A Relational Modal Logic for Higher-Order Stateful ADTs (Technical Appendix)

Derek Dreyer
dreyer@mpi-sws.org

Georg Neis
neis@mpi-sws.org

Andreas Rossberg
rossberg@mpi-sws.org

Lars Birkedal
birkedal@itu.dk

November 3, 2009

Contents

This appendix is a supplement to the paper. Things defined in the paper are not repeated here.

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

1.1 Syntax

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

1.2 Dynamic Semantics

$\boxed{e \overset{k}{\leadsto} e'}$

$$
\begin{array}{rcll}
\mathsf{if}\,\mathsf{true}\,\mathsf{then}\, e_1\,\mathsf{else}\, e_2 & \overset{0}{\leadsto} & e_1 & \\
\mathsf{if}\,\mathsf{false}\,\mathsf{then}\, e_1\,\mathsf{else}\, e_2 & \overset{0}{\leadsto} & e_2 & \\
\mathsf{fst}\,\langle v_1, v_2\rangle & \overset{0}{\leadsto} & v_1 & \\
\mathsf{snd}\,\langle v_1, v_2\rangle & \overset{0}{\leadsto} & v_2 & \\
\mathsf{case}\,(\mathsf{inl}\, v)\,\mathsf{of}\,\mathsf{inl}\, x_1 \Rightarrow e_1 \mid \mathsf{inr}\, x_2 \Rightarrow e_2 & \overset{0}{\leadsto} & [v/x_1]e_1 & \\
\mathsf{case}\,(\mathsf{inr}\, v)\,\mathsf{of}\,\mathsf{inl}\, x_1 \Rightarrow e_1 \mid \mathsf{inr}\, x_2 \Rightarrow e_2 & \overset{0}{\leadsto} & [v/x_2]e_2 & \\
(\lambda x:\tau.\, e)\, v & \overset{0}{\leadsto} & [v/x]e & \\
(\Lambda\alpha.\, e)\,\tau & \overset{0}{\leadsto} & [\tau/\alpha]e & \\
\mathsf{unpack}\,(\mathsf{pack}\,\tau, v\,\mathsf{as}\,\exists\alpha.\,\tau_1)\,\mathsf{as}\,\alpha, x\,\mathsf{in}\, e & \overset{0}{\leadsto} & [\tau/\alpha][v/x]e & \\
\mathsf{unroll}\,(\mathsf{roll}\, v) & \overset{1}{\leadsto} & v & \\
l == l & \overset{0}{\leadsto} & \mathsf{true} & \\
l == l' & \overset{0}{\leadsto} & \mathsf{false} & \text{where } l \neq l' \\
E[e] & \overset{k}{\leadsto} & E[e'] & \text{if } e \overset{k}{\leadsto} e'
\end{array}
$$

$\boxed{e \leadsto^n e'}$

$$
\frac{}{e \leadsto^0 e} \qquad \frac{e \leadsto^n e'' \quad e'' \overset{k}{\leadsto} e'}{e \leadsto^{n+k} e'}
$$

$\boxed{(h;e) \overset{\bar{l}}{\longmapsto} (h';e')}$

$$\frac{l \notin \mathrm{dom}(h)}{(h;E[\mathsf{ref}\, v]) \overset{l}{\longmapsto} (h[l \mapsto v];E[l])} \qquad \frac{h(l) = v}{(h;E[!l]) \overset{\epsilon}{\longmapsto} (h;E[v])} \qquad \frac{l \in \mathrm{dom}(h)}{(h;E[l{:=}v]) \overset{\epsilon}{\longmapsto} (h[l \mapsto v];E[\langle\rangle])}$$

$\boxed{(h;e) \overset{\bar{l}}{\longmapsto}^{n} (h';e')}$

$$\frac{}{(h;e) \overset{\epsilon}{\longmapsto}^{0} (h;e)} \qquad \frac{(h;e) \overset{\bar{l}}{\longmapsto}^{n} (h'';e'') \quad (h'';e'') \overset{\overline{l'}}{\longmapsto} (h';e')}{(h;e) \overset{\bar{l},\overline{l'}}{\longmapsto}^{n+1} (h';e')} \qquad \frac{(h;e) \overset{\bar{l}}{\longmapsto}^{n} (h';e'') \quad e'' \rightsquigarrow^{m} e'}{(h;e) \overset{\bar{l}}{\longmapsto}^{n+m} (h';e')}$$

$\boxed{(h;e) \Downarrow^{n} (h';e')}$

$$\begin{array}{lcl}
(h;e) \Downarrow^{n} (h';e') & \overset{\mathrm{def}}{=} & \exists \bar{l}.\ (h;e) \overset{\bar{l}}{\longmapsto}^{n} (h';e') \wedge \\
& & \nexists k, h'', e'', \overline{l'}.\ e' \overset{k}{\rightsquigarrow} e'' \vee (h';e') \overset{\overline{l'}}{\longmapsto} (h'';e'') \\
(h;e) \Downarrow^{n} & \overset{\mathrm{def}}{=} & \exists h', e'.\ (h;e) \Downarrow^{n} (h';e') \\
(h;e) \Downarrow & \overset{\mathrm{def}}{=} & \exists n.\ (h;e) \Downarrow^{n}
\end{array}$$

1.3 Static Semantics

$$\begin{array}{lrcl} \textit{Variable Context} & \Gamma & ::= & \cdot \mid \Gamma, \alpha \mid \Gamma, x : \tau \\ \textit{Heap Context} & \Sigma & ::= & \cdot \mid \Sigma, l : \tau \end{array}$$

$\boxed{\vdash \Gamma}$

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

$\boxed{\vdash \Sigma}$

$$\frac{}{\vdash \cdot} \qquad \frac{\vdash \Sigma \qquad \cdot \vdash \tau}{\vdash \Sigma, l : \tau}$$

$\boxed{\Gamma \vdash \tau}$

$$\frac{\alpha \in \Gamma}{\Gamma \vdash \alpha} \qquad \frac{}{\Gamma \vdash \mathsf{unit}} \qquad \frac{}{\Gamma \vdash \mathsf{int}} \qquad \frac{}{\Gamma \vdash \mathsf{bool}} \qquad \frac{\Gamma \vdash \tau}{\Gamma \vdash \mathsf{ref}\ \tau}$$

$$\frac{\Gamma \vdash \tau_1 \qquad \Gamma \vdash \tau_2}{\Gamma \vdash \tau_1 \times \tau_2} \qquad \frac{\Gamma \vdash \tau_1 \qquad \Gamma \vdash \tau_2}{\Gamma \vdash \tau_1 + \tau_2} \qquad \frac{\Gamma \vdash \tau_1 \qquad \Gamma \vdash \tau_2}{\Gamma \vdash \tau_1 \to \tau_2} \qquad \frac{\Gamma, \alpha \vdash \tau}{\Gamma \vdash \forall \alpha.\, \tau} \qquad \frac{\Gamma, \alpha \vdash \tau}{\Gamma \vdash \exists \alpha.\, \tau} \qquad \frac{\Gamma, \alpha \vdash \tau}{\Gamma \vdash \mu \alpha.\, \tau}$$

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

$$\frac{\Gamma(x) = \tau}{\Gamma; \Sigma \vdash x : \tau} \qquad \frac{}{\Gamma; \Sigma \vdash \langle\rangle : \mathsf{unit}} \qquad \frac{}{\Gamma; \Sigma \vdash n : \mathsf{int}}$$

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

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

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

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

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

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

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

$$\frac{\Gamma; \Sigma \vdash e : [\mu \alpha.\, \tau/\alpha]\tau}{\Gamma; \Sigma \vdash \mathsf{roll}\, e : \mu \alpha.\, \tau} \qquad \frac{\Gamma; \Sigma \vdash e : \mu \alpha.\, \tau}{\Gamma; \Sigma \vdash \mathsf{unroll}\, e : [\mu \alpha.\, \tau/\alpha]\tau} \qquad \frac{\Sigma(l) = \tau}{\Gamma; \Sigma \vdash l : \mathsf{ref}\ \tau} \qquad \frac{\Gamma; \Sigma \vdash e : \tau}{\Gamma; \Sigma \vdash \mathsf{ref}\, e : \mathsf{ref}\ \tau}$$

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

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

$$\frac{\mathrm{FV}(h) = \emptyset \qquad \mathrm{FL}(h) \subseteq \mathrm{dom}(h)}{\vdash h} \qquad\qquad \frac{\forall l \in \mathrm{dom}(\Sigma).\ \cdot; \Sigma \vdash h(l) : \Sigma(l)}{\vdash h : \Sigma}$$

1.4 Contexts and Contextual Equivalence

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

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

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

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

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

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

$$\frac{\vdash C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_1) \qquad \Gamma'; \Sigma' \vdash e_2 : \tau_2}{\vdash \langle C, e_2\rangle : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_1 \times \tau_2)} \qquad \frac{\Gamma'; \Sigma' \vdash e_1 : \tau_1 \qquad \vdash C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_2)}{\vdash \langle e_1, C\rangle : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_1 \times \tau_2)}$$

$$\frac{\vdash C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_1 \times \tau_2)}{\vdash \mathsf{fst}\ C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_1)} \qquad \frac{\vdash C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_1 \times \tau_2)}{\vdash \mathsf{snd}\ C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_2)}$$

$$\frac{\vdash C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_1)}{\vdash \mathsf{inl}\ C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_1 + \tau_2)} \qquad \frac{\vdash C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_2)}{\vdash \mathsf{inr}\ C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_1 + \tau_2)}$$

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

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

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

$$\frac{\vdash C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma', x : \tau_1; \Sigma' \vdash \tau_2)}{\vdash \lambda x{:}\tau_1.\, C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_1 \to \tau_2)} \qquad \frac{\vdash C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_2 \to \tau') \qquad \Gamma'; \Sigma' \vdash e_2 : \tau_2}{\vdash C\, e_2 : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau')}$$

$$\frac{\Gamma'; \Sigma' \vdash e_1 : \tau_2 \to \tau' \qquad \vdash C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau_2)}{\vdash e_1\, C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \tau')} \qquad \frac{\vdash C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma', \alpha; \Sigma' \vdash \tau')}{\vdash \Lambda\alpha.\, C : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\Gamma'; \Sigma' \vdash \forall\alpha.\, \tau')}$$

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

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

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

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

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

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

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

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

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

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

Definition 1.1 (Contextual Equivalence)
Let $\Gamma; \Sigma \vdash e_1 : \tau$ and $\Gamma; \Sigma \vdash e_2 : \tau$.

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

2 LADR

2.1 Well-formedness

$$\begin{array}{llll} \textit{Delayed Assertions} & H', J' & ::= & e_1 \hookrightarrow_i e_2 \mid H' * J' \mid H' \vee J' \mid \exists \mathcal{X}.H' \mid \Box P' \\ \textit{Delayed Formulas} & P', Q' & ::= & e_1 = e_2 \mid e_1 \rightsquigarrow^0 e_2 \mid e_1 \rightsquigarrow^1 e_2 \mid e_1 \rightsquigarrow^* e_2 \mid \top \mid \bot \mid \\ & & & P' \wedge Q' \mid P' \vee Q' \mid P' \Rightarrow Q' \mid \forall \mathcal{X}.P' \mid \exists \mathcal{X}.P' \mid \forall \mathcal{R}.P' \mid \exists \mathcal{R}.P' \mid \\ & & & \overline{e} \in P' \mid a \mid \overline{x}.P' \mid \mathrm{Val} \mid \mathrm{Const}_{\tau_b} \mid \mathrm{Loc} \mid \mathrm{Term}_i \mid \triangleright P \end{array}$$

$\boxed{\vdash \mathcal{X} \text{ ok}}$

$$\frac{}{\vdash \cdot \text{ ok}} \qquad \frac{\vdash \mathcal{X} \text{ ok} \quad x \notin \mathcal{X}}{\vdash \mathcal{X}, x \text{ ok}} \qquad \frac{\vdash \mathcal{X} \text{ ok} \quad \alpha \notin \mathcal{X}}{\vdash \mathcal{X}, \alpha \text{ ok}}$$

$\boxed{\mathcal{X} \vdash e : \mathrm{Term}}$

$$\frac{\mathrm{FV}(e) \subseteq \mathcal{X}}{\mathcal{X} \vdash e : \mathrm{Term}}$$

$\boxed{\vdash \mathcal{R} \text{ ok}}$

$$\frac{}{\vdash \cdot \text{ ok}} \qquad \frac{\vdash \mathcal{R} \text{ ok} \quad a \notin \mathcal{R}}{\vdash \mathcal{R}, a \text{ ok}} \qquad \frac{\vdash \mathcal{R} \text{ ok} \quad p \notin \mathcal{R}}{\vdash \mathcal{R}, p \text{ ok}}$$

$\boxed{\mathcal{X}; \mathcal{R} \vdash \mathcal{L} \text{ ok}}$

$$\frac{}{\mathcal{X}; \mathcal{R} \vdash \cdot \text{ ok}}$$

$$\frac{\begin{array}{c} p \in \mathcal{R} \quad p \notin \mathrm{dom}(\mathcal{L}) \quad \mathrm{arity}(p) = \mathrm{arity}(a) \quad \vdash \mathcal{R}, a \text{ ok} \\ \mathcal{X}; \mathcal{R}, a \vdash A : \mathrm{Rel}(0) \quad \mathcal{X}; \mathcal{R}, a \vdash H : \mathrm{Asrt} \quad H \text{ delayed} \end{array}}{\mathcal{X}; \mathcal{R} \vdash \mathcal{L}, p \propto a.(A, H) \text{ ok}}$$

$\boxed{\mathcal{X}; \mathcal{R} \vdash \mathcal{P} \text{ ok}}$

$$\frac{\mathcal{X}; \mathcal{R} \vdash P_1 : \mathrm{Rel}(0) \ \cdots \ \mathcal{X}; \mathcal{R} \vdash P_n : \mathrm{Rel}(0)}{\mathcal{X}; \mathcal{R} \vdash P_1, \ldots, P_n \text{ ok}}$$

$\boxed{\vdash \mathcal{X}; \mathcal{R}; \mathcal{L}; \mathcal{P} \text{ ok}}$

$$\frac{\vdash \mathcal{X} \text{ ok} \quad \vdash \mathcal{R} \text{ ok} \quad \mathcal{X}; \mathcal{R} \vdash \mathcal{L} \text{ ok} \quad \mathcal{X}; \mathcal{R} \vdash \mathcal{P} \text{ ok}}{\vdash \mathcal{X}; \mathcal{R}; \mathcal{L}; \mathcal{P} \text{ ok}}$$

$\boxed{\mathcal{X}; \mathcal{R} \vdash P : \mathrm{Rel}(n)}$

$$\frac{\mathcal{X} \vdash e_1 : \mathrm{Term} \quad \mathcal{X} \vdash e_2 : \mathrm{Term}}{\mathcal{X}; \mathcal{R} \vdash e_1 = e_2 : \mathrm{Rel}(0)}$$

$$\frac{\mathcal{X} \vdash e_1 : \mathrm{Term} \quad \mathcal{X} \vdash e_2 : \mathrm{Term}}{\mathcal{X}; \mathcal{R} \vdash e_1 \rightsquigarrow^* e_2 : \mathrm{Rel}(0)} \qquad \frac{\mathcal{X} \vdash e_1 : \mathrm{Term} \quad \mathcal{X} \vdash e_2 : \mathrm{Term}}{\mathcal{X}; \mathcal{R} \vdash e_1 \rightsquigarrow^0 e_2 : \mathrm{Rel}(0)} \qquad \frac{\mathcal{X} \vdash e_1 : \mathrm{Term} \quad \mathcal{X} \vdash e_2 : \mathrm{Term}}{\mathcal{X}; \mathcal{R} \vdash e_1 \rightsquigarrow^1 e_2 : \mathrm{Rel}(0)}$$

$$\frac{}{\mathcal{X}; \mathcal{R} \vdash \top : \mathrm{Rel}(0)} \qquad \frac{}{\mathcal{X}; \mathcal{R} \vdash \bot : \mathrm{Rel}(0)}$$

$$\frac{\mathcal{X}; \mathcal{R} \vdash P : \mathrm{Rel}(0) \quad \mathcal{X}; \mathcal{R} \vdash Q : \mathrm{Rel}(0)}{\mathcal{X}; \mathcal{R} \vdash P \wedge Q : \mathrm{Rel}(0)} \qquad \frac{\mathcal{X}; \mathcal{R} \vdash P : \mathrm{Rel}(0) \quad \mathcal{X}; \mathcal{R} \vdash Q : \mathrm{Rel}(0)}{\mathcal{X}; \mathcal{R} \vdash P \vee Q : \mathrm{Rel}(0)}$$

$$\frac{\mathcal{X};\mathcal{R} \vdash P : \mathrm{Rel}(0) \quad \mathcal{X};\mathcal{R} \vdash Q : \mathrm{Rel}(0)}{\mathcal{X};\mathcal{R} \vdash P \Rightarrow Q : \mathrm{Rel}(0)}$$

$$\frac{\vdash \mathcal{X}, \mathcal{X}' \text{ ok} \quad \mathcal{X}, \mathcal{X}';\mathcal{R} \vdash P : \mathrm{Rel}(0)}{\mathcal{X};\mathcal{R} \vdash \forall \mathcal{X}'.P : \mathrm{Rel}(0)} \qquad \frac{\vdash \mathcal{X}, \mathcal{X}' \text{ ok} \quad \mathcal{X}, \mathcal{X}';\mathcal{R} \vdash P : \mathrm{Rel}(0)}{\mathcal{X};\mathcal{R} \vdash \exists \mathcal{X}'.P : \mathrm{Rel}(0)}$$

$$\frac{\vdash \mathcal{R}, \mathcal{R}' \text{ ok} \quad \mathcal{X};\mathcal{R}, \mathcal{R}' \vdash P : \mathrm{Rel}(0)}{\mathcal{X};\mathcal{R} \vdash \forall \mathcal{R}'.P : \mathrm{Rel}(0)} \qquad \frac{\vdash \mathcal{R}, \mathcal{R}' \text{ ok} \quad \mathcal{X};\mathcal{R}, \mathcal{R}' \vdash P : \mathrm{Rel}(0)}{\mathcal{X};\mathcal{R} \vdash \exists \mathcal{R}'.P : \mathrm{Rel}(0)}$$

$$\frac{\vdash \mathcal{R}, a \text{ ok} \quad \mathcal{X};\mathcal{R}, a \vdash A : \mathrm{Rel}(0) \quad \mathcal{X};\mathcal{R}, a \vdash H : \mathrm{Asrt} \quad H \text{ delayed}}{\mathcal{X};\mathcal{R} \vdash \propto a.(A, H) : \mathrm{Rel}(0)}$$

$$\frac{\mathcal{X};\mathcal{R} \vdash P : \mathrm{Rel}(0)}{\mathcal{X};\mathcal{R} \vdash \triangleright P : \mathrm{Rel}(0)} \qquad \frac{\mathcal{X};\mathcal{R} \vdash P : \mathrm{Rel}(0)}{\mathcal{X};\mathcal{R} \vdash \Box P : \mathrm{Rel}(0)}$$

$$\frac{\mathcal{X};\mathcal{R} \vdash R : \mathrm{Rel}(n) \quad \mathcal{X} \vdash e_1 : \mathrm{Term} \ \cdots \ \mathcal{X} \vdash e_n : \mathrm{Term}}{\mathcal{X};\mathcal{R} \vdash (e_1, \ldots, e_n) \in R : \mathrm{Rel}(0)}$$

$$\frac{a \in \mathcal{R} \quad \mathrm{arity}(a) = n}{\mathcal{X};\mathcal{R} \vdash a : \mathrm{Rel}(n)} \qquad \frac{p \in \mathcal{R} \quad \mathrm{arity}(p) = n}{\mathcal{X};\mathcal{R} \vdash p : \mathrm{Rel}(n)}$$

$$\frac{\vdash \mathcal{X}, x_1, \ldots, x_n \text{ ok} \quad \mathcal{X}, x_1, \ldots, x_n;\mathcal{R} \vdash P : \mathrm{Rel}(0)}{\mathcal{X};\mathcal{R} \vdash (x_1, \ldots, x_n).P : \mathrm{Rel}(n)}$$

$$\frac{\vdash \mathcal{R}, r \text{ ok} \quad \mathrm{arity}(r) = n \quad \mathcal{X};\mathcal{R}, r \vdash R : \mathrm{Rel}(n) \quad R \text{ contractive in } r}{\mathcal{X};\mathcal{R} \vdash \mu r.R : \mathrm{Rel}(n)}$$

$$\frac{\mathcal{X};\mathcal{R} \vdash R : \mathrm{Rel}(2)}{\mathcal{X};\mathcal{R} \vdash \uparrow R : \mathrm{Rel}(2)} \qquad \frac{}{\mathcal{X};\mathcal{R} \vdash \mathrm{Term}_i : \mathrm{Rel}(1)} \qquad \frac{}{\mathcal{X};\mathcal{R} \vdash \mathrm{Val} : \mathrm{Rel}(1)}$$

$$\frac{\mathcal{X};\mathcal{R} \vdash H : \mathrm{Asrt} \quad \mathcal{X};\mathcal{R} \vdash J : \mathrm{Asrt}}{\mathcal{X};\mathcal{R} \vdash H \Rrightarrow J : \mathrm{Rel}(0)}$$

$\boxed{\mathcal{X};\mathcal{R} \vdash H : \mathrm{Asrt}}$

$$\frac{}{\mathcal{X};\mathcal{R} \vdash e_1 \hookrightarrow_i e_2 : \mathrm{Asrt}}$$

$$\frac{\mathcal{X};\mathcal{R} \vdash H : \mathrm{Asrt} \quad \mathcal{X};\mathcal{R} \vdash J : \mathrm{Asrt}}{\mathcal{X};\mathcal{R} \vdash H * J : \mathrm{Asrt}} \qquad \frac{\mathcal{X};\mathcal{R} \vdash H : \mathrm{Asrt} \quad \mathcal{X};\mathcal{R} \vdash J : \mathrm{Asrt}}{\mathcal{X};\mathcal{R} \vdash H \vee J : \mathrm{Asrt}}$$

$$\frac{\vdash \mathcal{X}, \mathcal{X}' \text{ ok} \quad \mathcal{X}, \mathcal{X}';\mathcal{R} \vdash H : \mathrm{Asrt}}{\mathcal{X};\mathcal{R} \vdash \exists \mathcal{X}'.H : \mathrm{Asrt}} \qquad \frac{\mathcal{X};\mathcal{R} \vdash P : \mathrm{Rel}(0)}{\mathcal{X};\mathcal{R} \vdash \Box P : \mathrm{Asrt}}$$

2.2 Additional Inference Rules

$\boxed{\mathcal{C} \vdash \mathcal{J}}$

$$\frac{\mathcal{C} \vdash \bot}{\mathcal{C} \vdash \mathcal{J}} \qquad \frac{\mathcal{C} \vdash P \vee Q \quad \mathcal{C}, P \vdash \mathcal{J} \quad \mathcal{C}, Q \vdash \mathcal{J}}{\mathcal{C} \vdash \mathcal{J}} \qquad \frac{\mathcal{C} \vdash \exists \mathcal{X}.P \quad \mathcal{C}, \mathcal{X}, P \vdash \mathcal{J}}{\mathcal{C} \vdash \mathcal{J}} \qquad \frac{\mathcal{C} \vdash \exists \mathcal{R}.P \quad \mathcal{C}, \mathcal{R}, P \vdash \mathcal{J}}{\mathcal{C} \vdash \mathcal{J}}$$

