, v_2) \in \mathcal{V}[\text{exn}]\emptyset$, $(h''_1, h''_2) : W''$ and $\langle h''_1; K'_1[\text{raise } v_1] \rangle \downarrow^{<W''.k}$.
 - To show: $\text{consistent}(W'')$ and $\langle h''_2; K'_2[\text{try } \text{raise } v_2 \text{ with } z.(\text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp; \text{raise } z); \text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp] \rangle \downarrow^{<W''.k}$.
 - From $(h''_1, h''_2) : W''$ we know $h''_2(l_y) = \text{ff}$.
 - Hence, $\langle h''_2; K'_2[(\text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp; \text{raise } v_2); \text{if } !l_y = \text{ff} \text{ then } l_x := \text{tt} \text{ else } \perp] \rangle \downarrow^{<W''.k}$ if $\langle h''_2[l_x \mapsto \text{tt}]; K'_2[\text{raise } v_2] \rangle \downarrow^{<W''.k}$.
 - Note that $(h''_1, h''_2) : W''$ implies $(h''_1, h''_2[l_x \mapsto \text{tt}]) : W''$.
 - The claims thus follow from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\text{unit}]\emptyset$.
- Combining these yields the claims.

4.2.2 Callback With Lock

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

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

$$\begin{aligned}
&\text{let } \langle \text{inc}, \text{poll} \rangle = \bullet \text{ in} \\
&\text{call/cc } (k_0. \text{let } r = \text{ref } k_0 \text{ in} \\
&\quad \text{let } b = \text{ref tt} \text{ in} \\
&\quad \text{let } g = (\lambda_. \text{call/cc } (k. r := k)) \text{ in} \\
&\quad \text{let } h = (\lambda_. b := \text{ff}; \text{throw } \langle \rangle \text{ to } !r) \text{ in} \\
&\quad \text{inc } g; (\text{if } !b \text{ then } \text{inc } h \text{ else } \langle \rangle); \text{if } \text{poll } \langle \rangle = 2 \text{ then } \langle \rangle \text{ else } \perp)
\end{aligned}$$

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.

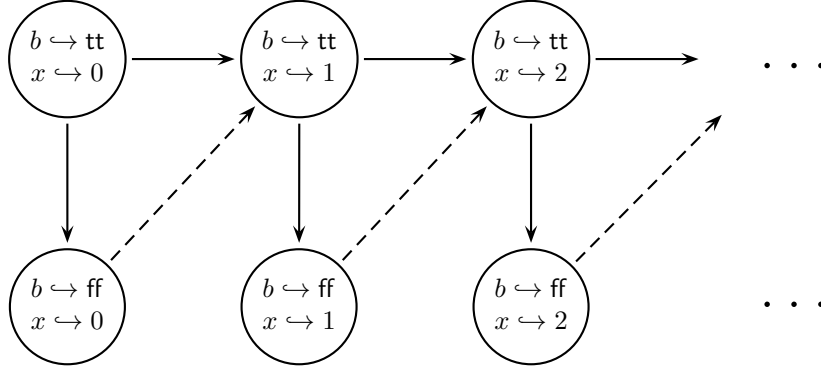
We show $;\cdot; \cdot \vdash e_1 \lesssim_{\log} e_2 : ((\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}) \times (\text{unit} \rightarrow \text{int})$:

- This reduces to showing $(W, e_1, e_2) \in \mathcal{E}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \times \langle \text{unit} \rightarrow \text{int} \rangle] \emptyset$, where $W \in \mathcal{S}[\cdot]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \times \langle \text{unit} \rightarrow \text{int} \rangle] \emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_1] \rangle \downarrow^{<W.k}$.
- To show: $\text{consistent}(W)$ 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
 - $v_1 := \langle v_1^1, v_1^2 \rangle$,
 - $v_1^1 := \lambda f. \text{if } !l_b \text{ then } (l_b := \text{ff}; f \langle \rangle; l_x := !l_x + 1; l_b := \text{tt}) \text{ else } \langle \rangle$,
 - $v_1^2 := \lambda z. !l_x$,
 - $\widehat{h}_1 := h_1 \uplus \{l_b \mapsto \text{tt}\} \uplus \{l_x \mapsto 0\}$, 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
 - $v_2 := \langle v_2^1, v_2^2 \rangle$,
 - $v_2^1 := \lambda f. \text{if } !l_b \text{ then } (l_b := \text{ff}; \text{let } n = !l_x \text{ in } f \langle \rangle; l_x := n + 1; l_b := \text{tt}) \text{ else } \langle \rangle$,
 - $v_2^2 := \lambda z. !l_x$, and
 - $h'_2 := h_2 \uplus \{l_b \mapsto \text{tt}\} \uplus \{l_x \mapsto 0\}$.

- Let

- $H(\langle o, i \rangle) := \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_b) = \widetilde{h}_2(l_b) = o \wedge \widetilde{h}_1(l_x) = \widetilde{h}_2(l_x) = i\}$
- $\varphi := \{(\langle \text{tt}, i \rangle, \langle \text{tt}, i + 1 \rangle) \mid i \in \mathbb{N}\}^*$
- $\delta := (\varphi \uplus \{(\langle \text{tt}, i \rangle, \langle \text{ff}, i \rangle) \mid i \in \mathbb{N}\} \uplus \{(\langle \text{ff}, i \rangle, \langle \text{tt}, i + 1 \rangle) \mid i \in \mathbb{N}\})^*$
- $\iota_s := (s, \delta, \varphi, \emptyset, H)$
- $W_s := W[\Sigma_1 := W.\Sigma_1, l_b:\text{bool}, l_x:\text{int}][\omega := W.\omega, \iota_s]$

The island represents the following STS:



- It is easy to see that $W_{\langle \text{tt}, 0 \rangle} \sqsupseteq^{\text{pub}} W$ and, using monotonicity (Lemma 10), that $(\widehat{h}_1, \widehat{h}_2) : W_{\langle \text{tt}, 0 \rangle}$.
- It thus suffices to show $(W_{\langle \text{tt}, 0 \rangle}, v_1, v_2) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \times \langle (\text{unit} \rightarrow \text{int}) \rangle] \emptyset$, which splits into two parts.
- We show $(W_{\langle \text{tt}, 0 \rangle}, v_1^1, v_2^1) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle] \emptyset$:
 - Suppose $W' \sqsupseteq W_{\langle \text{tt}, 0 \rangle}$, $(W', \lambda y. e_3, \lambda y. e_4) \in \mathcal{V}[\langle \text{unit} \rightarrow \text{unit} \rangle] \emptyset$, $(W', K'_1, K'_2) \in \mathcal{K}[\langle \text{unit} \rangle] \emptyset$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K'_1[\text{if } !l_b \text{ then } (l_b := \text{ff}; (\lambda y. e_3) \langle \rangle; l_x := !l_x + 1; l_b := \text{tt}) \text{ else } \langle \rangle] \rangle \downarrow^{<W'.k}$.
 - To show: consistent(W') and $\langle h'_2; K'_2[\text{if } !l_b \text{ then } (l_b := \text{ff}; \text{let } n = !l_x \text{ in } (\lambda y. e_4) \langle \rangle; l_x := n + 1; l_b := \text{tt}) \text{ else } \langle \rangle] \rangle \downarrow$
 - Notation: we write W'_s to denote the world obtained from W' by setting our island's current state to s .
 - Case $W' = W'_{\langle \text{tt}, i \rangle}$ for some i :
 - * Then $(h'_1, h'_2) : W'$ implies $h'_1(l_b) = h'_2(l_b) = \text{tt}$ and $h'_1(l_x) = h'_2(l_x) = i$.
 - * Hence $\langle h'_1; K'_1[\text{if } !l_b \text{ then } (l_b := \text{ff}; (\lambda y. e_3) \langle \rangle; l_x := !l_x + 1; l_b := \text{tt}) \text{ else } \langle \rangle] \rangle \downarrow^{<W'.k}$ implies $\langle h'_1[l_b \mapsto \text{ff}]; K'_1[e_3[\langle \rangle/y]; (\lambda y. e_3) \langle \rangle; l_x := !l_x + 1; l_b := \text{tt}] \rangle \downarrow^{<W'.k}$.
 - * Similarly, $\langle h'_2; K'_2[\text{if } !l_b \text{ then } (l_b := \text{ff}; \text{let } n = !l_x \text{ in } (\lambda y. e_4) \langle \rangle; l_x := n + 1; l_b := \text{tt}) \text{ else } \langle \rangle] \rangle \downarrow$ if $\langle h'_2[l_b \mapsto \text{ff}]; K'_2[e_4[\langle \rangle/y]; l_x := i + 1; l_b := \text{tt}] \rangle \downarrow$.

