Realistic Realizability: Specifying ABIs You Can Count On

Technical Appendix

ANDREW WAGNER, Northeastern University, USA
ZACHARY EISBACH, Northeastern University, USA
AMAL AHMED, Northeastern University, USA

Contents

List of Figures

Authors' Contact Information: Andrew Wagner, Northeastern University, Boston, USA, ahwagner@ccs.neu.edu; Zachary Eisbach, Northeastern University, Boston, USA, eisbach.z@northeastern.edu; Amal Ahmed, Northeastern University, Boston, USA, amal@ccs.neu.edu.

A Source

A.1 Syntax

$$
\begin{array}{lcll}
\mathsf{Type} & \ni \mathsf{T} & ::= & \mathbb{Z} \mid \overline{\mathsf{T}_1} \rightarrow \mathsf{T}_2 \mid \mathsf{X} \\
\mathsf{Expr} & \ni \mathsf{e} & ::= & \mathsf{x} \mid \mathsf{let}\,\mathsf{x} = \mathsf{e}_1; \mathsf{e}_2 \mid \mathsf{n} \mid \mathsf{e}_1 \oplus \mathsf{e}_2 \mid \mathsf{fn}\,\mathsf{f}\,\overline{\mathsf{x}}\{\mathsf{e}\} \mid \mathsf{e}_1\,\overline{\mathsf{e}_2} \mid \{\overline{\mathsf{s} : \mathsf{e}}\} \mid \mathsf{e.s} \mid \mathsf{s}\,\mathsf{e} \mid \mathsf{case}\,\mathsf{e}_1\,\{\overline{\mathsf{s}\,\mathsf{x} \Longrightarrow \mathsf{e}_2}\} \\
\mathsf{Ctx} & \ni \Gamma & ::= & \varnothing \mid \Gamma, \mathsf{x} : \mathsf{T} \\
\mathsf{Sig} & \ni \Sigma & ::= & \varnothing \mid \Sigma, \mathsf{m}\,\mathsf{k}\,\mathsf{X}\,\{\overline{\mathsf{s} : \mathsf{T}}\} \\
\mathsf{Mode} & \ni \mathsf{m} & ::= & \mathsf{rigid} \mid \mathsf{flex} \\
\mathsf{Kind} & \ni \mathsf{k} & ::= & \mathsf{struct} \mid \mathsf{enum}
\end{array}
$$

Fig. A.1. Syntax for source.

A.2 Statics

$\boxed{\Sigma; \Gamma \vdash \mathsf{e} : \mathsf{T}}$

$$\text{(SRC-STAT-LET)}\quad \frac{\Gamma_1 \vdash \mathsf{e}_1 : \mathsf{T}_1 \quad \Gamma_2, \mathsf{x} : \mathsf{T}_1 \vdash \mathsf{e}_2 : \mathsf{T}_2 \quad \Gamma_2 \not\ni \mathsf{x}}{\Gamma_1, \Gamma_2 \vdash \mathsf{let}\, \mathsf{x} = \mathsf{e}_1; \mathsf{e}_2 : \mathsf{T}_2}$$

$$\text{(SRC-STAT-VAR)}\quad \Sigma; \mathsf{x} : \mathsf{T} \vdash \mathsf{x} : \mathsf{T}$$

$$\text{(SRC-STAT-DUP)}\quad \frac{\Gamma \ni \mathsf{x} : \mathsf{T}' \quad \Sigma; \Gamma, \mathsf{x} : \mathsf{T}' \vdash \mathsf{e} : \mathsf{T}}{\Sigma; \Gamma \vdash \mathsf{e} : \mathsf{T}}$$

$$\text{(SRC-STAT-DROP)}\quad \frac{\Sigma; \Gamma \vdash \mathsf{e} : \mathsf{T}}{\Sigma; \Gamma, \mathsf{x} : \mathsf{T}' \vdash \mathsf{e} : \mathsf{T}}$$

$$\text{(SRC-STAT-I-}\mathbb{Z}\text{)}\quad \varnothing \vdash \mathsf{n} : \mathbb{Z}$$

$$\text{(SRC-STAT-}\oplus\text{-}\mathbb{Z}\text{)}\quad \frac{\Gamma_1 \vdash \mathsf{e}_1 : \mathbb{Z} \quad \Gamma_2 \vdash \mathsf{e}_2 : \mathbb{Z}}{\Gamma_1, \Gamma_2 \vdash \mathsf{e}_1 \oplus \mathsf{e}_2 : \mathbb{Z}}$$

$$\text{(SRC-STAT-I-}\rightarrow\text{)}\quad \frac{\Gamma, \mathsf{z_f} : \overline{\mathsf{T_i}}^{i<n} \rightarrow \mathsf{T}, \overline{\mathsf{x} : \mathsf{T_i}}^{i<n} \vdash \mathsf{e} : \mathsf{T} \qquad \Gamma \not\ni \mathsf{z_f}, \overline{\mathsf{x}}^{i<n} \text{ distinct}}{\Gamma \vdash \mathsf{fn}\, \mathsf{z_f}\, \overline{\mathsf{x_i}}^{i<n} \{\mathsf{e}\} : \overline{\mathsf{T_i}}^{i<n} \rightarrow \mathsf{T}}$$

$$\text{(SRC-STAT-E-}\rightarrow\text{)}\quad \frac{\overline{\Gamma_i \vdash \mathsf{e_i} : \mathsf{T_i}}^{i<n} \qquad \Gamma_f \vdash \mathsf{e_f} : \overline{\mathsf{T_i}}^{i<n} \rightarrow \mathsf{T}}{\overline{\Gamma_i}^{i<n}, \Gamma_f \vdash \mathsf{e_f}\, \overline{\mathsf{e_i}}^{i<n} : \mathsf{T}}$$

$$\text{(SRC-STAT-I-struct)}\quad \frac{\Sigma \ni \mathsf{rigid\ struct}\, \mathsf{X}\, \{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\} \qquad \overline{\Sigma; \Gamma_i \vdash \mathsf{e_i} : \mathsf{T_i}}^{i<n}}{\Sigma; \overline{\Gamma_i}^{i} \vdash \{\overline{\mathsf{s_i} : \mathsf{e_i}}^{i<n}\} : \mathsf{X}}$$

$$\text{(SRC-STAT-E-struct)}\quad \frac{\Sigma \ni \mathsf{m\ struct}\, \mathsf{X}\, \{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\} \qquad \Sigma; \Gamma \vdash \mathsf{e} : \mathsf{X} \qquad j < n}{\Sigma; \Gamma \vdash \mathsf{e.s_j} : \mathsf{T_j}}$$

$$\text{(SRC-STAT-I-enum)}\quad \frac{\Sigma \ni \mathsf{m\ enum}\, \mathsf{X}\, \{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\} \qquad \Sigma; \Gamma \vdash \mathsf{e_j} : \mathsf{T_j} \qquad j < n}{\Sigma; \Gamma \vdash \mathsf{s_j}\, \mathsf{e_j} : \mathsf{X}}$$

$$\text{(SRC-STAT-E-enum)}\quad \frac{\Sigma \ni \mathsf{rigid\ enum}\, \mathsf{X}\, \{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\} \qquad \Sigma; \Gamma_1 \vdash \mathsf{e} : \mathsf{X} \qquad \overline{\Sigma; \Gamma_2, \mathsf{x_i} : \mathsf{T_i} \vdash \mathsf{e_i} : \mathsf{T}}^{i<n} \qquad \Gamma_2 \not\ni \overline{\mathsf{x}}^{i<n}}{\Sigma; \Gamma_1, \Gamma_2 \vdash \mathsf{case}\, \mathsf{e}\, \{\overline{\mathsf{s_i}\, \mathsf{x_i} \Rightarrow \mathsf{e_i}}\} : \mathsf{T}}$$

$\boxed{\Sigma \vdash \mathsf{T}}$

$$\text{(SRC-TY-WF-INT)}\quad \Sigma \vdash \mathbb{Z}$$

$$\text{(SRC-TY-WF-FUN)}\quad \frac{\Sigma \vdash \mathsf{T}_1 \quad \Sigma \vdash \mathsf{T}_2}{\Sigma \vdash \overline{\mathsf{T}_1} \rightarrow \mathsf{T}_2}$$

$$\text{(SRC-TY-WF-STRUCT)}\quad \frac{\Sigma \ni \mathsf{m\ struct}\, \mathsf{X}\, \{-\}}{\Sigma \vdash \mathsf{X}}$$

$$\text{(SRC-TY-WF-ENUM)}\quad \frac{\Sigma \ni \mathsf{m\ enum}\, \mathsf{X}\, \{-\}}{\Sigma \vdash \mathsf{X}}$$

$\boxed{\vdash \Sigma}$

$$\text{(SRC-SIG-WF)}\quad \frac{\mathsf{rigid\ struct}\, \mathsf{X}\, \{\overline{\mathsf{s} : \mathsf{T}}\} \in \Sigma \Rightarrow \overline{\Sigma \vdash \mathsf{T}} \qquad \mathsf{rigid\ enum}\, \mathsf{X}\, \{\overline{\mathsf{s} : \mathsf{T}}\} \in \Sigma \Rightarrow \overline{\Sigma \vdash \mathsf{T}}}{\vdash \Sigma}$$

Fig. A.2. Statics for source.

B Target

B.1 Syntax

$$
\begin{array}{llll}
\texttt{Word} & \ni & \texttt{w} & ::= \texttt{n} \mid \texttt{null} \mid \ell \mid ☣ \\
\texttt{Expr} & \ni & \texttt{e} & ::= \ \texttt{x} \mid \texttt{f} \mid \texttt{w} \mid \texttt{const}\,\texttt{x} = \texttt{e}_1;\ \texttt{e}_2 \mid \texttt{e}_1\,(\overline{\texttt{e}_2}) \mid \texttt{e}_1 \oplus \texttt{e}_2 \\
 & & & \mid \texttt{if}\,(\texttt{e}_1)\,\{\texttt{e}_2\}\ \texttt{else}\ \{\texttt{e}_3\} \mid \texttt{malloc}\,(\texttt{e}) \mid *\texttt{e} \\
 & & & \mid *\texttt{e}_1 = \texttt{e}_2;\ \texttt{e}_3 \mid \texttt{free}\,(\texttt{e}_1)\,;\ \texttt{e}_2 \mid \texttt{++e} \mid \texttt{--e} \\
\texttt{Funs} & \ni & \texttt{F} & ::= \varnothing \mid \texttt{F}, \texttt{f}\,(\overline{\texttt{x}})\,\{\texttt{e}\} \\
\texttt{Ctx} & \ni & \texttt{K} & ::= \ \texttt{const}\,\texttt{x} = \texttt{K};\ \texttt{e} \mid \texttt{K}\,(\overline{\texttt{e}}) \mid \texttt{w}_1\,(\overline{\texttt{w}_2}, \texttt{K}, \overline{\texttt{e}}) \\
 & & & \mid \texttt{K} \oplus \texttt{e} \mid \texttt{w} \oplus \texttt{K} \mid \texttt{if}\,(\texttt{K})\,\{\texttt{e}_1\}\ \texttt{else}\ \{\texttt{e}_2\} \mid \texttt{malloc}\,(\texttt{K}) \\
 & & & \mid *\texttt{K} \mid *\texttt{K} = \texttt{e}_1;\ \texttt{e}_2 \mid *\texttt{w} = \texttt{K};\ \texttt{e} \mid \texttt{free}\,(\texttt{K})\,;\ \texttt{e} \mid \texttt{++K} \mid \texttt{--K}
\end{array}
$$