$\boxed{\mathcal{C} \vdash P}$

$$\frac{}{\mathcal{C}, P \vdash P} \qquad \frac{}{\mathcal{C} \vdash \top} \qquad \frac{\mathcal{C} \vdash P \quad \mathcal{C} \vdash Q}{\mathcal{C} \vdash P \wedge Q} \qquad \frac{\mathcal{C} \vdash P \wedge Q}{\mathcal{C} \vdash P} \qquad \frac{\mathcal{C} \vdash P \wedge Q}{\mathcal{C} \vdash Q}$$

$$\frac{\mathcal{C} \vdash P}{\mathcal{C} \vdash P \vee Q} \qquad \frac{\mathcal{C} \vdash Q}{\mathcal{C} \vdash P \vee Q}$$

$$\frac{\mathcal{C}, P \vdash Q}{\mathcal{C} \vdash P \Rightarrow Q} \qquad \frac{\mathcal{C} \vdash P \Rightarrow Q \quad \mathcal{C} \vdash P}{\mathcal{C} \vdash Q}$$

$$\frac{\mathcal{C}, \mathcal{X} \vdash P}{\mathcal{C} \vdash \forall \mathcal{X}.P} \qquad \frac{\mathcal{C} \vdash \forall \mathcal{X}.P \quad \mathcal{C} \vdash \gamma : \mathcal{X}}{\mathcal{C} \vdash \gamma P} \qquad \frac{\mathcal{C}, \mathcal{R} \vdash P}{\mathcal{C} \vdash \forall \mathcal{R}.P} \qquad \frac{\mathcal{C} \vdash \forall \mathcal{R}.P \quad \mathcal{C} \vdash \varphi : \mathcal{R}}{\mathcal{C} \vdash \varphi P}$$

$$\frac{\mathcal{C} \vdash \gamma : \mathcal{X} \quad \mathcal{C} \vdash \gamma P}{\mathcal{C} \vdash \exists \mathcal{X}.P} \qquad \frac{\mathcal{C} \vdash \varphi : \mathcal{R} \quad \mathcal{C} \vdash \varphi P}{\mathcal{C} \vdash \exists \mathcal{R}.P}$$

$$\frac{}{\mathcal{C} \vdash H \Rrightarrow H} \text{ (ENTAIL-REFL)} \qquad \frac{\mathcal{C} \vdash H \Rrightarrow H' \quad \mathcal{C} \vdash H' \Rrightarrow H''}{\mathcal{C} \vdash H \Rrightarrow H''} \text{ (ENTAIL-TRANS)}$$

$$\frac{}{\mathcal{C} \vdash H_1 * H_2 \Rrightarrow H_1} \text{ (ENTAIL-WEAKEN)}$$

$$\frac{\mathcal{C} \vdash H_1 \Rrightarrow H_1' \quad \mathcal{C} \vdash H_2 \Rrightarrow H_2'}{\mathcal{C} \vdash H_1 * H_2 \Rrightarrow H_1' * H_2'} \text{ (ENTAIL-}*\text{)}$$

$$\frac{}{\mathcal{C} \vdash H_1 * H_2 \Rrightarrow H_2 * H_1} \text{ (ENTAIL-}*\text{-COMM)}$$

$$\frac{}{\mathcal{C} \vdash H_1 * (H_2 * H_3) \Rrightarrow (H_1 * H_2) * H_3} \text{ (ENTAIL-}*\text{-ASSOC-L)}$$

$$\frac{}{\mathcal{C} \vdash (H_1 * H_2) * H_3 \Rrightarrow H_1 * (H_2 * H_3)} \text{ (ENTAIL-}*\text{-ASSOC-R)}$$

$$\frac{}{\mathcal{C} \vdash H_1 \Rrightarrow H_1 \vee H_2} \text{ (ENTAIL-}\vee\text{-INTRO-L)} \qquad \frac{}{\mathcal{C} \vdash H_2 \Rrightarrow H_1 \vee H_2} \text{ (ENTAIL-}\vee\text{-INTRO-R)}$$

$$\frac{\mathcal{C} \vdash H_1 \Rrightarrow H' \quad \mathcal{C} \vdash H_2 \Rrightarrow H'}{\mathcal{C} \vdash H_1 \vee H_2 \Rrightarrow H'} \text{ (ENTAIL-}\vee\text{-ELIM)}$$

$$\frac{\mathcal{C} \vdash \gamma : \mathcal{X}}{\mathcal{C} \vdash \gamma H \Rrightarrow \exists \mathcal{X}.H} \text{ (ENTAIL-}\exists\text{-INTRO)} \qquad \frac{\mathcal{C}, \mathcal{X} \vdash H \Rrightarrow H'}{\mathcal{C} \vdash \exists \mathcal{X}.H \Rrightarrow H'} \text{ (ENTAIL-}\exists\text{-ELIM)}$$

$$\frac{}{\mathcal{C} \vdash e_1 \hookrightarrow_i e_2 * e_1' \hookrightarrow_i e_2' \Rrightarrow \square(e_1 \neq e_1')} \text{ (ENTAIL-}\hookrightarrow\text{-SEP)}$$

2.3 Model

2.3.1 Interpretation of Absolute Propositions

$\boxed{\|A\|\delta\overline{e}}$

$$
\begin{array}{rcl}
\|e_1 = e_2\|\delta & \stackrel{\text{def}}{=} & e_1 = e_2 \\
\|\top\|\delta & \stackrel{\text{def}}{=} & \top \\
\|\bot\|\delta & \stackrel{\text{def}}{=} & \bot \\
\|A \wedge B\|\delta & \stackrel{\text{def}}{=} & \|A\|\delta \wedge \|B\|\delta \\
\|A \vee B\|\delta & \stackrel{\text{def}}{=} & \|A\|\delta \vee \|B\|\delta \\
\|A \Rightarrow B\|\delta & \stackrel{\text{def}}{=} & \|A\|\delta \Rightarrow \|B\|\delta \\
\|\forall\mathcal{X}.A\|\delta & \stackrel{\text{def}}{=} & \forall\gamma \in [\![\mathcal{X}]\!] \,.\, \|\gamma A\|\delta \\
\|\exists\mathcal{X}.A\|\delta & \stackrel{\text{def}}{=} & \exists\gamma \in [\![\mathcal{X}]\!] \,.\, \|\gamma A\|\delta \\
\|\forall\mathcal{R}.A\|\delta & \stackrel{\text{def}}{=} & \forall\delta' \in [\![\mathcal{R}]\!] \,.\, \|A\|(\delta,\delta') \\
\|\exists\mathcal{R}.A\|\delta & \stackrel{\text{def}}{=} & \exists\delta' \in [\![\mathcal{R}]\!] \,.\, \|A\|(\delta,\delta') \\
\|\overline{e} \in A\|\delta & \stackrel{\text{def}}{=} & \|A\|\delta\overline{e} \\
\|a\|\delta\overline{e} & \stackrel{\text{def}}{=} & \delta(a)\overline{e} \\
\|\overline{x}.A\|\delta\overline{e} & \stackrel{\text{def}}{=} & \|A[\overline{e}/\overline{x}]\|\delta \\
\|\mathrm{Val}\|\delta e & \stackrel{\text{def}}{=} & e \text{ value} \\
\|\mathrm{Loc}\|\delta e & \stackrel{\text{def}}{=} & e \in \mathrm{Loc}
\end{array}
$$

2.3.2 Properties

Lemma 2.1
$W = \triangleright\triangleleft W$

Proof: Follows easily from the definitions. □

Lemma 2.2

1. $\triangleright W \supseteq W$
2. If $W' \supseteq W$, then $W' \sqsupseteq W$.
3. If $W' \supseteq W$, then $\triangleright W' \supseteq \triangleright W$.
4. If $W' \sqsupseteq W$, then $\triangleright W' \sqsupseteq \triangleright W$.
5. If $W'' \supseteq W'$ and $W' \supseteq W$, then $W'' \supseteq W$.
6. If $W'' \sqsupseteq W'$ and $W' \sqsupseteq W$, then $W'' \sqsupseteq W$.

Proof: Follows easily from the definitions. □

Lemma 2.3

1. If $W' \supseteq \triangleright W$, then there is $\widehat{W'} \supseteq W$ such that $\triangleright\widehat{W'} = W'$.
2. If $W' \sqsupseteq \triangleright W$, then there is $\widehat{W'} \sqsupseteq W$ such that $\triangleright\widehat{W'} = W'$.

Proof: In each case define $\widehat{W'} := (W'.k+1, W'.d, W'.\varsigma_1, W'.\varsigma_2, \mathcal{I})$, where

$$\begin{array}{ll} \mathrm{dom}(\mathcal{I}) = \mathrm{dom}(W'.\mathcal{I}) & \\ \quad \mathcal{I}(\iota) = W'.\mathcal{I}(\iota) & \text{if } \iota \notin \mathrm{dom}(W.\mathcal{I}) \\ \quad \mathcal{I}(\iota) = (W'.\mathcal{I}(\iota).CP, W'.\mathcal{I}(\iota).PL, \lfloor W.\mathcal{I}(\iota).HL \rfloor_{W'.k+1}) & \text{otherwise} \end{array}$$

□

Corollary 2.4
If $W' \sqsupseteq W$, then there is $\overleftarrow{W'} \sqsupseteq \triangleleft W$ such that $\triangleright\overleftarrow{W'} = W'$.

Proof: Since $W = \triangleright\triangleleft W$ by Lemma 2.1, the claim follows by Lemma 2.3. □

Lemma 2.5

1. If $W' \supseteq \triangleleft\triangleright W$, then there is $\widetilde{W'} \supseteq W$ such that $\triangleleft\triangleright\widetilde{W'} = W'$.
2. If $W' \sqsupseteq \triangleleft\triangleright W$, then there is $\widetilde{W'} \sqsupseteq W$ such that $\triangleleft\triangleright\widetilde{W'} = W'$.

Proof: In each case define $\widetilde{W'} := (W'.k, W'.d, W'.\varsigma_1, W'.\varsigma_2, \mathcal{I})$, where

$$\begin{array}{ll} \mathrm{dom}(\mathcal{I}) = \mathrm{dom}(W'.\mathcal{I}) & \\ \quad \mathcal{I}(\iota) = W'.\mathcal{I}(\iota) & \text{if } \iota \notin \mathrm{dom}(W.\mathcal{I}) \\ \quad \mathcal{I}(\iota) = (W'.\mathcal{I}(\iota).CP, W'.\mathcal{I}(\iota).PL, \lfloor W.\mathcal{I}(\iota).HL \rfloor_{W'.k}) & \text{otherwise} \end{array}$$

□

Lemma 2.6

1. If $W_1' \supseteq W_1$ and $\triangleright W_1 = \triangleright W_2$, then there is $W_2' \supseteq W_2$ such that $\triangleright W_1' = \triangleright W_2'$.
2. If $W_1' \sqsupseteq W_1$ and $\triangleright W_1 = \triangleright W_2$, then there is $W_2' \sqsupseteq W_2$ such that $\triangleright W_1' = \triangleright W_2'$.

Proof: In each case define $W_2' := (W_1'.k, W_1'.d, W_1'.\varsigma_1, W_1'.\varsigma_2, \mathcal{I})$, where

$$\begin{array}{ll} \mathrm{dom}(\mathcal{I}) = \mathrm{dom}(W_1'.\mathcal{I}) & \\ \quad \mathcal{I}(\iota) = W_1'.\mathcal{I}(\iota) & \text{if } \iota \notin \mathrm{dom}(W_2.\mathcal{I}) \\ \quad \mathcal{I}(\iota) = (W_1'.\mathcal{I}(\iota).CP, W_1'.\mathcal{I}(\iota).PL, \lfloor W_2.\mathcal{I}(\iota).HL \rfloor_{W_1'.k}) & \text{otherwise} \end{array}$$

□

Lemma 2.7

1. If P is delayed and $\triangleright W_1 = \triangleright W_2$, then $[\![P]\!]\delta W_1 = [\![P]\!]\delta W_2$.
2. If H is delayed and $\triangleright W_1 = \triangleright W_2$, then $[\![H]\!]\delta W_1 = [\![H]\!]\delta W_2$.

Proof: Each by primary induction on $W.k$ and secondary induction on the "size" of the formula. By symmetry it suffices to show only one direction. The interesting cases are:

1. • Case $P = P_1 \Rightarrow P_2$ where P_1, P_2 are delayed:
   – Suppose $[\![P_1 \Rightarrow P_2]\!]\delta W_1$, $W_2' \supseteq W_2$, and $[\![P_1]\!]\delta W_2'$.
   – To show: $[\![P_2]\!]\delta W_2'$

- If $W_2'.k = 0$, there is nothing to show, so assume $W_2'.k > 0$.
- By Lemma 2.6 there is $W_1' \sqsupseteq W_1$ with $\triangleright W_1' = \triangleright W_2'$.
- Hence instantiating $[\![P_1 \Rightarrow P_2]\!]\delta W_1$ yields $[\![P_2]\!]\delta W_1'$ if we can show $[\![P_1]\!]\delta W_1'$.
- By induction, the former is equivalent to $[\![P_2]\!]\delta W_2'$ and the latter to $[\![P_1]\!]\delta W_2'$.

- Case $P = \triangleright P'$:
  - Suppose $[\![\triangleright P']\!]\delta W_1$, *i.e.,* $[\![P']\!]\delta(\triangleright W_1)$.
  - To show: $[\![\triangleright P']\!]\delta W_2$, *i.e.,* $[\![P']\!]\delta(\triangleright W_2)$
  - Since $\triangleright\triangleright W_1 = \triangleright\triangleright W_2$, we are done by induction.
- Case $P = \mathrm{Term}_i$:
  - Suppose $[\![\mathrm{Term}_i]\!]\delta W_1 e$, *i.e.,* $\mathrm{FL}(e) \subseteq W_1.\varsigma_i$.
  - To show: $[\![\mathrm{Term}_i]\!]\delta W_2 e$, *i.e.,* $\mathrm{FL}(e) \subseteq W_2.\varsigma_i$
  - Since $\triangleright W_1 = \triangleright W_2$, we know $W_1.\varsigma_i = W_2.\varsigma_i$.

2. - Case $H = e_1 \hookrightarrow_i e_2$: analogously to previous case
   - Case $H = \Box P$ where P is delayed:
     - Suppose $[\![\Box P]\!]\delta W_1$ and $W_2' \sqsupseteq W_2$.
     - To show: $[\![P]\!]\delta W_2'$
     - If $W_2'.k = 0$, there is nothing to show, so assume $W_2'.k > 0$.
     - By Lemma 2.6 there is $W_1' \sqsupseteq W_1$ with $\triangleright W_1' = \triangleright W_2'$.
     - Hence instantiating $[\![\Box P]\!]\delta W_1$ yields $[\![P]\!]\delta W_1'$.
     - By induction, this is equivalent to $[\![P]\!]\delta W_2'$.

□

Corollary 2.8

1. If P is delayed, then $[\![P]\!]\delta W = [\![P]\!]\delta(\triangleleft\triangleright W)$.
2. If H is delayed, then $[\![H]\!]\delta W = [\![H]\!]\delta(\triangleleft\triangleright W)$.

Proof: Since $\triangleright W = \triangleright\triangleleft\triangleright W$ by Lemma 2.1, the claim follows by Lemma 2.7. □

Lemma 2.9
If $[\![\mathcal{P}]\!]\delta W$ and $W' \sqsupseteq W$, then $[\![\dagger\mathcal{P}]\!]\delta W'$.

Proof: Follows easily from the definitions and Lemma 2.2. □

Lemma 2.10
If $W' \sqsupseteq W$, then $[\![H]\!]\delta W' \supseteq [\![H]\!]\delta W$.

Proof: By induction on the structure of H. If $W.k = 0$, then $W'.k = 0$ and so there is nothing to show. Otherwise the only interesting cases are:

- Case $H = e_1 \hookrightarrow_i e_2$:

$$\begin{aligned}
&[\![e_1 \hookrightarrow_i e_2]\!]\delta W(h_1, h_2) \\
\iff &\mathrm{FL}(e_1), \mathrm{FL}(e_2) \subseteq W.\varsigma_i \ \wedge\ e_1, e_2 \in \mathrm{Val} \ \wedge\ h_i(e_1) = e_2 \\
\implies &\mathrm{FL}(e_1), \mathrm{FL}(e_2) \subseteq W'.\varsigma_i \ \wedge\ e_1, e_2 \in \mathrm{Val} \ \wedge\ h_i(e_1) = e_2 \\
\iff &[\![e_1 \hookrightarrow_i e_2]\!]\delta W'(h_1, h_2)
\end{aligned}$$

- Case $H = \Box P$:

$$\begin{aligned}
& [\![\Box P]\!]\delta W(h_1, h_2) \\
\Longrightarrow\ & [\![\Box P]\!]\delta W \\
\Longrightarrow\ & \forall W'' \sqsupseteq W.\ [\![P]\!]\delta W'' \\
\Longrightarrow\ & \forall W'' \sqsupseteq W'.\ [\![P]\!]\delta W'' && \text{by Lemma 2.2} \\
\Longrightarrow\ & [\![\Box P]\!]\delta W' \\
\Longrightarrow\ & [\![\Box P]\!]\delta W'(h_1, h_2)
\end{aligned}$$

□

Lemma 2.11
If $W' \vdash (h_1; e_1) \approx (h_2; e_2) : \Psi$, $W' \sqsupseteq W$ and $W'.k = W.k$ as well as $W'.\varsigma_1 = W.\varsigma_1$ and $W'.\varsigma_2 = W.\varsigma_2$, then $W \vdash (h_1; e_1) \approx (h_2; e_2) : \Psi$.

Proof: Easy to verify using Lemma 2.2. □

Lemma 2.12
If $W.k > 0$, then $[\![A]\!]\delta W = \|A\|\delta$.

Proof: Easy induction. □

Lemma 2.13 (Substitution)

1. $[\![\mathcal{L}]\!](\delta, a{\mapsto}\|A\|\delta)W = [\![\mathcal{L}[A/a]]\!]\delta W$
2. $[\![P]\!](\delta, a{\mapsto}\|A\|\delta)W = [\![P[A/a]]\!]\delta W$
3. $[\![H]\!](\delta, a{\mapsto}\|A\|\delta)W = [\![H[A/a]]\!]\delta W$
4. $\|B\|(\delta, a{\mapsto}\|A\|\delta) = \|B[A/a]\|\delta$

Proof: By mutual induction, a primary one on $W.k$ and a secondary one on the "size" of the formula, where (2) uses (1) and (3) uses (2). □

Lemma 2.14

1. If $h_1, h_2 :_\omega W$, $W' \sqsupseteq W$, and $W'.I|_\omega = \lfloor W.\mathcal{I}|_\omega \rfloor_{W'.k}$, then $h_1, h_2 :_\omega W'$.
2. If $h_1, h_2 : W$, then $h_1, h_2 : \triangleright W$.

Proof:

1. If $W'.k = 0$, this holds vacuously. So suppose $W'.k > 0$ and thus $W.k > 0$. By assumption we know that there are $h_1^1, \ldots, h_1^n, h_2^1, \ldots, h_2^n$ with

$$h_1 = h_1^1 \uplus \cdots \uplus h_1^n \text{ and } h_2 = h_2^1 \uplus \cdots \uplus h_2^n$$

such that

$$\forall i \in \{1, \ldots, n\}.\ (\triangleright W, h_1^i, h_2^i) \in W.\mathcal{I}(\iota_i).HL(W.\mathcal{I}(\iota_i).CP)$$

where

$$S = \iota_1, \ldots, \iota_n.$$

It suffices to show:

$$\forall i \in \{1, \ldots, n\}.\ (\triangleright W', h_1^i, h_2^i) \in W'.\mathcal{I}(\iota_i).HL(W'.\mathcal{I}(\iota_i).CP)$$

- Suppose $i \in \{1, \ldots, n\}$.
- Hence $(\triangleright W, h_1^i, h_2^i) \in W.\mathcal{I}(\iota_i).HL(W.\mathcal{I}(\iota_i).CP)$.
- By Lemma 2.2 and definition of *HeapRel*, $(\triangleright W', h_1^i, h_2^i) \in W.\mathcal{I}(\iota_i).HL(W.\mathcal{I}(\iota_i).CP)$.
- Hence $(\triangleright W', h_1^i, h_2^i) \in \lfloor W.\mathcal{I}(\iota_i) \rfloor_{W'.k}.HL(W.\mathcal{I}(\iota_i).CP)$.
- Consequently, $(\triangleright W', h_1^i, h_2^i) \in W'.\mathcal{I}(\iota_i).HL(W'.\mathcal{I}(\iota_i).CP)$.

2. Follows easily from part (1) and the definitions.

□

Lemma 2.15
If $[\![\mathcal{L}]\!]\delta W\omega$ and $W' \sqsupseteq W$, then $[\![\mathcal{L}]\!]\delta W'\omega$.

Proof: By induction on the structure of $\mathcal{L}$. Easy to verify using Lemma 2.2. □

Lemma 2.16
If $[\![H]\!]\delta W(h_1, h_2)$ and $h_1' \supseteq h_1$ and $h_2' \supseteq h_2$, then $[\![H]\!]\delta W(h_1', h_2')$.

Proof: By induction on the structure of H. If $W.k = 0$, there is nothing to show. Otherwise the interesting cases are:

- Case $H = e_1 \hookrightarrow_i e_2$:
  - We know $h_i(e_1) = e_2$ and need to show $h_i'(e_1) = e_2$.
  - This follows from $h_i' \supseteq h_i$.
- Case $H = H_1 * H_2$:
  - We know there are h_1^1, h_1^2 with $h_1 = h_1^1 \uplus h_1^2$ and h_2^1, h_2^2 with $h_2 = h_2^1 \uplus h_2^2$ such that $[\![H_1]\!]\delta W(h_1^1, h_2^1)$ and $[\![H_2]\!]\delta W(h_2^1, h_2^2)$.
  - Let $h_i^3 = h_i'|_{\mathrm{dom}(h_i') \setminus \mathrm{dom}(h_i)}$.
  - Then $[\![H_2]\!]\delta W(h_1^2 \uplus h_1^3, h_2^2 \uplus h_2^3)$ by induction.
  - Furthermore, $h_i^1 \uplus h_i^2 \uplus h_i^3 = h_i'$.
- Case $H = \Box P$:

$$\begin{aligned} & [\![\Box P]\!]\delta W(h_1, h_2) \\ \iff & [\![\Box P]\!]\delta W \\ \iff & [\![\Box P]\!]\delta W(h_1', h_2') \end{aligned}$$

□

Lemma 2.17 (Monotonicity of $[\![P]\!]$ wrt. $\supseteq$)
If $[\![P]\!]\delta W\overline{e}$ and $W' \supseteq W$, then $[\![P]\!]\delta W'\overline{e}$.

Proof: By primary induction on $W.k$ and secondary induction on the "size" of P. If $W'.k = 0$, then there is nothing to show. Otherwise the interesting cases are:

- Case $P = P_1 \Rightarrow P_2$:
  - Suppose $W'' \supseteq W'$ and $[\![P_1]\!]\delta W''$.
  - Using Lemma 2.2, we can instantiate the assumption and get $[\![P_2]\!]\delta W''$. (If $W''.k = 0$, this holds trivially.)
- Case $P = \propto a.(B, H)$:
  - We know $[\![p \propto a.(B, H)]\!](\delta, p{\mapsto}\mathrm{pop}(\iota))W\{\iota\}$, for some ι and some $p \notin \mathrm{dom}(\delta)$.
  - By Lemma 2.2 we know $W' \sqsupseteq W$ and thus Lemma 2.15 yields $[\![p \propto a.(B, H)]\!](\delta, p{\mapsto}\mathrm{pop}(\iota))W'\{\iota\}$.
  - Hence $[\![\propto a.(B, H)]\!]\delta W'$.
- Case $P = \Box P'$:
  - Suppose $W'' \supseteq W'$.
  - By Lemma 2.2, $W'' \supseteq W$.
  - Instantiating the assumption yields $[\![P']\!]\delta W''$. (If $W''.k = 0$, this holds trivially.)
- Case $P = \triangleright P'$:
  - We know $[\![P']\!]\delta(\triangleright W)$.
  - By Lemma 2.2, $\triangleright W' \supseteq \triangleright W$.
  - Hence $[\![P']\!]\delta(\triangleright W')$ by induction, and thus $[\![\triangleright P']\!]\delta W'$.
- Case $P = r$:
  - We know $\delta(r)W\overline{e}$.
  - $\delta(r)W'\overline{e}$ then follows from $\delta(r) \in \mathit{SemRel}^{\mathrm{arity}(r)}$.
- Case $P = \uparrow R$:
  - Suppose $W'' \supseteq W'$ and $h_1, h_2 : W''$.
  - By Lemma 2.2, $W'' \supseteq W$.
  - Instantiating the assumption yields $W'' \vdash (h_1; e_1) \approx (h_2; e_2) : [\![R]\!]\delta$.
- Case $P = \mathrm{Term}_i$:
  - We know $\mathrm{FL}(e) \subseteq W.\varsigma_i$.
  - By assumption, $W.\varsigma_i \subseteq W'.\varsigma_i$.
  - Hence $\mathrm{FL}(e) \subseteq W'.\varsigma_i$ and thus $[\![\mathrm{Term}_i]\!]\delta W'(e)$.
- Case $P = H \Rrightarrow J$:
  - Suppose $W'' \supseteq W'$ and $[\![H]\!]\delta W''(h_1, h_2)$.