- * It is easy to see that $W'_{\langle \text{ff}, i \rangle} \sqsupseteq^{\text{pub}} W'$ and, using monotonicity (Lemma 10), that $(h'_1[l_b \mapsto \text{ff}], h'_2[l_b \mapsto \text{ff}]) : W'_{\langle \text{ff}, i \rangle}$.
 - * Also, $\text{consistent}(W'_{\langle \text{ff}, i \rangle})$ would imply $\text{consistent}(W')$.
 - * Since $(W'_{\langle \text{ff}, i \rangle}, \langle \cdot, \cdot \rangle) \in \mathcal{V}[\![\text{unit}]\!]\emptyset$ and thus $(W'_{\langle \text{ff}, i \rangle}, e_3[\langle \cdot \rangle / y], e_4[\langle \cdot \rangle / y]) \in \mathcal{E}[\![\text{unit}]\!]\emptyset$, it suffices to show $(W'_{\langle \text{ff}, i \rangle}, K'_1[\bullet; l_x := !l_x + 1; l_b := \text{tt}], K'_2[\bullet; l_x := i + 1; l_b := \text{tt}]) \in \mathcal{K}[\![\text{unit}]\!]\emptyset$.
 - * First suppose $W'' \sqsupseteq^{\text{pub}} W'_{\langle \text{ff}, i \rangle}$, $(h''_1, h''_2) : W''$, and $\langle h''_1; K'_1[\langle \cdot \rangle; l_x := !l_x + 1; l_b := \text{tt}] \rangle \downarrow^{<W''.k}$.
 - * To show: $\text{consistent}(W'')$ and $\langle h''_2; K'_2[\langle \cdot \rangle; l_x := i + 1; l_b := \text{tt}] \rangle \downarrow$
 - * Note that the only public successor of $\langle \text{ff}, i \rangle$ is $\langle \text{ff}, i \rangle$ itself and therefore $W'' = W''_{\langle \text{ff}, i \rangle}$.
 - * Hence $(h''_1, h''_2) : W''$ implies $h''_1(l_x) = i$ and thus $\langle h''_1[l_x \mapsto (i+1)][l_b \mapsto \text{tt}]; K'_1[\langle \cdot \rangle] \rangle \downarrow^{<W''.k}$.
 - * Note that $\langle h''_2; K'_2[\langle \cdot \rangle; l_x := i + 1; l_b := \text{tt}] \rangle \downarrow$ if $\langle h''_2[l_x \mapsto (i+1)][l_b \mapsto \text{tt}]; K'_2[\langle \cdot \rangle] \rangle \downarrow$.
 - * It is easy to see, using monotonicity (Lemma 10), that $W''_{\langle \text{tt}, i+1 \rangle} \sqsupseteq^{\text{pub}} W'_{\langle \text{tt}, i+1 \rangle} \sqsupseteq^{\text{pub}} W'$.
 - * Furthermore, using $(h''_1, h''_2) : W''$, $W''_{\langle \text{tt}, i+1 \rangle} \sqsupseteq W''$, and monotonicity (Lemma 10) it is easy to see that $(h''_1[l_x \mapsto (i+1)][l_b \mapsto \text{tt}], h''_2[l_x \mapsto (i+1)][l_b \mapsto \text{tt}]) : W''_{\langle \text{tt}, i+1 \rangle}$.
 - * Also, $\text{consistent}(W''_{\langle \text{tt}, i+1 \rangle})$ would imply $\text{consistent}(W'')$.
 - * Since $(W''_{\langle \text{tt}, i+1 \rangle}, \langle \cdot, \cdot \rangle) \in \mathcal{V}[\![\text{unit}]\!]\emptyset$, the claims therefore follow from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\![\text{unit}]\!]\emptyset$.
 - * Now suppose $W'' \sqsupseteq^{\text{pub}} W'_{\langle \text{ff}, i \rangle}$ and $(W'', v'_1, v'_2) \in \mathcal{V}[\![\text{exn}]\!]\emptyset$.
 - * To show: $(W'', K'_1[\text{raise } v'_1; l_x := !l_x + 1; l_b := \text{tt}], K'_2[\text{raise } v'_2; l_x := i + 1; l_b := \text{tt}]) \in \mathcal{O}$
 - * By Lemma 12 it suffices to show $(W'', K'_1[\text{raise } v'_1], K'_2[\text{raise } v'_2]) \in \mathcal{O}$, which follows from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\![\text{unit}]\!]\emptyset$.
- Case $W' = W'_{\langle \text{ff}, i \rangle}$ for some i :
- * Then $(h'_1, h'_2) : W'$ implies $h'_1(l_b) = h'_2(l_b) = \text{ff}$ and $h'_1(l_x) = h'_2(l_x) = i$.
 - * Hence $\langle h'_1; K'_1[\text{if } !l_b \text{ then } (l_b := \text{ff}; (\lambda y. e_3) \langle \cdot \rangle; l_x := !l_x + 1; l_b := \text{tt}) \text{ else } \langle \cdot \rangle] \rangle \downarrow^{<W'.k}$ implies $\langle h'_1; K'_1[\langle \cdot \rangle] \rangle \downarrow^{<W'.k}$.
 - * Similarly, $\langle h'_2; K'_2[\text{if } !l_b \text{ then } (l_b := \text{ff}; \text{let } n = !l_x \text{ in } (\lambda y. e_4) \langle \cdot \rangle; l_x := n+1; l_b := \text{tt}) \text{ else } \langle \cdot \rangle] \rangle \downarrow$ if $\langle h'_2; K'_2[\langle \cdot \rangle] \rangle \downarrow$.
 - * Since $(W', \langle \cdot, \cdot \rangle) \in \mathcal{V}[\![\text{unit}]\!]\emptyset$ the claims then follow from $(W', K'_1, K'_2) \in \mathcal{K}[\![\text{unit}]\!]\emptyset$.
- We show $(W_{\langle \text{tt}, 0 \rangle}, v_1^2, v_2^2) \in \mathcal{V}[\![\text{unit} \rightarrow \text{int}]\!]\emptyset$:
 - Suppose $W' \sqsupseteq W_{\langle \text{tt}, 0 \rangle}$, $(W', K'_1, K'_2) \in \mathcal{K}[\![\text{int}]\!]\emptyset$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K'_1[!l_x] \rangle \downarrow^{<W'.k}$.
 - To show: $\text{consistent}(W')$ 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 $(W', i, i) \in \mathcal{V}[\![\text{int}]\!]\emptyset$ the claims then follow from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\![\text{int}]\!]\emptyset$.

4.2.3 Higher-Order Profiling

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

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. p 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:

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

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.

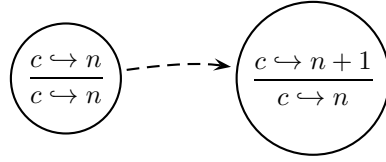
Formally, we show

$$; ; \cdot \vdash e_1 \lesssim_{\log} e_2 : ((\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}) \rightarrow (\text{unit} \rightarrow \text{unit}) \rightarrow ((\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}) \rightarrow \text{int}.$$

- This reduces to showing $(\widetilde{W}, e_1, e_2) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \rightarrow (\text{unit} \rightarrow \text{unit}) \rightarrow \langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \rightarrow \text{int}] \emptyset$, where $\widetilde{W} \in \mathcal{S}[\cdot]$.
- This boils down to showing $(W, e'_1, e'_2) \in \mathcal{E}[\text{int}] \emptyset$, where
 - $W \supseteq \widetilde{W}$,
 - $e'_1 := \text{let } \langle g', g'' \rangle = p g_1 \text{ in } (f_1 g'; g' \langle \rangle; a_1 g'; g'' \langle \rangle)$,
 - $e'_2 := \text{let } \langle g', g'' \rangle = p g_2 \text{ in } (f_2 g'; g_2 \langle \rangle; a_2 g'; g'' \langle \rangle + 1)$,
 - $(W, f_1, f_2) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle] \emptyset$,
 - $(W, g_1, g_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}] \emptyset$, and
 - $(W, a_1, a_2) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle] \emptyset$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\text{int}] \emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e'_1] \rangle \downarrow^{<W.k}$.
- To show: $\text{consistent}(W)$ 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
 - $H(n) := \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_1) = \widetilde{h}_2(l_2) + n\}$
 - $\iota_s := (s, \{(0, 1)\}^*, \emptyset^*, \emptyset, H)$
 - $W_s := W[\Sigma_1 := W.\Sigma_1, l_1:\text{int}][\Sigma_2 := W.\Sigma_2, l_2:\text{int}][\omega := W.\omega, \iota_s]$

The island represents the following STS:



- It is easy to see that $W_0 \sqsupseteq^{\text{pub}} W$ and, using monotonicity (Lemma 10), that $(\widehat{h}_1, \widehat{h}_2) : W_0$.
- We show $(W_0, f_1 g'_1, f_2 g'_2) \in \mathcal{E}[\text{unit}]\emptyset$:
 - Since $(W, f_1, f_2) \in \mathcal{V}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}]\emptyset$, it suffices to show $(W_0, g'_1, g'_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset$.
 - So suppose $W' \sqsupseteq W_0$, $(W', K'_1, K'_2) \in \mathcal{K}[\text{unit}]\emptyset$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K'_1[l_1 := !l_1 + 1; g_1 \langle \rangle] \rangle \downarrow^{<W'.k}$.
 - To show: $\text{consistent}(W')$ 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 $(W', g_1 \langle \rangle, g_2 \langle \rangle) \in \mathcal{E}[\text{unit}]\emptyset$, which follows from $(W, g_1, g_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset$ and $(W', \langle \rangle, \langle \rangle) \in \mathcal{V}[\text{unit}]\emptyset$.
- It thus suffices to show $(W_0, K_1[\bullet; g'_1 \langle \rangle; a_1 g'_1; (\lambda_{-} !l_1) \langle \rangle], K_2[\bullet; g_2 \langle \rangle; a_2 g'_2; (\lambda_{-} !l_2) \langle \rangle + 1]) \in \mathcal{K}[\text{unit}]\emptyset$.
- So first suppose $W' \sqsupseteq^{\text{pub}} W_0$, $(h'_1, h'_2) : W'$, 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: $\text{consistent}(W')$ and $\langle h'_2; K_2[\langle \rangle; g_2 \langle \rangle; a_2 g'_2; (\lambda_{\cdot} !l_2) \langle \rangle + 1] \rangle \downarrow$, *i.e.*, $\langle h'_2; K_2[g_2 \langle \rangle; a_2 g'_2; (\lambda_{\cdot} !l_2) \langle \rangle + 1] \rangle \downarrow$
 - Notation: we write W'_s for the world obtained from W' by setting the current state of our island to s .
 - Note that $W'_1 \supseteq W'$.
 - 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 $(W, g_1, g_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset$ and $(W'_1, \langle \rangle, \langle \rangle) \in \mathcal{V}[\text{unit}]\emptyset$ we get $(W'_1, g_1 \langle \rangle, g_2 \langle \rangle) \in \mathcal{E}[\text{unit}]\emptyset$.
 - Furthermore, it is obvious that $\text{consistent}(W'_1)$ would imply $\text{consistent}(W')$.
 - It thus suffices to show $(W'_1, K_1[\bullet; a_1 g'_1; (\lambda_{\cdot} !l_1) \langle \rangle], K_2[\bullet; a_2 g'_2; (\lambda_{\cdot} !l_2) \langle \rangle + 1]) \in \mathcal{K}[\text{unit}]\emptyset$.
 - So first suppose $W'' \supseteq^{\text{pub}} W'_1$, $(h''_1, h''_2) : W''$, and $\langle h''_1; K_1[\langle \rangle; a_1 g'_1; (\lambda_{\cdot} !l_1) \langle \rangle] \rangle \downarrow^{<W''.k}$, *i.e.*, $\langle h''_1; K_1[a_1 g'_1; (\lambda_{\cdot} !l_1) \langle \rangle] \rangle \downarrow^{<W''.k}$.
 - * To show: $\text{consistent}(W'')$ and $\langle h''_2; K_2[\langle \rangle; a_2 g'_2; (\lambda_{\cdot} !l_2) \langle \rangle + 1] \rangle \downarrow$, *i.e.*, $\langle h''_2; K_2[a_2 g'_2; (\lambda_{\cdot} !l_2) \langle \rangle + 1] \rangle \downarrow$.
 - * Following the proof of $(W_0, f_1 g'_1, f_2 g'_2) \in \mathcal{E}[\text{unit}]\emptyset$ above, we can easily show $(W'', a_1 g'_1, a_2 g'_2) \in \mathcal{E}[\text{unit}]\emptyset$.
 - * It thus suffices to show $(W'', K_1[\bullet; (\lambda_{\cdot} !l_1) \langle \rangle], K_2[\bullet; (\lambda_{\cdot} !l_2) \langle \rangle + 1]) \in \mathcal{K}[\text{unit}]\emptyset$.
 - * So first suppose $W''' \supseteq^{\text{pub}} W''$, $(h'''_1, h'''_2) : W'''$, and $\langle h'''_1; K_1[\langle \rangle; (\lambda_{\cdot} !l_1) \langle \rangle] \rangle \downarrow^{<W'''.k}$.
 - To show: $\text{consistent}(W''')$ and $\langle h'''_2; K_2[\langle \rangle; (\lambda_{\cdot} !l_2) \langle \rangle + 1] \rangle \downarrow$
 - From $(h'''_1, h'''_2) : W'''$ and $W''' \supseteq^{\text{pub}} W''$ we know $h'''_1(l_1) = n+1$ and $h'''_2(l_2) = n$, for some n .
 - Hence $\langle h'''_1; K_1[\langle \rangle; (\lambda_{\cdot} !l_1) \langle \rangle] \rangle \downarrow^{<W'''.k}$ implies $\langle h'''_1; K_1[n+1] \rangle \downarrow^{<W'''.k}$.
 - Similarly $\langle h'''_2; K_2[\langle \rangle; (\lambda_{\cdot} !l_2) \langle \rangle + 1] \rangle \downarrow$ if $\langle h'''_2; K_2[n+1] \rangle \downarrow$.
 - It is easy to see that $W''' = W'''_1 \supseteq^{\text{pub}} W''_1 \supseteq^{\text{pub}} W'_1 \supseteq^{\text{pub}} W$.
 - Since $(W''', n+1, n+1) \in \mathcal{V}[\text{int}]\emptyset$, the claims then follow from instantiating $(W, K_1, K_2) \in \mathcal{K}[\text{int}]\emptyset$.
 - * Now suppose $W''' \supseteq^{\text{pub}} W''$ and $(W''', v_1, v_2) \in \mathcal{V}[\text{exn}]\emptyset$.
 - To show: $(W''', K_1[\text{raise } v_1; (\lambda_{\cdot} !l_1) \langle \rangle], K_2[\text{raise } v_2; (\lambda_{\cdot} !l_2) \langle \rangle + 1]) \in \mathcal{O}$
 - By Lemma 12 it suffices to show $(W''', K_1[\text{raise } v_1], K_2[\text{raise } v_2]) \in \mathcal{O}$.
 - Since $W' \supseteq^{\text{pub}} W$ we know $W'_1 \supseteq^{\text{pub}} W$ and thus $W''' \supseteq^{\text{pub}} W$.
 - The claim then follows from instantiating $(W, K_1, K_2) \in \mathcal{K}[\text{int}]\emptyset$.
 - Now suppose $W'' \supseteq^{\text{pub}} W'_1$ and $(W'', v_1, v_2) \in \mathcal{V}[\text{exn}]\emptyset$.
 - * To show: $(W'', K_1[\text{raise } v_1; a_1 g'_1; (\lambda_{\cdot} !l_1) \langle \rangle], K_2[\text{raise } v_2; a_2 g'_2; (\lambda_{\cdot} !l_2) \langle \rangle + 1]) \in \mathcal{O}$
 - * By Lemma 12 it suffices to show $(W'', K_1[\text{raise } v_1], K_2[\text{raise } v_2]) \in \mathcal{O}$.
 - * Since $W' \supseteq^{\text{pub}} W$ we know $W'_1 \supseteq^{\text{pub}} W$ and thus $W'' \supseteq^{\text{pub}} W$.
 - * The claim then follows from instantiating $(W, K_1, K_2) \in \mathcal{K}[\text{int}]\emptyset$.
- Now suppose $W' \supseteq^{\text{pub}} W_0$ and $(W', v_1, v_2) \in \mathcal{V}[\text{exn}]\emptyset$.

- To show: $(W', K_1[\text{raise } v_1; g'_1 \langle \rangle; a_1 g'_1; (\lambda_{-}. !l_1) \langle \rangle], K_2[\text{raise } v_2; g_2 \langle \rangle; a_2 g'_2; (\lambda_{-}. !l_2) \langle \rangle + 1]) \in \mathcal{O}$
- By Lemma 12 it suffices to show $(W', K_1[\text{raise } v_1], K_2[\text{raise } v_2]) \in \mathcal{O}$.
- Since $W' \sqsupseteq^{\text{pub}} W$, this follows from instantiating $(W, K_1, K_2) \in \mathcal{K}[\text{int}]\emptyset$.

4.2.4 Single Return

$$\begin{aligned}
\tau &= (\text{unit} \rightarrow \text{unit}) \rightarrow \text{int} \\
e_1 &= \lambda f. \text{let } x = \text{ref } 0 \text{ in let } y = \text{ref } 0 \text{ in} \\
&\quad f \langle \rangle; x := !y; y := 1; !x \\
e_2 &= \lambda f. \text{let } x = \text{ref } 0 \text{ in let } y = \text{ref } 0 \text{ in} \\
&\quad f \langle \rangle; x := !y; y := 2; !x
\end{aligned}$$

The programs are not equivalent in **HOSC** as the following context C demonstrates:

$$\begin{aligned}
&\text{let } g = \bullet \text{ in} \\
&\text{call/cc } (k_0. \text{let } r = \text{ref } k_0 \text{ in} \\
&\quad \text{let } b = \text{ref } \text{tt} \text{ in} \\
&\quad \text{let } f = (\lambda_{-}. \text{call/cc } (k. r := k)) \text{ in} \\
&\quad \text{let } x = g f \text{ in} \\
&\quad \text{if } !b \text{ then } b := \text{ff}; \text{throw } \langle \rangle \text{ to } !r \text{ else } x)
\end{aligned}$$

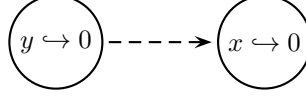
It is easy to verify that $C[e_1]$ yields 1, while $C[e_2]$ yields 2.

They are, however, equivalent in **HOSE**. We show $;\cdot; \vdash e_1 \lesssim_{\log} e_2 : \tau$. The other direction is analogous.

- This reduces to showing $(W_0, e_1, e_2) \in \mathcal{V}[\tau]\emptyset$, where $W_0 \in \mathcal{S}[\cdot]$.
- So suppose $W \sqsupseteq W_0$, $(W, v_1, v_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset$, $(W, K_1, K_2) \in \mathcal{K}[\text{int}]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e'_1[v_1/f]] \rangle \downarrow^{<W.k}$ (where e'_1 is the body of e_1).
- To show: $\langle h_2; K_2[e'_2[v_2/f]] \rangle \downarrow$ and $\text{consistent}(W)$ (where e'_2 is the body of e_2)
- $\langle h_1; K_1[e'_1[v_1/f]] \rangle \downarrow^{<W.k}$ implies $\langle \widehat{h}_1; K_1[v_1 \langle \rangle; l_x^1 := !l_y^1; l_y^1 := 1; !l_x^1] \rangle \downarrow^{<W.k}$, where $\widehat{h}_1 = h_1 \uplus \{l_x^1 \mapsto 0\} \uplus \{l_y^1 \mapsto 0\}$.
- Similarly, $\langle h_2; K_2[e'_2[v_2/f]] \rangle \downarrow$ if $\langle \widehat{h}_2; K_2[v_2 \langle \rangle; l_x^2 := !l_y^2; l_y^2 := 2; !l_x^2] \rangle \downarrow$, where $\widehat{h}_2 = h_2 \uplus \{l_x^2 \mapsto 0\} \uplus \{l_y^2 \mapsto 0\}$ and l_x^2, l_y^2 are fresh.
- Let
 - $H(\text{ff}) := \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_y^1) = \widetilde{h}_2(l_y^2) = 0\}$
 - $H(\text{tt}) := \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_x^1) = \widetilde{h}_2(l_x^2) = 0\}$
 - $\varphi := \emptyset^*$
 - $\delta := (\varphi \uplus \{\text{ff}, \text{tt}\})^*$
 - $\iota_s := (s, \delta, \varphi, \emptyset, H)$

$$- W_s := W[\Sigma_1 := W.\Sigma_1, l_x^1:\text{int}, l_y^1:\text{int}][\Sigma_2 := W.\Sigma_2, l_x^2:\text{int}, l_y^2:\text{int}][\omega := W.\omega, \iota_s]$$