$$
\begin{array}{llll}
\ell & \in & \mathsf{Loc} & \triangleq \langle \mathsf{id} : (\mathbb{N} + \mathsf{code}), \mathsf{off} : \mathbb{N} \rangle \\
\psi & \in & \mathsf{Sizes} & \triangleq \mathsf{Loc}_{\mathbb{N}^+} \xrightharpoonup{\mathsf{fin}} \mathbb{N}^+ \\
\mu & \in & \mathsf{Mem} & \triangleq \mathbb{N}^+ \times \mathbb{N} \xrightharpoonup{\mathsf{fin}} \texttt{Word} \\
 & & \mathsf{Loc}_X & \triangleq \{\ell : \mathsf{Loc} \mid \ell.\mathsf{id} \in X\} \\
 & & \langle - \rangle_{\texttt{F}} & : \mathrm{dom}(\texttt{F}) \xrightarrow{\mathsf{inj}} \mathsf{Loc}_{\mathsf{code}} \\
 & & \mathsf{span}(\psi) & \triangleq [\langle b, i \rangle \mid b \in \mathrm{dom}(\psi) \land i < \psi(b)] \\
 & & \mathsf{ok}_{\texttt{F}}(\texttt{e}) & \triangleq \forall k, \psi', \mu', \texttt{e}'.\ \texttt{F} \vdash (\varnothing, \varnothing, \texttt{e}) \longrightarrow^k (\psi', \mu', \texttt{e}') \not\twoheadrightarrow \implies \texttt{e}' \in \mathbb{Z} \land \mu' = \varnothing
\end{array}
$$

$$
\begin{array}{lll}
\texttt{null} & \triangleq & \langle 0, 0 \rangle \\
\texttt{e}_1; \texttt{e}_2 & \triangleq & \begin{cases} \texttt{const}\,\texttt{x} = \texttt{e}_1;\ \texttt{e}_2 & (\texttt{x} \text{ does not appear free in } \texttt{e}_2) \end{cases} \\
\texttt{e}_1\,[\texttt{e}_2] & \triangleq & *(\texttt{e}_1 + \texttt{e}_2) \\
\texttt{havoc} & \triangleq & \texttt{malloc}\,(-1)
\end{array}
$$

$$
\begin{array}{llll}
[\![+]\!](\texttt{n}_1, \texttt{n}_2) & \in & \mathbb{Z} & \triangleq n_1 + n_2 \\
[\![=]\!](\texttt{n}_1, \texttt{n}_2) & \in & \mathbb{Z} & \triangleq \begin{cases} 1 & (n_1 = n_2) \\ 0 & (n_1 \neq n_2) \end{cases} \\
[\![+]\!](\ell, \texttt{n}) & \in & \mathsf{Loc} & \triangleq \begin{cases} \langle b, i + n \rangle & (\ell = \langle b, i \rangle) \end{cases}
\end{array}
$$

Fig. B.1. Syntax, structures, and desugaring for target.

B.2 Dynamics

$\boxed{\mathtt{F} \vdash (\psi, \mu, \mathtt{e}) \rightarrow_{[h]} (\psi', \mu', \mathtt{e}')}$ Presupposes $\mathrm{dom}(\mu) \subseteq \mathsf{span}(\psi)$

$$\text{(TRG-DYN-LET)}\ \frac{}{\mathtt{const}\ \mathtt{x} = \mathtt{w};\ \mathtt{e} \rightarrow_h \mathtt{e}[\mathtt{w}/\mathtt{x}]} \qquad \text{(TRG-DYN-FUNPTR)}\ \frac{\mathtt{F} \ni \mathtt{f}\ (\overline{\mathtt{x}})\ \{\mathtt{e}\}}{\mathtt{F} \vdash \mathtt{f} \rightarrow_h \langle \mathtt{f} \rangle_{\mathtt{F}}} \qquad \text{(TRG-DYN-APP)}\ \frac{\mathtt{F} \ni \mathtt{f}\ (\overline{\mathtt{x}})\ \{\mathtt{e}\}}{\mathtt{F} \vdash \langle \mathtt{f} \rangle_{\mathtt{F}}\ (\overline{\mathtt{w}}) \rightarrow_h \mathtt{e}\overline{[\mathtt{w}/\mathtt{x}]}}$$

$$\text{(TRG-DYN-BOP)}\ \frac{\mathtt{w} = [\![\oplus]\!](\mathtt{w}_1, \mathtt{w}_2)}{\mathtt{w}_1 \oplus \mathtt{w}_2 \rightarrow_h \mathtt{w}} \qquad \text{(TRG-DYN-IF-TRUTHY)}\ \frac{\mathtt{w} \notin \{\mathtt{null}, 0, ☣\}}{\mathtt{if}\ (\mathtt{w})\ \{\mathtt{e}_1\}\ \mathtt{else}\ \{\mathtt{e}_2\} \rightarrow_h \mathtt{e}_1} \qquad \text{(TRG-DYN-IF-FALSY)}\ \frac{\mathtt{w} \in \{\mathtt{null}, 0\}}{\mathtt{if}\ (\mathtt{w})\ \{\mathtt{e}_1\}\ \mathtt{else}\ \{\mathtt{e}_2\} \rightarrow_h \mathtt{e}_2}$$

$$\text{(TRG-DYN-MALLOC)}\ \frac{n > 0 \quad \psi' = \psi[b \mapsto n] \quad \mu' = \mu[\langle b, i \rangle \mapsto ☣ \mid i < n] \quad \ell = \langle b, 0 \rangle \quad b \in \mathbb{N}^+ \setminus \mathrm{dom}(\psi)}{(\psi, \mu, \mathtt{malloc}\ (\mathtt{n})) \rightarrow_h (\psi', \mu', \ell)}$$

$$\text{(TRG-DYN-LOAD)}\ \frac{\mu(\ell) = \mathtt{w}}{(\mu, *\ell) \rightarrow_h (\mu, \mathtt{w})} \qquad \text{(TRG-DYN-STORE)}\ \frac{\ell \in \mathrm{dom}(\mu) \quad \mu' = \mu[\ell \mapsto \mathtt{w}]}{(\mu, *\ell = \mathtt{w};\ \mathtt{e}) \rightarrow_h (\mu', \mathtt{e})}$$

$$\text{(TRG-DYN-FREE)}\ \frac{\ell = \langle b, 0 \rangle \quad \psi(b) = n \quad \mathsf{span}(b \mapsto n) \subseteq \mathrm{dom}(\mu) \quad \mu' = \mu \setminus \mathsf{span}(b \mapsto n)}{(\psi, \mu, \mathtt{free}\ (\ell);\ \mathtt{e}) \rightarrow_h (\psi, \mu', \mathtt{e})}$$

$$\text{(TRG-DYN-INCR)}\ \frac{\mu(\ell) = \mathtt{n} \quad n' = n + 1 \quad \mu' = \mu[\ell \mapsto n']}{(\mu, {++}\ell) \rightarrow_h (\mu', \mathtt{n}')} \qquad \text{(TRG-DYN-DECR)}\ \frac{\mu(\ell) = \mathtt{n} \quad n' = n - 1 \quad \mu' = \mu[\ell \mapsto n']}{(\mu, {--}\ell) \rightarrow_h (\mu', \mathtt{n}')}$$

$$\text{(TRG-DYN-CTX)}\ \frac{\mathtt{F} \vdash (\psi, \mu, \mathtt{e}) \rightarrow_h (\psi', \mu', \mathtt{e}')}{\mathtt{F} \vdash (\psi, \mu, \mathtt{K}[\mathtt{e}]) \rightarrow (\psi', \mu', \mathtt{K}[\mathtt{e}'])}$$

Fig. B.2. Dynamics for target.

C Compiler

$\boxed{\Sigma; \Gamma \vdash e : T \rightsquigarrow \mathtt{e} \dashv \mathtt{F}}$

(COMP-LET)
$$\frac{\Gamma_1 \vdash e_1 : T_1 \rightsquigarrow \mathtt{e}_1 \quad \Gamma_2, x : T_1 \vdash e_2 : T_2 \rightsquigarrow \mathtt{e}_2 \quad \Gamma_2 \not\ni x \quad \mathtt{e} = \mathtt{const}\ \mathtt{x} = \mathtt{e}_1;\ \mathtt{e}_2}{\Gamma_1, \Gamma_2 \vdash \mathsf{let}\ x = e_1; e_2 : T_2 \rightsquigarrow \mathtt{e}}$$

(COMP-VAR)
$$\Sigma; x : T \vdash x : T \rightsquigarrow \mathtt{x}$$

(COMP-DUP)
$$\frac{\Gamma \ni x : T' \quad \Sigma; \Gamma, x : T' \vdash e : T \rightsquigarrow \mathtt{e}}{\Sigma; \Gamma \vdash e : T \rightsquigarrow \underline{\mathtt{dup}}_{T'}\ (\mathtt{x})\ ; \mathtt{e}}$$

(COMP-DROP)
$$\frac{\Sigma; \Gamma \vdash e : T \rightsquigarrow \mathtt{e}}{\Sigma; \Gamma, x : T' \vdash e : T \rightsquigarrow \underline{\mathtt{drop}}^{\Sigma}_{T'}\ (\mathtt{x})\ ; \mathtt{e}}$$

(COMP-I-$\mathbb{Z}$)
$$\varnothing \vdash n : \mathbb{Z} \rightsquigarrow \mathtt{n}$$

(COMP-$\oplus$-$\mathbb{Z}$)
$$\frac{\Gamma_1 \vdash e_1 : \mathbb{Z} \rightsquigarrow \mathtt{e}_1 \quad \Gamma_2 \vdash e_2 : \mathbb{Z} \rightsquigarrow \mathtt{e}_2 \quad \mathtt{e} = \mathtt{e}_1 \oplus \mathtt{e}_2}{\Gamma_1, \Gamma_2 \vdash e_1 \oplus e_2 : \mathbb{Z} \rightsquigarrow \mathtt{e}}$$

(COMP-I-$\rightarrow$)
$$\frac{\begin{array}{c} \Gamma = \overline{y_j : T_j}^{j<m} \quad \Gamma \not\ni z_f, \overline{x}^{i<n}\ \text{distinct} \quad \mathtt{F} \supseteq \left\{ \begin{array}{l} \Gamma, z_f : \overline{T_i}^{i<n} \rightarrow T, \overline{x : T_i}^{i<n} \vdash e : T \rightsquigarrow \mathtt{e} \dashv \mathtt{F} \\ \mathtt{call}_k \left(\mathtt{z_f}, \overline{\mathtt{x_i}}^{i<n}\right) \left\{ \overline{\mathtt{const}\ \mathtt{y_j} = *(\mathtt{z_f} + 3 + \mathtt{j});\ \underline{\mathtt{dup}}_{T_j}\ (\mathtt{y_j})}^{j<m} ; \mathtt{e} \right\} \\ \mathtt{destr}_k\ (\mathtt{z_f}) \left\{ \overline{\mathtt{const}\ \mathtt{y_j} = *(\mathtt{z_f} + 3 + \mathtt{j});\ \underline{\mathtt{drop}}_{T_j}\ (\mathtt{y_j})}^{j<m} ; \mathtt{free}\ (\mathtt{z_f})\ ;\ 0 \right\} \end{array} \right\} \\ \mathtt{e_f} = \mathtt{const}\ \mathtt{z_f} = \mathtt{malloc}\ (3 + \mathtt{m});\ *\mathtt{z_f} = 1;\ *(\mathtt{z_f} + 1) = \mathtt{call}_k;\ *(\mathtt{z_f} + 2) = \mathtt{destr}_k;\ \overline{*(\mathtt{z_f} + 3 + \mathtt{j}) = \mathtt{y_j};}^{j<m}\ \mathtt{z_f} \end{array}}{\Gamma \vdash \mathsf{fn}\ z_f\ \overline{x_i}^{i<n} \{e\} : \overline{T_i}^{i<n} \rightarrow T \rightsquigarrow \mathtt{e_f} \dashv \mathtt{F}}$$

(COMP-E-$\rightarrow$)
$$\frac{\overline{\Gamma_i \vdash e_i : T_i \rightsquigarrow \mathtt{e_i}}^{i<n} \quad \Gamma_f \vdash e_f : \overline{T_i}^{i<n} \rightarrow T \rightsquigarrow \mathtt{e_f} \quad \mathtt{e} = \mathtt{const}\ \mathtt{x_f} = \mathtt{e_f};\ (*(\mathtt{x_f} + 1)) \left(\mathtt{x_f}, \overline{\mathtt{e_i}}^{i<n}\right)}{\overline{\Gamma_i}^{i<n}, \Gamma_f \vdash e_f\ \overline{e_i}^{i<n} : T \rightsquigarrow \mathtt{e}}$$