– TS: $[\![J]\!]\delta W''(h_1, h_2)$

– Since $W'' \supseteq W$ by Lemma 2.2, this follows by instantiating the assumption.

□

Lemma 2.18
If $[\![\mathcal{P}]\!]\delta W$, then $[\![\triangleleft \mathcal{P}]\!]\delta(\triangleright W)$.

Proof: Consider a single proposition P and assume $[\![P]\!]\delta W$. If P is of the form $\triangleright P'$, we need to show $[\![P']\!]\delta(\triangleright W)$, which is equivalent to the assumption. Otherwise, we need to show $[\![P]\!]\delta(\triangleright W)$, which follows from the assumption by Lemmas 2.2 and 2.17. □

2.4 Soundness of the Inference Rules

Theorem 2.19
The following rule is sound:

$$\frac{\mathcal{C} \vdash e_1 = e_2 \quad \mathcal{C} \vdash \mathcal{J}[e_1/x]}{\mathcal{C} \vdash \mathcal{J}[e_2/x]} \text{ REPLACE}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- If $W.k = 0$, there is nothing to show.
- Otherwise the first premise yields $\gamma e_1 = \gamma e_2$ and thus the claim follows from instantiating the second premise.

□

Theorem 2.20
The following rule is sound:

$$\frac{\mathcal{C} \vdash \mathcal{J}}{\mathcal{C}, \mathcal{X}, \mathcal{R}, \mathcal{P} \vdash \mathcal{J}} \text{ WEAKEN}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}, \mathcal{X}, \mathcal{R}, \mathcal{P}]\!]$.
- Let $\gamma' := \gamma|_{\mathcal{C}.\mathcal{X}}$ and $\delta' := \delta|_{\mathcal{C}.\mathcal{R}}$.
- It is easy to see that then $(\gamma', \delta', W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- Thus the claim follows from instantiating the premise.

□

Theorem 2.21
The following rule is sound:

$$\frac{\mathcal{C} \vdash P \quad \mathcal{C}, P \vdash \mathcal{J}}{\mathcal{C} \vdash \mathcal{J}} \text{ CUT}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- Instantiating the first premise yields $[\![\gamma P]\!]\delta W$.
- Consequently, $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}, P]\!]$ and thus the claim follows from instantiating the second premise.

□

Theorem 2.22
The following rule is sound:

$$\frac{\mathcal{C} \vdash P}{\mathcal{C}, \mathcal{L} \vdash P}\ \mathcal{L}\text{-WEAKEN}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}, \mathcal{L}]\!]$.
- To show: $[\![\gamma P]\!]\delta W$
- If $W.k = 0$, there is nothing to show, so assume $W.k > 0$.
- Say $\mathcal{L} = p_1 \propto a.(B_1, H_1), \ldots, p_n \propto a.(B_n, H_n)$.
- From $[\![\gamma(\mathcal{C}.\mathcal{L}), \gamma\mathcal{L}]\!]\delta W\omega_1$ we know that there are $\iota_1, \ldots, \iota_n$ such that
  1. $[\![\gamma(\mathcal{C}.\mathcal{L})]\!]\delta W\omega_1'$ and
  2. $[\![\gamma\mathcal{L}]\!]\delta W\{\iota_1, \ldots, \iota_n\}$

  where $\omega_1' := \omega_1 \setminus \{\iota_1, \ldots, \iota_n\}$.
- It is easy to see that then $(\gamma, \delta, W, \omega_1', \omega_2 \uplus \{\iota_1, \ldots, \iota_n\}) \in [\![\mathcal{C}]\!]$.
- Now instantiate the premise to get $[\![\gamma P]\!]\delta W$.

□

Theorem 2.23
The following rule is sound:

$$\frac{\mathcal{C} \vdash P}{\mathcal{C} \vdash \triangleright P}\ \triangleright\text{-MONO}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\triangleright\gamma P]\!]\delta W$
- If $W.k = 0$, there is nothing to show.
- Otherwise we need to show $[\![\gamma P]\!]\delta(\triangleright W)$.
- Instantiating the assumption yields $[\![\gamma P]\!]\delta W$.
- The goal then follows from Lemmas 2.2 and 2.17.

□

Theorem 2.24
The following rule is sound:

$$\frac{\triangleleft\mathcal{C} \vdash P}{\mathcal{C} \vdash \triangleright P}\ \triangleright\text{-WEAKEN}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\triangleright\gamma P]\!]\delta W$
- If $W.k = 0$, there is nothing to show.
- Otherwise we need to show $[\![\gamma P]\!]\delta(\triangleright W)$.
- We show $(\gamma, \delta, \triangleright W, \omega_1, \omega_2) \in [\![\triangleleft\mathcal{C}]\!]$:
  - We need to show $[\![\gamma(\mathcal{C}.\mathcal{L})]\!]\delta(\triangleright W)\omega_1$ and $[\![\triangleleft\gamma(\mathcal{C}.\mathcal{P})]\!]\delta(\triangleright W)$.
  - The former follows from $[\![\gamma(\mathcal{C}.\mathcal{L})]\!]\delta W\omega_1$, Lemma 2.2, and Lemma 2.15.
  - The latter follows from $[\![\gamma(\mathcal{C}.\mathcal{P})]\!]\delta W$ and Lemma 2.18.
- Now instantiate the premise to get $[\![\gamma P]\!]\delta(\triangleright W)$.

□

Theorem 2.25
The following rule is sound:

$$\frac{\mathcal{C}, \triangleright P \vdash P}{\mathcal{C} \vdash P}\ \text{LÖB}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- We show $[\![\gamma P]\!]\delta W$ by induction on $W.k$.
- Case $W.k = 0$: trivial
- Case $W.k > 0$:
  - By induction we know $[\![\gamma P]\!]\delta(\triangleright W)$.
  - Hence it is easy to see that $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}, \triangleright P]\!]$.
  - Instantiating the premise then yields the goal.

□

Theorem 2.26
The following rule is sound:

$$\frac{\mathcal{C} \vdash \triangleright(P \Rightarrow Q)}{\mathcal{C} \vdash \triangleright P \Rightarrow \triangleright Q}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W' \sqsupseteq W$ and $[\![\triangleright\gamma P]\!]\delta W'$.
- To show: $[\![\triangleright\gamma Q]\!]\delta W'$

- If $W'.k = 0$, there is nothing to show.
- Otherwise we need to show $[\![\gamma Q]\!]\delta(\triangleright W')$.
- If $(\triangleright W').k = 0$, there is nothing to show, so assume $W'.k > 1$ and thus $W.k > 1$.
- We know $[\![\gamma P]\!]\delta(\triangleright W')$.
- Instantiating the premise yields $[\![\triangleright(\gamma P \Rightarrow \gamma Q)]\!]\delta W$, *i.e.,* $[\![\gamma P \Rightarrow \gamma Q]\!]\delta(\triangleright W)$.
- By Lemma 2.2, $\triangleright W' \supseteq \triangleright W$.
- Hence we get $[\![\gamma Q]\!]\delta(\triangleright W')$.

□

Theorem 2.27
The following rule is sound:

$$\frac{\mathcal{C} \vdash \triangleright P \Rightarrow \triangleright Q}{\mathcal{C} \vdash \triangleright(P \Rightarrow Q)}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\triangleright(\gamma P \Rightarrow \gamma Q)]\!]\delta W$
- If $W.k = 0$, there is nothing to show.
- Otherwise we need to show $[\![\gamma P \Rightarrow \gamma Q]\!]\delta(\triangleright W)$.
- If $(\triangleright W).k = 0$, there is nothing to show, so assume $W.k > 1$.
- Now suppose $W' \supseteq \triangleright W$ and $[\![\gamma P]\!]\delta W'$.
- To show: $[\![\gamma Q]\!]\delta W'$
- If $W'.k = 0$, there is nothing to show, so assume $W'.k > 0$.
- Instantiating the premise yields $[\![\triangleright\gamma P \Rightarrow \triangleright\gamma Q]\!]\delta W$.
- By Lemma 2.3 there is $\widehat{W'} \supseteq W$ with $\triangleright\widehat{W'} = W'$.
- Hence we get $[\![\triangleright\gamma Q]\!]\delta\widehat{W'}$ if we can show $[\![\triangleright\gamma P]\!]\delta\widehat{W'}$.
- Note that the former is equivalent to $[\![\gamma Q]\!]\delta W'$ (which is what we want to show) and the latter to $[\![\gamma P]\!]\delta W'$ (which we assumed to hold).

□

Theorem 2.28
The following rule is sound:

$$\frac{\mathcal{C} \vdash \triangleright(P \wedge Q)}{\mathcal{C} \vdash \triangleright P \wedge \triangleright Q}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\triangleright\gamma P \wedge \triangleright\gamma Q]\!]\delta W$
- If $W.k = 0$, there is nothing to show, so assume $W.k > 0$.
- Instantiating the premise yields $[\![\triangleright(\gamma P \wedge \gamma Q)]\!]\delta W$, *i.e.,* $[\![\gamma P \wedge \gamma Q]\!]\delta(\triangleright W)$.
- Consequently, $[\![\gamma P]\!]\delta(\triangleright W)$ and $[\![\gamma Q]\!]\delta(\triangleright W)$. (If $(\triangleright W).k = 0$, this holds trivially.)
- Hence $[\![\triangleright\gamma P]\!]\delta W$ and $[\![\triangleright\gamma Q]\!]\delta W$ and thus $[\![\triangleright\gamma P \wedge \triangleright\gamma Q]\!]\delta W$.

□

Theorem 2.29
The following rule is sound:

$$\frac{\mathcal{C} \vdash \triangleright P \wedge \triangleright Q}{\mathcal{C} \vdash \triangleright(P \wedge Q)}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\triangleright(\gamma P \wedge \gamma Q)]\!]\delta W$
- If $W.k = 0$, there is nothing to show, so assume $W.k > 0$.
- Instantiating the premise yields $[\![\triangleright\gamma P \wedge \triangleright\gamma Q]\!]\delta W$, *i.e.,* $[\![\triangleright\gamma P]\!]\delta W$ and $[\![\triangleright\gamma Q]\!]\delta W$.
- Consequently, $[\![\gamma P]\!]\delta(\triangleright W)$ and $[\![\gamma Q]\!]\delta(\triangleright W)$.
- Hence $[\![\gamma P \wedge \gamma Q]\!]\delta(\triangleright W)$ and thus $[\![\triangleright(\gamma P \wedge \gamma Q)]\!]\delta W$.

□

Theorem 2.30
The following rule is sound:

$$\frac{\mathcal{C} \vdash \triangleright(P \vee Q)}{\mathcal{C} \vdash \triangleright P \vee \triangleright Q}$$

Proof: As for conjunction. □

Theorem 2.31
The following rule is sound:

$$\frac{\mathcal{C} \vdash \triangleright P \vee \triangleright Q}{\mathcal{C} \vdash \triangleright(P \vee Q)}$$

Proof: As for conjunction. □

Theorem 2.32
The following rule is sound:

$$\frac{\mathcal{C} \vdash \triangleright \forall \mathcal{X}.P}{\mathcal{C} \vdash \forall \mathcal{X}.\triangleright P}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\forall \mathcal{X}.\triangleright \gamma P]\!]\delta W$
- If $W.k = 0$, there is nothing to show.
- So assume $W.k > 0$ and suppose $\gamma' \in [\![\mathcal{X}]\!]$.
- To show: $[\![\triangleright(\gamma, \gamma')P]\!]\delta W$
- Instantiating the premise yields $[\![\triangleright \forall \mathcal{X}.\gamma P]\!]\delta W$, *i.e.,* $[\![\forall \mathcal{X}.\gamma P]\!]\delta(\triangleright W)$.
- Instantiating this yields $[\![(\gamma, \gamma')P]\!]\delta(\triangleright W)$, *i.e.,* $[\![\triangleright(\gamma, \gamma')P]\!]\delta W$.

□

Theorem 2.33
The following rule is sound:

$$\frac{\mathcal{C} \vdash \forall \mathcal{X}.\triangleright P}{\mathcal{C} \vdash \triangleright \forall \mathcal{X}.P}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\triangleright \forall \mathcal{X}.\gamma P]\!]\delta W$
- If $W.k = 0$, there is nothing to show.
- Otherwise we need to show $[\![\forall \mathcal{X}.\gamma P]\!]\delta(\triangleright W)$.
- So suppose $\gamma' \in [\![\mathcal{X}]\!]$.
- To show: $[\![(\gamma, \gamma')P]\!]\delta(\triangleright W)$
- Instantiating the premise yields $[\![\triangleright(\gamma, \gamma')P]\!]\delta W$, *i.e.,* $[\![(\gamma, \gamma')P]\!]\delta(\triangleright W)$.

□

Theorem 2.34
The following rule is sound:

$$\frac{\mathcal{C} \vdash \triangleright \forall \mathcal{R}.P}{\mathcal{C} \vdash \forall \mathcal{R}.\triangleright P}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.

- To show: $[\![\forall\mathcal{R}.\triangleright\gamma P]\!]\delta W$
- If $W.k = 0$, there is nothing to show.
- So assume $W.k > 0$ and suppose $\delta' \in [\![\mathcal{R}]\!]$.
- To show: $[\![\triangleright\gamma P]\!](\delta,\delta')W$, *i.e.,* $[\![\gamma P]\!](\delta,\delta')(\triangleright W)$.
- Instantiating the premise yields $[\![\triangleright\forall\mathcal{R}.\gamma P]\!]\delta W$, *i.e.,* $[\![\forall\mathcal{R}.\gamma P]\!]\delta(\triangleright W)$.
- Again, if $(\triangleright W).k = 0$, there is nothing to show.
- Otherwise, instantiating $[\![\forall\mathcal{R}.\gamma P]\!]\delta(\triangleright W)$ yields $[\![\gamma P]\!](\delta,\delta')(\triangleright W)$.

□

Theorem 2.35
The following rule is sound:

$$\frac{\mathcal{C} \vdash \forall\mathcal{R}.\triangleright P}{\mathcal{C} \vdash \triangleright\forall\mathcal{R}.P}$$

Proof:

- Suppose $(\gamma,\delta,W,\omega_1,\omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\triangleright\forall\mathcal{R}.\gamma P]\!]\delta W$
- If $W.k = 0$, there is nothing to show.
- Otherwise we need to show $[\![\forall\mathcal{R}.\gamma P]\!]\delta(\triangleright W)$.
- If $(\triangleright W).k = 0$, there is nothing to show.
- Otherwise suppose $\delta' \in [\![\mathcal{R}]\!]$.
- To show: $[\![\gamma P]\!](\delta,\delta')(\triangleright W)$
- Instantiating the premise yields $[\![\triangleright\gamma P]\!](\delta,\delta')W$, *i.e.,* $[\![\gamma P]\!](\delta,\delta')(\triangleright W)$.

□

Theorem 2.36
The following rule is sound:

$$\frac{\mathcal{C} \vdash \triangleright\exists\mathcal{X}.P}{\mathcal{C} \vdash \exists\mathcal{X}.\triangleright P}$$

Proof: As for universal quantification. □

Theorem 2.37
The following rule is sound:

$$\frac{\mathcal{C} \vdash \exists\mathcal{X}.\triangleright P}{\mathcal{C} \vdash \triangleright\exists\mathcal{X}.P}$$

Proof: As for universal quantification. □

Theorem 2.38
The following rule is sound:

$$\frac{\mathcal{C} \vdash \triangleright \exists \mathcal{R}.P}{\mathcal{C} \vdash \exists \mathcal{R}.\triangleright P}$$

Proof: As for universal quantification. □

Theorem 2.39
The following rule is sound:

$$\frac{\mathcal{C} \vdash \exists \mathcal{R}.\triangleright P}{\mathcal{C} \vdash \triangleright \exists \mathcal{R}.P}$$

Proof: As for universal quantification. □

Theorem 2.40
The following rule is sound:

$$\frac{\dagger\mathcal{C} \vdash P}{\mathcal{C} \vdash \Box P}\ \Box\text{-INTRO}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\Box\gamma P]\!]\delta W$.
- If $W.k = 0$, there is nothing to show.
- Otherwise suppose $W' \sqsupseteq W$.
- To show: $[\![\gamma P]\!]\delta W'$
- We show $(\gamma, \delta, W', \omega_1, \mathrm{dom}(W'.\mathcal{I}) \setminus \omega_1) \in [\![\dagger\mathcal{C}]\!]$:
  - We need to show $[\![\gamma\mathcal{C}.\mathcal{L}]\!]\delta W'\omega_1$ and $[\![\gamma\dagger(\mathcal{C}.\mathcal{P})]\!]\delta W'$.
  - The former follows from $[\![\gamma\mathcal{C}.\mathcal{L}]\!]\delta W\omega_1$ and Lemma 2.15.
  - The latter follows from $[\![\gamma\mathcal{C}.\mathcal{P}]\!]\delta W$ and Lemma 2.9.
- Now instantiating the premise yields $[\![\gamma P]\!]\delta W'$.

□

Theorem 2.41
The following rule is sound:

$$\frac{\mathcal{C} \vdash A}{\mathcal{C} \vdash \Box A}\ \Box\text{-INTRO-ABS}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\Box\gamma A]\!]\delta W$
- If $W.k = 0$, there is nothing to show.

- Otherwise suppose $W' \sqsupseteq W$.
- To show: $[\![\gamma A]\!]\delta W'$
- If $W'.k = 0$, there is nothing to show.
- So assume $W'.k > 0$ and thus $W.k > 0$.
- Instantiating the premise yields $[\![\gamma A]\!]\delta W$.
- By Lemma 2.12, this is equivalent to $\|\gamma A\|\delta$, which in turn is equivalent to $[\![\gamma A]\!]\delta W'$.

□

Theorem 2.42
The following rule is sound:

$$\frac{\mathcal{C} \vdash e \in \mathrm{Term}_i}{\mathcal{C} \vdash \Box(e \in \mathrm{Term}_i)}\ \Box\text{-INTRO-TERM}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$
- To show: $[\![\Box(\gamma e \in \mathrm{Term}_i)]\!]\delta W$
- If $W.k = 0$, there is nothing to show.
- Otherwise suppose $W' \sqsupseteq W$.
- To show: $[\![\gamma e \in \mathrm{Term}_i]\!]\delta W'$
- If $W'.k = 0$, there is nothing to show.
- Otherwise we need to show $\mathrm{FL}(\gamma e) \subseteq W'.\varsigma_i$.
- Instantiating the premise yields $[\![\gamma e \in \mathrm{Term}_i]\!]\delta W$, *i.e.,* $\mathrm{FL}(\gamma e) \subseteq W.\varsigma_i$.
- By definition of $\sqsupseteq$ we know $W.\varsigma_i \subseteq W'.\varsigma_i$.

□

Theorem 2.43
The following rule is sound:

$$\frac{\mathcal{C} \vdash \Box P}{\mathcal{C} \vdash P}\ \Box\text{-ELIM}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- If $W.k = 0$, there is nothing to show.
- Otherwise we can instantiate the premise with $W \sqsupseteq W$ to get $[\![\gamma P]\!]\delta W$.

□

Theorem 2.44
The following rule is sound:

$$\frac{\mathcal{C} \vdash \triangleright\Box P}{\mathcal{C} \vdash \Box\triangleright P}\ \triangleright\Box\text{-SWAP}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\Box\triangleright\gamma P]\!]\delta W$
- If $W.k = 0$, there is nothing to show.
- Otherwise suppose $W' \sqsupseteq W$.
- To show: $[\![\triangleright\gamma P]\!]\delta W'$
- If $W'.k = 0$, there is nothing to show.
- Otherwise we need to show $[\![\gamma P]\!]\delta(\triangleright W')$.
- Instantiating the premise yields $[\![\Box\gamma P]\!]\delta(\triangleright W)$.
- By Lemma 2.2, $\triangleright W' \sqsupseteq \triangleright W$.
- Hence $[\![\gamma P]\!]\delta(\triangleright W')$, *i.e.,* $[\![\triangleright\gamma P]\!]\delta W'$.

□

Theorem 2.45
The following rule is sound:

$$\frac{\mathcal{C} \vdash \Box\triangleright P}{\mathcal{C} \vdash \triangleright\Box P}\ \triangleright\Box\text{-SWAP}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\triangleright\Box\gamma P]\!]\delta W$
- If $W.k = 0$, there is nothing to show.
- Otherwise we need to show $[\![\Box\gamma P]\!]\delta(\triangleright W)$.
- So suppose $W' \sqsupseteq \triangleright W$.
- By Lemma 2.3 there is $\widehat{W'} \supseteq W$ with $\triangleright\widehat{W'} = W'$.
- Instantiating the premise yields $[\![\triangleright\gamma P]\!]\delta\widehat{W'}$, *i.e.,* $[\![\gamma P]\!]\delta W'$.

□

Theorem 2.46
The following rule is sound:

$$\frac{\mathcal{C} \vdash \overline{e} \in \overline{x}.P}{\mathcal{C} \vdash P[\overline{e}/\overline{x}]} \text{ ELEM}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- If $W.k = 0$, there is nothing to show. Otherwise:

$$\begin{aligned} & [\![\gamma\overline{e} \in \overline{x}.\gamma P]\!]\delta W \\ \iff & [\![\overline{x}.\gamma P]\!]\delta W(\gamma\overline{e}) \\ \iff & [\![\gamma P[\gamma\overline{e}/\overline{x}]]\!]\delta W \\ \iff & [\![\gamma(P[\overline{e}/\overline{x}])]\!]\delta W \end{aligned}$$

□

Theorem 2.47
The following rule is sound:

$$\frac{\mathcal{C} \vdash \overline{e} \in \mu r.R}{\mathcal{C} \vdash \overline{e} \in R[\mu r.R/r]} \text{ ELEM-}\mu$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- If $W.k = 0$, there is nothing to show. Otherwise:

$$\begin{aligned} & [\![\gamma\overline{e} \in \gamma R[\mu r.\gamma R]]\!]\delta W \\ \iff & [\![\gamma R[\mu r.\gamma R]]\!]\delta W(\gamma\overline{e}) \\ \iff & [\![\mu r.\gamma R]\!]\delta W(\gamma\overline{e}) \\ \iff & [\![\gamma\overline{e} \in \mu r.\gamma R]\!]\delta W \\ \iff & [\![\gamma(\overline{e} \in \mu r.R)]\!]\delta W \end{aligned}$$

□

Theorem 2.48
The following rule is sound:

$$\frac{p \propto a.(B, H) \in \mathcal{C}.\mathcal{L} \quad \mathcal{C} \vdash \overline{e} \in p}{\mathcal{C} \vdash \Box(\overline{e} \in p)} \text{ POP-MONO}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$
- To show: $[\![\Box(\gamma\overline{e} \in p)]\!]\delta W$

- If $W.k = 0$, there is nothing to show.
- Otherwise suppose $W' \sqsupseteq W$.
- To show: $[\![\gamma\overline{e} \in p]\!]\delta W'$
- If $W'.k = 0$, there is nothing to show.
- Otherwise we need to show $[\![p]\!]\delta W'(\gamma\overline{e})$.
- From the first premise we know that there is ι such that $[\![p \propto a.(\gamma B, \gamma H)]\!]\delta W\{\iota\}$.
- Hence $\delta(p) = \mathrm{pop}(\iota)$.
- So it remains to show $\gamma\overline{e} \in W'.\mathcal{I}(\iota).CP$.
- Instantiating the second premise yields $[\![\gamma\overline{e} \in p]\!]\delta W$, *i.e.,* $\gamma\overline{e} \in W.\mathcal{I}(\iota).CP$.
- By definition of $\sqsupseteq$, $W.\mathcal{I}(\iota).CP \subseteq W'.\mathcal{I}(\iota).CP$.

□

Theorem 2.49
The following rule is sound:

$$\frac{p \propto a.(B, H) \in \mathcal{C}.\mathcal{L} \quad \mathcal{C} \vdash A \equiv p}{\mathcal{C} \vdash B[A/a]}\ \textsc{pop-law}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\gamma(B[A/a])]\!]\delta W$
- By Lemma 2.13 it suffices to show $[\![\gamma B]\!](\delta, a{\mapsto}[\![\gamma A]\!]\delta W)W$.
- If $W.k = 0$, there is nothing to show.
- Otherwise, by Lemma 2.12, this reduces to showing $\|\gamma B\|(\delta, a{\mapsto}\|\gamma A\|\delta)$.
- From the first premise we know that there is ι such that $[\![p \propto a.(\gamma B, \gamma H)]\!]\delta W\{\iota\}$.
- Hence $\delta(p) = \mathrm{pop}(\iota)$.
- We know $W.\mathcal{I}(\iota).CP \in W.\mathcal{I}(\iota).PL$, *i.e.,* $\|\gamma B\|(\delta, a{\mapsto}W.\mathcal{I}(\iota).CP)$.
- It remains to show $\|\gamma A\|\delta = W.\mathcal{I}(\iota).CP$.
- This follows from instantiating the second premise with $W \supseteq W$.