The island represents the following STS:



- Note that $W_{\text{ff}} \sqsupseteq^{\text{pub}} W$.
- Using monotonicity (Lemma 10), it is thus easy to see that $(\widehat{h}_1, \widehat{h}_2) : W_{\text{ff}}$.
- Furthermore, $\text{consistent}(W_{\text{ff}})$ would imply $\text{consistent}(W)$.
- We show $(W_{\text{ff}}, v_1 \langle \rangle, v_2 \langle \rangle) \in \mathcal{E}[\text{unit}]\emptyset$:
 - This follows easily from $(W, v_1, v_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset$, using monotonicity (Lemma 10) and Lemma 12.
- We show $(W_{\text{ff}}, K_1[\bullet; l_x^1 := !l_y^1; l_y^1 := 1; !l_x^1], K_2[\bullet; l_x^2 := !l_y^2; l_y^2 := 2; !l_x^2]) \in \mathcal{K}[\text{unit}]\emptyset$:
 1. – Suppose $W' \sqsupseteq^{\text{pub}} W_{\text{ff}}$ and $(W', v'_1, v'_2) \in \mathcal{V}[\text{exn}]\emptyset$.
 - To show: $(W', K_1[\text{raise } v'_1; l_x^1 := !l_y^1; l_y^1 := 1; !l_x^1], K_2[\text{raise } v'_2; l_x^2 := !l_y^2; l_y^2 := 2; !l_x^2]) \in \mathcal{O}$
 - By Lemma 12 it suffices to show $(W', K_1[\text{raise } v'_1], K_2[\text{raise } v'_2]) \in \mathcal{O}$.
 - This follows from $(W, K_1, K_2) \in \mathcal{K}[\text{int}]\emptyset$.
 2. – Now instead suppose $W' \sqsupseteq^{\text{pub}} W_{\text{ff}}$, $(h'_1, h'_2) : W', \langle h'_1; K_1[l_x^1 := !l_y^1; l_y^1 := 1; !l_x^1] \rangle \downarrow^{<W'.k}$.
 - To show: $\langle h'_2; K_2[l_x^2 := !l_y^2; l_y^2 := 2; !l_x^2] \rangle \downarrow$
 - Note that $(h'_1, h'_2) : W'$ and $W' \sqsupseteq^{\text{pub}} W_{\text{ff}}$ imply $h'_i(l_y^i) = 0$.
 - Hence $\langle h'_1; K_1[l_x^1 := !l_y^1; l_y^1 := 1; !l_x^1] \rangle \downarrow^{<W'.k}$ implies $\langle h'_1[l_x^1 \mapsto 0][l_y^1 \mapsto 1]; K_1[0] \rangle \downarrow^{<W'.k}$.
 - Also, $\langle h'_2; K_2[l_x^2 := !l_y^2; l_y^2 := 2; !l_x^2] \rangle \downarrow$ if $\langle h'_2[l_x^2 \mapsto 0][l_y^2 \mapsto 0]; K_2[0] \rangle \downarrow$.
 - Let W'_{tt} be obtained from W' by setting the current state of our island to tt.
 - Note that $W'_{\text{tt}} \sqsupseteq^{\text{pub}} W$.
 - Since $(W'_{\text{tt}}, 0, 0) \in \mathcal{V}[\text{int}]\emptyset$, $(W, K_1, K_2) \in \mathcal{K}[\text{int}]\emptyset$ then yields $(W'_{\text{tt}}, K_1[0], K_2[0]) \in \mathcal{O}$.
 - Since also $(h'_1[l_x^1 \mapsto 0][l_y^1 \mapsto 1], h'_2[l_x^2 \mapsto 0][l_y^2 \mapsto 0]) : W'_{\text{tt}}$, the claims then follow from instantiating this.
- Putting all this together then yields the claims.

4.3 HOSC

4.3.1 One-Shot Continuations

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

We show $;\cdot;\vdash \text{callcc} \lesssim_{\log} \text{callcc}' : \forall\alpha. \tau_\alpha \rightarrow \alpha$.

- This reduces to showing $(W_0, \text{callcc}, \text{callcc}') \in \mathcal{V}[\forall\alpha. \tau_\alpha \rightarrow \alpha]\emptyset$, where $W_0 \in \mathcal{S}[\cdot]$.
- So suppose $W_1 \sqsupseteq W_0$ and $(\tau_1, \tau_2, r) \in \text{SomeValRel}$.
- To show: $(W_1, \lambda f. \text{call/cc}(x. f x), \lambda f. \text{let } r = \text{ref } (\text{cont } \bullet) \text{ in } G_r^{T_2} f) \in \mathcal{V}[\tau_\alpha \rightarrow \alpha]\rho$, 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 $\langle h_1; K_1[\text{call/cc}(x. f_1 x)] \rangle \downarrow^{<W.k}$.
- To show: $\langle h_2; K_2[\text{let } r = \text{ref } (\text{cont } \bullet) \text{ in } G_r^{T_2} f_2] \rangle \downarrow$
- $\langle h_1; K_1[\text{call/cc}(x. f_1 x)] \rangle \downarrow^{<W.k}$ implies $\langle h_1; K_1[f_1(\text{cont } K_1)] \rangle \downarrow^{<W.k}$.
- Similarly, $\langle h_2; K_2[\text{let } r = \text{ref } (\text{cont } \bullet) \text{ in } G_r^{T_2} f_2] \rangle \downarrow$ if $\langle \widehat{h}_2; K_2[f_2(\text{cont } (\text{throw } \bullet \text{ to } !l_r))] \rangle \downarrow$, where
 - $K := K_2[\text{let } x = \bullet \text{ in callcc1 } \tau_2 (\lambda z. G_{l_r}^{T_2} (\lambda _. \text{throw } x \text{ to } z))]$
 - $e_l := \text{cont } (\text{let } y = \bullet \text{ in if } !l \text{ then } (l := \text{ff}; \text{throw } y \text{ to } \text{cont } K) \text{ else } \perp)$
 - $\widehat{h}_2 := h_2 \uplus \{l_r \mapsto e_{l_b}\} \uplus \{l_b \mapsto \text{tt}\}$
 - and l_r, l_b are distinct and fresh.
- Let
 - $H(\langle \rangle) := \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \exists l \in \text{dom}(h_2). \widetilde{h}_2(l_r) = e_l \wedge \widetilde{h}_2(l) = \text{tt}\}$
 - $\iota := (\langle \rangle, \emptyset^*, \emptyset^*, \emptyset, H)$
 - $\widehat{W} := W[\Sigma_2 := W.\Sigma_2, l_r:\text{cont } \tau_2, l_b:\text{bool}][\omega := (W.\omega, \iota)]$

- It is easy to see that $\widehat{W} \sqsupseteq^{\text{pub}} W$ 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 $(\widehat{W}, f_1 (\text{cont } K_1), f_2 (\text{cont } (\text{throw } \bullet \text{ to } !l_r))) \in \mathcal{E}[\alpha]\rho$.
- Since $(W, f_1, f_2) \in \mathcal{V}[\tau_\alpha]\rho$, this reduces to showing $(\widehat{W}, \text{cont } K_1, \text{cont } (\text{throw } \bullet \text{ to } !l_r)) \in \mathcal{V}[\text{cont } \alpha]\rho$.
- So suppose $W' \sqsupseteq^{\text{pub}} \widehat{W}$, $(W', v'_1, v'_2) \in \mathcal{V}[\alpha]\rho$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K_1[v'_1] \rangle \downarrow^{<W'.k}$.
- To show: $\langle h'_2; \text{throw } v'_2 \text{ to } !l_r \rangle \downarrow$
- From $(h'_1, h'_2) : W'$ we know that $h'_2(l_r) = e_l$ and $h'_2(l) = \text{tt}$, for some l .
- Hence $\langle h'_2; \text{throw } v'_2 \text{ to } !l_r \rangle \downarrow$ if $\langle h'_2[l \mapsto \text{ff}]; K_2[\text{callcc1 } \tau_2 (\lambda z. G_{l_r}^{\tau_2} (\lambda _ . \text{throw } v'_2 \text{ to } z))] \rangle \downarrow$ if $\langle h'_2[l \mapsto \text{ff}][l_r \mapsto e_{l'}] \uplus \{l' \mapsto \text{tt}\}; K_2[v'_2] \rangle \downarrow$, where l' is fresh.
- Let $W'' := W'[\Sigma_2 := W'.\Sigma_2, l' : \text{bool}]$.
- It is easy to see that $W'' \sqsupseteq^{\text{pub}} W'$ and, using monotonicity (Lemma 10), that $(h'_1, h'_2[l \mapsto \text{ff}][l_r \mapsto e_{l'}] \uplus \{l' \mapsto \text{tt}\}) : W''$.
- Also by monotonicity (Lemma 10) we know $(W'', v'_1, v'_2) \in \mathcal{V}[\alpha]\rho$.
- Hence, using $W'' \sqsupseteq^{\text{pub}} W$ and instantiating $(W, K_1, K_2) \in \mathcal{K}[\alpha]\rho$ yields the claim.