(COMP-I-struct)
$$\frac{\Sigma \ni \mathsf{rigid\ struct}\ X \left\{\overline{s_i : T_i}^{i<n}\right\} \quad \overline{\Sigma; \Gamma_i \vdash e_i : T_i \rightsquigarrow \mathtt{e_i}}^{i<n} \quad \mathtt{e} = \mathtt{const}\ \mathtt{x} = \mathtt{malloc}\ (\mathtt{n} + 1);\ *\mathtt{x} = 1;\ \overline{*(\mathtt{x} + \mathtt{i} + 1) = \mathtt{e_i};}^{i<n}\ \mathtt{x}}{\Sigma; \overline{\Gamma_i}^{i} \vdash \left\{\overline{s_i : e_i}^{i<n}\right\} : X \rightsquigarrow \mathtt{e}}$$

(COMP-E-struct)
$$\frac{\begin{array}{c} \Sigma \ni m\ \mathsf{struct}\ X \left\{\overline{s_i : T_i}^{i<n}\right\} \\ \Sigma; \Gamma \vdash e : X \rightsquigarrow \mathtt{e} \quad j < n \quad \mathtt{e_j} = \mathtt{const}\ \mathtt{x} = \mathtt{e};\ \mathtt{const}\ \mathtt{x_j} = *\left(\mathtt{x} + \underline{\mathtt{sel}}^{s_j}_{\Sigma.X} + 1\right);\ \underline{\mathtt{dup}}_{T_j}\ (\mathtt{x_j})\ ; \underline{\mathtt{drop}}^{\Sigma}_{X}\ (\mathtt{x})\ ; \mathtt{x_j} \end{array}}{\Sigma; \Gamma \vdash e.s_j : T_j \rightsquigarrow \mathtt{e_j}}$$

(COMP-I-enum)
$$\frac{\begin{array}{c} \Sigma \ni m\ \mathsf{enum}\ X \left\{\overline{s_i : T_i}^{i<n}\right\} \\ \Sigma; \Gamma \vdash e_j : T_j \rightsquigarrow \mathtt{e_j} \quad j < n \quad \mathtt{e} = \mathtt{const}\ \mathtt{x} = \mathtt{malloc}\ (3);\ *\mathtt{x} = 1;\ *(\mathtt{x} + 1) = \underline{\mathtt{sel}}^{s_j}_{\Sigma.X};\ *(\mathtt{x} + 2) = \mathtt{e_j};\ \mathtt{x} \end{array}}{\Sigma; \Gamma \vdash s_j\ e_j : X \rightsquigarrow \mathtt{e}}$$

(COMP-E-enum)
$$\frac{\begin{array}{c} \Sigma \ni \mathsf{rigid\ enum}\ X \left\{\overline{s_i : T_i}^{i<n}\right\} \quad \Sigma; \Gamma_1 \vdash e : X \rightsquigarrow \mathtt{e} \quad \overline{\Sigma; \Gamma_2, x_i : T_i \vdash e_i : T \rightsquigarrow \mathtt{e_i}}^{i<n} \quad \Gamma_2 \not\ni \overline{x}^{i<n} \\ \mathtt{e}' = \mathtt{const}\ \mathtt{x} = \mathtt{e};\ \mathtt{const}\ \mathtt{y} = *(\mathtt{x} + 1);\ \overline{\mathtt{if}\ (\mathtt{y} = \mathtt{i})\ \left\{\mathtt{const}\ \mathtt{x_i} = *(\mathtt{x} + 2);\ \underline{\mathtt{dup}}_{T_i}\ (\mathtt{x_i})\ ; \underline{\mathtt{drop}}^{\Sigma}_{X}\ (\mathtt{x})\ ; \mathtt{e_i}\right\}}^{i<n}\ \mathtt{else}\ \{\mathtt{havoc}\} \end{array}}{\Sigma; \Gamma_1, \Gamma_2 \vdash \mathsf{case}\ e\ \left\{\overline{s_i\ x_i \Rightarrow e_i}\right\} : T \rightsquigarrow \mathtt{e}'}$$

Fig. C.1. Core compiler for expressions.

$\boxed{\Sigma \dashv \mathsf{F}}$

(COMP-Σ)

$$\frac{\forall\, \mathsf{m}\;\mathsf{k}\;\mathsf{X}\;\{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\} \in \Sigma.\ \mathsf{m} = \mathsf{rigid} \wedge \mathsf{F} \supseteq \left\{\mathtt{destr}_{\mathsf{X}}\,(\mathtt{r})\,\left\{\underline{\mathtt{destr}}{}^{\Sigma}_{\mathsf{X}}\,(\mathtt{r})\right\}, \overline{\mathtt{sel}^{\mathsf{s_i}}_{\mathsf{X}}\,()\,\left\{\underline{\mathtt{sel}}{}^{\mathsf{s_i}}_{\Sigma.\mathsf{X}}\right\}}^{i<n}\right\}}{\Sigma \dashv \mathsf{F}}$$

Fig. C.2. Core compiler for programs.

$$\underline{\mathtt{dup}}_{\mathsf{T}}\,(\mathtt{x}) \triangleq \begin{cases} \mathtt{-1} & (\mathsf{T} = \mathbb{Z}) \\ \mathtt{++x} & (\text{otherwise}) \end{cases}$$

$$\underline{\mathtt{drop}}{}^{\Sigma}_{\mathsf{T}}\,(\mathtt{x}) \triangleq \begin{cases} \mathtt{-1} & (\mathsf{T} = \mathbb{Z}) \\ \mathtt{const\ y = --x;\ if\ (y)\ \{y\}\ else}\ \left\{\underline{\mathtt{destr}}{}^{\Sigma}_{\mathsf{T}}\,(\mathtt{x})\right\} & (\text{otherwise}) \end{cases}$$

$$\underline{\mathtt{destr}}_{\mathbb{Z}}\,(\mathtt{x}) \triangleq \mathtt{havoc}$$

$$\underline{\mathtt{destr}}_{\overline{\mathsf{T_1}} \to \mathsf{T_2}}\,(\mathtt{x}) \triangleq \mathtt{*(x+2)\,(x)}$$

$$\underline{\mathtt{destr}}{}^{\Sigma}_{\mathsf{X}}\,(\mathtt{x}) \triangleq \begin{cases} \overline{\mathtt{const\ x_i = x[i+1];}\ \underline{\mathtt{drop}}{}^{\Sigma}_{\mathsf{T_i}}\,(\mathtt{x_i})\,;}^{i<n}\ \mathtt{free\,(x)\,;\ 0} & (\Sigma \ni \mathsf{rigid\ struct\ X}\ \{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\}) \\ \mathtt{destr}_{\mathsf{X}}\,(\mathtt{x}) & (\Sigma \ni \mathsf{flex\ struct\ X}\ \{\cdots\}) \end{cases}$$

$$\underline{\mathtt{destr}}{}^{\Sigma}_{\mathsf{X}}\,(\mathtt{x}) \triangleq \begin{cases} \overline{\begin{array}{l}\mathtt{if\ (x[1] = i)\ \{} \\ \quad \overline{\mathtt{const\ x_i = x[2];}\ \underline{\mathtt{drop}}{}^{\Sigma}_{\mathsf{T_i}}\,(\mathtt{x_i})\,;\ \mathtt{free\,(x)\,;\ 0}}^{i<n} \\ \mathtt{\}\ else\ \{havoc\}}\end{array}} & (\Sigma \ni \mathsf{rigid\ enum\ X}\ \{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\}) \\ \mathtt{destr}_{\mathsf{X}}\,(\mathtt{x}) & (\Sigma \ni \mathsf{flex\ enum\ X}\ \{\cdots\}) \end{cases}$$

$$\underline{\mathtt{sel}}{}^{\mathsf{s_j}}_{\Sigma.\mathsf{X}} \triangleq \begin{cases} \mathtt{j} & (\Sigma \ni \mathsf{rigid\ k\ X}\ \{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\} \wedge j < n), \\ \mathtt{sel}^{\mathsf{s_j}}_{\mathsf{X}}\,() & (\Sigma \ni \mathsf{flex\ k\ X}\ \{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\} \wedge j < n), \end{cases}$$

Fig. C.3. Macros for the core compiler.

D Logic

$$
\begin{array}{llll}
P, Q, R & \in \mathit{Prd} & \triangleq & \left\{P : \mathsf{Wld} \to \mathsf{Res} \to \mathbb{P} \mid \forall\, \rho, \omega \sqsubseteq \omega^{+}.\ P(\omega, \rho) \Rightarrow P(\omega^{+}, \rho)\right\} \\
 & & & \text{A predicate on worlds and resources that is closed under world extension.} \\
\hat{P}, \hat{Q}, \hat{R} & \in \mathit{Prd}\,(X) & \triangleq & X \to \mathit{Prd} \\
\omega & \in \mathsf{Wld} & \triangleq & \langle \mathsf{step} : \mathbb{N}, \mathsf{sizes} : \mathsf{Sizes} \rangle \\
\rho & \in \mathsf{Res} & \triangleq & \mathsf{Loc}_{\mathbb{N}^{+}} \xrightharpoonup{\text{fin}} \mathsf{Cell} \\
 & & & \text{A logical memory with two kinds of cells, which forms a tree.} \\
\chi & \in \mathsf{Cell} & \triangleq & \mathsf{unq}(\mathtt{Word}) \mid \mathsf{shr}(\mathbb{N}^{+}, \mathsf{Res}) \\
 & & & \text{Either a unique, owned word, or a shared, reference-counted resource.} \\
\gamma & \in \mathsf{CtxSub} & \triangleq & \mathtt{Var} \xrightharpoonup{\text{fin}} \mathtt{Word} \\
\varsigma & \in \mathsf{SigSub} & \triangleq & \mathsf{TypeName} \xrightharpoonup{\text{fin}} \mathsf{DataSub} \\
\delta & \in \mathsf{DataSub} & \triangleq & \Big\{\delta : \Big\langle \mathsf{kind} : \mathsf{Kind}, \mathsf{sel} : \mathsf{Sel} \xrightharpoonup{\text{fin}} \langle \mathsf{off} : \mathbb{N}, \mathsf{semty} : \mathtt{Word} \to \mathit{Prd} \rangle \Big\rangle \mid \\
 & & & \quad \forall\, \mathsf{s}_1 \neq \mathsf{s}_2.\ \delta.\mathsf{sel}(\mathsf{s}_1).\mathsf{off} \neq \delta.\mathsf{sel}(\mathsf{s}_2).\mathsf{off} \Big\}
\end{array}
$$

Fig. D.1. Semantic domains.

$\omega_1 \sqsubseteq \omega_2 \triangleq \omega_1.\mathsf{step} \geq \omega_2.\mathsf{step} \wedge \omega_1.\mathsf{sizes} \subseteq \omega_2.\mathsf{sizes}$
World extension: step index can go down and new locations can be allocated.

$\blacktriangleright\omega \triangleq \begin{cases}\omega[\mathsf{step} := k] & (\omega.\mathsf{step} = k+1)\end{cases}$
Later: decrement the step index if possible.

$r_1 \sharp r_2 \triangleq \exists r.\ r_1 \bullet r_2 = r \wedge \checkmark r$
Two resources are compatible if their composition is defined and valid.

$r_1 \leq r_2 \triangleq \exists r_0.\ r_0 \bullet r_1 = r_2$
A sub-resource is one that can be extended to the other resource.

$\checkmark \chi \triangleq \top$

$\chi_1 \bullet \chi_2 \triangleq \begin{cases}\mathsf{shr}(n_1 + n_2, \rho) & (\chi_1 = \mathsf{shr}(n_1, \rho) \wedge \chi_2 = \mathsf{shr}(n_2, \rho))\end{cases}$
Only shared cells can be composed; they must agree on the resource and add counts.

$\mathsf{erase}(\chi) \triangleq \begin{cases}\mathtt{w}, & \chi = \mathsf{unq}(\mathtt{w}) \\ \mathtt{n}, & \chi = \mathsf{shr}(n, -)\end{cases}$
Erasure of a unique logical cell to a physical one only keeps the word, while shared logical cells keep the reference count; resource erasure handles the rest.