□

Theorem 2.50
The following rule is sound:

$$\frac{p \propto a.(B, H) \in \mathcal{C}.\mathcal{L}}{\mathcal{C} \vdash \exists a.a \equiv p}\ \textsc{pop-snap}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\exists a.\gamma a \equiv \gamma p]\!]\delta W$
- If $W.k = 0$, there is nothing to show, so assume $W.k > 0$.
- From the premise we know that there is ι such that $[\![p \propto a.(\gamma B, \gamma H)]\!]\delta W\{\iota\}$.
- Hence $\delta(p) = \text{pop}(\iota)$.
- Let $\delta' := \delta, a{\mapsto}W.\mathcal{I}(\iota).CP$.
- It suffices to show $[\![\gamma a \equiv \gamma p]\!]\delta' W$.
- If $W.k = 0$, there is nothing to show.
- Otherwise this follows from the fact that $W.\mathcal{I}(\iota).CP = W'.\mathcal{I}(\iota).CP$ for any $W' \sqsupseteq W$.

□

Theorem 2.51
The following rule is sound:

$$\frac{\begin{array}{c} p \propto a.(B', H') \in \mathcal{C}.\mathcal{L} \\ \mathcal{C} \vdash \forall a.B \equiv B' \\ \mathcal{C} \vdash \Box(\forall a.B \Rightarrow (H \Leftrightarrow H')) \end{array}}{\mathcal{C} \vdash \propto a.(B, H)} \propto\text{-INTRO}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- If $W.k = 0$, there is nothing to show.
- Otherwise we need to show $[\![\tilde{p} \propto a.(\gamma B, \gamma H)]\!](\delta, \tilde{p}{\mapsto}\text{pop}(\iota))W\{\iota\}$ for some ι.
- From the first premise and $[\![\gamma(\mathcal{C}.\mathcal{L})]\!]\delta W\omega_1$ we know $[\![p \propto a.(\gamma B', \gamma H')]\!]\delta W\{\iota\}$ for some ι.
- We need to show:
  1. $W.\mathcal{I}(\iota).PL = \{CP \mid \|\gamma B\|\delta, a{\mapsto}CP)\}$
     - We know implies $W.\mathcal{I}(\iota).PL = \{CP \mid \|\gamma B'\|(\delta, a{\mapsto}CP)\}$.
     - It remains to show $\|\gamma B'\|(\delta, a{\mapsto}CP) = \|\gamma B\|(\delta, a{\mapsto}CP)$, for any CP.
     - This follows from instantiating the second premise and Lemma 2.12.
  2. $\forall CP \in W.\mathcal{I}(\iota).PL.\ \forall W' \sqsupseteq {\triangleright}W.$
     $(W', h_1, h_2) \in W.\mathcal{I}(\iota).HL(CP) \iff [\![\gamma H]\!](\delta, a{\mapsto}CP)({\triangleleft}W')(h_1, h_2)$
     - We know $\forall CP \in W.\mathcal{I}(\iota).PL.\ \forall W' \sqsupseteq {\triangleright}W.$
       $(W', h_1, h_2) \in W.\mathcal{I}(\iota).HL(CP) \iff [\![\gamma H']\!](\delta, a{\mapsto}CP)({\triangleleft}W')(h_1, h_2)$

- It remains to show $[\![\gamma H']\!](\delta, a{\mapsto}CP)(\triangleleft W') = [\![\gamma H]\!](\delta, a{\mapsto}CP)(\triangleleft W')$, for any $CP \in W.\mathcal{I}(\iota).PL$ and $W' \sqsupseteq \triangleright W$.
- By symmetry it suffices to show only one direction.
- So suppose $[\![\gamma H']\!](\delta, a{\mapsto}CP)(\triangleleft W')(h_1, h_2)$.
- By Lemma 2.3 there is $\widehat{W'} \sqsupseteq W$ with $\triangleright\widehat{W'} = W'$.
- Since $\triangleright\triangleleft W' = W'$ by Lemma 2.1, Lemma 2.7 yields $[\![\gamma H']\!](\delta, a{\mapsto}CP)\widehat{W'}(h_1, h_2)$.
- Part (1) and Lemma 2.12 let us instantiate the third premise to get $[\![\gamma H \Leftrightarrow \gamma H']\!](\delta, a{\mapsto}CP)\widehat{W'}(h_1, h_2)$.
- Consequently, $[\![\gamma H]\!](\delta, a{\mapsto}CP)\widehat{W'}(h_1, h_2)$ and thus we get $[\![\gamma H]\!](\delta, a{\mapsto}CP)(\triangleleft W')(h_1, h_2)$ by Lemma 2.7 again.

□

Theorem 2.52
The following rule is sound:

$$\frac{\mathcal{C} \vdash \propto a.(B, H) \quad \mathcal{C}, p, p \propto a.(B, H) \vdash P \qquad \forall p' \propto a.(B', H') \in \mathcal{C}.\mathcal{L}\colon\ \mathcal{C}, \forall a.B \equiv B', \Box(\forall a.B \Rightarrow (H \Leftrightarrow H')) \vdash P}{\mathcal{C} \vdash P}\ \propto\text{-ELIM}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\gamma P]\!]\delta W$
- If $W.k = 0$, there is nothing to show.
- So assume $W.k > 0$.
- Instantiating the first premise yields $[\![\tilde{p} \propto a.(\gamma B, \gamma H)]\!]\delta' W\{\iota\}$ for some ι, where $\tilde{\delta} = \delta, \tilde{p}{\mapsto}\mathrm{pop}(\iota)$.
- There are two cases:

  1. $\iota \in \omega_1$
     - From $[\![\gamma(\mathcal{C}.\mathcal{L})]\!]\delta W\omega_1$ we then know $\left[\!\!\left[\hat{p} \propto a.(\gamma\hat{B}, \gamma\hat{H})\right]\!\!\right]\delta W\{\iota\}$ for some $\hat{p} \propto a.(\hat{B}, \hat{H}) \in \mathcal{C}.\mathcal{L}$.
     - It suffices to show $\left[\!\!\left[\forall a.\gamma B \equiv \gamma\hat{B}\right]\!\!\right]\delta W$ and $\left[\!\!\left[\Box(\forall a.\gamma B \Rightarrow (\gamma H \Leftrightarrow \gamma\hat{H}))\right]\!\!\right]\delta W$, because this lets us instantiate the third premise to get $[\![\gamma P]\!]\delta W$.
     - We show the former:
       * From $[\![\tilde{p} \propto a.(\gamma B, \gamma H)]\!]\tilde{\delta} W\{\iota\}$ and $\left[\!\!\left[\hat{p} \propto a.(\gamma\hat{B}, \gamma\hat{H})\right]\!\!\right]\delta W\{\iota\}$ we know $\|\gamma B\|(\delta, a{\mapsto}CP) = \|\gamma\hat{B}\|(\delta, a{\mapsto}CP)$ for any CP.
       * It is easy to see that, together with Lemma 2.12, this implies $\left[\!\!\left[\forall a.\gamma B \equiv \gamma\hat{B}\right]\!\!\right]\delta W$.
     - We show the latter:
       * Suppose $W' \sqsupseteq W$ and let $\delta' := \delta, a{\mapsto}CP$ for some CP.

* To show: $\left[\!\left[\gamma B \Rightarrow (\gamma H \Leftrightarrow \gamma \hat{H})\right]\!\right] \delta' W'$
* If $W'.k = 0$, there is nothing to show
* So assume $W'.k > 0$.
* Now suppose $W'' \sqsupseteq W'$ and $[\![\gamma B]\!]\delta' W''$.
* To show: $\left[\!\left[\gamma H \Leftrightarrow \gamma \hat{H}\right]\!\right] \delta' W''$
* If $W''.k = 0$, there is nothing to show.
* So assume $W''.k > 0$.
* By symmetry it suffices to show one direction.
* Suppose $W''' \sqsupseteq W''$ and $[\![\gamma H]\!]\delta' W'''(h_1, h_2)$.
* To show: $\left[\!\left[\gamma \hat{H}\right]\!\right] \delta' W'''(h_1, h_2)$
* From $[\![\tilde{p} \propto a.(\gamma B, \gamma H)]\!]\tilde{\delta} W\{\iota\}$ and $\left[\!\left[\hat{p} \propto a.(\gamma \hat{B}, \gamma \hat{H})\right]\!\right] \delta W\{\iota\}$ we know $[\![\gamma H]\!]\delta'(\triangleleft \widetilde{W}) = \left[\!\left[\gamma \hat{H}\right]\!\right] \delta'(\triangleleft \widetilde{W})$ for any $\widetilde{W} \sqsupseteq \triangleright W$, if $CP \in W.\mathcal{I}(\iota).PL$.
* Note that $[\![\gamma B]\!]\delta' W''$ with Lemma 2.12 implies $CP \in W.\mathcal{I}\iota.PL$.
* Further note that $W''' \sqsupseteq W$ and thus $\triangleright W''' \sqsupseteq \triangleright W$ by Lemma 2.2.
* Hence $[\![\gamma H]\!]\delta'(\triangleleft\triangleright W''') = \left[\!\left[\gamma \hat{H}\right]\!\right] \delta'(\triangleleft\triangleright W''')$.
* Consequently, $[\![\gamma H]\!]\delta' W'''(h_1, h_2)$ and Lemma 2.8 yield $\left[\!\left[\gamma \hat{H}\right]\!\right] \delta' W'''(h_1, h_2)$.

2. $\iota \in \omega_2$
   - Let $\omega_1' := \omega_1 \uplus \{\iota\}$ and $\omega_2' := \omega_2 \setminus \{\iota\}$, so $\mathrm{dom}(W.\mathcal{I}) = \omega_1' \uplus \omega_2'$.
   - Let $\delta'' := \delta, p \mapsto \mathrm{pop}(\iota)$.
   - We show $(\gamma, \delta'', W, \omega_1', \omega_2') \in [\![\mathcal{C}, p, p \propto a.(B, H)]\!]$:
     * This reduces to showing $[\![p \propto a.(\gamma B, \gamma H)]\!]\delta'' W\{\iota\}$.
     * This in turn follows from $[\![\tilde{p} \propto a.(\gamma B, \gamma H)]\!]\tilde{\delta} W\{\iota\}$ and the definition of δ''.
   - We now instantiate the second premise to get $[\![\gamma P]\!]\delta W$.

□

Theorem 2.53
The following rule is sound:

$$\frac{\mathcal{C} \vdash (e_1', e_2') \in \uparrow R \quad \mathcal{C} \vdash e_1 \rightsquigarrow^* e_1' \quad \mathcal{C} \vdash e_2 \rightsquigarrow^* e_2'}{\mathcal{C} \vdash (e_1, e_2) \in \uparrow R}\ \uparrow\text{-EXPAND}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![(\gamma e_1, \gamma e_2) \in \uparrow \gamma R]\!]\delta W$
- If $W.k = 0$, there is nothing to show.
- Otherwise suppose $W' \sqsupseteq W$ and $h_1, h_2 : W'$.

- To show: $W' \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- $\mathrm{FL}(\gamma e_i) \subseteq W.\varsigma_i \subseteq W'.\varsigma_i$ follows from the definition of $\supseteq$ and the implicit assumption $\mathcal{C} \vdash e_i \in \mathrm{Term}_i$.
- Now assume $W'.d = \rightarrow$ (the other direction is analogously).
- Suppose $(h_1; \gamma e_1) \Downarrow^j (h_1'; e_1'')$ where $j < W'.k$.
- Instantiating the first two premises yields $W' \vdash (h_1; \gamma e_1') \approx (h_2; \gamma e_2') : [\![\gamma R]\!]\delta$ and $\gamma e_1 \rightsquigarrow^* \gamma e_1'$.
- The latter implies $(h_1; \gamma e_1) \overset{\epsilon}{\longmapsto}^{j_1} (h_1; \gamma e_1')$ for some j_1 and thus $(h_1; \gamma e_1') \Downarrow^{j-j_1} (h_1'; e_1'')$ and $j_1 \leq j$.
- Consequently, there is h_2', e_2'', W'' such that:
  1. $W''.k = W'.k - j + j_1$
  2. $W'' \sqsupseteq W'$
  3. $(h_2; \gamma e_2') \Downarrow (h_2'; e_2'')$
  4. $[\![\gamma R]\!]\delta W''(e_1'', e_2'')$
  5. $h_1', h_2' : W''$
- Instantiating the third premise yields $\gamma e_2 \rightsquigarrow^* \gamma e_2'$, which implies $(h_2; \gamma e_2) \overset{\epsilon}{\longmapsto}^* (h_2; \gamma e_2')$.
- Hence $(h_2; \gamma e_2) \Downarrow (h_2'; e_2'')$.
- Let $W''' := \underbrace{\triangleright \ldots \triangleright}_{j_1 \text{ times}} W''$, so:
  1. $W'''.k = W''.k - j_1 = W'.k - j$
  2. $W''' \sqsupseteq W'$ by Lemma 2.2
  3. $[\![\gamma R]\!]\delta W'''(e_1'', e_2'')$ by Lemma 2.2 and Lemma 2.17
  4. $h_1', h_2' : W'''$ by Lemma 2.14

□

Theorem 2.54
The following rule is sound:

$$\frac{\mathcal{C} \vdash (e_1', e_2') \in \uparrow R \quad \mathcal{C} \vdash e_1' \rightsquigarrow^0 e_1 \quad \mathcal{C} \vdash e_2' \rightsquigarrow^0 e_2}{\mathcal{C} \vdash (e_1, e_2) \in \uparrow R} \uparrow\text{-REDUCE}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- If $W.k = 0$, there is nothing to show.
- Otherwise suppose $W' \supseteq W$ and $h_1, h_2 : W'$.

- To show: $W' \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- $\mathrm{FL}(\gamma e_i) \subseteq W.\varsigma_i \subseteq W'.\varsigma_i$ follows from the definition of $\supseteq$ and the implicit assumption $\mathcal{C} \vdash e_i \in \mathrm{Term}_i$.
- Now assume $W'.d = \rightarrow$ (the other direction is analogously).
- Suppose $(h_1; \gamma e_1) \Downarrow^j (h_1'; e_1'')$ where $j < W'.k$.
- Instantiating the first two premises yields $W' \vdash (h_1; \gamma e_1') \approx (h_2; \gamma e_2') : [\![\gamma R]\!]\delta$ and $\gamma e_1' \rightsquigarrow^0 \gamma e_1$.
- The latter implies $(h_1; \gamma e_1') \overset{\epsilon}{\longmapsto}{}^0 (h_1; \gamma e_1)$ and thus $(h_1; \gamma e_1') \Downarrow^j (h_1'; e_1'')$.
- Consequently, there is h_2', e_2'', W'' such that:
  1. $W''.k = W'.k - j$
  2. $W'' \sqsupseteq W'$
  3. $(h_2; \gamma e_2') \Downarrow (h_2'; e_2'')$
  4. $[\![\gamma R]\!]\delta W''(e_1'', e_2'')$
  5. $h_1', h_2' : W''$
- Instantiating the third premise yields $\gamma e_2' \rightsquigarrow^0 \gamma e_2$, which implies $(h_2; \gamma e_2') \overset{\epsilon}{\longmapsto}{}^0 (h_2; \gamma e_2)$.
- Hence $(h_2; \gamma e_2) \Downarrow (h_2'; e_2'')$.

□

Theorem 2.55
The following rule is sound:

$$\frac{\begin{array}{c}\triangleleft\mathcal{C} \vdash (e_1', e_2') \in \uparrow R \\ \mathcal{C} \vdash e_1 \rightsquigarrow^1 e_1' \quad \mathcal{C} \vdash e_2 \rightsquigarrow^1 e_2'\end{array}}{\mathcal{C} \vdash (e_1, e_2) \in \uparrow R}\ \uparrow\text{-UNROLL}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- If $W.k = 0$, there is nothing to show.
- Otherwise suppose $W' \supseteq W$ and $h_1, h_2 : W'$.
- To show: $W' \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- $\mathrm{FL}(\gamma e_i) \subseteq W.\varsigma_i \subseteq W'.\varsigma_i$ follows from the definition of $\supseteq$ and the implicit assumption $\mathcal{C} \vdash e_i \in \mathrm{Term}_i$.
- Now assume $W'.d = \rightarrow$ (the other direction is analogously).
- Suppose $(h_1; \gamma e_1) \Downarrow^j (h_1'; e_1'')$ where $j < W'.k$.

- Instantiating the second premise yields $\gamma e_1 \rightsquigarrow^1 \gamma e_1'$, which implies $(h_1; \gamma e_1) \xmapsto{\epsilon}{}^1 (h_1; \gamma e_1')$ and thus $(h_1; \gamma e_1') \Downarrow^{j-1} (h_1'; e_1'')$ and $1 \leq j$.
- It is easy to see that $(\gamma, \delta, \triangleright W, \omega_1, \omega_2) \in [\![\triangleleft \mathcal{C}]\!]$.
- Furthermore, $\triangleright W' \supseteq \triangleright W$ by Lemma 2.2.
- Note that $j < W'.k$ and $1 \leq j$ imply $(\triangleright W').k > 0$.
- Instantiating the first premise accordingly yields $\triangleright W' \vdash (h_1; \gamma e_1') \approx (h_2; \gamma e_2') : [\![\gamma R]\!]\delta$.
- Consequently, there is h_2', e_2'', W'' such that:
  1. $W''.k = W'.k - 1 - j + 1 = W'.k - j$
  2. $W'' \sqsupseteq \triangleright W'$ $(\sqsupseteq W')$
  3. $(h_2; \gamma e_2') \Downarrow (h_2'; e_2'')$
  4. $[\![\gamma R]\!]\delta W''(e_1'', e_2'')$
  5. $h_1', h_2' : W''$
- Instantiating the third premise yields $\gamma e_2 \rightsquigarrow^1 \gamma e_2'$, which implies $(h_2; \gamma e_2) \xmapsto{\epsilon}{}^1 (h_2; \gamma e_2')$.
- Hence $(h_2; \gamma e_2) \Downarrow (h_2'; e_2'')$.

□

Theorem 2.56
The following rule is sound:

$$\frac{\mathcal{C} \vdash (e_1, e_2) \in R \quad \mathcal{C} \vdash R : \mathrm{VRel}}{\mathcal{C} \vdash (e_1, e_2) \in \uparrow R} \uparrow\text{-RETURN}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- If $W.k = 0$, there is nothing to show.
- Otherwise suppose $W' \supseteq W$ and $h_1, h_2 : W'$.
- To show: $W' \vdash (h_1; \gamma(E_1[e_1])) \approx (h_2; \gamma(E_2[e_2])) : [\![\gamma R]\!]\delta$
- $\mathrm{FL}(\gamma e_i) \subseteq W.\varsigma_i \subseteq W'.\varsigma_i$ follows from the definition of $\supseteq$ and the implicit assumption $\mathcal{C} \vdash e_i \in \mathrm{Term}_i$.
- Now assume $W'.d = \rightarrow$ (the other direction is analogously).
- Suppose $j < W'.k$ and $(h_1; \gamma e_1) \Downarrow^j (h_1'; e_1')$.
- Instantiating the first premise yields $[\![\gamma R]\!]\delta W(\gamma e_1, \gamma e_2)$ and thus $[\![\gamma R]\!]\delta W'(\gamma e_1, \gamma e_2)$ by Lemma 2.17.
- Instantiating the second premise then implies that γe_1 and γe_2 are values.

- Consequently, $j = 0$ and $h_1' = h_1$ and $e_1' = \gamma e_1$.
- All in all, we have:
  1. $W'.k = W'.k - j$
  2. $W' \sqsupseteq W'$
  3. $(h_2; \gamma e_2) \Downarrow (h_2; \gamma e_2)$
  4. $[\![\gamma R]\!]\delta W'(e_1', \gamma e_2)$
  5. $h_1', h_2 : W'$

□

Theorem 2.57
The following rule is sound:

$$\frac{\mathcal{C} \vdash (e_1, e_2) \in \uparrow S \quad \dagger\mathcal{C}, x_1, x_2, (x_1, x_2) \in S \vdash (E_1[x_1], E_2[x_2]) \in \uparrow R}{\mathcal{C} \vdash (E_1[e_1], E_2[e_2]) \in \uparrow R} \uparrow\text{-BIND}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- If $W.k = 0$, there is nothing to show.
- Otherwise suppose $W' \supseteq W$ and $h_1, h_2 : W'$.
- To show: $W' \vdash (h_1; \gamma(E_1[e_1])) \approx (h_2; \gamma(E_2[e_2])) : [\![\gamma R]\!]\delta$
- $\mathrm{FL}(\gamma(E_i[e_i])) \subseteq W.\varsigma_i \subseteq W'.\varsigma_i$ follows from the definition of $\supseteq$ and the implicit assumption $\mathcal{C} \vdash E_i[e_i] \in \mathrm{Term}_i$.
- Now assume $W'.d = \rightarrow$ (the other direction is analogously).
- Suppose $j < W'.k$ and $(h_1; \gamma(E_1[e_1])) \Downarrow^j (h_1''; e_1'')$.
- This implies $(h_1; \gamma(E_1[e_1])) \xmapsto{\bar{l}}{}^{j_1} (h_1'; (\gamma E_1)[e_1'])$ and $(h_1'; (\gamma E_1)[e_1']) \Downarrow^{j-j_1} (h_1''; e_1'')$ (for some $j_1 \leq j, \bar{l}, h_1', e_1'$) with $(h_1; \gamma e_1) \Downarrow^{j_1} (h_1'; e_1')$.
- Instantiating the first premise with $(h_1; \gamma e_1) \Downarrow^{j_1} (h_1'; e_1')$ yields h_2', e_2', W'' such that
  1. $W''.k = W'.k - j_1$,
  2. $W'' \sqsupseteq W'$,
  3. $(h_2; \gamma e_2) \Downarrow (h_2'; e_2')$,
  4. $[\![\gamma S]\!]\delta W''(e_1', e_2')$, and
  5. $h_1', h_2' : W''$.
- Let
  - $\gamma' := \gamma, x_1 \mapsto e_1', x_2 \mapsto e_2'$

– $\omega_2' := \mathrm{dom}(W''.\mathcal{I}) \setminus \omega_1$

and note that $\mathrm{dom}(W''.\mathcal{I}) = \omega_1 \uplus \omega_2'$.

- Note that $j < W'.k$ and $j_1 \leq j$ and $W''.k = W'.k - j_1$ imply $W''.k > 0$.
- We show $(\gamma', \delta, W'', \omega_1, \omega_2') \in [\![\dagger\mathcal{C}, x_1, x_2, (x_1, x_2) \in S]\!]$:
  - $[\![\gamma\mathcal{C}.\mathcal{L}]\!]\delta W''\omega_1$ follows from $[\![\gamma\mathcal{C}.\mathcal{L}]\!]\delta W\omega_1$, Lemma 2.2, and Lemma 2.15.
  - $[\![\dagger\gamma\mathcal{C}.\mathcal{P}]\!]\delta W''$ follows from $[\![\gamma\mathcal{C}.\mathcal{P}]\!]\delta W$, Lemma 2.2, and Lemma 2.9.
  - $[\![\gamma'((x_1, x_2) \in S)]\!]\delta W''$ is $[\![(e_1', e_2') \in \gamma S]\!]\delta W''$, which is equivalent to $[\![\gamma S]\!]\delta W''(e_1', e_2')$ and thus already known.
- Instantiating the second premise now yields $W'' \vdash (h_1'; (\gamma E_1)[e_1']) \approx (h_2'; (\gamma E_2)[e_2']) : [\![\gamma R]\!]\delta$.
- Instantiating this with $(h_1'; (\gamma E_1)[e_1']) \Downarrow^{j-j_1} (h_1''; e_1'')$ yields h_2'', e_2'', W''' such that
  1. $W'''.k = W''.k - j + j_1$ $(= W'.k - j)$,
  2. $W''' \sqsupseteq W''$ $(\sqsupseteq W')$,
  3. $(h_2'; (\gamma E_2)[e_2']) \Downarrow (h_2''; e_2'')$ (and thus $(h_2; \gamma(E_2[e_2])) \Downarrow (h_2''; e_2'')$),
  4. $[\![\gamma R]\!]\delta W'''(e_1'', e_2'')$, and
  5. $h_1'', h_2'' : W'''$.