4.3.2 Local State Release 2

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

We show $\cdot; \cdot; \cdot \vdash e_1 \lesssim_{\log} e_2 : (\text{unit} \rightarrow \text{ref int}) \times (\text{ref int} \rightarrow \text{bool})$:

- This reduces to showing $(W, e_1, e_2) \in \mathcal{E}[(\text{unit} \rightarrow \text{ref int}) \times (\text{ref int} \rightarrow \text{bool})]\emptyset$, where $W \in \mathcal{S}[\cdot]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[(\text{unit} \rightarrow \text{ref int}) \times (\text{ref int} \rightarrow \text{bool})]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_1] \rangle \downarrow^{<W.k}$.
- To show: $\text{consistent}(W)$ 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
 - $\widehat{h}_1 := h_1 \uplus \{l_x^1 \mapsto 0\} \uplus \{l_b \mapsto \text{ff}\}$,
 - $v_1 := (\lambda _ . l_b := \text{tt}; l_x^1)$,
 - $v_3 := (\lambda y. y == l_x^1 \text{ andalso } !l_b)$, and
 - l_x^1, l_b are fresh and distinct.

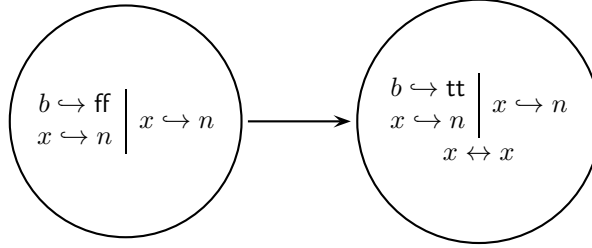
- Similarly, $\langle h_2; K_2[e_2] \rangle \downarrow$ if $\langle \widehat{h}_2; K_2[\langle v_2, v_4 \rangle] \rangle \downarrow$, where

- $\widehat{h}_2 := h_2 \uplus \{l_x^2 \mapsto 0\}$,
- $v_2 := (\lambda _. l_x^2)$,
- $v_4 := (\lambda y. y == l_x^2)$, and
- l_x^2 is fresh.

- Let

- $H(1) := \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_b) = \text{ff} \wedge \exists n. \widetilde{h}_1(l_x^1) = n = \widetilde{h}_2(l_x^2)\}$
- $\mathbf{z} := \{l_x^1, l_x^2\}$
- $H(2) := \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_b) = \text{tt} \wedge \exists n. \widetilde{h}_1(l_x^1) = n = \widetilde{h}_2(l_x^2)\}$
- $\varphi := \{(1, \mathbf{z})\}^*$
- $\delta := \varphi$
- $\iota_s := (s, \delta, \varphi, \emptyset, H)$
- $W_s := W[\Sigma_1 := W.\Sigma_1, l_x^1:\text{int}, l_b:\text{bool}][\Sigma_2 := W.\Sigma_2, l_x^2:\text{int}][\omega := W.\omega, \iota_s]$

The island represents the following STS:



- It is easy to see that $W_1 \sqsupseteq^{\text{pub}} W$ and, using monotonicity (Lemma 10), that $(\widehat{h}_1, \widehat{h}_2) : W_1$.
- Also, $\text{consistent}(W_1)$ would imply $\text{consistent}(W)$.
- It thus suffices to show $(W_1, \langle v_1, v_3 \rangle, \langle v_2, v_4 \rangle) \in \mathcal{V}[(\text{unit} \rightarrow \text{ref int}) \times (\text{ref int} \rightarrow \text{bool})] \emptyset$, which splits into two parts.
- We show $(W_1, v_1, v_2) \in \mathcal{V}[\text{unit} \rightarrow \text{ref int}] \emptyset$:
 - Suppose $W' \sqsupseteq W_1$, $(W', K'_1, K'_2) \in \mathcal{K}[\text{ref int}] \emptyset$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K'_1[l_b := \text{tt}; l_x^1] \rangle \downarrow^{<W'.k}$.
 - To show: $\text{consistent}(W')$ and $\langle h'_2; K'_2[l_x^2] \rangle \downarrow$
 - $\langle h'_1; K'_1[l_b := \text{tt}; l_x^1] \rangle \downarrow^{<W'.k}$ implies $\langle h'_1[l_b \mapsto \text{tt}]; K'_1[l_x^1] \rangle \downarrow^{<W'.k}$.
 - Let \widehat{W}' be the world obtained from W' by setting our island's current state to \mathbf{z} .
 - It is easy to see that $\widehat{W}' \sqsupseteq^{\text{pub}} W'$ and, using monotonicity (Lemma 10), that $(h'_1[l_b \mapsto \text{tt}], h'_2) : \widehat{W}'$.

- Also, $\text{consistent}(\widehat{W}')$ would imply $\text{consistent}(W')$.
- Since $(\widehat{W}', K'_1, K'_2) \in \mathcal{K}[\llbracket \text{ref int} \rrbracket \emptyset]$, it therefore remains to show $(\widehat{W}', l_x^1, l_x^2) \in \mathcal{V}[\llbracket \text{ref int} \rrbracket \emptyset]$.
- So suppose $W'' \sqsupseteq \widehat{W}'$.
- Notice that $\text{bij}(W''.\omega(p).s) = \text{bij}(\widehat{W}'.\omega(p).s) = \text{bij}(2) = \text{bij}(\{\langle l_x^1, l_x^2 \rangle\}) = \{\langle l_x^1, l_x^2 \rangle\}$.
- Furthermore:

$$\begin{aligned}
& W''.\omega(p).H(W''.\omega(p).s) \\
&= \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_b) = b \wedge \exists n. \widetilde{h}_1(l_x^1) = n = \widetilde{h}_2(l_x^2)\} \\
&= \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_b) = b \wedge l_x^1 \notin \text{dom}(\widetilde{h}_1) \wedge l_x^2 \notin \text{dom}(\widetilde{h}_2)\} \\
&\otimes \{(\widetilde{W}, \{l_x^1 \mapsto n_1\}, \{l_x^2 \mapsto n_2\}) \in \text{HeapAtom} \mid n_1 = n_2\} \\
&= \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_b) = b \wedge l_x^1 \notin \text{dom}(\widetilde{h}_1) \wedge l_x^2 \notin \text{dom}(\widetilde{h}_2)\} \\
&\otimes \{(\widetilde{W}, \{l_x^1 \mapsto v_1\}, \{l_x^2 \mapsto v_2\}) \in \text{HeapAtom} \mid (\widetilde{W}, v_1, v_2) \in \mathcal{V}[\llbracket \text{int} \rrbracket \emptyset]\}
\end{aligned}$$

- We show $(W_1, v_3, v_4) \in \mathcal{V}[\llbracket \text{ref int} \rightarrow \text{bool} \rrbracket \emptyset]$:
 - Suppose $W' \sqsupseteq W_1$, $(W', l_1, l_2) \in \mathcal{V}[\llbracket \text{ref int} \rrbracket \emptyset]$, $(W', K'_1, K'_2) \in \mathcal{K}[\llbracket \text{ref int} \rrbracket \emptyset]$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K'_1[l_1 == l_x^1 \text{ andalso } !l_b] \rangle \downarrow^{<W'.k}$.
 - To show: $\text{consistent}(W')$ and $\langle h'_2; K'_2[l_2 == l_x^2] \rangle \downarrow$
 - We know $(l_1, l_2) \in \text{bij}(W'.\omega(i).s)$ 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 $h'_1(l_b) = \text{tt}$.
 - * Consequently, $\langle h'_1; K'_1[l_1 == l_x^1 \text{ andalso } !l_b] \rangle \downarrow^{<W'.k}$ implies $\langle h'_1; K'_1[\text{tt}] \rangle \downarrow^{<W'.k}$.
 - * Similarly, $\langle h'_2; K'_2[l_2 == l_x^2] \rangle \downarrow$ if $\langle h'_2; K'_2[\text{tt}] \rangle \downarrow$.
 - * Since $(W', \text{tt}, \text{tt}) \in \mathcal{V}[\llbracket \text{bool} \rrbracket \emptyset]$, the claims now follow from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\llbracket \text{ref int} \rrbracket \emptyset]$.
 - Case $l_1 \neq l_x^1$ and $l_2 \neq l_x^2$:
 - * Then $\langle h'_1; K'_1[l_1 == l_x^1 \text{ andalso } !l_b] \rangle \downarrow^{<W'.k}$ implies $\langle h'_1; K'_1[\text{ff}] \rangle \downarrow^{<W'.k}$.
 - * Similarly, $\langle h'_2; K'_2[l_2 == l_x^2] \rangle \downarrow$ if $\langle h'_2; K'_2[\text{ff}] \rangle \downarrow$.
 - * Since $(W', \text{ff}, \text{ff}) \in \mathcal{V}[\llbracket \text{bool} \rrbracket \emptyset]$, the claims now follow from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\llbracket \text{ref int} \rrbracket \emptyset]$.

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 exist 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 be 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`.