$\checkmark \rho \triangleq \forall (\ell_1, \rho_1) \in \mathsf{objs}(\rho).\ \rho \sharp_{\mathsf{sh}} \rho_1 \wedge \forall (\ell_2, \rho_2) \in \mathsf{objs}(\rho).\ (\ell_1 = \ell_2 \wedge \rho_1 = \rho_2) \vee (\ell_1 \neq \ell_2 \wedge \rho_1 \sharp_{\mathsf{sh}} \rho_2)$
For a resource to be valid, any reachable object must be compatible with the root, as well as with any other reachable object.

$$\rho_1 \bullet \rho_2 \triangleq \begin{cases} \quad [\ell \mapsto \chi \in \rho_1 \mid \ell \notin \mathrm{dom}(\rho_2)] & \\ \uplus\ [\ell \mapsto \chi \in \rho_2 \mid \ell \notin \mathrm{dom}(\rho_1)] & (\rho_1 \sharp_{\mathsf{sh}} \rho_2) \\ \uplus\ [\ell \mapsto \chi_1 \bullet \chi_2 \mid \rho_1(\ell) = \chi_1 \wedge \rho_2(\ell) = \chi_2] & \end{cases}$$
Disjoint locations are included unchanged.
Overlapping locations must have composable cells.

$\mathsf{erase}(\rho) \triangleq \begin{cases}\left[\ell \mapsto \mathsf{erase}(\chi) \mid \ell \mapsto \chi \in \rho \bullet \left(\bigodot_{(\ell, \rho_\ell) \in \mathsf{objs}(\rho)} \rho_\ell\right)\right] & (\checkmark \rho)\end{cases}$
First, flatten the logical heap by composing the root and all objects, getting the total counts. Then erase the flat heap (without recurring).

$\mathsf{objs}(\rho) \triangleq \left[(\ell, \rho_\ell) \mid \rho \twoheadrightarrow \ell \mapsto \mathsf{shr}(-, \rho_\ell)\right]$
Collects the reachable objects (shared resources).

$\rho_1 \sharp_{\mathsf{sh}} \rho_2 \triangleq \forall \ell \in \mathrm{dom}(\rho_1) \cap \mathrm{dom}(\rho_2).\ \rho_1(\ell) \sharp \rho_2(\ell)$
Shallow or weak compatibility; doesn't check recursively. Used to define validity above.

$\boxed{\rho \twoheadrightarrow \rho'}$ ρ can reach ρ' via jumps or discarding cells.

$$\frac{}{\ell \mapsto \mathsf{shr}(-, \rho) \twoheadrightarrow \rho}\ (\twoheadrightarrow\text{-JUMP}) \qquad \frac{\rho_1 \geq \rho_2}{\rho_1 \twoheadrightarrow \rho_2}\ (\twoheadrightarrow\text{-SUB}) \qquad \frac{\rho_1 \twoheadrightarrow \rho_2 \quad \rho_2 \twoheadrightarrow \rho_3}{\rho_1 \twoheadrightarrow \rho_3}\ (\twoheadrightarrow\text{-TRANS})$$

Fig. D.2. Operators and relations on semantic objects.

$$\ell \mapsto \mathtt{w} \quad (\omega, \rho) \triangleq \rho = \ell \mapsto \mathsf{unq}(\mathtt{w})$$
Points-to predicate only identifies unique cells.

$$\mathit{size}\,(\ell,\ n) \quad (\omega, \rho) \triangleq \rho = \varnothing \land \exists\, b.\ \ell = \langle b, 0\rangle \land \omega.\mathsf{sizes}(b) = n$$
Asserts ℓ is a head pointer to a block of size n, *without any ownership.*

$$\ulcorner P \urcorner \quad (\omega, \rho) \triangleq \rho = \varnothing \land P$$
Lifts propositions from the meta-logic.

$$@_\ell\, P \quad (\omega, \rho) \triangleq \exists\, \rho_p.\ \rho = \ell \mapsto \mathsf{shr}(1, \rho_p) \land P(\omega, \rho_p)$$
Jump modality: asserts ℓ shares a res. satisfying P, and confers 1 share of the count.

$$\Diamond P \quad (\omega, \rho) \triangleq \exists\, \rho_p.\ \rho \twoheadrightarrow \rho_p \land P(\omega, \rho_p)$$
Reachable modality: asserts a res. satisfying P is reachable from the current res.

$$!\, P \quad (\omega, \rho) \triangleq \rho = \varnothing \land P(\omega, \varnothing)$$
Persistence modality: P but without owning anything.

$$\triangleright P \quad (\omega, \rho) \triangleq \omega.\mathsf{step} = 0 \lor (\omega.\mathsf{step} > 0 \land P(\blacktriangleright\omega, \rho))$$
Later modality: out of steps or P holds one step later.

$$\mathit{wp}_{\mathtt{F}}\ (\mathtt{e})\ \{\hat{Q}\} \quad (\omega, \rho) \triangleq \left\{\begin{array}{l} \forall\, \omega^+ \sqsupseteq \omega, \rho_f \sharp \rho, k < \omega^+.\mathsf{step}, \psi', \mu', \mathtt{e}', \\ \psi = \omega^+.\mathsf{sizes}, \omega' = \left\langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \right\rangle. \\ \qquad \mathtt{F} \vdash (\psi, \mathsf{erase}(\rho \bullet \rho_f), \mathtt{e}) \rightarrow^k (\psi', \mu', \mathtt{e}') \not\rightarrow \\ \quad \Rightarrow \quad \exists\, \rho' \sharp \rho_f. \\ \qquad\qquad\quad \psi' \supseteq \psi \\ \qquad\quad \land \quad \mathsf{erase}(\rho' \bullet \rho_f) = \mu' \\ \qquad\quad \land \quad \mathtt{e}' \in \mathtt{Word} \\ \qquad\quad \land \quad \hat{Q}(\mathtt{e}')(\omega', \rho') \end{array}\right.$$
Weakest precondition modality: $\mathtt{e}$ is safe to run with the current res.,
and if it halts within the given step budget, it preserves arbitrary frames,
respects the world order, and terminates at a state and value satisfying $\hat{Q}$.

$$\mathit{emp} \quad (\omega, \rho) \triangleq \rho = \varnothing$$
$$P \star Q \quad (\omega, \rho) \triangleq \exists\, \rho_p, \rho_q.\ \rho = \rho_p \bullet \rho_q \land P(\omega, \rho_p) \land Q(\omega, \rho_q)$$
$$P \mathrel{-\!\!\star} Q \quad (\omega, \rho) \triangleq \forall\, \omega^+ \sqsupseteq \omega, \rho_p \sharp \rho, \rho_q.\ \rho \bullet \rho_p = \rho_q \Rightarrow P(\omega^+, \rho_p) \Rightarrow Q(\omega^+, \rho_q)$$
$$\top \quad (\omega, \rho) \triangleq \top$$
$$\bot \quad (\omega, \rho) \triangleq \bot$$
$$P \land Q \quad (\omega, \rho) \triangleq P(\omega, \rho) \land Q(\omega, \rho)$$
$$P \lor Q \quad (\omega, \rho) \triangleq P(\omega, \rho) \lor Q(\omega, \rho)$$
$$P \Rightarrow Q \quad (\omega, \rho) \triangleq \forall\, \omega^+ \sqsupseteq \omega.\ P(\omega^+, \rho) \Rightarrow Q(\omega^+, \rho)$$
$$\forall\, \hat{P} \quad (\omega, \rho) \triangleq \forall\, \omega^+ \sqsupseteq \omega, x.\ \hat{P}(x)(\omega^+, \rho)$$
$$\exists\, \hat{P} \quad (\omega, \rho) \triangleq \exists\, x.\ \hat{P}(x)(\omega, \rho)$$

$$\{P\}\ \mathtt{e}\ \{\hat{Q}\}_{\mathtt{F}} \triangleq\ !\ \left(P \mathrel{-\!\!\star} \mathit{wp}_{\mathtt{F}}\ (\mathtt{e})\ \{\hat{Q}\}\right)$$
$$P \equiv Q \triangleq\ !\ (P \mathrel{-\!\!\star} Q) \star\ !\ (Q \mathrel{-\!\!\star} P)$$

$$P \vDash Q \triangleq \forall\, \rho, \omega.\ \checkmark\, \rho \Rightarrow P(\omega, \rho) \Rightarrow Q(\omega, \rho)$$
Entailment is only required to hold on valid resources.

Fig. D.3. Semantic predicates.

$$\text{(REFL)}\ \ P \vDash P \qquad \text{(TRANS)}\ \ \frac{P \vDash Q \quad Q \vDash R}{P \vDash R} \qquad (\vee\text{-R})\ \ \frac{P \vDash Q_i}{P \vDash Q_1 \vee Q_2} \qquad (\vee\text{-L})\ \ \frac{P \vDash R \quad Q \vDash R}{P \vee Q \vDash R} \qquad (\wedge\text{-R})\ \ \frac{P \vDash Q \quad P \vDash R}{P \vDash Q \wedge R} \qquad (\wedge\text{-L})\ \ P_1 \wedge P_2 \vDash P_i$$

$$(\wedge\text{-MONO})\ \ \frac{P_1 \vDash Q_1 \quad P_2 \vDash Q_2}{P_1 \wedge P_2 \vDash Q_1 \wedge Q_2} \qquad (\forall\text{-R})\ \ \frac{\forall x.\, P \vDash \hat{Q}(x)}{P \vDash \forall\, \hat{Q}} \qquad (\forall\text{-L})\ \ \frac{\exists x.\, \hat{P}(x) \vDash Q}{\forall\, \hat{P} \vDash Q} \qquad (\exists\text{-R})\ \ \frac{\exists x.\, P \vDash \hat{Q}(x)}{P \vDash \exists\, \hat{Q}} \qquad (\exists\text{-L})\ \ \frac{\forall x.\, \hat{P}(x) \vDash Q}{\exists\, \hat{P} \vDash Q}$$

Fig. D.4. Standard intuitionistic logic rules.

$$(emp\text{-LR})\ \ P \dashv\vDash P \star emp \qquad (\ulcorner - \urcorner\text{-R})\ \ \frac{P}{\vDash \ulcorner P \urcorner} \qquad (\ulcorner - \urcorner\text{-L})\ \ \frac{P \Rightarrow Q \vDash R}{\ulcorner P \urcorner \star Q \vDash R} \qquad (\star\text{-COM})\ \ P \star Q \dashv\vDash Q \star P \qquad (\star\text{-ASC})\ \ P \star (Q \star R) \dashv\vDash (P \star Q) \star R$$

$$(\star\text{-MONO})\ \ \frac{P_1 \vDash Q_1 \quad P_2 \vDash Q_2}{P_1 \star P_2 \vDash Q_1 \star Q_2} \qquad (-\!\!\star\text{-R})\ \ \frac{P \star Q \vDash R}{P \vDash Q -\!\!\star R} \qquad (-\!\!\star\text{-L})\ \ P \star (P -\!\!\star Q) \vDash Q \qquad (-\!\!\star\text{-MONO})\ \ \frac{Q_1 \vDash P_1 \quad P_2 \vDash Q_2}{P_1 -\!\!\star P_2 \vDash Q_1 -\!\!\star Q_2}$$

$$(-\!\!\star\text{-}emp)\ \ P \dashv\vDash emp -\!\!\star P \qquad (-\!\!\star\text{-SELF})\ \ \vDash P -\!\!\star P \qquad (-\!\!\star\text{-CURRY})\ \ (P \star Q) -\!\!\star R \dashv\vDash P -\!\!\star (Q -\!\!\star R) \qquad (\star\text{-}\exists)\ \ P \star \exists\, \hat{Q} \dashv\vDash \exists\, x.\, P \star \hat{Q}(x)$$

$$(\equiv\text{-REFL})\ \ \vDash P \equiv P \qquad (\equiv\text{-SYM})\ \ P \equiv Q \dashv\vDash Q \equiv P \qquad (\equiv\text{-TRANS})\ \ \frac{\vDash P \equiv Q \quad \vDash Q \equiv R}{\vDash P \equiv R} \qquad (\equiv\text{-L})\ \ P \star (P \equiv Q) \vDash Q$$

Fig. D.5. Standard separation logic rules.