□

Theorem 2.58
The following rule is sound:

$$\frac{\mathcal{C}.\mathcal{L} = \overline{p \propto a.(B, H)} \quad \mathcal{C}, \overline{a}, \overline{p \equiv a} \vdash \{* \overline{H}\}\ e_1 \approx e_2\ \{R\}}{\mathcal{C} \vdash (e_1, e_2) \in \uparrow R}\ \uparrow\text{-IMPURE}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- If $W.k = 0$, there is nothing to show.
- Otherwise suppose $W' \sqsupseteq W$ and $h_1, h_2 : W'$.
- To show: $W' \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- $\mathrm{FL}(\gamma e_i) \subseteq W.\varsigma_i \subseteq W'.\varsigma_i$ follows from the definition of $\sqsupseteq$ and the implicit assumption $\mathcal{C} \vdash e_i \in \mathrm{Term}_i$.
- If $W'.k = 0$, there is nothing more to show, so assume $W'.k > 0$.
- Say $\omega_1 = \{\iota_1, \ldots, \iota_n\}$ and $\omega_2 = \{\iota_{n+1}, \ldots, \iota_m\}$.
- From $h_1, h_2 : W'$ we know there is $h_1' \subseteq h_1$ and $h_2' \subseteq h_2$ with $h_1', h_2' :_{\mathrm{dom}(W'.\mathcal{I})} W'$.
- Let $\omega_2' := \mathrm{dom}(W'.\mathcal{I}) \setminus \omega_1$.

- Consequently, for $i \in \{1,2\}$ there is $h_i'^1$ and $h_i'^2$ with $h_i' = h_i'^1 \uplus h_i'^2$ such that $h_1'^1, h_2'^1 :_{\omega_1} W'$ and $h_1'^2, h_2'^2 :_{\omega_2'} W'$.
- The former yields $h_i'^{1,1}, \ldots, h_i'^{1,n}$ with $h_i'^1 = h_i'^{1,1} \uplus \cdots \uplus h_i'^{1,n}$ such that $(\triangleright W', h_1'^{1,j}, h_2'^{1,j}) \in W'.\mathcal{I}(\iota_j).HL(W'.\mathcal{I}(\iota_j).CP)$ for each $j \in \{1, \ldots, n\}$.
- Note that from $[\![\gamma(\mathcal{C}.\mathcal{L})]\!]\delta W\omega_1$, Lemma 2.2, and Lemma 2.15 we know $[\![p_j \propto a_j.(\gamma B_j, \gamma H_j)]\!]\delta(\triangleright W)\{\iota_j\}$ for each $j \in \{1, \ldots, n\}$.
- Since $\triangleright W' \supseteq \triangleright W$ by Lemma 2.2 we thus get $[\![\gamma H_j]\!](\delta, a_j \mapsto W'.\mathcal{I}(\iota_j).CP)(\triangleleft\triangleright W')(h_1'^{1,j}, h_2'^{1,j})$ for each $j \in \{1, \ldots, n\}$.
- By Lemma 2.8, $[\![\gamma H_j]\!](\delta, a_j \mapsto W'.\mathcal{I}(\iota_j).CP)W'(h_1'^{1,j}, h_2'^{1,j})$ for each $j \in \{1, \ldots, n\}$.
- Let $\delta' := \delta, \overline{a \mapsto W'.\mathcal{I}(\iota).CP}$, so $[\![\gamma(* \overline{H})]\!]\delta' W'(h_1'^1, h_2'^1)$.
- We show $(\gamma, \delta', W', \omega_1, \omega_2') \in [\![\mathcal{C}, \overline{a}, \overline{p \equiv a}]\!]$:
  - We need to show $[\![\gamma\mathcal{C}.\mathcal{L}]\!]\delta W'\omega_1$ and $[\![\gamma(\mathcal{C}.\mathcal{P})]\!]\delta' W'$ and $[\![\overline{p \equiv a}]\!]\delta' W'$.
  - The first follows by Lemma 2.2 and Lemma 2.15.
  - The second follows by Lemma 2.17.
  - The third follows from $\delta'(a_j) = W'.\mathcal{I}(\iota_j).CP$ and $\delta'(p_j) = \mathrm{pop}(\iota_j)$ and the definition of $\supseteq$.
- We now instantiate the second premise to get $W' \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$

□

Theorem 2.59
The following rule is sound:

$$\frac{\mathcal{C} \vdash \Box P}{\mathcal{C} \vdash H \Rrightarrow \Box P} \text{ (ENTAIL-}\Box\text{-INTRO)}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\gamma H \Rrightarrow \Box\gamma P]\!]\delta W$
- If $W.k = 0$, there is nothing to show, so assume $W.k > 0$.
- Now suppose $W' \supseteq W$ and $[\![\gamma H]\!]\delta W'(h_1, h_2)$.
- We need to show $[\![\Box\gamma P]\!]\delta W'(h_1, h_2)$.
- If $W'.k = 0$, there is nothing to show, so assume $W'.k > 0$.
- Hence we need to show $[\![\Box\gamma P]\!]\delta W'$, which follows from instantiating the premise and applying Lemma 2.17.

□

Theorem 2.60
The following rule is sound:

$$\frac{\mathcal{C} \vdash H \Rrightarrow \Box P}{\mathcal{C} \vdash H \Rrightarrow H * \Box P} \text{ (ENTAIL-STRENGTHEN)}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\gamma H \Rrightarrow \gamma H * \Box \gamma P]\!]\delta W$
- If $W.k = 0$, there is nothing to show, so assume $W.k > 0$.
- Now suppose $W' \sqsupseteq W$ and $[\![\gamma H]\!]\delta W'(h_1, h_2)$.
- We need to show $[\![\gamma H * \Box \gamma P]\!]\delta W'(h_1, h_2)$.
- If $W'.k = 0$, there is nothing to show, so assume $W'.k > 0$.
- It suffices to show $[\![\gamma H]\!]\delta W'(h_1, h_2)$ and $[\![\Box \gamma P]\!]\delta W'$.
- The former is already known.
- The latter follows from instantiating the premise.

□

Theorem 2.61
The following rule is sound:

$$\frac{\mathcal{C}, \Box P \vdash H \Rrightarrow H'}{\mathcal{C} \vdash \Box P * H \Rrightarrow H'} \text{ (ENTAIL-}\Box\text{-ELIM)}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\Box \gamma P * \gamma H \Rrightarrow \gamma H']\!]\delta W$
- If $W.k = 0$, there is nothing to show, so assume $W.k > 0$.
- Now suppose $W' \sqsupseteq W$ and $[\![\Box \gamma P * \gamma H]\!]\delta W'(h_1, h_2)$.
- We need to show $[\![\gamma H']\!]\delta W'(h_1, h_2)$.
- If $W'.k = 0$, there is nothing to show, so assume $W'.k > 0$.
- From $[\![\Box \gamma P * \gamma H]\!]\delta W'(h_1, h_2)$ we thus know $[\![\Box \gamma P]\!]\delta W'$ and $[\![\gamma H]\!]\delta W'(h_1, h_2)$ (using Lemma 2.16).
- We show $(\gamma, \delta, W', \omega_1, \mathrm{dom}(W'.\mathcal{I}) \setminus \omega_1) \in [\![\mathcal{C}, \Box P]\!]$:
  - It remains to show $[\![\gamma \mathcal{C}.\mathcal{L}]\!]\delta W'$.

– This follows from $[\![\gamma\mathcal{C}.\mathcal{L}]\!]\delta W$, Lemma 2.2, and Lemma 2.15.

- Instantiating the premise now yields $[\![\gamma H']\!]\delta W'(h_1, h_2)$.

□

Theorem 2.62
The following rule is sound:

$$\frac{}{\mathcal{C} \vdash e_1 \hookrightarrow_i e_2 \Rrightarrow \Box(e_1 \in \mathrm{Loc} \wedge e_1 \in \mathrm{Val}_i \wedge e_2 \in \mathrm{Val}_i)} \text{ (ENTAIL-}\hookrightarrow\text{-VAL)}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$.
- To show: $[\![\gamma e_1 \hookrightarrow_i \gamma e_2 \Rrightarrow \Box(\gamma e_1 \in \mathrm{Loc} \wedge \gamma e_1 \in \mathrm{Val}_i \wedge \gamma e_2 \in \mathrm{Val}_i)]\!]\delta W$
- If $W.k = 0$, there is nothing to show, so assume $W.k > 0$.
- Now suppose $W' \sqsupseteq W$ and $[\![\gamma e_1 \hookrightarrow_i \gamma e_2]\!]\delta W'(h_1, h_2)$.
- We need to show $[\![\Box(\gamma e_1 \in \mathrm{Loc} \wedge \gamma e_1 \in \mathrm{Val}_i \wedge \gamma e_2 \in \mathrm{Val}_i)]\!]\delta W'(h_1, h_2)$.
- If $W'.k = 0$, there is nothing to show, so assume $W'.k > 0$.
- Now suppose $W'' \sqsupseteq W'$.
- If $W''.k = 0$, there is nothing to show, so assume $W''.k > 0$.
- Hence we need to show $[\![\gamma e_1 \in \mathrm{Loc}]\!]\delta W''$ and $[\![\gamma e_1 \in \mathrm{Val}_i]\!]\delta W''$ and $[\![\gamma e_2 \in \mathrm{Val}_i]\!]\delta W''$, which all follow from $[\![\gamma e_1 \hookrightarrow_i \gamma e_2]\!]\delta W'(h_1, h_2)$ with the help of Lemma 2.17.

□

Theorem 2.63
The following rule is sound:

$$\frac{\begin{array}{c}\mathcal{C} \vdash B[A/a] \\ \mathcal{C}, p, p \propto a.(B, H'), p \equiv A \vdash \{H\}\ e_1 \approx e_2\ \{R\}\end{array}}{\mathcal{C} \vdash \{H\}\ e_1 \approx e_2\ \{R\}} \text{ ISL-NEW}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, $\vdash h_i$, $\mathrm{dom}(h_i) \supseteq W.\varsigma_i$, $h_i = h_i^1 \uplus h_i^2$, $[\![\gamma H]\!]\delta W(h_1^1, h_2^1)$, and $h_1^2, h_2^2 :_{\omega_2} W$.
- To show: $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- Let
  - $\delta' := \delta, p \mapsto \mathrm{pop}(\iota)$ (where ι is fresh)
  - $CP := \|\gamma A\|\delta$

- $PL := \{CP' \mid \|\gamma B\|\delta, a{\mapsto}CP'\}$
- $HL := \lambda CP'.\ \{(W'', h_1', h_2') \mid W'' \sqsupseteq \triangleright W \ \wedge\ [\![\gamma H']\!](\delta, a{\mapsto}CP')(\triangleleft W'')(h_1', h_2')\}$
- $\omega_1' := \omega_1 \uplus \{\iota\}$
- $W' := (W.k, W.d, W.\varsigma_1, W.\varsigma_2, (W.\mathcal{I}, \iota{\mapsto}(CP, PL, HL)))$

- We show $W' \in \mathit{World}$:
  - It suffices to show $CP \in PL$ and monotonicity of HL.
  - The former follows from the first premise and Lemma 2.13.
  - For the latter suppose $W''' \sqsupseteq W''$ and $(W'', h_1', h_2') \in HL$, *i.e.,* $W'' \sqsupseteq \triangleright W$ and $[\![\gamma H']\!](\delta, a{\mapsto}CP')(\triangleleft W'')(h_1', h_2')$.
  - By Lemma 2.2 we have $W''' \sqsupseteq \triangleright W$.
  - It remains to show $[\![\gamma H']\!](\delta, a{\mapsto}CP')(\triangleleft W''')(h_1', h_2')$.
  - By Lemma 2.4 there is $\overleftarrow{W'''} \sqsupseteq \triangleleft W''$ with $\triangleright\overleftarrow{W'''} = W'''$.
  - Hence $[\![\gamma H']\!](\delta, a{\mapsto}CP')\overleftarrow{W'''}(h_1', h_2')$ by Lemma 2.10.
  - Lemma 2.8 now yields $[\![\gamma H']\!](\delta, a{\mapsto}CP')(\triangleleft\triangleright\overleftarrow{W'''})(h_1', h_2')$.
  - The claim then follows from $\triangleright\overleftarrow{W'''} = W'''$.
- $W' \supseteq W$ is easy to see and thus $W' \sqsupseteq W$ by Lemma 2.2.
- We show $(\gamma, \delta', W', \omega_1', \omega_2) \in [\![\mathcal{C}, p, p \propto a.(B, H'), p \equiv A]\!]$:
  - By assumption we know $[\![\gamma(\mathcal{C}.\mathcal{L})]\!]\delta W\omega_1$.
  - By Lemma 2.15 we get $[\![\gamma(\mathcal{C}.\mathcal{L})]\!]\delta' W'\omega_1$.
  - Using Lemma 2.2 it is easy to verify that $[\![p \propto a.(\gamma B, \gamma H')]\!]\delta' W'\{\iota\}$ holds by construction.
  - Consequently, $[\![\gamma(\mathcal{C}.\mathcal{L}, p \propto a.(B, H'))]\!]\delta' W'\omega_1'$.
  - Also, $[\![\gamma(\mathcal{C}.\mathcal{P})]\!]\delta' W'$ follows from $[\![\gamma(\mathcal{C}.\mathcal{P})]\!]\delta W$, $W' \supseteq W$, and Lemma 2.17.
  - It remains to show $[\![p \equiv \gamma A]\!]\delta' W'$ (we show only one direction, the other is analogously):
    - Suppose $W'' \supseteq W'$.
    - If $W''.k = 0$, there is nothing to show.
    - Otherwise we need to show $[\![\gamma A]\!]\delta W''\overline{e}$, knowing $[\![p]\!]\delta' W''\overline{e}$.
    - Since $\delta'(p) = \mathrm{pop}(\iota)$ and $W'' \supseteq W'$, the latter implies $\|\gamma A\|\delta\overline{e}$.
    - This in turn is equivalent to $[\![\gamma A]\!]\delta W''\overline{e}$ by Lemma 2.12.
- Furthermore, note that $[\![\gamma H]\!]\delta' W'(h_1^1, h_2^1)$ by Lemma 2.10, and $h_1^2, h_2^2 :_{\omega_2} W'$ by Lemma 2.14.
- We now instantiate the second premise to get $W' \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$.
- Finally Lemma 2.11 yields the claim.

□

Theorem 2.64
The following rule is sound:

$$\frac{\begin{array}{c}\mathcal{C}.\mathcal{L} = \overline{p \propto a.(B, H)} \quad \mathcal{C} \vdash \bigwedge \overline{p \subseteq A} \quad \mathcal{C} \vdash \bigwedge \overline{B[A/a]} \\ \mathcal{C}' = \dagger\mathcal{C}, \overline{p \equiv A} \quad \mathcal{C}' \vdash H \Rrightarrow * \overline{H[A/a]} \quad \mathcal{C}' \vdash (e_1, e_2) \in \uparrow R\end{array}}{\mathcal{C} \vdash \{H\}\ e_1 \approx e_2\ \{R\}}\ \text{ISL-UPD}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, $\vdash h_i$, $\mathrm{dom}(h_i) \supseteq W.\varsigma_i$, $h_i = h_i^1 \uplus h_i^2$, $[\![\gamma H]\!]\delta W(h_1^1, h_2^1)$, and $h_1^2, h_2^2 :_{\omega_2} W$.
- To show: $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- We know $\omega_1 = \{\iota_1, \ldots, \iota_n\}$ with $[\![p_i \propto a_i.(\gamma B_i, \gamma H_i)]\!]\delta W\{\iota_i\}$ for all i.
- Let $W' := (W.k, W.d, W.\varsigma_1, W.\varsigma_2, \mathcal{I})$, where

$$\begin{array}{ll}\mathrm{dom}(\mathcal{I}) = \mathrm{dom}(W.\mathcal{I}) & \\ \quad \mathcal{I}(\iota) := (\|\gamma A\|\delta, W.\mathcal{I}(\iota).PL, W.\mathcal{I}(\iota).HL) & \text{if } \iota \in \omega_1 \\ \quad \mathcal{I}(\iota) := W.\mathcal{I}(\iota) & \text{otherwise}\end{array}$$

- We show $W' \in \mathit{World}$:
  - It suffices to prove $\mathcal{I}(\iota_i).CP \in \mathcal{I}(\iota_i).PL$ for all i, *i.e.,* $\|\gamma A_i\|\delta \in W.\mathcal{I}(\iota_i).PL$.
  - Because of $[\![p_i \propto a_i.(\gamma B_i, \gamma H_i)]\!]\delta W\{\iota_i\}$, this reduces to showing $\|\gamma B_i\|(\delta, a_i \mapsto \|\gamma A_i\|\delta)$.
  - This follows from instantiating the assumption $\mathcal{C} \vdash \bigwedge \overline{B[A/a]}$ and Lemma 2.13.
- We show $W' \sqsupseteq W$:
  - It suffices to prove $\mathcal{I}(\iota_i).CP \supseteq W.\mathcal{I}(\iota_i).CP$ for all i, *i.e.,* $\|\gamma A_i\|\delta \supseteq W.\mathcal{I}(\iota_i).CP$.
  - From instantiating $\mathcal{C} \vdash \bigwedge \overline{p \subseteq A}$ we get $[\![p_i \subseteq \gamma A_i]\!]\delta W$.
  - Instantiating this with W yields $[\![p_i]\!]\delta W \subseteq [\![\gamma A_i]\!]\delta W$.
  - Note that $\delta(p_i) = \mathrm{pop}(\iota_i)$ and thus $[\![p_i]\!]\delta W = W.\mathcal{I}(\iota_i).CP$.
  - Finally, $[\![\gamma A_i]\!]\delta W = \|\gamma A_i\|\delta$ by Lemma 2.12.
- We show $(\gamma, \delta, W', \omega_1, \omega_2) \in [\![\mathcal{C}']\!]$:
  - It is easy to see that $[\![p_i \propto a_i.(\gamma B_i, \gamma H_i)]\!]\delta W'\{\iota_i\}$ holds for all i by construction of $\mathcal{I}$ in terms of $W.\mathcal{I}$.
  - Consequently, $[\![\gamma\mathcal{C}'.\mathcal{L}]\!]\delta W'\omega_1$.
  - Also, $[\![\gamma(\dagger\mathcal{C}.\mathcal{P})]\!]\delta W'$ follows from $[\![\gamma(\mathcal{C}.\mathcal{P})]\!]\delta W$, $W' \sqsupseteq W$, and Lemma 2.9.
  - It remains to show $[\![p_i \equiv \gamma A_i]\!]\delta W'$ (we show only one direction, the other is analogously):
    - Suppose $W'' \supseteq W'$ and $[\![p_i]\!]\delta W''\overline{e}$.
    - If $W''.k = 0$, there is nothing to show.
    - Otherwise, since $\delta(p_i) = \mathrm{pop}(\iota_i)$, this implies $\|\gamma A_i\|\delta\overline{e}$.

$*$ The latter is equivalent to $[\![\gamma A_i]\!]\delta W''\overline{e}$ by Lemma 2.12.

- We show $h_1, h_2 : W'$:
  - We prove $h_1^1, h_2^1 :_{\omega_1} W'$ and $h_1^2, h_2^2 :_{\omega_2} W'$, which, using the assumptions, implies the claim.
  - The second property follows from the given $h_1^2, h_2^2 :_{\omega_2} W$ by Lemma 2.14.
  - For the first property, note that $[\![\gamma H]\!]\delta W(h_1^1, h_2^1)$ with Lemma 2.10 and $\mathcal{C}' \vdash H \Rrightarrow * \overline{H[A/a]}$ imply the existence of $h_i^{1,1}, \ldots, h_i^{1,n}$ with $h_i^1 = h_i^{1,1} \uplus \cdots \uplus h_i^{1,n}$, such that $[\![\gamma(H_i[A_i/a_i])]\!]\delta W'(h_1^{1,i}, h_2^{1,i})$.
  - It suffices to show $(\triangleright W', h_1^{1,i}, h_2^{1,i}) \in W'.\mathcal{I}(\iota_i).HL(W'.\mathcal{I}(\iota_i).CP)$, *i.e.,* $(\triangleright W', h_1^{1,i}, h_2^{1,i}) \in W'.\mathcal{I}(\iota_i).HL(\|\gamma A_i\|\delta)$.
  - Due to $[\![p_i \propto a_i.(\gamma B_i, \gamma H_i)]\!]\delta W'\{\iota_i\}$ this reduces to showing $(\triangleright W').k < W'.k$, which is clear, and $[\![\gamma H_i]\!](\delta, a_i \mapsto \|\gamma A_i\|\delta)(\triangleleft\triangleright W')(h_1^{1,i}, h_2^{1,i})$.
  - This follows from $[\![\gamma(H_i[A_i/a_i])]\!]\delta W'(h_1^{1,i}, h_2^{1,i})$ by Lemmas 2.8 and 2.13.
- We now instantiate $\mathcal{C}' \vdash (e_1, e_2) \in \uparrow R$ to get $W' \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$.
- Finally, Lemma 2.11 yields the claim.

□

Theorem 2.65
The following rule is sound:

$$\frac{\mathcal{C} \vdash \{H\}\ e_1' \approx e_2'\ \{R\} \quad \mathcal{C} \vdash e_1 \rightsquigarrow^* e_1' \quad \mathcal{C} \vdash e_2 \rightsquigarrow^* e_2'}{\mathcal{C} \vdash \{H\}\ e_1 \approx e_2\ \{R\}}\ \text{EXPAND}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, $\vdash h_i$, $\mathrm{dom}(h_i) \supseteq W.\varsigma_i$, $h_i = h_i^1 \uplus h_i^2$, $[\![\gamma H]\!]\delta W(h_1^1, h_2^1)$, and $h_1^2, h_2^2 :_{\omega_2} W$.
- To show: $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- $\mathrm{FL}(\gamma e_i) \subseteq W.\varsigma_i$ follows from the implicit assumption $\mathcal{C} \vdash e_i \in \mathrm{Term}_i$.
- Now assume $W.d = \rightarrow$ (the other direction is analogously).
- Suppose $(h_1; \gamma e_1) \Downarrow^j (h_1'; e_1'')$ where $j < W.k$.
- Instantiating the first two premises yields $W \vdash (h_1; \gamma e_1') \approx (h_2; \gamma e_2') : [\![\gamma R]\!]\delta$ and $\gamma e_1 \rightsquigarrow^* \gamma e_1'$.
- The latter implies $(h_1; \gamma e_1) \overset{\epsilon}{\longmapsto}{}^{j_1} (h_1; \gamma e_1')$ for some j_1 and thus $(h_1; \gamma e_1') \Downarrow^{j-j_1} (h_1'; e_1'')$ and $j_1 \leq j$.
- Consequently, there is h_2', e_2'', W' such that:
  1. $W'.k = W.k - j + j_1$

2. $W' \sqsupseteq W$
3. $(h_2; \gamma e_2') \Downarrow (h_2'; e_2'')$
4. $[\![\gamma R]\!]\delta W'(e_1'', e_2'')$
5. $h_1', h_2' : W'$

- Instantiating the third premise yields $\gamma e_2 \rightsquigarrow^* \gamma e_2'$, which implies $(h_2; \gamma e_2) \overset{\epsilon}{\longmapsto}{}^* (h_2; \gamma e_2')$.
- Hence $(h_2; \gamma e_2) \Downarrow (h_2'; e_2'')$.
- Let $W'' := \underbrace{\triangleright \ldots \triangleright}_{j_1 \text{ times}} W'$, so:
  1. $W''.k = W'.k - j_1 = W.k - j$
  2. $W'' \sqsupseteq W$ by Lemma 2.2
  3. $[\![\gamma R]\!]\delta W''(e_1'', e_2'')$ by Lemma 2.2 and Lemma 2.17
  4. $h_1', h_2' : W''$ by Lemma 2.14

□

Theorem 2.66
The following rule is sound:

$$\frac{\mathcal{C} \vdash \{H\}\ e_1' \approx e_2'\ \{R\} \quad \mathcal{C} \vdash e_1' \rightsquigarrow^0 e_1 \quad \mathcal{C} \vdash e_2' \rightsquigarrow^0 e_2}{\mathcal{C} \vdash \{H\}\ e_1 \approx e_2\ \{R\}}\ \text{REDUCE}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, $\vdash h_i$, $\mathrm{dom}(h_i) \supseteq W.\varsigma_i$, $h_i = h_i^1 \uplus h_i^2$, $[\![\gamma H]\!]\delta W(h_1^1, h_2^1)$, and $h_1^2, h_2^2 :_{\omega_2} W$.
- To show: $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- $\mathrm{FL}(\gamma e_i) \subseteq W.\varsigma_i$ follows from the implicit assumption $\mathcal{C} \vdash e_i \in \mathrm{Term}_i$.
- Now assume $W.d = \rightarrow$ (the other direction is analogously).
- Suppose $(h_1; \gamma e_1) \Downarrow^j (h_1'; e_1'')$ where $j < W.k$.
- Instantiating the first two premises yields $W \vdash (h_1; \gamma e_1') \approx (h_2; \gamma e_2') : [\![\gamma R]\!]\delta$ and $\gamma e_1' \rightsquigarrow^0 \gamma e_1$.
- The latter implies $(h_1; \gamma e_1') \overset{\epsilon}{\longmapsto}{}^0 (h_1; \gamma e_1)$ and thus $(h_1; \gamma e_1') \Downarrow^j (h_1'; e_1'')$.
- Consequently, there is h_2', e_2'', W' such that:
  1. $W'.k = W'.k - j$
  2. $W' \sqsupseteq W$
  3. $(h_2; \gamma e_2') \Downarrow (h_2'; e_2'')$
  4. $[\![\gamma R]\!]\delta W'(e_1'', e_2'')$

5. $h_1', h_2' : W'$

- Instantiating the third premise yields $\gamma e_2' \rightsquigarrow^0 \gamma e_2$, which implies $(h_2; \gamma e_2') \xmapsto{\epsilon}{}^0 (h_2; \gamma e_2)$.
- Hence $(h_2; \gamma e_2) \Downarrow (h_2'; e_2'')$.