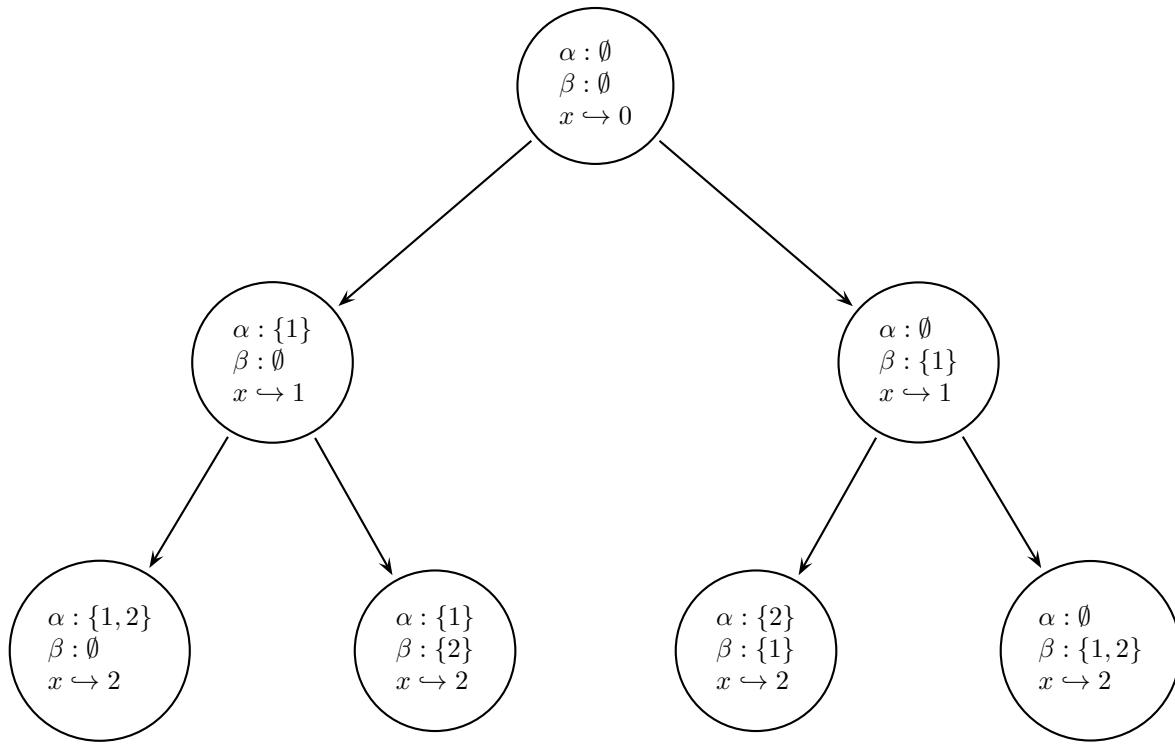
4.3.3 Twin Abstraction

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

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

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

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



4.4 FOS

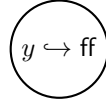
4.4.1 Deferred Divergence 3

$$\begin{aligned}
\tau &= ((\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}) \rightarrow \text{unit} \\
e_1 &= \text{let } y = \text{ref ff in} \\
&\quad \lambda f: (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}. f (\lambda z: \text{unit}. y := \text{tt}); \\
&\quad \quad \text{if } !y \text{ then } \perp \text{ else } \langle \rangle \\
e_2 &= \lambda f: (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}. f (\lambda z: \text{unit}. \perp)
\end{aligned}$$

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

- This reduces to showing $(W, e_2, e_1) \in \mathcal{E}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$, 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: $\text{consistent}(W)$ and $\langle h_2; K_2[e_1] \rangle \downarrow$
- Observe that $\langle h_2; K_2[e_1] \rangle \downarrow$ if $\langle h_2 \uplus \{l_y \mapsto \text{ff}\}; K_2[\widehat{e}_1[l_y/y]] \rangle \downarrow$, where \widehat{e}_1 is the body of e_1 and l_y any free location.
- Let
 - $H(\langle \rangle) := \{(\widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_2(l_y) = \text{ff}\}$
 - $\iota := (\langle \rangle, \emptyset^*, \emptyset^*, \emptyset, H)$
 - $\widehat{W} := W[\Sigma_2 := W.\Sigma_2, l_y: \text{bool}][\omega := W.\omega, \iota]$

The island represents the following STS:



- Note that $\widehat{W} \sqsupseteq^{\text{pub}} W$ and $(h_1, h_2 \uplus \{l_y \mapsto \text{ff}\}) : \widehat{W}$.
- 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 $W' \sqsupseteq W$, $(W', f_1, f_2) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$, $(W', K'_1, K'_2) \in \mathcal{K}[\langle \text{unit} \rangle \emptyset]$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K'_1[f_1(\lambda _ . \perp)] \rangle \downarrow^{<W'.k}$.
- To show: $\text{consistent}(W')$ and $\langle h'_2; K'_2[f_2(\lambda _ . l_y := \text{tt}); \text{if } !l_y \text{ then } \perp \text{ else } \langle \rangle] \rangle \downarrow$
- We show $(W', f_1(\lambda _ . \perp), f_2(\lambda _ . l_y := \text{tt})) \in \mathcal{E}[\langle \text{unit} \rangle \emptyset]$:
 - Since $(W', f_1, f_2) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \emptyset]$, it suffices to show $(W', (\lambda _ . \perp), (\lambda _ . l_y := \text{tt})) \in \mathcal{V}[\langle \text{unit} \rightarrow \text{unit} \rangle \emptyset]$.
 - This holds trivially, because $\langle h'_1; K'_1[\perp] \rangle$ diverges for any h''_1 and K''_1 .
- We show $(W', K'_1, K'_2[\bullet; \text{if } !l_y \text{ then } \perp \text{ else } \langle \rangle]) \in \mathcal{K}[\langle \text{unit} \rangle \emptyset]$:
 - So suppose $W'' \sqsupseteq^{\text{pub}} W'$, $(h''_1, h''_2) : W''$, and $\langle h''_1; K'_1[\langle \rangle] \rangle \downarrow^{<W''.k}$.

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

4.5 FOSC

4.5.1 Callback With Lock

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

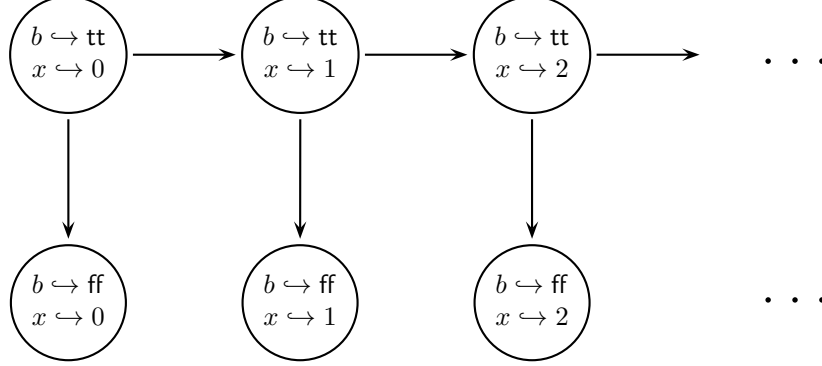
We already showed that e_1 approximates e_2 in the higher-order-state setting without control. This proof had to use private transitions, because the approximation *does not* hold in the presence of control. In the first-order-state setting, however, the approximation *does* hold in the presence of control—see the following proof, which does not make use of private transitions.

We show $;\cdot; \vdash e_1 \lesssim_{\log} e_2 : ((\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}) \times (\text{unit} \rightarrow \text{int})$:

- This reduces to showing $(W, e_1, e_2) \in \mathcal{E}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}] \times (\text{unit} \rightarrow \text{int}) \emptyset$, where $W \in \mathcal{S}[\cdot]$.
- So suppose $(W, K_1, K_2) \in \mathcal{K}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}] \times (\text{unit} \rightarrow \text{int}) \emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[e_1] \rangle \downarrow^{<W.k}$.
- To show: $\text{consistent}(W)$ 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
 - $v_1 := \langle v_1^1, v_1^2 \rangle$,
 - $v_1^1 := \lambda f. \text{if } !l_b \text{ then } (l_b := \text{ff}; f \langle \rangle; l_x := !l_x + 1; l_b := \text{tt}) \text{ else } \langle \rangle$,
 - $v_1^2 := \lambda z. !l_x$,
 - $\widehat{h}_1 := h_1 \uplus \{l_b \mapsto \text{tt}\} \uplus \{l_x \mapsto 0\}$, 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
 - $v_2 := \langle v_2^1, v_2^2 \rangle$,
 - $v_2^1 := \lambda f. \text{if } !l_b \text{ then } (l_b := \text{ff}; \text{let } n = !l_x \text{ in } f \langle \rangle; l_x := n + 1; l_b := \text{tt}) \text{ else } \langle \rangle$,
 - $v_2^2 := \lambda z. !l_x$, and
 - $h'_2 := h_2 \uplus \{l_b \mapsto \text{tt}\} \uplus \{l_x \mapsto 0\}$.
- Let
 - $H(\langle o, i \rangle) := \{(\widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_b) = \widetilde{h}_2(l_b) = o \wedge \widetilde{h}_1(l_x) = \widetilde{h}_2(l_x) = i\}$
 - $\varphi := \{(\langle \text{tt}, i \rangle, \langle \text{tt}, i + 1 \rangle) \mid i \in \mathbb{N}\}^*$
 - $\delta := (\varphi \uplus \{(\langle \text{tt}, i \rangle, \langle \text{ff}, i \rangle) \mid i \in \mathbb{N}\} \uplus \{(\langle \text{ff}, i \rangle, \langle \text{tt}, i + 1 \rangle) \mid i \in \mathbb{N}\})^*$
 - $\iota_s := (s, \delta, \varphi, \emptyset, H)$

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

The island represents the following STS:



- It is easy to see that $W_{\langle \text{tt}, 0 \rangle} \sqsupseteq^{\text{pub}} W$ and $(\widehat{h}_1, \widehat{h}_2) : W_{\langle \text{tt}, 0 \rangle}$.
- It thus suffices to show $(W_{\langle \text{tt}, 0 \rangle}, v_1, v_2) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle \times \langle (\text{unit} \rightarrow \text{int}) \rangle] \emptyset$, which splits into two parts.
- We show $(W_{\langle \text{tt}, 0 \rangle}, v_1^1, v_2^1) \in \mathcal{V}[\langle (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit} \rangle] \emptyset$:
 - Suppose $W' \sqsupseteq W_{\langle \text{tt}, 0 \rangle}$, $(W', \lambda y. e_3, \lambda y. e_4) \in \mathcal{V}[\langle \text{unit} \rightarrow \text{unit} \rangle] \emptyset$, $(W', K'_1, K'_2) \in \mathcal{K}[\langle \text{unit} \rangle] \emptyset$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K'_1[\text{if } !l_b \text{ then } (l_b := \text{ff}; (\lambda y. e_3) \langle \rangle; l_x := !l_x + 1; l_b := \text{tt}) \text{ else } \langle \rangle] \rangle \downarrow^{<W'.k}$.
 - To show: $\text{consistent}(W')$ and $\langle h'_2; K'_2[\text{if } !l_b \text{ then } (l_b := \text{ff}; \text{let } n = !l_x \text{ in } (\lambda y. e_4) \langle \rangle; l_x := n + 1; l_b := \text{tt}) \text{ else } \langle \rangle] \rangle \downarrow$
 - Notation: we write W'_s to denote the world obtained from W' by setting our island's current state to s .
 - Case $W' = W'_{\langle \text{tt}, i \rangle}$ for some i :
 - * Then $(h'_1, h'_2) : W'$ implies $h'_1(l_b) = h'_2(l_b) = \text{tt}$ and $h'_1(l_x) = h'_2(l_x) = i$.
 - * Hence $\langle h'_1; K'_1[\text{if } !l_b \text{ then } (l_b := \text{ff}; (\lambda y. e_3) \langle \rangle; l_x := !l_x + 1; l_b := \text{tt}) \text{ else } \langle \rangle] \rangle \downarrow^{<W'.k}$ implies $\langle h'_1[l_b \mapsto \text{ff}]; K'_1[e_3[\langle \rangle/y]; (\lambda y. e_3) \langle \rangle; l_x := !l_x + 1; l_b := \text{tt}] \rangle \downarrow^{<W'.k}$.
 - * Similarly, $\langle h'_2; K'_2[\text{if } !l_b \text{ then } (l_b := \text{ff}; \text{let } n = !l_x \text{ in } (\lambda y. e_4) \langle \rangle; l_x := n + 1; l_b := \text{tt}) \text{ else } \langle \rangle] \rangle \downarrow$ if $\langle h'_2[l_b \mapsto \text{ff}]; K'_2[e_4[\langle \rangle/y]; l_x := i + 1; l_b := \text{tt}] \rangle \downarrow$.
 - * It is easy to see that $W'_{\langle \text{ff}, i \rangle} \sqsupseteq W'$ and $(h'_1[l_b \mapsto \text{ff}], h'_2[l_b \mapsto \text{ff}]) : W'_{\langle \text{ff}, i \rangle}$.
 - * Also, $\text{consistent}(W'_{\langle \text{ff}, i \rangle})$ would imply $\text{consistent}(W')$.
 - * Since $(W'_{\langle \text{ff}, i \rangle}, \langle \rangle, \langle \rangle) \in \mathcal{V}[\langle \text{unit} \rangle] \emptyset$ and thus $(W'_{\langle \text{ff}, i \rangle}, e_3[\langle \rangle/y], e_4[\langle \rangle/y]) \in \mathcal{E}[\langle \text{unit} \rangle] \emptyset$, it suffices to show $(W'_{\langle \text{ff}, i \rangle}, K'_1[\bullet; l_x := !l_x + 1; l_b := \text{tt}], K'_2[\bullet; l_x := i + 1; l_b := \text{tt}]) \in \mathcal{K}[\langle \text{unit} \rangle] \emptyset$.
 - * So suppose $W'' \sqsupseteq^{\text{pub}} W'_{\langle \text{ff}, i \rangle}$, $(h''_1, h''_2) : W''$, and $\langle h''_1; K'_1[\langle \rangle; l_x := !l_x + 1; l_b := \text{tt}] \rangle \downarrow^{<W''.k}$.
 - * To show: $\text{consistent}(W'')$ and $\langle h''_2; K'_2[\langle \rangle; l_x := i + 1; l_b := \text{tt}] \rangle \downarrow$
 - * Note that the only public successor of $\langle \text{ff}, i \rangle$ is $\langle \text{ff}, i \rangle$ itself and therefore $W'' = W''_{\langle \text{ff}, i \rangle}$.

- * Hence $(h'_1, h'_2) : W''$ implies $h'_1(l_x) = i$ and thus $\langle h'_1[l_x \mapsto (i+1)][l_b \mapsto \text{tt}]; K'_1[\langle \rangle] \rangle \downarrow^{<W''.k}$.
 - * Note that $\langle h'_2; K'_2[\langle \rangle; l_x := i+1; l_b := \text{tt}] \rangle \downarrow$ if $\langle h'_2[l_x \mapsto (i+1)][l_b \mapsto \text{tt}]; K'_2[\langle \rangle] \rangle \downarrow$.
 - * It is easy to see that $W''_{\langle \text{tt}, i+1 \rangle} \sqsupseteq^{\text{pub}} W'_{\langle \text{tt}, i+1 \rangle} \sqsupseteq^{\text{pub}} W'$.
 - * Furthermore, using $(h'_1, h'_2) : W''$ it is easy to see that $(h'_1[l_x \mapsto (i+1)][l_b \mapsto \text{tt}], h'_2[l_x \mapsto (i+1)][l_b \mapsto \text{tt}]) : W''_{\langle \text{tt}, i+1 \rangle}$.
 - * Also, $\text{consistent}(W''_{\langle \text{tt}, i+1 \rangle})$ would imply $\text{consistent}(W'')$.
 - * Since $(W''_{\langle \text{tt}, i+1 \rangle}, \langle \rangle, \langle \rangle) \in \mathcal{V}[\llbracket \text{unit} \rrbracket \emptyset]$, the claims therefore follow from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\llbracket \text{unit} \rrbracket \emptyset]$.
- Case $W' = W'_{\langle \text{ff}, i \rangle}$ for some i :
- * Then $(h'_1, h'_2) : W'$ implies $h'_1(l_b) = h'_2(l_b) = \text{ff}$ and $h'_1(l_x) = h'_2(l_x) = i$.
 - * Hence $\langle h'_1; K'_1[\text{if } !l_b \text{ then } (l_b := \text{ff}; (\lambda y. e_3) \langle \rangle; l_x := !l_x + 1; l_b := \text{tt}) \text{ else } \langle \rangle] \rangle \downarrow^{<W'.k}$ implies $\langle h'_1; K'_1[\langle \rangle] \rangle \downarrow^{<W'.k}$.
 - * Similarly, $\langle h'_2; K'_2[\text{if } !l_b \text{ then } (l_b := \text{ff}; \text{let } n = !l_x \text{ in } (\lambda y. e_4) \langle \rangle; l_x := n+1; l_b := \text{tt}) \text{ else } \langle \rangle] \rangle \downarrow$ if $\langle h'_2; K'_2[\langle \rangle] \rangle \downarrow$.
 - * Since $(W', \langle \rangle, \langle \rangle) \in \mathcal{V}[\llbracket \text{unit} \rrbracket \emptyset]$ the claims then follow from $(W', K'_1, K'_2) \in \mathcal{K}[\llbracket \text{unit} \rrbracket \emptyset]$.

- We show $(W_{\langle \text{tt}, 0 \rangle}, v_1^2, v_2^2) \in \mathcal{V}[\llbracket \text{unit} \rightarrow \text{int} \rrbracket \emptyset]$:

- Suppose $W' \sqsupseteq W_{\langle \text{tt}, 0 \rangle}$, $(W', K'_1, K'_2) \in \mathcal{K}[\llbracket \text{int} \rrbracket \emptyset]$, $(h'_1, h'_2) : W'$, and $\langle h'_1; K'_1[!l_x] \rangle \downarrow^{<W'.k}$.
- To show: $\text{consistent}(W')$ 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 $(W', i, i) \in \mathcal{V}[\llbracket \text{int} \rrbracket \emptyset]$ the claims then follow from instantiating $(W', K'_1, K'_2) \in \mathcal{K}[\llbracket \text{int} \rrbracket \emptyset]$.

4.5.2 Higher-Order Profiling

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

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

Formally, we show

$$; \cdot \vdash e_1 \lesssim_{\log} e_2 : ((\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}) \rightarrow (\text{unit} \rightarrow \text{unit}) \rightarrow ((\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}) \rightarrow \text{int}.$$