$$(!\text{-UNR})\ \ !P \dashv\vDash !P \star !P \qquad (!\text{-}\wedge\text{-}emp)\ \ !P \dashv\vDash emp \wedge P \qquad (!\text{-L})\ \ !P \vDash P \qquad (!\text{-DROP})\ \ !P \vDash emp \qquad (!\text{-IDEM})\ \ !P \dashv\vDash !!P \qquad (!\text{-MONO})\ \ \frac{P \vDash Q}{!P \vDash !Q}$$

$$(!\text{-}emp)\ \ emp \vDash !\, emp \qquad (!\text{-}\ulcorner - \urcorner)\ \ \ulcorner P \urcorner \vDash !\ulcorner P \urcorner \qquad (!\text{-}size\,(-, -))\ \ size\,(\ell, n) \vDash !\, size\,(\ell, n) \qquad (!\text{-}\{-\} - \{-\})\ \ \{P\}\,\mathsf{e}\,\{\hat{Q}\} \vDash !\,\{P\}\,\mathsf{e}\,\{\hat{Q}\}$$

$$(!\text{-}\equiv)\ \ P \equiv Q \vDash !\,(P \equiv Q) \qquad (!\text{-}\star)\ \ !\,(P \star Q) \dashv\vDash !P \star !Q \qquad (!\text{-}\wedge)\ \ !\,(P \wedge Q) \dashv\vDash !P \wedge !Q \qquad (!\text{-}\wedge_1)\ \ !P \wedge Q \dashv\vDash !\,(P \wedge Q)$$

$$(!\text{-}\wedge/\star)\ \ !\,(P \wedge Q) \dashv\vDash !\,(P \star Q) \qquad (!\text{-}\forall)\ \ \frac{\hat{P} \in Prd\,(X) \quad X \text{ is inhabited}}{!\forall\, \hat{P} \dashv\vDash \forall\, !\hat{P}} \qquad (!\text{-}\triangleright)\ \ !\triangleright P \vDash \triangleright !P \qquad (\triangleright\text{-}!)\ \ emp \wedge \triangleright !P \vDash !\triangleright P$$

Fig. D.6. Unrestricted modality rules.

$$(\triangleright\text{-R})\quad P \vDash \triangleright P$$

$$(\triangleright\text{-IND})\quad \frac{P \wedge \triangleright Q \vDash Q}{P \vDash Q}$$

$$(\triangleright\text{-MONO})\quad \frac{P \vDash Q}{\triangleright P \vDash \triangleright Q}$$

$$(\triangleright\text{-}\wedge)\quad \triangleright (P \wedge Q) \dashv\vDash \triangleright P \wedge \triangleright Q$$

$$(\triangleright\text{-}\star)\quad \triangleright (P \star Q) \dashv\vDash \triangleright P \star \triangleright Q$$

$$(\triangleright\text{-}\mathrel{-\!\star})\quad \triangleright (P \mathrel{-\!\star} Q) \vDash \triangleright P \mathrel{-\!\star} \triangleright Q$$

Fig. D.7. Later modality rules.

$$(@\text{-MONO})\quad \frac{P \vDash Q}{@_\ell P \vDash @_\ell Q}$$

$$(@\text{-}!)\quad @_\ell P \star !Q \dashv\vDash @_\ell (P \star !Q)$$

$$(@\text{-}\vee)\quad @_\ell (P \vee Q) \dashv\vDash @_\ell P \vee @_\ell Q$$

$$(@\text{-}\exists)\quad @_\ell \exists \hat{P} \dashv\vDash \exists @_\ell \hat{P}$$

$$(@\text{-}\triangleright)\quad @_\ell \triangleright P \vDash \triangleright @_\ell P$$

$$(@\text{-}\bot)\quad @_\ell \bot \vDash \bot$$

$$(\Diamond\text{-R})\quad P \vDash \Diamond P$$

$$(\Diamond\text{-MONO})\quad \frac{P \vDash Q}{\Diamond P \vDash \Diamond Q}$$

$$(\Diamond\text{-BIND})\quad \frac{P \vDash \Diamond Q}{\Diamond P \vDash \Diamond Q}$$

$$(\Diamond\text{-IDEM})\quad \Diamond \Diamond P \vDash \Diamond P$$

$$(\Diamond\text{-}@)\quad @_\ell P \vDash \Diamond P$$

$$(\Diamond\text{-DROP})\quad \Diamond (P \star Q) \vDash \Diamond P$$

$$(\Diamond\text{-}!)\quad \frac{P \vDash \Diamond !Q}{P \vDash P \star !Q}$$

Fig. D.8. Non-standard entailments.

$$\textsc{(wp-ramify)}\quad \left(\forall\, \mathtt{w}.\ \hat{P}(\mathtt{w}) \mathrel{-\!\!\star} \hat{Q}(\mathtt{w})\right) \star wp\,(\mathtt{e})\,\{\hat{P}\} \vDash wp\,(\mathtt{e})\,\{\hat{Q}\}$$

$$\textsc{(wp-frame)}\quad P \star wp\,(\mathtt{e})\,\{\hat{Q}\} \vDash wp\,(\mathtt{e})\,\{\mathtt{w}.\ P \star \hat{Q}(\mathtt{w})\}$$

$$\textsc{(wp-mono)}\quad \frac{\forall\, \mathtt{w}.\ \hat{P}(\mathtt{w}) \vDash \hat{Q}(\mathtt{w})}{wp\,(\mathtt{e})\,\{\hat{P}\} \vDash wp\,(\mathtt{e})\,\{\hat{Q}\}}$$

$$\textsc{(wp-val)}\quad \hat{Q}(\mathtt{w}) \vDash wp\,(\mathtt{w})\,\{\hat{Q}\}$$

$$\textsc{(wp-bind)}\quad wp\,(\mathtt{e})\,\{\mathtt{w}.\ wp\,(\mathtt{K}[\mathtt{w}])\,\{\hat{Q}\}\} \vDash wp\,(\mathtt{K}[\mathtt{e}])\,\{\hat{Q}\}$$

$$\textsc{(wp-let)}\quad \triangleright\, wp\,(\mathtt{e}[\mathtt{w}/\mathtt{x}])\,\{\hat{Q}\} \vDash wp\,(\mathtt{const\ x = w;\ e})\,\{\hat{Q}\}$$

$$\textsc{(wp-seq)}\quad wp\,(\mathtt{e}_1)\,\{\_.\ \triangleright\, wp\,(\mathtt{e}_2)\,\{\hat{Q}\}\} \vDash wp\,(\mathtt{e}_1;\mathtt{e}_2)\,\{\hat{Q}\}$$

$$\textsc{(wp-bop)}\quad \frac{\mathtt{w} = [\![\oplus]\!](\mathtt{w}_1, \mathtt{w}_2)}{\triangleright\, \hat{Q}(\mathtt{w}) \vDash wp\,(\mathtt{w}_1 \oplus \mathtt{w}_2)\,\{\hat{Q}\}}$$

$$\textsc{(wp-funptr)}\quad \frac{\mathtt{F} \ni \mathtt{f}\,(\overline{\mathtt{x}})\,\{\mathtt{e}\}}{\triangleright\, \hat{Q}(\langle \mathtt{f}\rangle_{\mathtt{F}}) \vDash wp_{\mathtt{F}}\,(\mathtt{f})\,\{\hat{Q}\}}$$

$$\textsc{(wp-app)}\quad \frac{\mathtt{F} \ni \mathtt{f}\,(\overline{\mathtt{x}})\,\{\mathtt{e}\}}{\triangleright\, wp_{\mathtt{F}}\left(\mathtt{e}[\overline{\mathtt{w}/\mathtt{x}}]\right)\{\hat{Q}\} \vDash wp_{\mathtt{F}}\,(\langle \mathtt{f}\rangle_{\mathtt{F}}\,(\overline{\mathtt{w}}))\,\{\hat{Q}\}}$$

$$\textsc{(wp-if-t)}\quad \frac{\mathtt{w} \notin \{\mathtt{null}, 0, ☣\}}{\triangleright\, wp\,(\mathtt{e}_1)\,\{\hat{Q}\} \vDash wp\,(\mathtt{if\ (w)\ \{e_1\}\ else\ \{e_2\}})\,\{\hat{Q}\}}$$

$$\textsc{(wp-if-f)}\quad \frac{\mathtt{w} \in \{\mathtt{null}, 0\}}{\triangleright\, wp\,(\mathtt{e}_2)\,\{\hat{Q}\} \vDash wp\,(\mathtt{if\ (w)\ \{e_1\}\ else\ \{e_2\}})\,\{\hat{Q}\}}$$

$$\textsc{(wp-malloc)}\quad \frac{n > 0}{\triangleright \left(\forall\, \mathsf{Loc}_{\mathbb{N}^+}.\ \left(\bigstar_{i<n} (\ell + i) \mapsto ☣\right) \mathrel{-\!\!\star} size\,(\ell,\, n) \mathrel{-\!\!\star} \hat{Q}(\ell)\right) \vDash wp\,(\mathtt{malloc\ (n)})\,\{\hat{Q}\}}$$

$$\textsc{(wp-free)}\quad \left(\bigstar_{i<n} (\ell + i) \mapsto \mathtt{w}_i\right) \star size\,(\ell,\, n) \star \triangleright\, wp\,(\mathtt{e})\,\{\hat{Q}\} \vDash wp\,(\mathtt{free\ (}\ell\mathtt{)\ ;\ e})\,\{\hat{Q}\}$$

$$\textsc{(wp-load)}\quad \frac{P \vDash \Diamond\, \ell \mapsto \mathtt{w}}{P \star \triangleright \left(P \mathrel{-\!\!\star} \hat{Q}(\mathtt{w})\right) \vDash wp\,(*\ell)\,\{\hat{Q}\}}$$

$$\textsc{(wp-store)}\quad \ell \mapsto - \star \triangleright \left(\ell \mapsto \mathtt{w} \mathrel{-\!\!\star} wp\,(\mathtt{e})\,\{\hat{Q}\}\right) \vDash wp\,(*\ell = \mathtt{w};\ \mathtt{e})\,\{\hat{Q}\}$$

$$\textsc{(wp-incr-own)}\quad \frac{n' = n + 1}{\ell \mapsto \mathtt{n} \star \triangleright \left(\ell \mapsto \mathtt{n}' \mathrel{-\!\!\star} \hat{Q}(\mathtt{n}')\right) \vDash wp\,(\mathtt{++}\ell)\,\{\hat{Q}\}}$$

$$\textsc{(wp-decr-own)}\quad \frac{n' = n - 1}{\ell \mapsto \mathtt{n} \star \triangleright \left(\ell \mapsto \mathtt{n}' \mathrel{-\!\!\star} \hat{Q}(\mathtt{n}')\right) \vDash wp\,(\mathtt{--}\ell)\,\{\hat{Q}\}}$$

$$\textsc{(wp-incr-share)}\quad \frac{P \vDash \Diamond\, @_\ell\, Q}{P \star \triangleright \left(\forall\, n > 1.\ P \mathrel{-\!\!\star} @_\ell\, Q \mathrel{-\!\!\star} \hat{R}(\mathtt{n})\right) \vDash wp\,(\mathtt{++}\ell)\,\{\hat{R}\}}$$

$$\textsc{(wp-decr-share)}\quad @_\ell\, P \star \triangleright \left(\forall\, n.\ (\ulcorner n > 0 \urcorner \lor (\ulcorner n = 0 \urcorner \star \ell \mapsto 0 \star P)) \mathrel{-\!\!\star} \hat{Q}(\mathtt{n})\right) \vDash wp\,(\mathtt{--}\ell)\,\{\hat{Q}\}$$

$$\textsc{(wp-share)}\quad \ell \mapsto 1 \star P \star (@_\ell\, P \mathrel{-\!\!\star} wp\,(\mathtt{e})\,\{\hat{Q}\}) \vDash wp\,(\mathtt{e})\,\{\hat{Q}\}$$

$$\textsc{(ht-app)}\quad P \star \{P\}\,\mathtt{e}\,\{\hat{Q}\} \vDash wp\,(\mathtt{e})\,\{\hat{Q}\}$$

Fig. D.9. Weakest preconditions.