□

Theorem 2.67
The following rule is sound:

$$\frac{\mathcal{C} \vdash \{H\}\ e_1 \xmapsto{\mathcal{C}_1}{}_1\ e_1'\ \{H'\} \quad \mathcal{C}, \mathcal{C}_1 \vdash \{H'\}\ e_1' \approx e_2\ \{R\}}{\mathcal{C} \vdash \{H\}\ e_1 \approx e_2\ \{R\}}\ \text{STEP-L}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, $\vdash h_i$, $\mathrm{dom}(h_i) \supseteq W.\varsigma_i$, $h_i = h_i^1 \uplus h_i^2$, $[\![\gamma H]\!]\delta W(h_1^1, h_2^1)$ and $h_1^2, h_2^2 :_{\omega_2} W$.
- To show: $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- $\mathrm{FL}(\gamma e_i) \subseteq W.\varsigma_i$ follows from the implicit assumption $\mathcal{C} \vdash e_i \in \mathrm{Term}_i$.
- Case $W.d = \rightarrow$:
  - From the first premise we know $\mathcal{C}_1 = \overline{x, x \in \mathrm{Val}_1}$.
  - Suppose $(h_1; \gamma e_1) \Downarrow^j (h_1''; e_1'')$ with $j < W.k$, *i.e.*, $(h_1; \gamma e_1) \xmapsto{\bar{l} \ldots}{}^j (h_1''; e_1'')$.
  - Instantiate the first premise with h_i^1 and $\bar{l}$ to get $h_1^{1'}$ with
    - $(h_1^1; \gamma e_1) \xmapsto{\bar{l}}{}^1 (h_1^{1'}; \gamma' e_1')$ and
    - $[\![\gamma' H']\!]\delta W'(h_1^{1'}, h_2^1)$, where
    - $\gamma' := \gamma, \overline{x \mapsto l}$ and
    - $W' := W[\varsigma_1 := W.\varsigma_1 \uplus \{\bar{l}\}]$, so $W' \supseteq W$.
  - Note that $(h_1^1; \gamma e_1) \xmapsto{\bar{l}}{}^1 (h_1^{1'}; \gamma' e_1')$ implies $(h_1; \gamma e_1) \xmapsto{\bar{l}}{}^1 (h_1^{1'} \uplus h_1^2; \gamma' e_1')$.
  - This also means $j \geq 1$ and thus $W'.k > 1$.
  - We show $(\gamma', \delta, \triangleright W', \omega_1, \omega_2) \in [\![\mathcal{C}, \overline{x, x \in \mathrm{Val}_1}]\!]$:
    - This reduces to showing $[\![\gamma(\mathcal{C}.\mathcal{L})]\!]\delta(\triangleright W')\omega_1$ and $[\![\gamma(\mathcal{C}.\mathcal{P}), \overline{l \in \mathrm{Val}_1}]\!]\delta(\triangleright W')$.
    - The former follows from $[\![\gamma(\mathcal{C}.\mathcal{L})]\!]\delta W \omega_1$, Lemma 2.2, and Lemma 2.15.
    - The latter follows from $[\![\gamma(\mathcal{C}.\mathcal{P})]\!]\delta W$, Lemma 2.2, Lemma 2.17, and the construction of W'.
  - Instantiating the second premise now yields $\triangleright W' \vdash (h_1^{1'} \uplus h_1^2; \gamma' e_1') \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$.
  - Since $(h_1; \gamma e_1) \xmapsto{\overline{l_1 \ldots} j} (h_1''; e_1'')$, this implies $(h_1^{1'} \uplus h_1^2; \gamma' e_1') \xmapsto{\ldots}{}^{j-1} (h_1''; e_1'')$
  - Consequently, because $j - 1 < (\triangleright W').k$, there is h_2'', e_2'', W'' with:
    1. $W''.k = (\triangleright W').k - j + 1\ (= W.k - j)$

2. $W'' \sqsupseteq \triangleright W'$ $(\sqsupseteq W' \sqsupseteq W)$
3. $(h_2; \gamma e_2) \Downarrow (h_2''; e_2'')$
4. $[\![\gamma R]\!] \delta W''(e_1'', e_2'')$
5. $h_1'', h_2'' : W''$

- Case $W.d = \leftarrow$:
  - Suppose $(h_2; \gamma e_2) \Downarrow^j (h_2''; e_2'')$ with $j < W.k$.
  - Instantiate the first premise with h_i^1 and fresh $\bar{l}$ to get $h_1^{1'}$ with
    - $(h_1^1; \gamma e_1) \overset{\bar{l}}{\longmapsto}^1 (h_1^{1'}; \gamma' e_1')$ and
    - $[\![\gamma' H']\!] \delta W'(h_1^{1'}, h_1^1)$, where
    - $\gamma' := \gamma, \overline{x \mapsto l}$ and
    - $W' := W[\varsigma_1 := W.\varsigma_1 \uplus \{\bar{l}\}]$.
  - It is easy to see that $(\gamma', \delta, W', \omega_1, \omega_2) \in [\![\mathcal{C}, \overline{x, x \in \mathrm{Val}_1}]\!]$.
  - Instantiating the second premise now yields $W' \vdash (h_1^{1'} \uplus h_1^2; \gamma' e_1') \approx (h_2; \gamma e_2) : [\![\gamma R]\!] \delta$.
  - Consequently, because $j < W'.k$, there is h_1'', e_1'', W'' with:
    1. $W''.k = W'.k - j$ $(= W.k - j)$
    2. $W'' \sqsupseteq W'$ $(\sqsupseteq W)$
    3. $(h_1^{1'} \uplus h_1^2; \gamma' e_1') \Downarrow (h_1''; e_1'')$
    4. $[\![\gamma R]\!] \delta W''(e_1'', e_2'')$
    5. $h_1'', h_2'' : W''$
  - It remains to show $(h_1; \gamma e_1) \Downarrow (h_1''; e_1'')$.
  - This follows since $(h_1^1; \gamma e_1) \overset{\bar{l}}{\longmapsto}^1 (h_1^{1'}; \gamma' e_1')$ implies $(h_1; \gamma e_1) \overset{\bar{l}}{\longmapsto}^1 (h_1^{1'} \uplus h_1^2; \gamma' e_1')$.

□

Theorem 2.68
The following rule is sound:

$$\frac{\mathcal{C} \vdash \{H\}\ e_2 \overset{\mathcal{C}_2}{\longmapsto}_2 e_2'\ \{H'\} \quad \mathcal{C}, \mathcal{C}_2 \vdash \{H'\}\ e_1 \approx e_2'\ \{R\}}{\mathcal{C} \vdash \{H\}\ e_1 \approx e_2\ \{R\}}\ \textsc{step-r}$$

Proof: Symmetric to rule STEP-L. □

Theorem 2.69
The following rule is sound:

$$\frac{\mathcal{C} \vdash \{H_1\}\ e_1 \overset{\mathcal{C}_1}{\longmapsto}_1 e_1'\ \{H_1'\} \quad \mathcal{C} \vdash \{H_2\}\ e_2 \overset{\mathcal{C}_2}{\longmapsto}_2 e_2'\ \{H_2'\} \quad \triangleleft \mathcal{C}, \mathcal{C}_1, \mathcal{C}_2 \vdash \{H_1' * H_2'\}\ e_1' \approx e_2'\ \{R\}}{\mathcal{C} \vdash \{H_1 * H_2\}\ e_1 \approx e_2\ \{R\}}\ \textsc{step-lr}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, $\vdash h_i$, $\mathrm{dom}(h_i) \supseteq W.\varsigma_i$, $h_i = h_i^1 \uplus h_i^2$, $[\![\gamma H_1 * \gamma H_2]\!] \delta W(h_1^1, h_2^1)$ and $h_1^2, h_2^2 :_{\omega_2} W$.

- To show: $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- $\mathrm{FL}(\gamma e_i) \subseteq W.\varsigma_i$ follows from the implicit assumption $\mathcal{C} \vdash e_i \in \mathrm{Term}_i$.
- From $[\![\gamma H_1 * \gamma H_2]\!]\delta W(h_1^1, h_2^1)$ we know that there is $h_i^{1,1}$ and $h_i^{1,2}$ with $h_i^1 = h_i^{1,1} \uplus h_i^{1,2}$ such that $[\![\gamma H_i]\!]\delta W(h_1^{1,i}, h_2^{1,i})$.
- Assume $W.d = \rightarrow$ (the other direction is analogously).
- From the first premise we know $\mathcal{C}_1 = \overline{x_1, x_1 \in \mathrm{Val}_1}$.
- Suppose $(h_1; \gamma e_1) \Downarrow^j (h_1''; e_1'')$ with $j < W.k$, *i.e.,* $(h_1; \gamma e_1) \overset{\overline{l_1} \ldots}{\longmapsto}{}^j (h_1''; e_1'')$.
- Instantiate the first premise with $h_i^{1,1}$ and $\overline{l_1}$ to get $h_1^{1,1'}$ with
  - $(h_1^{1,1}; \gamma e_1) \overset{\overline{l_1}}{\longmapsto}{}^1 (h_1^{1,1'}; \gamma_1 e_1')$ and
  - $[\![\gamma_1 H_1']\!]\delta W_1(h_1^{1,1'}, h_2^{1,1})$, where
  - $\gamma_1 := \gamma, \overline{x_1 \mapsto l_1}$ and
  - $W_1 := W[\varsigma_1 := W.\varsigma_1 \uplus \{\overline{l_1}\}]$.
- From the second premise we know $\mathcal{C}_2 = \overline{x_2, x_2 \in \mathrm{Val}_2}$.
- Instantiate the second premise with $h_i^{1,2}$ and fresh $\overline{l_2}$ to get $h_2^{1,2'}$ with
  - $(h_2^{1,2}; \gamma e_2) \overset{\overline{l_2}}{\longmapsto}{}^1 (h_2^{1,2'}; \gamma_2 e_2')$ and
  - $[\![\gamma_2 H_2']\!]\delta W_2(h_1^{1,2}, h_2^{1,2'})$, where
  - $\gamma_2 := \gamma, \overline{x_2 \mapsto l_2}$ and
  - $W_2 := W[\varsigma_2 := W.\varsigma_2 \uplus \{\overline{l_2}\}]$.
- Let $\gamma' := \gamma, \overline{x_1 \mapsto l_1}, \overline{x_2 \mapsto l_2}$ and $W' := \triangleright(W.k, W.d, W_1.\varsigma_1, W_2.\varsigma_2, W.\mathcal{I})$.
- It is easy to see that $W' \in \mathit{World}$ and $W' \supseteq \triangleright W$.
- We show $(\gamma', \delta, W', \omega_1, \omega_2) \in [\![\triangleleft\mathcal{C}, \overline{x_1, x_1 \in \mathrm{Val}_1}, \overline{x_2, x_2 \in \mathrm{Val}_2}]\!]$:
  - This reduces to showing $[\![\gamma(\mathcal{C}.\mathcal{L})]\!]\delta W'\omega_1$ and $[\![\triangleleft\gamma(\mathcal{C}.\mathcal{P}), \overline{l_1 \in \mathrm{Val}_1}, \overline{l_2 \in \mathrm{Val}_2}]\!]\delta W'$.
  - The former follows from $[\![\gamma(\mathcal{C}.\mathcal{L})]\!]\delta W\omega_1$, Lemma 2.2, and Lemma 2.15.
  - The latter follows from $[\![\gamma(\mathcal{C}.\mathcal{P})]\!]\delta W$, Lemma 2.18, Lemma 2.2, Lemma 2.17, and the construction of W'.
- Let $h_1' := h_1^{1,1'} \uplus h_1^{1,2} \uplus h_1^2$ and $h_2' := h_2^{1,1} \uplus h_2^{1,2'} \uplus h_2^2$.
- From $h_1^2, h_2^2 :_{\omega_2} W$ we get $h_1^2, h_2^2 :_{\omega_2} W'$ by Lemma 2.14.
- Note that $(h_1^{1,1}; \gamma e_1) \overset{\overline{l_1}}{\longmapsto}{}^1 (h_1^{1,1'}; \gamma_1 e_1')$ implies $(h_1; \gamma e_1) \overset{\overline{l_1}}{\longmapsto}{}^1 (h_1'; \gamma' e_1')$.
- Consequently, $W.k > 1$ and thus $W'.k > 0$.

- Furthermore we have $[\![\gamma' H_1' * \gamma' H_2']\!]\delta W'(h_1^{1,1'} \uplus h_1^{1,2}, h_2^{1,1} \uplus h_2^{1,2'})$ due to $W' \sqsupseteq W_i$ and Lemma 2.10.
- It is also easy to see that $\vdash h_i'$ and $\mathrm{dom}(h_i') \supseteq W'.\varsigma_i$.
- Hence we can instantiate the third premise to get $W' \vdash (h_1'; \gamma' e_1') \approx (h_2'; \gamma' e_2') : [\![\gamma R]\!]\delta$.
- We know that $(h_1'; \gamma' e_1') \overset{\cdots}{\longmapsto}^{j-1} (h_1''; e_1'')$.
- Consequently, because $j - 1 < W'.k$, there is h_2'', e_2'', W'' with:
  1. $W''.k = W'.k - j + 1$ $(= W.k - j)$
  2. $W'' \sqsupseteq W'$ $(\sqsupseteq W)$
  3. $(h_2'; \gamma' e_2') \Downarrow (h_2''; e_2'')$
  4. $[\![\gamma R]\!]\delta W''(e_1'', e_2'')$
  5. $h_1'', h_2'' : W''$
- It remains to show $(h_2; \gamma e_2) \Downarrow (h_2''; e_2'')$.
- This follows since $(h_2^{1,2}; \gamma e_2) \overset{\overline{l_2}}{\longmapsto}^1 (h_2^{1,2'}; \gamma_2 e_2')$ implies $(h_2; \gamma e_2) \overset{\overline{l_2}}{\longmapsto}^1 (h_2'; \gamma_2 e_2')$

□

Theorem 2.70
The following rule is sound:

$$\frac{\mathcal{C} \vdash H \Rrightarrow H' \quad \mathcal{C} \vdash \{H'\}\ e_1 \approx e_2\ \{R\}}{\mathcal{C} \vdash \{H\}\ e_1 \approx e_2\ \{R\}}\ \textsc{sep-entail}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, $\vdash h_i$, $\mathrm{dom}(h_i) \supseteq W.\varsigma_i$, $h_i = h_i^1 \uplus h_i^2$, $[\![\gamma H]\!]\delta W(h_1^1, h_2^1)$, and $h_1^2, h_2^2 :_{\omega_2} W$.
- To show: $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- Instantiating the first premise yields $[\![\gamma H']\!]\delta W(h_1^1, h_2^1)$.
- Hence we can instantiate the second premise and get $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$.

□

Theorem 2.71
The following rule is sound:

$$\frac{\mathcal{C} \vdash \Box P \quad \mathcal{C} \vdash \{H * \Box P\}\ e_1 \approx e_2\ \{R\}}{\mathcal{C} \vdash \{H\}\ e_1 \approx e_2\ \{R\}}\ \textsc{sep-cut}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, $\vdash h_i$, $\mathrm{dom}(h_i) \supseteq W.\varsigma_i$, $h_i = h_i^1 \uplus h_i^2$, $[\![\gamma H]\!]\delta W(h_1^1, h_2^1)$, and $h_1^2, h_2^2 :_{\omega_2} W$.

- To show: $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- Instantiating the first premise yields $[\![\Box\gamma P]\!]\delta W$.
- Consequently, we have $[\![\gamma H * \Box\gamma P]\!]\delta W(h_1^1, h_2^1)$.
- Now instantiate the second premise to get $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$.

□

Theorem 2.72
The following rule is sound:

$$\frac{\mathcal{C}, \Box P \vdash \{H\}\ e_1 \approx e_2\ \{R\}}{\mathcal{C} \vdash \{H * \Box P\}\ e_1 \approx e_2\ \{R\}}\ \Box\text{-SHIFT}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, $\vdash h_i$, $\mathrm{dom}(h_i) \supseteq W.\varsigma_i$, $h_i = h_i^1 \uplus h_i^2$, $[\![\gamma H * \Box\gamma P]\!]\delta W(h_1^1, h_2^1)$, and $h_1^2, h_2^2 :_{\omega_2} W$.
- To show: $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- From $[\![\gamma H * \Box\gamma P]\!]\delta W(h_1^1, h_2^1)$ we get $[\![\gamma H]\!]\delta W(h_1^1, h_2^1)$ (using Lemma 2.16) and $[\![\Box\gamma P]\!]\delta W$.
- The latter implies that $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}, \Box P]\!]$.
- Hence we can instantiate the premise to get $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$.

□

Theorem 2.73
The following rule is sound:

$$\frac{\mathcal{C} \vdash \{H_1\}\ e_1 \approx e_2\ \{R\} \quad \mathcal{C} \vdash \{H_2\}\ e_1 \approx e_2\ \{R\}}{\mathcal{C} \vdash \{H_1 \vee H_2\}\ e_1 \approx e_2\ \{R\}}\ \text{SEP-}\vee$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, $\vdash h_i$, $\mathrm{dom}(h_i) \supseteq W.\varsigma_i$, $h_i = h_i^1 \uplus h_i^2$, $[\![\gamma H_1 \vee \gamma H_2]\!]\delta W(h_1^1, h_2^1)$, and $h_1^2, h_2^2 :_{\omega_2} W$.
- To show: $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- From $[\![\gamma H_1 \vee \gamma H_2]\!]\delta W(h_1^1, h_2^1)$ we know that $[\![\gamma H_1]\!]\delta W(h_1^1, h_2^1)$ or $[\![\gamma H_2]\!]\delta W(h_1^1, h_2^1)$ holds.
- Instantiating the according premise yields $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$.

□

Theorem 2.74
The following rule is sound:

$$\frac{\mathcal{C}, \mathcal{X} \vdash \{H\}\ e_1 \approx e_2\ \{R\}}{\mathcal{C} \vdash \{\exists \mathcal{X}.H\}\ e_1 \approx e_2\ \{R\}}\ \text{SEP-}\exists$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, $\vdash h_i$, $\mathrm{dom}(h_i) \supseteq W.\varsigma_i$, $h_i = h_i^1 \uplus h_i^2$, $[\![\exists \mathcal{X}.\gamma H]\!]\delta W(h_1^1, h_2^1)$, and $h_1^2, h_2^2 :_{\omega_2} W$.
- To show: $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$
- From $[\![\exists \mathcal{X}.\gamma H]\!]\delta W(h_1^1, h_2^1)$ we know that there is $\gamma' : \mathcal{X}$ such that $[\![(\gamma, \gamma')H]\!]\delta W(h_1^1, h_2^1)$.
- Hence it is easy to see that $((\gamma, \gamma'), \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}, \mathcal{X}]\!]$.
- Instantiating the premise then yields $W \vdash (h_1; \gamma e_1) \approx (h_2; \gamma e_2) : [\![\gamma R]\!]\delta$.

□

Theorem 2.75
The following rule is sound:

$$\frac{\mathcal{C} \vdash e \rightsquigarrow^1 e'}{\mathcal{C} \vdash \{H\}\ e \longmapsto_i e'\ \{H\}}\ \textsc{unroll}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, and $[\![\gamma H]\!]\delta W(h_1, h_2)$.
- Instantiating the premise yields $\left[\!\left[\gamma e \rightsquigarrow^1 \gamma e'\right]\!\right]\delta W$.
- Hence we know $\gamma e \rightsquigarrow^1 \gamma e'$, which implies $(h_1; \gamma e) \overset{\epsilon}{\longmapsto}{}^1 (h_1; \gamma e')$.

□

Theorem 2.76
The following rule is sound:

$$\frac{\mathcal{C} \vdash e \in \mathrm{Val}_i \quad \mathcal{C} \vdash A \subseteq \mathrm{Val}_i \quad \mathcal{C}' = x, x \in \mathrm{Val}_i}{\mathcal{C} \vdash \{H\}\ E[\mathsf{ref}\ e] \overset{\mathcal{C}'}{\longmapsto}_i E[x]\ \{H * x \hookrightarrow_i e * \Box(x \notin A)\}}\ \textsc{alloc}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, and $[\![\gamma H]\!]\delta W(h_1, h_2)$.
- Instantiating the first premise yields that γe is a value.
- Now suppose $l \notin \mathrm{dom}(h_i) \cup W.\varsigma_i$.
- Consequently, $(h_i; \gamma(E[\mathsf{ref}\ e])) \overset{l}{\longmapsto}{}^1 (h_i \uplus \{l \mapsto \gamma e\}; \gamma E[l])$.
- Let $\hat{h}_i := h_i \uplus \{l \mapsto \gamma e\}$ and $\hat{h}_{\neg i} = h_{\neg i}$.
- It remains to show $[\![\gamma H * l \hookrightarrow_i \gamma e * \Box(l \notin \gamma A)]\!]\delta W'(\hat{h}_1, \hat{h}_2)$, where $W' = W[\varsigma_i := W.\varsigma_i \uplus \{l\}]$.
- From $[\![\gamma H]\!]\delta W(h_1, h_2)$ we get $[\![\gamma H]\!]\delta W'(h_1, h_2)$ by Lemma 2.10.
- Is is also clear that we have $[\![l \hookrightarrow_i \gamma e]\!]\delta W'(\{l \mapsto \gamma e\}, \emptyset)$.

- Hence it remains to show $[\![\Box(l \notin \gamma A)]\!]\delta W'(\emptyset, \emptyset)$, *i.e.,* $[\![\Box(l \notin \gamma A)]\!]\delta W'$.
- So suppose $W'' \sqsupseteq W'$ and $W''.k > 0$ (otherwise there is nothing to show).
- Now suppose $W''' \supseteq W''$ and $[\![l \in \gamma A]\!]\delta W'''$.
- If $W'''.k = 0$, there is nothing to show.
- Otherwise we know $\|l \in \gamma A\|\delta$ and thus $[\![l \in \gamma A]\!]\delta W$ by Lemma 2.12, and need to derive a contradiction.
- From instantiating the second premise with we get $[\![l \in \mathrm{Val}_i]\!]\delta W$ and thus $l \in W.\varsigma_i$.
- This contradicts $l \notin \mathrm{dom}(h_i) \cup W.\varsigma_i$.