- This reduces to showing $(\widetilde{W}, e_1, e_2) \in \mathcal{V}[\llbracket ((\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}) \rightarrow (\text{unit} \rightarrow \text{unit}) \rightarrow ((\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}) \rightarrow \text{int} \rrbracket \emptyset]$, where $\widetilde{W} \in \mathcal{S}[\cdot]$.
- This boils down to showing $(W, e'_1, e'_2) \in \mathcal{E}[\llbracket \text{int} \rrbracket \emptyset]$, where

$$- W \sqsupseteq \widetilde{W},$$

- $e'_1 := \text{let } \langle g', g'' \rangle = p \ g_1 \text{ in } (f_1 \ g'; g' \ \langle \rangle; a_1 \ g'; g'' \ \langle \rangle),$
- $e'_2 := \text{let } \langle g', g'' \rangle = p \ g_2 \text{ in } (f_2 \ g'; g_2 \ \langle \rangle; a_2 \ g'; g'' \ \langle \rangle + 1),$
- $(W, f_1, f_2) \in \mathcal{V}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}]\emptyset,$
- $(W, g_1, g_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset,$ and
- $(W, a_1, a_2) \in \mathcal{V}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}]\emptyset.$
- So suppose $(W, K_1, K_2) \in \mathcal{K}[\text{int}]\emptyset,$ $(h_1, h_2) : W,$ 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
 - $H(n) := \{(\widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_1) = \widetilde{h}_2(l_2) + n\}$
 - $\iota_s := (s, \emptyset^*, \emptyset^*, \emptyset, H)$
 - $W_s := W[\Sigma_1 := W.\Sigma_1, l_1:\text{int}][\Sigma_2 := W.\Sigma_2, l_2:\text{int}][\omega := W.\omega, \iota_s]$
- It is easy to see that $W_0 \sqsupseteq^{\text{pub}} W$ and $(\widehat{h}_1, \widehat{h}_2) : W_0.$
- We show $(W_0, f_1 \ g'_1, f_2 \ g'_2) \in \mathcal{E}[\text{unit}]\emptyset:$
 - Since $(W, f_1, f_2) \in \mathcal{V}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}]\emptyset,$ it suffices to show $(W_0, g'_1, g'_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset.$
 - So suppose $W' \sqsupseteq W_0,$ $(W', K'_1, K'_2) \in \mathcal{K}[\text{unit}]\emptyset,$ $(h'_1, h'_2) : W',$ 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 $(W', g_1 \ \langle \rangle, g_2 \ \langle \rangle) \in \mathcal{E}[\text{unit}]\emptyset,$ which follows from $(W, g_1, g_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset$ and $(W', \langle \rangle, \langle \rangle) \in \mathcal{V}[\text{unit}]\emptyset.$

- It thus suffices to show $(W_0, K_1[\bullet; g'_1 \langle \rangle; a_1 g'_1; (\lambda_{-} !l_1) \langle \rangle], K_2[\bullet; g_2 \langle \rangle; a_2 g'_2; (\lambda_{-} !l_2) \langle \rangle + 1]) \in \mathcal{K}[\text{unit}]\emptyset$.
- So suppose $W' \supseteq^{\text{pub}} W_0$, $(h'_1, h'_2) : W'$, 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 $W'_1 \supseteq W'$. But because we are in the first-order setting, $(h'_1, h'_2) : W'_1$ nevertheless follows from $(h'_1, h'_2) : W'$.
- It is easy to see that $W'_1 \supseteq W$, though.
- From $(W, g_1, g_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset$ and $(W'_1, \langle \rangle, \langle \rangle) \in \mathcal{V}[\text{unit}]\emptyset$ we get $(W'_1, g_1 \langle \rangle, g_2 \langle \rangle) \in \mathcal{E}[\text{unit}]\emptyset$.
- It thus suffices to show $(W'_1, K_1[\bullet; a_1 g'_1; (\lambda_{-} !l_1) \langle \rangle], K_2[\bullet; a_2 g'_2; (\lambda_{-} !l_2) \langle \rangle + 1]) \in \mathcal{K}[\text{unit}]\emptyset$.
- So suppose $W'' \supseteq^{\text{pub}} W'_1$, $(h''_1, h''_2) : W''$, 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 $(W_0, f_1 g'_1, f_2 g'_2) \in \mathcal{E}[\text{unit}]\emptyset$ above, we can easily show $(W'', a_1 g'_1, a_2 g'_2) \in \mathcal{E}[\text{unit}]\emptyset$.
- It thus suffices to show $(W'', K_1[\bullet; (\lambda_{-} !l_1) \langle \rangle], K_2[\bullet; (\lambda_{-} !l_2) \langle \rangle + 1]) \in \mathcal{K}[\text{unit}]\emptyset$.
- So suppose $W''' \supseteq^{\text{pub}} W''$, $(h'''_1, h'''_2) : W'''$, 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 $W''' \supseteq^{\text{pub}} W''$ 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 $W''' = W''' \supseteq^{\text{pub}} W'' \supseteq^{\text{pub}} W'_1 \supseteq^{\text{pub}} W$.
- Since $(W''', n + 1, n + 1) \in \mathcal{V}[\text{int}]\emptyset$, the claims then follow from instantiating $(W, K_1, K_2) \in \mathcal{K}[\text{int}]\emptyset$.

4.5.3 Irreversible State Change

$$\begin{aligned} e_1 &= \lambda f. \text{let } x = \text{ref tt in } f (\lambda_{\cdot}. x := \text{ff}); x := \text{tt}; \lambda_{\cdot}. !x \\ e_2 &= \lambda f. f (\lambda_{\cdot}. \langle \rangle); \lambda_{\cdot}. \text{tt} \end{aligned}$$

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

$$\begin{aligned} C &= \text{let } g = \bullet \text{ in} \\ &\quad \text{let } y = \text{ref } (\lambda_{\cdot}. \langle \rangle) \text{ in} \\ &\quad \text{let } f = (\lambda g'. y := g') \text{ in} \\ &\quad \text{let } f' = g f \text{ in} \\ &\quad !y \langle \rangle; f' \langle \rangle \end{aligned}$$

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 $\cdot; \cdot \vdash e_1 \lesssim_{\log} e_2 : (\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}$:

- This reduces to showing $(\widehat{W}, e_1, e_2) \in \mathcal{V}[(\text{unit} \rightarrow \text{unit}) \rightarrow \text{unit}]\emptyset$, where $\widehat{W} \in \mathcal{S}[\cdot]$.
- So suppose $W \sqsupseteq \widehat{W}$, $(W, f_1, f_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset$, $(W, K_1, K_2) \in \mathcal{K}[\text{unit}]\emptyset$, $(h_1, h_2) : W$, and $\langle h_1; K_1[\text{let } x = \text{ref tt in } f_1 (\lambda_{\cdot}. x := \text{ff}); x := \text{tt}; \lambda_{\cdot}. !x] \rangle \downarrow^{<W.k}$.
- To show: $\langle h_2; K_2[f_2 (\lambda_{\cdot}. \langle \rangle); \lambda_{\cdot}. \text{tt}] \rangle \downarrow$
- $\langle h_1; K_1[\text{let } x = \text{ref tt in } f_1 (\lambda_{\cdot}. x := \text{ff}); x := \text{tt}; \lambda_{\cdot}. !x] \rangle \downarrow^{<W.k}$ implies $\langle h'_1; K_1[f_1 (\lambda_{\cdot}. l_x := \text{ff}); l_x := \text{tt}; \lambda_{\cdot}. !l_x] \rangle \downarrow^{<W.k}$, where $h'_1 = h_1 \uplus \{l_x \mapsto \text{tt}\}$.
- Let
 - $H(\langle \rangle) := \text{HeapAtom}$
 - $\iota := (\langle \rangle, \emptyset^*, \emptyset^*, \emptyset, H)$
 - $W' := W[\Sigma_1 := W.\Sigma_1, l_x : \text{unit} \rightarrow \text{unit}][\omega := W.\omega, \iota]$
- It is easy to see that $W' \sqsupseteq^{\text{pub}} W$ and that $(h'_1, h_2) : W'$.
- We show $(W', f_1 (\lambda_{\cdot}. l_x := \text{ff}), f_2 (\lambda_{\cdot}. \langle \rangle)) \in \mathcal{E}[\text{unit}]\emptyset$:
 - Since $(W, f_1, f_2) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset$, it suffices to show $(W', \lambda_{\cdot}. l_x := \text{ff}, \lambda_{\cdot}. \langle \rangle) \in \mathcal{V}[\text{unit} \rightarrow \text{unit}]\emptyset$.
 - Since our island does not impose any constraints on l_x , this is obvious.
- It thus suffices to show $(W', K_1[\bullet; l_x := \text{tt}; \lambda_{\cdot}. !l_x], K_2[\bullet; \lambda_{\cdot}. \text{tt}]) \in \mathcal{K}[\text{unit}]\emptyset$.
- So suppose $W'' \sqsupseteq^{\text{pub}} W'$, $(h''_1, h''_2) : W''$, and $\langle h''_1; K_1[\langle \rangle; l_x := \text{tt}; \lambda_{\cdot}. !l_x] \rangle \downarrow^{<W''.k}$.
- To show: $\langle h''_2; K_2[\langle \rangle; \lambda_{\cdot}. \text{tt}] \rangle \downarrow$
- Note that $\langle h''_1; K_1[\langle \rangle; l_x := \text{tt}; \lambda_{\cdot}. !l_x] \rangle \downarrow^{<W''.k}$ implies $\langle h''_1[l_x \mapsto \text{tt}]; K_1[\lambda_{\cdot}. !l_x] \rangle \downarrow^{<W''.k}$.
- Furthermore, $\langle h''_2; K_2[\langle \rangle; \lambda_{\cdot}. \text{tt}] \rangle \downarrow$ if $\langle h''_2; K_2[\lambda_{\cdot}. \text{tt}] \rangle \downarrow$.

- Let
 - $H'(\langle \rangle) := \{(\widetilde{W}, \widetilde{h}_1, \widetilde{h}_2) \in \text{HeapAtom} \mid \widetilde{h}_1(l_x) = \text{tt}\}$
 - $\iota' := (\langle \rangle, \emptyset^*, \emptyset^*, \emptyset, H')$
 - W''' be the world obtained from W'' by replacing our previously installed island ι with ι' .
- It is easy to see that $W''' \sqsubseteq^{\text{pub}} W$ and $(h_1''[l_x \mapsto \text{tt}], h_2'') : W'''$.
- Because our island ι' enforces $l_x \leftrightarrow \text{tt}$, it is obvious that $(W''', \lambda_{-}. !l_x, \lambda_{-}. \text{tt}) \in \mathcal{V}[\text{unit} \rightarrow \text{bool}]\emptyset$.
- Instantiating $(W, K_1, K_2) \in \mathcal{K}[\text{unit}]\emptyset$ now yields the claim.