E ABI

$$\Sigma;\Gamma \vDash_{\mathsf{F}} \mathsf{e} : \mathsf{T} \triangleq \forall \mathsf{F}' \supseteq \mathsf{F}, \varsigma, \gamma.\ \mathcal{S}[\![\Sigma]\!]_{\mathsf{F}'}(\varsigma) \star \mathcal{C}[\![\Gamma]\!]^{\varsigma}_{\mathsf{F}'}(\gamma) \vDash \mathcal{E}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}'}(\mathsf{e}[\gamma])$$

$$\begin{array}{lcl}
\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma) & \triangleq & !\left(\begin{array}{l}
\ulcorner \mathrm{dom}(\varsigma) \supseteq \mathrm{dom}(\Sigma)\urcorner \\
\star \forall\ \mathsf{m}\ \mathsf{k}\ \mathsf{X}\ \{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\} \in \Sigma.\ \mathsf{let}\ \delta = \varsigma(\mathsf{X})\ \mathsf{in} \\
\quad \ulcorner \delta.\mathsf{kind} = \mathsf{k}\urcorner \\
\quad \star \ulcorner \mathrm{dom}(\delta.\mathsf{sel}) \supseteq \{\mathsf{s_i} \mid i < n\}\urcorner \\
\quad \star \forall\ i < n.\ !\ wp_{\mathsf{F}} \left(\langle \mathtt{sel}^{\mathsf{s_i}}_{\mathsf{X}}\rangle_{\mathsf{F}}\ ()\right) \{\mathtt{w}.\ \ulcorner \mathtt{w} = \delta.\mathsf{sel}(\mathsf{s_i}).\mathsf{off}\urcorner\} \\
\quad \star \forall\ i < n, \mathtt{w}.\ \delta.\mathsf{sel}(\mathsf{s_i}).\mathsf{semty}(\mathtt{w}) \equiv \triangleright \mathcal{V}[\![\mathsf{T_i}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}) \\
\quad \star \forall\ \ell.\ \{\ell \mapsto 0 \star \delta.\mathsf{obj}(\ell+1)\}\ \langle \mathtt{destr}_{\mathsf{X}}\rangle_{\mathsf{F}}\ (\ell)\ \{emp\}_{\mathsf{F}} \\
\quad \star \ulcorner \mathsf{m} = \mathsf{rigid} \Rightarrow \mathrm{dom}(\delta.\mathsf{sel}) \subseteq \{\mathsf{s_i} \mid i < n\} \wedge \forall i < n.\ \delta.\mathsf{sel}(\mathsf{s_i}).\mathsf{off} = i\urcorner
\end{array}\right) \\
\mathcal{C}[\![\Gamma]\!]^{\varsigma}_{\mathsf{F}}(\gamma) & \triangleq & \ulcorner \mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\Gamma)\urcorner \star \bigstar_{\mathsf{x}:\mathsf{T}\in\Gamma} \mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\gamma(\mathsf{x})) \\
\mathcal{E}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathsf{e}) & \triangleq & wp_{\mathsf{F}}\ (\mathsf{e})\ \{\mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}\} \\
\delta.\mathsf{obj}(\ell+1) & \triangleq & \left\{\begin{array}{ll}
size\,(\ell,\ 1 + |\mathrm{dom}(\delta.\mathsf{sel})|) & \\
\star \bigstar_{\mathsf{s}\in\mathrm{dom}(\delta.\mathsf{sel})} \exists\ \mathtt{w_s}.\ \left(\begin{array}{l} \ell + 1 + \delta.\mathsf{sel}(\mathsf{s}).\mathsf{off} \mapsto \mathtt{w_s} \\ \star \delta.\mathsf{sel}(\mathsf{s}).\mathsf{semty}(\mathtt{w_s})\end{array}\right) & (\delta.\mathsf{kind} = \mathsf{struct}) \\
\hline
size\,(\ell,\ 3) & \\
\star \bigvee_{\mathsf{s}\in\mathrm{dom}(\delta.\mathsf{sel})} \exists\ \mathtt{w_s}\ \left(\begin{array}{l} \ell + 1 \mapsto \delta.\mathsf{sel}(\mathsf{s}).\mathsf{off} \\ \star \ell + 2 \mapsto \mathtt{w_s} \\ \star \delta.\mathsf{sel}(\mathsf{s}).\mathsf{semty}(\mathtt{w_s})\end{array}\right) & (\delta.\mathsf{kind} = \mathsf{enum})
\end{array}\right.
\end{array}$$

Fig. E.1. Top-level interpretations.

$$\begin{array}{lcl}
\mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}) & \triangleq & \left\{\begin{array}{ll} \mathcal{U}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}) & (\mathsf{T} = \mathbb{Z}) \\ \ulcorner \mathtt{w} \in \mathsf{Loc} \setminus \mathtt{null}\urcorner \star \mathcal{R}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}) & (\text{otherwise}) \end{array}\right. \\
\mathcal{R}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\ell) & \triangleq & @_{\ell}\, \mathcal{O}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\ell+1) \\
\mathcal{U}[\![\mathbb{Z}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}) & \triangleq & \ulcorner \mathtt{w} \in \mathbb{Z}\urcorner \\
\mathcal{O}\left[\!\!\left[\overline{\mathsf{T_i}}^{i<n} \rightarrow \mathsf{T}\right]\!\!\right]^{\varsigma}_{\mathsf{F}}(\ell+1) & \triangleq & \left\{\begin{array}{l}
\exists\ \mathtt{call}, \mathtt{destr}, Env.\ \mathsf{let}\ Self = \ell+1 \mapsto \langle \mathtt{call}\rangle_{\mathsf{F}} \star \ell+2 \mapsto \langle \mathtt{destr}\rangle_{\mathsf{F}} \star Env\ \mathsf{in} \\
\quad Self \\
\quad \star \forall\ \overline{\mathtt{w_i}}^{i<n}.\{\bigstar_{i<n} \mathcal{V}[\![\mathsf{T_i}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w_i}) \star @_{\ell}\, Self\}\ \langle \mathtt{call}\rangle_{\mathsf{F}}\ \left(\ell, \overline{\mathtt{w_i}}^{i<n}\right)\ \{\mathtt{w}.\ \mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}_{\mathsf{F}} \\
\quad \star \{\ell \mapsto 0 \star Self\}\ \langle \mathtt{destr}\rangle_{\mathsf{F}}\ \ell\ \{emp\}_{\mathsf{F}}
\end{array}\right\} \\
\mathcal{O}[\![\mathsf{X}]\!]^{\varsigma}_{\mathsf{F}}(\ell+1) & \triangleq & \varsigma(\mathsf{X}).\mathsf{obj}(\ell+1)
\end{array}$$

Fig. E.2. Value interpretations.

F Proofs

F.1 Domains

Lemma F.1 (Cell Composition Commutative). *Composition of* Cell *is commutative:*

$$\chi_1 \bullet \chi_2 = \chi_2 \bullet \chi_1$$

Proof. Suppose we have χ_1, χ_2 such that $\chi_1 \bullet \chi_2$ is defined, meaning $\chi_1 = \mathsf{shr}(n_1, \rho)$ and $\chi_2 = \mathsf{shr}(n_2, \rho)$. Then $\chi_2 \bullet \chi_1$ is defined as well, and $\chi_1 \bullet \chi_2 = \mathsf{shr}(n_1 + n_2, \rho) = \chi_2 \bullet \chi_1$ by the commutativity of addition. □

Lemma F.2 (Res Composition Commutative). *Composition of* Res *is commutative:*

$$\rho_1 \bullet \rho_2 = \rho_2 \bullet \rho_1$$

Proof. Suppose we have ρ_1, ρ_2 such that $\rho_1 \bullet \rho_2$ is defined, meaning $\rho_1 \sharp_{\mathsf{sh}} \rho_2{}^{(\mathrm{H1})}$.
By unfolding $\bullet$ and observing the symmetry of the definition, it remains to show:

- $\rho_2 \sharp_{\mathsf{sh}} \rho_1{}^{(\mathrm{G1})}$
- $[\ell \mapsto \chi_1 \bullet \chi_2 \mid \rho_1(\ell) = \chi_1 \wedge \rho_2(\ell) = \chi_2] = [\ell \mapsto \chi_2 \bullet \chi_1 \mid \rho_2(\ell) = \chi_2 \wedge \rho_1(\ell) = \chi_1]^{(\mathrm{G2})}$

Unfolding $\sharp_{\mathsf{sh}}$ and using H1, it suffices to prove $\rho_2(\ell) \sharp \rho_1(\ell) \Leftrightarrow \rho_1(\ell) \sharp \rho_2(\ell)$. Since $\rho_1(\ell)$ and $\rho_2(\ell)$ are both Cell, we can use Cell Composition Commutative alongside the definition of $\sharp$ to prove G1, meaning $\rho_2 \bullet \rho_1$ is defined.

The two maps in G2 have the same domain, so again applying Cell Composition Commutative solves G2. □

Lemma F.3 (Cell Composition Associative). *Composition of* Cell *is associative:*

$$(\chi_1 \bullet \chi_2) \bullet \chi_3 = \chi_1 \bullet (\chi_2 \bullet \chi_3)$$

Proof. Suppose we have χ_1, χ_2, χ_3 such that the relevant compositions are defined. This means $\chi_1 = \mathsf{shr}(n_1, \rho)$, $\chi_2 = \mathsf{shr}(n_2, \rho)$, and $\chi_3 = \mathsf{shr}(n_3, \rho)$, for some $\rho \in$ Res and $n_1, n_2, n_3 \in \mathbb{N}^+$.

By definition, we have $(\chi_1 \bullet \chi_2) \bullet \chi_3 = \mathsf{shr}(n_1 + n_2 + n_3, \rho) = \chi_1 \bullet (\chi_2 \bullet \chi_3)$, using the associativity of addition. □

Lemma F.4 (Res Composition Associative). *Composition of* Res *is associative:*

$$(\rho_1 \bullet \rho_2) \bullet \rho_3 = \rho_1 \bullet (\rho_2 \bullet \rho_3)$$

Proof. Suppose we have ρ_1, ρ_2, ρ_3 such that the relevant compositions are defined. By the definition of $\bullet$, the domain of the resulting map in both cases is exactly $D = \mathrm{dom}(\rho_1) \cup \mathrm{dom}(\rho_2) \cup \mathrm{dom}(\rho_3)$. We proceed by cases, analyzing which domains each $\ell \mapsto \chi \in D$ came from, using the fact that disjoint locations are included unchanged when resources are composed:

(1) Consider a location in the domain of exactly one of the three resources; with almost no loss of generality suppose $\ell \mapsto \chi_1 \in \mathrm{dom}(\rho_1)$ and is in the the domain of neither ρ_2 nor ρ_3. In that case, $\ell \mapsto \chi_1 \in \rho_1 \bullet \rho_2$ as well as $(\rho_1 \bullet \rho_2) \bullet \rho_3$, by definition. Similarly, $\ell \mapsto \chi_1 \in \rho_1 \bullet (\rho_2 \bullet \rho_3)$ after first composing ρ_2 and ρ_3 (neither of which contain ℓ), so the two maps agree on ℓ

(2) Consider a location in the domain of exactly two of the three resources; with almost no loss of generality suppose $\ell \in \mathrm{dom}(\rho_1) \wedge \mathrm{dom}(\rho_2)$ with $\rho_1(\ell) = \chi_1$ and $\rho_2(\ell) = \chi_2$. When we compose $\rho_1 \bullet \rho_2$, we have $\ell \mapsto \chi_1 \bullet \chi_2$ in the resulting map, which is left unchanged when we compose it with ρ_3. Similarly, when we compose $\rho_2 \bullet \rho_3$, ℓ is left unchanged; when we then compose $\rho_1 \bullet (\rho_2 \bullet \rho_3)$ once again get $\ell \mapsto \chi_1 \bullet \chi_2$, so the two maps agree on ℓ.