□

Theorem 2.77
The following rule is sound:

$$\frac{\mathcal{C} \vdash H \Rrightarrow e_1 \hookrightarrow_i e_2}{\mathcal{C} \vdash \{H\}\ E[!e_1] \longmapsto_i E[e_2]\ \{H\}}\ \textsc{deref}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, and $[\![\gamma H]\!]\delta W(h_1, h_2)$.
- Instantiating the premise yields $[\![\gamma e_1 \hookrightarrow_i \gamma e_2]\!]\delta W(h_1, h_2)$.
- Hence $h_i(\gamma e_1) = \gamma e_2$ and γe_2 is a value.
- Consequently, $(h_i; \gamma(E[!e_1])) \overset{\epsilon}{\longmapsto}{}^1 (h_i; \gamma(E[e_2]))$.

□

Theorem 2.78
The following rule is sound:

$$\frac{\mathcal{C} \vdash e_2 \in \mathrm{Val}_i}{\mathcal{C} \vdash \{H * e_1 \hookrightarrow_i e_2'\}\ E[e_1 := e_2] \longmapsto_i E[\langle\rangle]\ \{H * e_1 \hookrightarrow_i e_2\}}\ \textsc{assign}$$

Proof:

- Suppose $(\gamma, \delta, W, \omega_1, \omega_2) \in [\![\mathcal{C}]\!]$, $W.k > 0$, and $[\![\gamma H * \gamma e_1 \hookrightarrow_i \gamma e_2']\!]\delta W(h_1, h_2)$.
- From $[\![\gamma H * \gamma e_1 \hookrightarrow_i \gamma e_2']\!]\delta W(h_1, h_2)$ we know $[\![\gamma H]\!]\delta W(h_1^1, h_2^1)$ and $[\![\gamma e_1 \hookrightarrow_i \gamma e_2']\!]\delta W(h_1^2, h_2^2)$, where $h_i = h_i^1 \uplus h_i^2$.
- Hence $[\![\gamma e_1 \in \mathrm{Val}_i]\!]\delta W$ and $\gamma e_1 \in \mathrm{dom}(h_i^2) \subseteq \mathrm{dom}(h_i)$.
- Instantiating the premise yields $[\![\gamma e_2 \in \mathrm{Val}_i]\!]\delta W$, so γe_2 is a value.
- Consequently, $(h_i; \gamma(E[e_1 := e_2])) \overset{\epsilon}{\longmapsto}{}^1 (h_i[\gamma e_1 \mapsto \gamma e_2]; \gamma E[\langle\rangle])$.

- Let $\hat{h}_i := h_i[\gamma e_1 \mapsto \gamma e_2]$ and $\hat{h}_{\neg i} := h_{\neg i}$.
- It remains to show $[\![\gamma H * \gamma e_1 \hookrightarrow_i \gamma e_2]\!]\delta W(\hat{h}_1, \hat{h}_2)$.
- Note that $\hat{h}_i = h_i^1 \uplus h_i^2[\gamma e_1 \mapsto \gamma e_2]$.
- Let $\hat{h}_i^2 := h_i^2[\gamma e_1 \mapsto \gamma e_2]$ and $\hat{h}_{\neg i}^2 := h_{\neg i}^2$, so $\hat{h}_i = h_i^1 \uplus \hat{h}_i^2$.
- Hence it suffices to show $[\![\gamma e_1 \hookrightarrow_i \gamma e_2]\!]\delta W(\hat{h}_1^2, \hat{h}_2^2)$, which follows from $[\![\gamma e_1 \in \mathrm{Val}_i]\!]\delta W$, $[\![\gamma e_2 \in \mathrm{Val}_i]\!]\delta W$, and $\hat{h}_i^2 = h_i^2[\gamma e_1 \mapsto \gamma e_2]$.

□

3 Soundness of the Logical Relation

Lemma 3.1
If $\mathcal{C} \vdash \rho(\alpha) : \mathrm{VRel}$ for all $\alpha \in \mathrm{dom}(\rho)$, then $\mathcal{C} \vdash \mathcal{V}[\![\tau]\!]\rho : \mathrm{VRel}$.

Lemma 3.2
If $\mathcal{C} \vdash \rho(\alpha) : \mathrm{Type}$ for all $\alpha \in \mathrm{dom}(\rho)$, then $\mathcal{C} \vdash \mathcal{V}[\![\tau]\!]\rho : \mathrm{Type}$.

Corollary 3.3
If $\mathcal{C} \vdash (v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$ and $\mathcal{C} \vdash \rho(\alpha) : \mathrm{Type}$ for all $\alpha \in \mathrm{dom}(\rho)$, then $\mathcal{C} \vdash \Box(v_1, v_2) \in \mathcal{V}[\![\tau]\!]\rho$.

Lemma 3.4 (Compatibility: Abstraction)
If $\dagger\mathcal{C}, x_1, x_2, (x_1, x_2) \in \mathcal{V}[\![\tau]\!]\rho \vdash (e_1, e_2) \in \mathcal{E}[\![\tau']\!]\rho$ and $\mathcal{C} \vdash \rho(\alpha) : \mathrm{Type}$ for all $\alpha \in \mathrm{dom}(\rho)$, then $\mathcal{C} \vdash (\lambda x_1{:}\gamma_1(\tau).e_1, \lambda x_2{:}\gamma_2(\tau).e_2) \in \mathcal{E}[\![\tau \to \tau']\!]\rho$.

Proof: By rule $\uparrow$-RETURN it suffices to show $\mathcal{C} \vdash (\lambda x_1{:}\gamma_1(\tau).e_1, \lambda x_2{:}\gamma_2(\tau).e_2) \in \mathcal{V}[\![\tau \to \tau']\!]\rho$. This means showing $\mathcal{C} \vdash \lambda x_i{:}\gamma_i(\tau).e_i \in \mathrm{Val}_i$ (for $i \in \{1,2\}$) and $\mathcal{C} \vdash \Box(\forall x_1, x_2.\ (x_1, x_2) \in \mathcal{V}[\![\tau]\!]\rho \Rightarrow ((\lambda x_1{:}\gamma_1(\tau).e_1)\, x_1, (\lambda x_2{:}\gamma_2(\tau).e_2)\, x_2) \in \mathcal{E}[\![\tau']\!]\rho)$. The former follows from the implicit assumption $\mathcal{C} \vdash \lambda x_i{:}\gamma_i(\tau).e_i \in \mathrm{Term}_i$. The latter reduces by rule $\Box$-INTRO to showing $\mathcal{C}_1 \vdash ((\lambda x_1{:}\gamma_1(\tau).e_1)\, x_1, (\lambda x_2{:}\gamma_2(\tau).e_2)\, x_2) \in \mathcal{E}[\![\tau']\!]\rho$, where $\mathcal{C}_1 = \dagger\mathcal{C}, x_1, x_2, (x_1, x_2) \in \mathcal{V}[\![\tau]\!]\rho$. Since we know $\mathcal{C}_1 \vdash x_i \in \mathrm{Val}_i$ and thus $\mathcal{C}_1 \vdash (\lambda x_i{:}\gamma_i(\tau).e_i)\, x_i \rightsquigarrow^* e_i$ for $i \in \{1,2\}$, this follows from the assumption by rule $\uparrow$-EXPAND. $\Box$

Lemma 3.5 (Compatibility: Instantiation)
If $\mathcal{C} \vdash (e_1, e_2) \in \mathcal{E}[\![\forall\alpha.\,\tau]\!]\rho$ and $\mathcal{C} \vdash \rho(\alpha) : \mathrm{Type}$ for all $\alpha \in \mathrm{dom}(\rho)$, then $\mathcal{C} \vdash (e_1\, \gamma_1(\tau'), e_2\, \gamma_2(\tau')) \in \mathcal{E}[\![\tau[\tau'/\alpha]]\!]\rho$.

Proof: By rule $\uparrow$-BIND it suffices to show $\mathcal{C}_1 \vdash (x_1\, \gamma_1(\tau'), x_2\, \gamma_2(\tau') \in \mathcal{E}[\![\tau[\tau'/\alpha]]\!]\rho$, where $\mathcal{C}_1 = \dagger\mathcal{C}, x_1, x_2, (x_1, x_2) \in \mathcal{V}[\![\forall\alpha.\,\tau]\!]\rho$. Unfolding the definition of $\mathcal{V}[\![\forall\alpha.\,\tau]\!]\rho$ and using rule $\Box$-ELIM lets us extend $\mathcal{C}_1$ to $\mathcal{C}_2 := \mathcal{C}_1, (x_1\, \gamma_1(\tau'), x_2\, \gamma_2(\tau')) \in \mathcal{E}[\![\tau]\!](\rho, \alpha{\mapsto}\mathcal{V}[\![\tau']\!]\rho)$. By Lemma 2.13 we are done. $\Box$

Lemma 3.6 (Compatibility: Unpack)
If $\dagger\mathcal{C}, \alpha_1, \alpha_2, r, r : \mathrm{Type}, x_1, x_2, (x_1, x_2) \in \mathcal{V}[\![\tau]\!](\rho, \alpha{\mapsto}r) \vdash (e_1', e_2') \in \mathcal{E}[\![\tau']\!]\rho$ and $\mathcal{C} \vdash (e_1, e_2) \in \mathcal{E}[\![\exists\alpha.\,\tau]\!]\rho$ and $\mathcal{C} \vdash \rho(\alpha) : \mathrm{Type}$ for all $\alpha \in \mathrm{dom}(\rho)$, then
$\mathcal{C} \vdash (\mathsf{unpack}\, e_1\, \mathsf{as}\, \alpha_1, x_1\, \mathsf{in}\, e_1', \mathsf{unpack}\, e_2\, \mathsf{as}\, \alpha_2, x_2\, \mathsf{in}\, e_2') \in \mathcal{E}[\![\tau']\!]\rho$.

Proof: By rule $\uparrow$-BIND it suffices to show $\mathcal{C}_1 \vdash (\mathsf{unpack}\, x_1'\, \mathsf{as}\, \alpha_1, x_1\, \mathsf{in}\, e_1', \mathsf{unpack}\, x_2'\, \mathsf{as}\, \alpha_2, x_2\, \mathsf{in}\, e_2') \in \mathcal{E}[\![\tau']\!]\rho$, where $\mathcal{C}_1 = \dagger\mathcal{C}, x_1', x_2', (x_1', x_2') \in \mathcal{V}[\![\exists\alpha.\,\tau]\!]\rho$. Unfolding the definition of $\mathcal{V}[\![\exists\alpha.\,\tau]\!]\rho$ lets us extend $\mathcal{C}_1$ to $\mathcal{C}_2 := \mathcal{C}_1, x_1' \in \mathrm{Val}_1, x_2' \in \mathrm{Val}_2, \alpha_1, \alpha_2, \alpha_1', \alpha_2', x_1, x_2, r, r : \mathrm{Type}, x_1' = (\mathsf{pack}\, \alpha_1, x_1\, \mathsf{as}\, \alpha_1'), x_2' = (\mathsf{pack}\, \alpha_2, x_2\, \mathsf{as}\, \alpha_2'), (x_1, x_2) \in \mathcal{V}[\![\tau]\!](\rho, \alpha{\mapsto}r)$. Note that we have $\mathcal{C}_2 \vdash x_i \in \mathrm{Val}_i$ and thus $\mathcal{C}_2 \vdash \mathsf{unpack}\, x_i'\, \mathsf{as}\, \alpha_i, x_i\, \mathsf{in}\, e_i' \rightsquigarrow^* e_i'$ for $i \in \{1,2\}$. Hence by rule $\uparrow$-EXPAND it suffices to show $\mathcal{C}_2 \vdash (e_1', e_2') \in \mathcal{E}[\![\tau']\!]\rho$, which follows from the assumption. $\Box$

Lemma 3.7 (Compatibility: Unroll)
If $\mathcal{C} \vdash (e_1, e_2) \in \mathcal{E}[\![\mu\alpha.\,\tau]\!]$ and $\mathcal{C} \vdash \rho(\alpha) : \mathrm{Type}$ for all $\alpha \in \mathrm{dom}(\rho)$, then $\mathcal{C} \vdash (\mathsf{unroll}\, e_1, \mathsf{unroll}\, e_2) \in \mathcal{E}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$.

Proof: By rule ↑-BIND it suffices to show $\mathcal{C}_1 \vdash (\mathsf{unroll}\, x_1, \mathsf{unroll}\, x_2) \in \mathcal{E}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$, where $\mathcal{C}_1 = \dagger\mathcal{C}, x_1, x_2, (x_1, x_2) \in \mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho$. Unfolding the definition of $\mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho$ lets us extend $\mathcal{C}_1$ to $\mathcal{C}_2 := \mathcal{C}_1, x_1 \in \mathrm{Val}_1, x_2 \in \mathrm{Val}_2, y_1, y_2, x_1 = \mathsf{roll}\, y_1, x_2 = \mathsf{roll}\, y_2, \triangleright(y_1, y_2) \in \mathcal{V}[\![\tau]\!](\rho, \alpha{\mapsto}\mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho)$. Note that we have $\mathcal{C}_2 \vdash y_i \in \mathrm{Val}_i$ and thus $\mathcal{C}_2 \vdash \mathsf{unroll}\, x_i \rightsquigarrow^1 y_i$ for $i \in \{1, 2\}$. Hence by rules ↑-UNROLL and ↑-RETURN it suffices to show $\triangleleft\mathcal{C}_2 \vdash (y_1, y_2) \in \mathcal{V}[\![\tau[\mu\alpha.\tau/\alpha]]\!]\rho$, which follows by Lemma 2.13 since $\triangleleft\mathcal{C}_2$ contains $(y_1, y_2) \in \mathcal{V}[\![\tau]\!](\rho, \alpha{\mapsto}\mathcal{V}[\![\mu\alpha.\,\tau]\!]\rho)$. □

Lemma 3.8 (Compatibility: Allocation)
If $\mathcal{C} \vdash (e_1, e_2) \in \mathcal{E}[\![\tau]\!]\rho$ and $\mathcal{C} \vdash \rho(\alpha) : \mathrm{Type}$ for all $\alpha \in \mathrm{dom}(\rho)$, then $\mathcal{C} \vdash (\mathsf{ref}\, e_1, \mathsf{ref}\, e_2) \in \mathcal{E}[\![\mathsf{ref}\, \tau]\!]\rho$.

Proof: We show $\mathcal{C}_0 \vdash (e_1, e_2) \in \mathcal{E}[\![\tau]\!]\rho \Rightarrow (\mathsf{ref}\, e_1, \mathsf{ref}\, e_2) \in \mathcal{E}[\![\mathsf{ref}\, \tau]\!]\rho$, where $\mathcal{C}_0 = \mathcal{C}.\mathcal{X}; \mathcal{C}.\mathcal{R}; \cdot; \mathcal{C}.\mathcal{P}$. The original claim then follows by rules $\mathcal{L}$-WEAKEN and ⇒-ELIM. Starting with rule ↑-BIND, we need to show $\mathcal{C}_1 \vdash (\mathsf{ref}\, x_1, \mathsf{ref}\, x_2) \in \mathcal{E}[\![\mathsf{ref}\, \tau]\!]\rho$, where $\mathcal{C}_1 = \dagger\mathcal{C}_0, x_1, x_2, (x_1, x_2) \in \mathcal{V}[\![\tau]\!]\rho$. Using rule ↑-IMPURE, we enter the separation judgment and are required to show $\{\Box\top\}\ \mathsf{ref}\, x_1 \approx \mathsf{ref}\, x_2\ \{\mathcal{V}[\![\mathsf{ref}\, \tau]\!]\rho\}$. Since $\mathcal{C}_1 \vdash \{\Box\top\}\ \mathsf{ref}\, x_i \overset{C^i}{\longmapsto}_i y_i\ \{y_i \hookrightarrow_i x_i\}$ (where $C^i = y_i, y_i \in \mathrm{Val}_i$) by rule ALLOC, we can apply rule STEP-LR such that it remains to show $\mathcal{C}_2 \vdash \{y_1 \hookrightarrow_1 x_1 * y_2 \hookrightarrow_2 x_2\}\ y_1 \approx y_2\ \{\mathcal{V}[\![\mathsf{ref}\, \tau]\!]\rho\}$ for $\mathcal{C}_2 = \triangleleft\mathcal{C}_1, y_1, y_2, y_1 \in \mathrm{Val}_1, y_2 \in \mathrm{Val}_2$. Now, using rule ISL-NEW, we create a new island $p \propto a.(B, H)$ with constant population A, where $A = \{(y_1, y_2)\}$, $B = (a \equiv A)$, and $H = \exists x_1, x_2.\ y_1 \hookrightarrow_1 x_1 * y_2 \hookrightarrow_2 x_2 * \Box\triangleright(x_1, x_2) \in \mathcal{V}[\![\tau]\!]\rho$, thus upgrading $\mathcal{C}_2$ to $\mathcal{C}_3 = \mathcal{C}_2, p, p \propto a.(B, H), p \equiv A$. Before we can switch back to the regular judgment using rule ISL-UPD (without actually updating anything), we need to show that H is currently satisfied. This follows easily from the current knowledge about the heap and the assumption $(x_1, x_2) \in \mathcal{V}[\![\tau]\!]\rho$ together with rule MONO. Back in the regular judgment with $\mathcal{C}_4 = \dagger\mathcal{C}_3, p \equiv A$, we must show $(y_1, y_2) \in \mathcal{E}[\![\mathsf{ref}\, \tau]\!]\rho$. This follows from rules ↑-RETURN and, after unfolding the definition of $\mathcal{V}[\![\mathsf{ref}\, \tau]\!]\rho$, ENTAIL-↪-VAL and ∝-INTRO. □

Lemma 3.9 (Compatibility: Assignment)
If $\mathcal{C} \vdash (e_1, e_2) \in \mathcal{E}[\![\mathsf{ref}\, \tau]\!]\rho$ and $\mathcal{C} \vdash (e_3, e_4) \in \mathcal{E}[\![\tau]\!]\rho$ and $\mathcal{C} \vdash \rho(\alpha) : \mathrm{Type}$ for all $\alpha \in \mathrm{dom}(\rho)$, then $\mathcal{C} \vdash (e_1 := e_3, e_2 := e_4) \in \mathcal{E}[\![\mathsf{unit}]\!]\rho$.

Proof: We show $\mathcal{C}_0 \vdash (e_1, e_2) \in \mathcal{E}[\![\mathsf{ref}\, \tau]\!]\rho \Rightarrow (e_3, e_4) \in \mathcal{E}[\![\tau]\!]\rho \Rightarrow (e_1 := e_3, e_2 := e_4) \in \mathcal{E}[\![\mathsf{unit}]\!]\rho$, where $\mathcal{C}_0 = \mathcal{C}.\mathcal{X}; \mathcal{C}.\mathcal{R}; \cdot; \mathcal{C}.\mathcal{P}$. The original claim then follows by rules $\mathcal{L}$-WEAKEN and ⇒-ELIM. Starting with rule ↑-BIND, we need to show $\mathcal{C}_1 \vdash (x_1 := x_3, x_2 := x_4) \in \mathcal{E}[\![\mathsf{unit}]\!]\rho$, where $\mathcal{C}_1 = \dagger\mathcal{C}_0, x_1, x_2, x_3, x_4, (x_1, x_2) \in \mathcal{V}[\![\mathsf{ref}\, \tau]\!]\rho, (x_3, x_4) \in \mathcal{V}[\![\tau]\!]\rho$. The assumption about x_1 and x_2 tells us that $\propto a.(\ldots, H)$, where $H = \exists y_1, y_2.\ x_1 \hookrightarrow_1 y_1 * x_2 \hookrightarrow_2 y_2 * \Box\triangleright(y_1, y_2) \in \mathcal{V}[\![\tau]\!]\rho$. With the help of rule ∝-ELIM and the fact that our $\mathcal{L}$ is empty, we can extend $\mathcal{C}_1$ to $\mathcal{C}_2 := \mathcal{C}_1, p, p \propto a.(\ldots, H)$ and hence use rule ↑-IMPURE to enter the separation judgment. Here we are required to show $\{H\}\ x_1 := x_3 \approx x_2 := x_4\ \{\mathcal{V}[\![\tau]\!]\rho\}$ under $\mathcal{C}_3 := \mathcal{C}_2, a, p \equiv a$. By combining rules ALLOC and STEP-LR, we need to show $\{H'\}\ \langle\rangle \approx \langle\rangle\ \{\mathcal{V}[\![\tau]\!]\rho\}$, where $H' = x_1 \hookrightarrow_1 x_3 * x_2 \hookrightarrow_2 x_4$. In order to switch back to the regular judgment using rule ISL-UPD, we are required to show that the heap law H is still satisfied. This follows from H' and the assumption $(x_3, x_4) \in \mathcal{V}[\![\tau]\!]\rho$ together with rule MONO. Consequently, it suffices to show $(\langle\rangle, \langle\rangle) \in \mathcal{E}[\![\tau]\!]\rho$ under $\mathcal{C}_4 := \dagger\mathcal{C}_3$, which follows by rule ↑-RETURN. □

Lemma 3.10 (Compatibility: Reference Equality)
If $\mathcal{C} \vdash (e_1, e_2) \in \mathcal{E}[\![\mathsf{ref}\, \tau]\!]\rho$ and $\mathcal{C} \vdash (e_3, e_4) \in \mathcal{E}[\![\mathsf{ref}\, \tau]\!]\rho$ and $\mathcal{C} \vdash \rho(\alpha) : \mathrm{Type}$ for all $\alpha \in \mathrm{dom}(\rho)$, then $\mathcal{C} \vdash (e_1 == e_3, e_2 == e_4) \in \mathcal{E}[\![\mathsf{bool}]\!]\rho$.

Proof: We show $\mathcal{C}_0 \vdash (e_1, e_2) \in \mathcal{E}[\![\mathsf{ref}\,\tau]\!]\rho \Rightarrow (e_3, e_4) \in \mathcal{E}[\![\mathsf{ref}\,\tau]\!]\rho \Rightarrow (e_1 == e_3, e_2 == e_4) \in \mathcal{E}[\![\mathsf{bool}]\!]\rho$, where $\mathcal{C}_0 = \mathcal{C}.\mathcal{X}; \mathcal{C}.\mathcal{R}; \cdot; \mathcal{C}.\mathcal{P}$. The original claim then follows by rules $\mathcal{L}$-WEAKEN and $\Rightarrow$-ELIM. Starting with rule $\uparrow$-BIND, we need to show $\mathcal{C}_1 \vdash (x_1 == x_3, x_2 == x_4) \in \mathcal{E}[\![\mathsf{bool}]\!]\rho$, where $\mathcal{C}_1 = \dagger\mathcal{C}_0, x_1, x_2, x_3, x_4, (x_1, x_2) \in \mathcal{V}[\![\mathsf{ref}\,\tau]\!]\rho, (x_3, x_4) \in \mathcal{V}[\![\mathsf{ref}\,\tau]\!]\rho$. The assumptions about x_1, x_2, x_3, x_4 tell us $\propto a.(B_1, H_1)$ and $\propto a.(B_3, H_3)$, where $B_i = (a \equiv \{(x_i, x_{i+1})\})$ and $H_i = \exists y_i, y_{i+1}.\ x_i \hookrightarrow_1 y_i * x_{i+1} \hookrightarrow_2 y_{i+1} * \Box\triangleright(y_i, y_{i+1}) \in \mathcal{V}[\![\tau]\!]\rho$. With the help of rule $\propto$-ELIM and the fact that our $\mathcal{L}$ is empty, we can extend $\mathcal{C}_1$ to $\mathcal{C}_2 := \mathcal{C}_1, p_1, p_1 \propto a.(B_1, H_1)$. Since $\mathcal{L}$ is now non-empty, another application of that rule requires us to show $(x_1 == x_3, x_2 == x_4) \in \mathcal{E}[\![\mathsf{bool}]\!]\rho$ twice—(1) under $\mathcal{C}_3 := \mathcal{C}_2, p_3, p_3 \propto a.(B_3, H_3)$ and, separately, (2) under $\mathcal{C}_3' := \mathcal{C}_2, \forall a.B_3 \equiv B_1$.

For (1) we use rule $\uparrow$-IMPURE to access the knowledge of how the heap looks like with respect to the locations in question. That is, we need to show $\{H_1 * H_3\}\ x_1 == x_3 \approx x_2 == x_4\ \{\mathcal{V}[\![\mathsf{bool}]\!]\rho\}$. By rule ENTAIL-$\hookrightarrow$-SEP, $H_1 * H_3$ implies $x_1 \neq x_3$ as well as $x_2 \neq x_4$. Consequently, we know $x_1 == x_3 \rightsquigarrow \mathsf{false}$ as well as $x_2 == x_4 \rightsquigarrow \mathsf{false}$. Using rule EXPAND and then leaving the separation judgment using rule ISL-UPD (without updating), it suffices to show $(\mathsf{false}, \mathsf{false}) \in \mathcal{E}[\![\mathsf{bool}]\!]\rho$. This follows by rule $\uparrow$-RETURN.