(3) Finally, consider a location ℓ in the domain of all three resources, with:
   - $\rho_1(\ell) = \chi_1{}^{(\mathrm{H1})}$
   - $\rho_2(\ell) = \chi_2{}^{(\mathrm{H2})}$
   - $\rho_3(\ell) = \chi_3{}^{(\mathrm{H3})}$

   When we compose $\rho_1 \bullet \rho_2$ first, we get $\ell \mapsto \chi_1 \bullet \chi_2$, and composing ρ_3 gives us $\ell \mapsto (\chi_1 \bullet \chi_2) \bullet \chi_3$. Similarly, when we compose $\rho_2 \bullet \rho_3$ first, then ρ_1, we get $\ell \mapsto \chi_1 \bullet (\chi_2 \bullet \chi_3)$. By Cell Composition Associative, these are the same and the maps agree with each other on ℓ.

Since each location in D is in one, two, or all three of the composite domains, and the two composed maps agree with each other in every case, the two maps are in fact equal. □

Lemma F.5 (Res Composition Unit). *The empty map is a unit for* Res *composition:*

$$\rho \bullet \varnothing = \rho$$

Proof. Let ρ be an arbitrary resource. Since $\mathrm{dom}(\rho) \cap \mathrm{dom}(\varnothing)$ is empty, $\rho \sharp_{\mathsf{sh}} \varnothing$ holds vacuously.

Unfolding the definition of $\bullet$ and using the fact that nothing is in $\mathrm{dom}(\varnothing)$, we have

- $[\ell \mapsto \chi \in \rho \mid \ell \notin \mathrm{dom}(\varnothing)] = \rho^{(\mathrm{H1})}$
- $[\ell \mapsto \chi \in \varnothing \mid \ell \notin \mathrm{dom}(\rho)] = \varnothing^{(\mathrm{H2})}$
- $[\ell \mapsto \chi_1 \bullet \chi_2 \mid \rho(\ell) = \chi_1 \wedge \varnothing(\ell) = \chi_2] = \varnothing^{(\mathrm{H3})}$

The disjoint union of these three smaller maps make up $\rho \bullet \varnothing$, which therefore is exactly ρ. □

Lemma F.6 (Reachable Extension Invariance).

$$\rho_1 \twoheadrightarrow \rho \Rightarrow \rho_1 \leq \rho_2 \Rightarrow \rho_2 \twoheadrightarrow \rho$$

Proof. Suppose we have ρ, ρ_1, and ρ_2 such that $\rho_1 \twoheadrightarrow \rho$ and $\rho_1 \leq \rho_2$. By $\twoheadrightarrow$-sub, we have $\rho_2 \twoheadrightarrow \rho_1$ from $\rho_1 \leq \rho_2$. When paired with $\rho_1 \twoheadrightarrow \rho$, we conclude $\rho_2 \twoheadrightarrow \rho$ using $\twoheadrightarrow$-trans. □

Lemma F.7 (Unique Extension Invariance).

$$\rho_1(\ell) = \mathsf{unq}(\mathtt{w}) \Rightarrow \rho_1 \leq \rho_2 \Rightarrow \rho_2(\ell) = \mathsf{unq}(\mathtt{w})$$

Proof. Suppose we have $\rho_1(\ell) = \mathsf{unq}(\mathtt{w})$, denoted χ_1. Unfolding $\leq$, there exists a ρ_0 such that $\rho_0 \bullet \rho_1 = \rho_2$. Let us denote $\rho_0(\ell) = \chi_0$.

If $\ell \notin \mathrm{dom}(\rho_0)$, then ρ_2 will map $\ell \mapsto \mathsf{unq}(\mathtt{w})$ by $\bullet$, and the proof is complete.

If $\ell \in \mathrm{dom}(\rho_0)$, we derive a contradiction. Note that $\rho_0 \bullet \rho_1$ is defined, meaning $\rho_0 \sharp_{\mathsf{sh}} \rho_1$. Since $\ell \in \mathrm{dom}(\rho_0) \cap \mathrm{dom}(\rho_1)$ in this case, unfolding $\sharp_{\mathsf{sh}}$ tells us $\chi_0 \sharp \chi_1$. However, this requires $\chi_0 \bullet \chi_1$ to be defined, which cannot be the case since $\chi_1 = \mathsf{unq}(\mathtt{w})$. □

Lemma F.8 (Shared Extension Monotonicity).

$$\rho_1(\ell) = \mathsf{shr}(n_1, \rho_\ell) \Rightarrow \rho_1 \leq \rho_2 \Rightarrow \exists\, n_2 \geq n_1.\ \rho_2(\ell) = \mathsf{shr}(n_2, \rho_\ell)$$

Proof. Suppose we have $\rho_1(\ell) = \mathsf{shr}(n_1, \rho_\ell)$, denoted χ_1. Unfolding $\leq$, there exists a ρ_0 such that $\rho_0 \bullet \rho_1 = \rho_2$. Let us denote $\rho_0(\ell) = \chi_0$.

If $\ell \notin \mathrm{dom}(\rho_0)$, then ρ_2 will map $\ell \mapsto \mathsf{shr}(n_1, \rho_\ell)$ by $\bullet$, and the proof is complete with $n_2 = n_1$.

If $\ell \in \mathrm{dom}(\rho_0)$, then ρ_2 will map $\ell \mapsto \chi_0 \bullet \chi_1$ by $\bullet$, which is defined since $\rho_0 \sharp_{\mathsf{sh}} \rho_1$ (as $\rho_0 \bullet \rho_1$ is defined). Since $\chi_1 = \mathsf{shr}(n_1, \rho_\ell)$, unfolding $\bullet$ for Cell tells us $\chi_0 = \mathsf{shr}(n_0, \rho_\ell)$. Therefore, $\chi_0 \bullet \chi_1 = \mathsf{shr}(n_0 + n_1, \rho_\ell)$, and there exists $n_2 = n_0 + n_1$. Since $n_0 \in \mathbb{N}^+$, $n_2 \geq n_1$ as required. □

Lemma F.9 (Compatability Extension Antitonicity).

$$\rho_2 \sharp_{\mathsf{sh}} \rho \Rightarrow \rho_1 \leq \rho_2 \Rightarrow \rho_1 \sharp_{\mathsf{sh}} \rho$$

Proof. Suppose we have ρ, ρ_1, and ρ_2 such that $\rho_2 \sharp_{\mathsf{sh}} \rho$ and $\rho_1 \leq \rho_2$. Unfolding $\sharp_{\mathsf{sh}}$, we must show that for some $\ell \in \mathrm{dom}(\rho_1) \cap \mathrm{dom}(\rho)$, we have $\rho_1(\ell) \sharp \rho(\ell)^{(\mathrm{G1})}$.

To do so, first observe $\ell \in \mathrm{dom}(\rho_2)$, from $\rho_1 \leq \rho_2$ by unfolding $\leq$ and subsequently $\bullet$. This, along with $\ell \in \mathrm{dom}(\rho)$ lets us instantiate $\rho_2 \sharp_{\mathsf{sh}} \rho$ with ℓ, giving us $\rho_2(\ell) \sharp \rho(\ell)$. Since these are both Cell, unfolding $\sharp$ and subsequently $\bullet$ tells us that for some n_1, n_2, and ρ',

- $\rho_2(\ell) = \mathsf{shr}(n_2, \rho')^{(\mathrm{H1})}$
- $\rho(\ell) = \mathsf{shr}(n_1, \rho')^{(\mathrm{H2})}$

To prove G1, unfolding $\sharp$ tells us that we must prove that $\rho_1(\ell) \bullet \rho(\ell)$ is defined; if it is, it is a Cell which is trivially valid. Since $\rho(\ell) = \mathsf{shr}(n_1, \rho')$ from H2, we must only prove that $\rho_1(\ell) = \mathsf{shr}(n, \rho')$ for some n.

To do so, suppose otherwise. Then, applying either Unique Extension Invariance or Shared Extension Monotonicity would contradict H1, since $\rho_1 \leq \rho_2$. Therefore, having $\rho_1(\ell) = \mathsf{shr}(n, \rho')$ is the only way for $\rho_2(\ell)$ to be $\mathsf{shr}(n_2, \rho')$, which we know must be the case. This means $\rho_1(\ell) \bullet \rho(\ell)$ is defined, solving G1 and completing the proof. □

Lemma F.10 (Valid Extension Antitonicity).

$$\checkmark\, \rho_2 \Rightarrow \rho_1 \leq \rho_2 \Rightarrow \checkmark\, \rho_1$$

Proof. Suppose we have ρ_1 and ρ_2 such that $\checkmark\, \rho_2$ and $\rho_1 \leq \rho_2$. Unfolding $\checkmark$, we must show, for arbitrary $(\ell', \rho'), (\ell'', \rho'') \in \mathsf{objs}(\rho_1)$,

- $\rho_1 \sharp_{\mathsf{sh}} \rho'^{(\mathrm{G1})}$
- $(\ell' = \ell'' \wedge \rho' = \rho'') \vee (\ell' \neq \ell'' \wedge \rho' \sharp_{\mathsf{sh}} \rho'')^{(\mathrm{G2})}$

In order to use information from $\checkmark\, \rho_2$, we first must show $(\ell', \rho'), (\ell'', \rho'') \in \mathsf{objs}(\rho_2)$.

For arbitrary $(\ell, \rho) \in \mathsf{objs}(\rho_1)$, unfolding objs tells us $\rho_1 \twoheadrightarrow \ell \mapsto \mathsf{shr}(-, \rho)$. Since $\rho_1 \leq \rho_2$, we have $\rho_2 \twoheadrightarrow \ell \mapsto \mathsf{shr}(-, \rho)$ from Reachable Extension Invariance, so $(\ell, \rho) \in \mathsf{objs}(\rho_2)$ as well.

Instantiating $\checkmark\, \rho_2$ with $(\ell', \rho'), (\ell'', \rho'')$, which are both in $\mathsf{objs}(\rho_2)$ from above, gives us

- $\rho_2 \sharp_{\mathsf{sh}} \rho'^{(\mathrm{H1})}$
- $(\ell' = \ell'' \wedge \rho' = \rho'') \vee (\ell' \neq \ell'' \wedge \rho' \sharp_{\mathsf{sh}} \rho'')^{(\mathrm{H2})}$

H2 immediately solves G2. To solve G1, apply Compatability Extension Antitonicity with H1 and $\rho_1 \leq \rho_2$. □

Lemma F.11 (Res Cross-Split).

$$\begin{aligned} &\rho_1 \bullet \rho_2 = \rho_3 \bullet \rho_4 \Rightarrow \exists\, \rho_{13}, \rho_{14}, \rho_{23}, \rho_{24}. \\ &\rho_{13} \bullet \rho_{14} = \rho_1 \ \wedge \rho_{23} \bullet \rho_{24} = \rho_2 \ \wedge \\ &\rho_{13} \bullet \rho_{23} = \rho_3 \ \wedge \rho_{14} \bullet \rho_{24} = \rho_4 \end{aligned}$$

Proof. Suppose we have $\rho_1, \rho_2, \rho_3, \rho_4$ such that $\rho_1 \bullet \rho_2 = \rho_3 \bullet \rho_4$, which we denote ρ. Observe by unfolding $\bullet$ that $\mathrm{dom}(\rho) = \mathrm{dom}(\rho_1) \cup \mathrm{dom}(\rho_2) = \mathrm{dom}(\rho_3) \cup \mathrm{dom}(\rho_4)$. To construct $\rho_{13}, \rho_{14}, \rho_{23}, \rho_{24}$, we consider each $\ell \in \mathrm{dom}(\rho)$ separately and proceed by cases; by observing which domains the location is in, we determine how each sub-resource should handle that location:

(1) If ℓ is in $\mathrm{dom}(\rho_1)$ or $\mathrm{dom}(\rho_2)$, or vice-versa, but not in $\mathrm{dom}(\rho_3)$ or $\mathrm{dom}(\rho_4)$, then $\rho_1 \bullet \rho_2 \neq \rho_3 \bullet \rho_4$ by the definition of $\bullet$, a contradiction.
(2) Suppose ℓ is in exactly one of $\mathrm{dom}(\rho_1), \mathrm{dom}(\rho_2)$ and exactly one of $\mathrm{dom}(\rho_3), \mathrm{dom}(\rho_4)$. Without loss of generality, say $\ell \in \mathrm{dom}(\rho_1), \mathrm{dom}(\rho_3)$ and $\ell \notin \mathrm{dom}(\rho_2), \mathrm{dom}(\rho_4)$. We therefore must have $\ell \notin \mathrm{dom}(\rho_{14}), \mathrm{dom}(\rho_{23}), \mathrm{dom}(\rho_{24})$. Since $\rho(\ell) = \rho_1(\ell) = \rho_3(\ell)$ by unfolding $\bullet$, we can set $\rho_{13}(\ell) = \rho(\ell)$. This way, $(\rho_{13} \bullet \rho_{14})(\ell) = \rho_1(\ell)$ and $(\rho_{13} \bullet \rho_{23})(\ell) = \rho_3(\ell)$.