For (2) we can derive $\{(x_3, x_4)\} = \{(x_1, x_2)\}$ from $\forall a.B_3 \equiv B_1$, and thus $x_3 = x_1$ and $x_4 = x_2$. Consequently, we know $x_1 == x_3 \rightsquigarrow \mathsf{true}$ as well as $x_2 == x_4 \rightsquigarrow \mathsf{true}$. All we need from here on are rules $\uparrow$-EXPAND and $\uparrow$-RETURN. □

Definition 3.11 (Logical Equivalence Judgment for Values)
Given $\Gamma; \Sigma \vdash v_1 : \tau$ and $\Gamma; \Sigma \vdash v_2 : \tau$, we define

$$\Gamma; \Sigma \vdash v_1 \approx^{log}_{\mathsf{val}} v_2 : \tau \quad \stackrel{\text{def}}{=} \quad \mathcal{X}; \mathcal{R}; \mathcal{L}; \mathcal{P} \vdash (\gamma_1 v_1, \gamma_2 v_2) \in \mathcal{V}[\![\tau]\!]\rho$$

where $\mathcal{X}$, $\mathcal{R}$, $\mathcal{L}$, $\mathcal{P}$, γ_1, γ_2, ρ are defined as in the case for terms.

Lemma 3.12 (Fundamental Property for Values)
If $\Gamma; \Sigma \vdash v : \tau$, then $\Gamma; \Sigma \vdash v \approx^{log}_{\mathsf{val}} v : \tau$.

Definition 3.13 (Wundertüte)
Suppose $\Gamma = \overline{\alpha}, \overline{x : \tau}$ and $\Sigma = \overline{l : \sigma}$.

$$\begin{aligned}
\mathrm{canonic}(k, d, \Gamma, \Sigma) := {} & (\mathcal{X}, \mathcal{R}, \mathcal{L}, \mathcal{P}, \gamma_1, \gamma_2, \rho, W, \delta) \text{ where} \\
\mathcal{X} &:= \overline{\alpha}_1, \overline{\alpha}_2, \overline{x}_1, \overline{x}_2 \\
\mathcal{R} &:= \overline{r}, \overline{p} \\
\mathcal{L} &:= \overline{p \propto a.(a \equiv \{(l,l)\}, \exists y_1, y_2.\ l \hookrightarrow_1 y_1 * l \hookrightarrow_2 y_2 * \Box\triangleright(y_1, y_2) \in \mathcal{V}[\![\sigma]\!])} \\
\mathcal{P} &:= \overline{r : \mathrm{Type}}, \overline{(x_1, x_2) \in \mathcal{V}[\![\tau]\!]\rho}, \overline{l \in \mathrm{Val}_1}, \overline{l \in \mathrm{Val}_2} \\
\gamma_i &:= \overline{\alpha \mapsto \alpha_i}, \overline{x \mapsto x_i} \\
\rho &:= \overline{\alpha \mapsto r} \\
W &:= (k, d, \mathrm{dom}(\Sigma), \mathrm{dom}(\Sigma), \mathcal{I}) \\
\mathrm{dom}(\mathcal{I}) &:= \{\iota_1, \ldots, \iota_n\} \\
\mathcal{I}(\iota_i) &:= (\{(l_i, l_i)\}, \{\{(l_i, l_i)\}\}, \lambda CP.\ \{(W, h_1, h_2) \in \mathit{HeapAtom}_k \mid \\
&\qquad\qquad [\![(h_1(l_i), h_2(l_i)) \in \mathcal{V}[\![\sigma_i]\!]]\!]\emptyset W\}) \\
\delta &:= \overline{p \mapsto \mathrm{pop}(\iota)}
\end{aligned}$$

Lemma 3.14
If $(\cdot, \mathcal{R}, \mathcal{L}, \mathcal{P}, \emptyset, \emptyset, \emptyset, W, \delta) = \text{canonic}(k, d, \cdot, \Sigma)$, then $(\emptyset, \delta, W, \text{dom}(W.\mathcal{I}), \emptyset) \in [\![\cdot; \mathcal{R}; \mathcal{L}; \mathcal{P}]\!]$.

Proof: For this we need to show $[\![\mathcal{L}]\!]\delta W \text{dom}(\mathcal{I})$ and $[\![\mathcal{P}]\!]\delta W$. The latter is obvious. For the former, we show:

$$[\![p_i \propto a.(a \equiv \{(l_i, l_i)\}, \exists y_1, y_2.\ l_i \hookrightarrow_1 y_1 * l_i \hookrightarrow_2 y_2 * \Box\triangleright(y_1, y_2) \in \mathcal{V}[\![\sigma_i]\!])]\!]\delta W\{\iota_i\}$$

This boils down to the fact that $[\![(h'_1(l_i), h'_2(l_i)) \in \mathcal{V}[\![\sigma_i]\!]]\!]\emptyset W'$ is equivalent to

$$[\![\exists y_1, y_2.\ l_i \hookrightarrow_1 y_1 * l_i \hookrightarrow_2 y_2 * \Box\triangleright(y_1, y_2) \in \mathcal{V}[\![\sigma_i]\!]]\!]\delta(\triangleleft W')(h'_1, h'_2).$$

□

Lemma 3.15 (Heap Parametricity)
If $\vdash h : \Sigma$ and $(\cdot, \mathcal{R}, \mathcal{L}, \mathcal{P}, \emptyset, \emptyset, \emptyset, W, \delta) = \text{canonic}(k, d, \cdot, \Sigma)$, then $h, h : W$.

Proof: This boils down to showing $h, h :_{\text{dom}(W.\mathcal{I})} W$. If $k = 0$, there is nothing to show. Otherwise, let $h^i = h|_{\{l_i\}}$, where we suppose $\Sigma = \overline{l : \sigma}$. We claim $(\triangleright W, h^i, h^i) \in W.\mathcal{I}(\iota_i).HL(W.\mathcal{I}(\iota_i).PL)$, *i.e.,* $(\triangleright W, h^i, h^i) \in \mathit{HeapAtom}_k$ and $[\![(h(l_i), h(l_i)) \in \mathcal{V}[\![\sigma_i]\!]]\!]\emptyset(\triangleright W)$. The former is obvious. For the latter, note that $\cdot; \Sigma \vdash h(l_i) : \Sigma(l_i)$, for which the Fundamental Property for Values yields $\cdot; \mathcal{R}; \mathcal{L}; \mathcal{P} \vdash (h(l_i), h(l_i)) \in \mathcal{V}[\![\sigma_i]\!]$. By Lemmas 3.14 and 2.17 we are done. □

Lemma 3.16 (Adequacy)
If $\cdot; \Sigma \vdash e_1 \approx^{log} e_2 : \tau$ and $\vdash h : \Sigma$, then $(h; e_1)\Downarrow$ iff $(h; e_2)\Downarrow$.

Proof: Suppose $(h; e_1) \Downarrow^j$ (the other direction is symmetric). Let $(\cdot, \mathcal{R}, \mathcal{L}, \mathcal{P}, \emptyset, \emptyset, \emptyset, W, \delta) = \text{canonic}(j + 1, \to, \Sigma)$. By unfolding the definition of $\approx^{log}$ we know $\cdot; \mathcal{R}; \mathcal{L}; \mathcal{P} \vdash (e_1, e_2) \in \mathcal{E}[\![\tau]\!]$. By Lemma 3.14, $[\![(e_1, e_2) \in \mathcal{E}[\![\tau]\!]]\!]\delta W$. Since $h, h : W$ by Heap Parametricity, this yields $W \vdash (h; e_1) \approx (h; e_2) : [\![\mathcal{V}[\![\tau]\!]]\!]\delta$. Finally, since $j < W.k$, we learn $(h; e_2)\Downarrow$. □

Theorem 3.17 (Soundness w.r.t. Contextual Equivalence)
If $\Gamma; \Sigma \vdash e_1 \approx^{log} e_2 : \tau$, then $\Gamma; \Sigma \vdash e_1 \approx^{ctx} e_2 : \tau$.

Proof: Suppose $\vdash \mathcal{C} : (\Gamma; \Sigma \vdash \tau) \rightsquigarrow (\cdot; \Sigma' \vdash \tau')$ and $\vdash h : \Sigma'$. By Congruence, $\cdot; \Sigma' \vdash C[e_1] \approx^{log} C[e_2] : \tau'$. By Adequacy, $(h; C[e_1])\Downarrow$ iff $(h; C[e_2])\Downarrow$. □

4 Examples

4.1 Name Generators

Consider:

$$\begin{array}{rcl} \tau & := & \exists\alpha.\,(\mathsf{unit} \to \alpha) \times (\alpha \times \alpha \to \mathsf{bool}) \\ e_1 & := & \mathsf{let}\, x = \mathsf{ref}\ 0\, \mathsf{in}\, \mathsf{pack}\, \mathsf{int}, \langle \lambda\_.{+}{+}x, \lambda y.\mathsf{fst}\, y = \mathsf{snd}\, y\rangle\, \mathsf{as}\, \tau \\ e_2 & := & \mathsf{pack}\, \mathsf{ref}\, \mathsf{unit}, \langle \lambda\_.\mathsf{ref}\, \langle\rangle, \lambda y.\mathsf{fst}\, y == \mathsf{snd}\, y\rangle\, \mathsf{as}\, \tau \end{array}$$

To prove these ADTs equivalent, we want to show $\vdash (e_1, e_2) \in \mathcal{E}[\![\tau]\!]$.

By $\uparrow$-IMPURE, we have to show $\vdash \{\Box\top\}\ e_1 \approx e_2\ \{\mathcal{V}[\![\tau]\!]\}$. By rules STEP-L, ALLOC and EXPAND, we need to show

$$\mathcal{C}_1 \vdash \{x \hookrightarrow_1 0\}\ e_1' \approx e_2\ \{\mathcal{V}[\![\tau]\!]\}$$

where e_1' is the body of the let and $\mathcal{C}_1 = x; \cdot; \cdot; x \in \mathrm{Val}_1$.

Using rule ISL-NEW we introduce an island p whose population is a partial bijection between the natural numbers that will be generated by e_1' and the set of locations allocated by e_2:

$$\begin{array}{rcl} B & := & \exists n.\, \exists b \subset \mathrm{Loc}.\, \mathrm{bij}(a, \{1, \ldots, n\}, b) \\ H & := & \exists n.\, (x \hookrightarrow_1 n) * \Box(\max(\mathrm{dom}(a), n) \wedge \mathrm{rng}(a) \subseteq \mathrm{Val}_2) \end{array}$$

The population law B states that a is a bijective relation of the form $\{1{\mapsto}l_1, \ldots, n{\mapsto}l_n\}$.[1] The heap law H then verifies that the state of x always is the maximum n in the domain of the current population, and that its locations are all valid in the current world. The latter property is important later to show that newly allocated references will always be fresh with respect to the current population. Given $A = \emptyset$ for the initial population, it is easy to verify that $\mathcal{C}_1 \vdash B[A/a]$. Consequently, we can now define $\mathcal{C}_2 = \mathcal{C}_1, p, p \propto a.(B, H), p \equiv \emptyset$ and need to show

$$\mathcal{C}_2 \vdash \{x \hookrightarrow_1 0\}\ e_1' \approx e_2\ \{\mathcal{V}[\![\tau]\!]\}$$

Both expressions are values, so we want to apply rule ISL-UPD (and $\uparrow$-RETURN, using monotonicity of the logical relation) to reduce the problem to

$$\mathcal{C}_3 \vdash (e_1', e_2) \in \mathcal{V}[\![\tau]\!]$$

where $\mathcal{C}_3 = \dagger\mathcal{C}_2, p \equiv \emptyset$. To do so, we first need to prove $\mathcal{C}_2 \vdash B[\emptyset/a]$, which follows as before, and $\mathcal{C}_3 \vdash x \hookrightarrow_1 0 \Rrightarrow H[\emptyset/a]$. The latter consists of eliminating the existential in H with $n = 0$ and then showing both parts of the separating conjunction. The first, $x \hookrightarrow_1 0$, is immediate from the assumption, while the second part is a propositional formula that we can prove separately and then cut into the entailment judgment.

Now, we unroll the definition of $\mathcal{V}[\![\exists\alpha.\tau]\!]$ and pick

$$r := (x_1, x_2).\, x_1 \in \mathrm{Val}_1 \wedge x_2 \in \mathrm{Val}_2 \wedge (x_1, x_2) \in p$$

We have to show $\mathcal{C}_3 \vdash r : \mathrm{Type}$ — which follows straightforwardly from rule POP-MONO. Now let $\rho = \alpha{\mapsto}r$. By the definition of $\mathcal{V}[\![\tau' \times \tau'']\!]\rho$, we still have to show

[1] The bij predicate as well as the other notation in B and H can be defined in our logic.

1. $\mathcal{C}_3 \vdash (\lambda\_.{+}{+}x, \lambda\_.\mathsf{ref}\,\langle\rangle) \in \mathcal{V}[\![\mathsf{unit} \to \alpha]\!]\rho$
2. $\mathcal{C}_3 \vdash (\lambda y.\mathsf{fst}\,y = \mathsf{snd}\,y, \lambda y.\mathsf{fst}\,y == \mathsf{snd}\,y) \in \mathcal{V}[\![\alpha \times \alpha \to \mathsf{bool}]\!]\rho$

Let us first turn to (1). We unroll the definition of $\mathcal{V}[\![\tau' \to \tau'']\!]$, and apply the introduction rules for $\Box$, $\forall$ and $\Rightarrow$, producing the goal

$$\mathcal{C}_4 \vdash ((\lambda\_.{+}{+}x)\,y_1, (\lambda\_.\mathsf{ref}\,\langle\rangle)\,y_2) \in \uparrow\mathcal{V}[\![\mathsf{unit} \to \alpha]\!]\rho$$

where $\mathcal{C}_4 = \dagger\mathcal{C}_2, y_1, y_2, (y_1, y_2) \in \mathcal{V}[\![\mathsf{unit}]\!]\rho$ (note that $\dagger\mathcal{C}_3 = \dagger\mathcal{C}_2$). By $\uparrow$-EXPAND, $\uparrow$-IMPURE and SEP-$\exists$, and expanding the $++$ notation, we have to show the equivalence

$$\mathcal{C}_5 \vdash \{x \hookrightarrow_1 n * \Box P\}\ (x := !x + 1; !x) \approx \mathsf{ref}\,\langle\rangle\ \{\mathcal{V}[\![\alpha]\!]\rho\}$$

where $\mathcal{C}_5 = \mathcal{C}_4, a, n, p \equiv a$ and P is the boxed proposition in H. We can step through the left computation using rules STEP-L and EXPAND and reach

$$\mathcal{C}_5 \vdash \{x \hookrightarrow_1 n + 1 * \Box P\}\ n + 1 \approx \mathsf{ref}\,\langle\rangle\ \{\mathcal{V}[\![\alpha]\!]\rho\}$$

The right side is more tricky, because we have to derive an appropriate freshness property for the new location. We first move $\Box P$ to the context (rule $\Box$-SHIFT), producing $\mathcal{C}_6 = \mathcal{C}_5, \Box(\max(\mathrm{dom}(a), n) \wedge \mathrm{rng}(a) \subseteq \mathrm{Val}_2)$. From there we can derive $\mathcal{C}_6 \vdash \mathrm{rng}(a) \subseteq \mathrm{Val}_2$ and then apply rules ALLOC and STEP-R to get the goal

$$\mathcal{C}_6, y \vdash \{x \hookrightarrow_1 n + 1 * y \hookrightarrow \langle\rangle * \Box(y \notin \mathrm{rng}(a)) * \Box P\}\ n + 1 \approx y\ \{\mathcal{V}[\![\alpha]\!]\rho\}$$

By SEP-ENTAIL and ENTAIL-$\hookrightarrow$-VAL, we can further strengthen the heap assertion to include $y \in \mathrm{Loc}$.

Now that the new names have been generated, we update the island with the new population $A = a \cup \{(n + 1, y)\}$, using rule ISL-UPD. To do so, we first have to show $\mathcal{C}_6 \vdash p \subseteq A$, which is easy given the assumption $p \equiv a$ in the context. Then we have to show that the population law still holds, *i.e.,* $\mathcal{C}_6 \vdash \exists n'.\exists b \subset \mathrm{Loc}.\,\mathrm{bij}(A, \{1, \ldots, n'\}, b)$. Assuming a suitable set of admissible rules about bijections, this can be derived by picking $n' = n + 1$ and $b = \mathrm{rng}(a) \cup \{y\}$, and using the assumption $\max(\mathrm{dom}(a), n)$. It also requires the assumptions $y \in \mathrm{Loc}$ and $y \notin \mathrm{rng}(a)$, which we can extract from the heap assertion (rule $\Box$-SHIFT). Likewise, we have to prove that the final heap assertion entails the heap law $H[A/a]$ under the environment $\mathcal{C}_7 = \dagger\mathcal{C}_6, p \equiv A$. Choosing $n + 1$ for the existential variable n in H, the first half, $x \hookrightarrow_1 n + 1$, follows directly from the heap assertion. The rest can again be derived using only propositional logic.

The final step in this part is to show $\mathcal{C}_7 \vdash (n+1, y) \in \uparrow\mathcal{V}[\![\alpha]\!]\rho$. In order to apply rule $\uparrow$-RETURN, a proof for $\mathcal{C}_7 \vdash \mathcal{V}[\![\alpha]\!]\rho : \mathrm{Type}$ is required — which we already proved above, modulo weakening. The rest then is by straightforward propositional reasoning, given the updated population $p \equiv A$ in $\mathcal{C}_7$ and our definition of r in terms of p.

For part (2) we start as before, yielding the goal

$$\mathcal{C}'_4 \vdash ((\lambda y.\mathsf{fst}\,y = \mathsf{snd}\,y)\,y_1, (\lambda y.\mathsf{fst}\,y == \mathsf{snd}\,y)\,y_2) \in \uparrow\mathcal{V}[\![\mathsf{bool}]\!]\rho$$

with $\mathcal{C}'_4 = \dagger\mathcal{C}_2, y_1, y_2, (y_1, y_2) \in \mathcal{V}[\![\alpha \times \alpha]\!]$. We can unfold the definitions of $\mathcal{V}[\![\tau' \times \tau'']\!]$ and $\mathcal{V}[\![\alpha]\!]$ in the context and eliminate the respective existential, producing

$$\mathcal{C}'_5 = \dagger\mathcal{C}_2, y_1, y_2, y'_1, y'_2, y''_1, y''_2, y_1{=}\langle y'_1, y''_1\rangle, y_2{=}\langle y'_2, y''_2\rangle, (y'_1, y'_2) \in r, (y''_1, y''_2) \in r.$$

Now y_1, y_2 in the judgment can be replaced by the respective pairs, and by $\uparrow$-EXPAND we are left with

$$\mathcal{C}_5' \vdash (y_1' = y_1'', y_2' == y_2'') \in \uparrow\mathcal{V}[\![\mathsf{bool}]\!]\rho.$$

At this point, the proof essentially boils down to the absolute proposition

$$\begin{array}{l}\forall a, y_1', y_1'', y_2', y_2''.\, B \Rightarrow (y_1', y_2') \in a \Rightarrow (y_1'', y_2'') \in a \Rightarrow \\ \quad \exists b \in \{\mathsf{true}, \mathsf{false}\}.\, (y_1' = y_1'' \rightsquigarrow b) \equiv (y_2' == y_2'' \rightsquigarrow b)\end{array}$$

Expanding out the definition of B, this can be proved by straightforward means in the meta logic and thus be assumed as an axiom.

4.2 Landin's Knot

We want to prove that Landin's Knot – the construction of a fixpoint using backpatching – works. That is, we want to prove the equivalence between the following two expressions of type $\tau_1 \to \tau_2$:

$$\begin{array}{rcl} e_1 & := & \mathsf{let}\, z = \mathsf{ref}\, (\lambda x.\bot)\, \mathsf{in}\, (z := (\lambda x.\mathsf{let}\, f = !y\, \mathsf{in}\, e); !z) \\ e_2 & := & \mathsf{fix}\, f(x).\, e \end{array}$$

where fix is a standard cbv fixpoint operator, which can be defined in our language as follows:

$$\begin{array}{rcl} \mathsf{fix}\, f(x).\, e & := & \lambda x.(\mathsf{unroll}\, v)\, v\, x \\ \text{where } v & := & \mathsf{roll}\, \lambda f'.(\lambda f.\lambda x.e)\, (\lambda x.(\mathsf{unroll}\, f')\, f'\, x) \end{array}$$

We need to show $\vdash (e_1, e_2) \in \mathcal{E}[\![\tau_1 \to \tau_2]\!]$, or, by rule $\uparrow$-IMPURE, $\vdash \{\Box\top\}\ e_1 \approx e_2\ \{\mathcal{V}[\![\tau_1 \to \tau_2]\!]\}$. By applying STEP-L several times, we can reduce this to showing $\{z \hookrightarrow_1 F\}\ F \approx e_2\ \{\mathcal{V}[\![\tau_1 \to \tau_2]\!]\}$, where F is the function value assigned to z in e_1.

By rule ISL-NEW we introduce an island p that records the fact that y will contain F, forever. That is, we choose $H = z \hookrightarrow_1 F$ as the heap law. We do not need the population for this proof, so we pick $B = \top$ and $A = \emptyset$. By rules ISL-UPD and $\uparrow$-RETURN, it remains to be shown that $(F, e_2) \in \mathcal{V}[\![\tau_1 \to \tau_2]\!]$ under the extended context.

At this point, we invoke rule LÖB to prove the equivalence of F and e_2 under the "coinductive" assumption $\triangleright(F, e_2) \in \mathcal{V}[\![\tau_1 \to \tau_2]\!]$. Unfolding the definition of $\mathcal{V}[\![\tau' \to \tau'']\!]$, we assume y_1, y_2 with $(y_1, y_2) \in \mathcal{V}[\![\tau_1]\!]$ and apply $\uparrow$-IMPURE again, such that we now have to show $\{z \hookrightarrow_1 F\}\ F\, y_1 \approx e_2\, y_2\ \{\mathcal{V}[\![\tau_2]\!]\}$. Note how our island re-establishes the crucial assertion about y pointing to F.

We use EXPAND to reach the point where both expressions have to make an essential step:

$$\{z \hookrightarrow_1 F\}\ (\mathsf{let}\, f = !z\, \mathsf{in}\, e[y_1/x]) \approx (\mathsf{unroll}\, v)\, v\, y_2\ \{\mathcal{V}[\![\tau_2]\!]\}$$

Now we can apply STEP-LR, using DEREF on the left and UNROLL on the right, yielding, after further reduction

$$\{z \hookrightarrow_1 F\}\ e[F/f][y_1/x] \approx e[e_2/f][y_2/x]\ \{\mathcal{V}[\![\tau_2]\!]\}$$

which we have to prove in an *earlier* world — removing the $\triangleright$-operator from the assumption $(F, e_2) \in \mathcal{V}[\![\tau_1 \to \tau_2]\!]$ that was introduced by rule LÖB.

We apply ISL-UPD once more (boxing and unboxing the monotonous assumptions $(y_1, y_2) \in \mathcal{V}[\![\tau_1]\!]$ and $(F, e_2) \in \mathcal{V}[\![\tau_1 \to \tau_2]\!]$ to have them survive) so that the goal becomes $(e[F/f][y_1/x], e[e_2/f][y_2/x]) \in \mathcal{V}[\![\tau_2]\!]$. By applying $\uparrow$-REDUCE twice this can be expanded to $((\lambda f.\lambda x.e)\, F\, y_1, (\lambda f.xe)\, e_2\, y_2) \in \mathcal{V}[\![\tau_2]\!]$.

Now use the introduction rules for implication and $\Box$ twice, discharging the assumptions $(y_1, y_2) \in \mathcal{V}[\![\tau_1]\!]$ and $(F, e_2) \in \mathcal{V}[\![\tau_1 \to \tau_2]\!]$. With the definition of $\mathcal{V}[\![\tau' \to \tau'']\!]$ this gives

$$(\lambda f.\lambda x.e, \lambda f.\lambda x.e) \in \mathcal{V}[\![(\tau_1 \to \tau_2) \to \tau_1 \to \tau_2]\!]$$

which holds by the Fundamental Property.