Note that all $\mathsf{unq}(-)$ resources must fall into this case, as we cannot compose unique Cells, but the composition is defined.

(3) Suppose ℓ is in exactly three of the four possible domains. Without loss of generality, consider $\ell \in \mathrm{dom}(\rho_1), \mathrm{dom}(\rho_2), \mathrm{dom}(\rho_3)$ but $\ell \notin \mathrm{dom}(\rho_4)$. We therefore must have $\ell \notin \mathrm{dom}(\rho_{14}), \mathrm{dom}(\rho_{24})$. Observe $\rho(\ell) = (\rho_1 \bullet \rho_2)(\ell) = \rho_3(\ell)$. Note that this Cell must be shared, otherwise the composition would be undefined. We can set $\rho_{13}(\ell) = \rho_1(\ell)$ and $\rho_{23}(\ell) = \rho_2(\ell)$. This way, $(\rho_{13} \bullet \rho_{23})(\ell) = (\rho_1 \bullet \rho_2)(\ell) = \rho_3(\ell)$, as intended. Also, since $\ell \notin \mathrm{dom}(\rho_{14}), \mathrm{dom}(\rho_{24})$, we have $(\rho_{13} \bullet \rho_{14})(\ell) = \rho_1(\ell)$ and $(\rho_{23} \bullet \rho_{24})(\ell) = \rho_2(\ell)$.

(4) Finally, consider when ℓ is in all four domains. Unfolding $\bullet$, it must be the case that $\rho(\ell) = (\rho_1 \bullet \rho_2)(\ell) = (\rho_3 \bullet \rho_4)(\ell) = \mathsf{shr}(n, \rho_\ell)$, noting that the Cell must be shared for the composition to be defined. Unfolding $\bullet$ again, we have
- $\rho_1(\ell) = \mathsf{shr}(n_1, \rho_\ell)^{(\mathrm{H1})}$
- $\rho_2(\ell) = \mathsf{shr}(n_2, \rho_\ell)^{(\mathrm{H2})}$
- $\rho_3(\ell) = \mathsf{shr}(n_3, \rho_\ell)^{(\mathrm{H3})}$
- $\rho_4(\ell) = \mathsf{shr}(n_4, \rho_\ell)^{(\mathrm{H4})}$

where $n_1 + n_2 = n_3 + n_4 = n$, or equivalently $n_1 - n_3 = n_4 - n_2$. We must find a way to split these reference counts across $\rho_{13}, \rho_{14}, \rho_{23}, \rho_{24}$. Without loss of generality, the differences above are non-negative, since if they were, we can swap their order. In this case, $n_1 \geq n_3$ and $n_4 \geq n_2$.

Let us set $\rho_{13}(\ell) = \mathsf{shr}(n_3, \rho_\ell)$, $\rho_{24}(\ell) = \mathsf{shr}(n_2, \rho_\ell)$, and $\ell \notin \mathrm{dom}(\rho_{23})$. If $n_4 - n_2 = n_1 - n_3$ is positive, set $\rho_{14}(\ell) = \mathsf{shr}(n_4 - n_2, \rho_\ell) = \mathsf{shr}(n_1 - n_3, \rho_\ell)$; otherwise, $\ell \notin \mathrm{dom}(\rho_{14})$ since the reference count must be in $\mathbb{N}^+$. We now confirm each of the four compositions agrees with the resources above:
- If $n_1 - n_3$ is positive, $(\rho_{13} \bullet \rho_{14})(\ell) = \mathsf{shr}(n_3 + (n_1 - n_3), \rho_\ell) = \mathsf{shr}(n_1, \rho_\ell) = \rho_1(\ell)$. If $n_1 - n_3 = 0$, then $n_1 = n_3$ and $(\rho_{13} \bullet \rho_{14})(\ell) = \mathsf{shr}(n_3, \rho_\ell) = \mathsf{shr}(n_1, \rho_\ell) = \rho_1(\ell)$.
- $(\rho_{23} \bullet \rho_{24})(\ell) = \mathsf{shr}(n_2, \rho_\ell) = \rho_2(\ell)$
- $(\rho_{13} \bullet \rho_{23})(\ell) = \mathsf{shr}(n_3, \rho_\ell) = \rho_3(\ell)$
- If $n_4 - n_2$ is positive, $(\rho_{14} \bullet \rho_{24})(\ell) = \mathsf{shr}((n_4 - n_2) + n_2, \rho_\ell) = \mathsf{shr}(n_4, \rho_\ell) = \rho_4(\ell)$. If $n_4 - n_2 = 0$, then $n_2 = n_4$ and $(\rho_{14} \bullet \rho_{24})(\ell) = \mathsf{shr}(n_2, \rho_\ell) = \mathsf{shr}(n_4, \rho_\ell) = \rho_4(\ell)$.

□

Lemma F.12 (Wld Extension Partial Order). Wld *is partially ordered by* $\sqsubseteq$.

Proof. Immediate from the definitions of Wld and $\sqsubseteq$, since $\geq$ partially orders $\mathbb{N}$ and $\subseteq$ partially orders Sizes. □

Lemma F.13 (Reachability Object Subresource).

$$\rho_1 \twoheadrightarrow \rho_2 \Rightarrow \rho_2 \leq \rho_1 \lor \exists\, (\ell, \rho) \in \mathsf{objs}(\rho_1).\ \rho_2 \leq \rho$$

Proof. We proceed by induction on the derivation of $\twoheadrightarrow$.

Case $\twoheadrightarrow$-jump

$$\frac{(\twoheadrightarrow\text{-JUMP})}{\ell_2 \mapsto \mathsf{shr}(-, \rho_2) \twoheadrightarrow \rho_2}$$

Here, $\rho_1 = \ell_2 \mapsto \mathsf{shr}(-, \rho_2)$. This means that $(\ell_2, \rho_2) \in \mathsf{objs}(\rho_1)$, since $\rho_1 \twoheadrightarrow \ell_2 \mapsto \mathsf{shr}(-, \rho_2)$ by reflexivity (since $\rho_1 \geq \rho_1$). Noting that $\rho_2 \leq \rho_2$ trivially completes the proof.

Case $\twoheadrightarrow$-sub

$$\frac{\rho_1 \geq \rho_2}{\rho_1 \twoheadrightarrow \rho_2}\ (\twoheadrightarrow\text{-SUB})$$

$\rho_2 \leq \rho_1$ by the rule's premise.

Case $\dashrightarrow$-TRANS

$$\frac{\rho_1 \dashrightarrow \rho_0 \quad \rho_0 \dashrightarrow \rho_2}{\rho_1 \dashrightarrow \rho_2} \;(\dashrightarrow\text{-TRANS})$$

By the inductive hypothesis, either

- $\rho_2 \leq \rho_0{}^{(\text{H1})}$, or
- $\exists\,(\ell', \rho') \in \mathsf{objs}(\rho_0).\ \rho_2 \leq \rho'^{(\text{H2})}$

If we have H2 by unfolding objs we have $\rho_0 \dashrightarrow \ell' \mapsto \mathsf{shr}(-, \rho')$. This means that $(\ell', \rho') \in \mathsf{objs}(\rho_1)$, noting $\rho_1 \dashrightarrow \rho_0 \dashrightarrow \ell' \mapsto \mathsf{shr}(-, \rho')$, which, when paired with $\rho_2 \leq \rho'$, completes the proof in this case.

Otherwise, we have H1. We can apply the inductive hypothesis to the other premise to obtain that either

- $\rho_0 \leq \rho_1{}^{(\text{H3})}$, or
- $\exists\,(\ell'', \rho'') \in \mathsf{objs}(\rho_1).\ \rho_0 \leq \rho''^{(\text{H4})}$

If we have H3, then $\rho_2 \leq \rho_0 \leq \rho_1$ and we are done by H1 and the transitivity of $\leq$.

Otherwise, we have H4. There therefore exists $(\ell'', \rho'') \in \mathsf{objs}(\rho_1)$ with $\rho_2 \leq \rho_0 \leq \rho''$, again using H1 and the transitivity of $\leq$ to complete the proof.

□

Lemma F.14 (Valid Reachability Monotonicity).

$$\checkmark\ \rho_1 \Rightarrow \rho_1 \dashrightarrow \rho_2 \Rightarrow \checkmark\ \rho_2$$

Proof. Suppose we have ρ_1 and ρ_2 such that $\checkmark\ \rho_1$ and $\rho_1 \dashrightarrow \rho_2$. Unfolding $\checkmark$, we must show, for some $(\ell', \rho'), (\ell'', \rho'') \in \mathsf{objs}(\rho_2)$,

- $\rho_2 \sharp_{\mathsf{sh}} \rho'^{(\text{G1})}$
- $(\ell' = \ell'' \wedge \rho' = \rho'') \vee (\ell' \neq \ell'' \wedge \rho' \sharp_{\mathsf{sh}} \rho'')^{(\text{G2})}$

In order to use information from $\checkmark\ \rho_1$, we first must show $(\ell', \rho'), (\ell'', \rho'') \in \mathsf{objs}(\rho_1)$.

For arbitrary $(\ell, \rho) \in \mathsf{objs}(\rho_2)$, unfolding objs tells us $\rho_2 \dashrightarrow \ell \mapsto \mathsf{shr}(-, \rho)$. Since $\rho_1 \dashrightarrow \rho_2$, we have $\rho_1 \dashrightarrow \rho_2 \dashrightarrow \ell \mapsto \mathsf{shr}(-, \rho)$ so $(\ell, \rho) \in \mathsf{objs}(\rho_1)$ as well by transitivity.

Instantiating $\checkmark\ \rho_1$ with $(\ell', \rho'), (\ell'', \rho'')$, which are both in $\mathsf{objs}(\rho_1)$ from above, gives us

- $\rho_1 \sharp_{\mathsf{sh}} \rho'^{(\text{H1})}$
- $(\ell' = \ell'' \wedge \rho' = \rho'') \vee (\ell' \neq \ell'' \wedge \rho' \sharp_{\mathsf{sh}} \rho'')^{(\text{H2})}$

H2 immediately solves G2. To solve G1, we first invoke Reachability Object Subresource with $\rho_1 \dashrightarrow \rho_2$ to obtain either

- $\rho_2 \leq \rho_1{}^{(\text{H3})}$, or
- $\exists\,(\ell, \rho) \in \mathsf{objs}(\rho_1).\ \rho_2 \leq \rho^{(\text{H4})}$

If we have H3, then applying Compatability Extension Antitonicity with H1 and H3 solves G1.

Otherwise, let $(\ell, \rho) \in \mathsf{objs}(\rho_1)$ with $\rho_2 \leq \rho$. By Compatability Extension Antitonicity, it suffices to show that $\rho \sharp_{\mathsf{sh}} \rho'$. Instantiating $\checkmark\ \rho_1$ with $(\ell, \rho), (\ell', \rho')$ gives us

- $\rho_1 \sharp_{\mathsf{sh}} \rho^{(\text{H5})}$
- $(\ell = \ell' \wedge \rho = \rho') \vee (\ell \neq \ell' \wedge \rho \sharp_{\mathsf{sh}} \rho')^{(\text{H6})}$

If $\ell \neq \ell' \wedge \rho \sharp_{\mathsf{sh}} \rho'$, we are done. We prove that this must be the case by deriving a contradiction from $\ell = \ell' \wedge \rho = \rho'$.

By H4 and $\dashrightarrow$-SUB, $\rho \dashrightarrow \rho_2$. But since $(\ell', \rho') = (\ell, \rho) \in \mathsf{objs}(\rho_2)$, we have $\rho_2 \dashrightarrow \ell \mapsto \mathsf{shr}(-, \rho)$. By transitivity, this means $(\ell, \rho) \in \mathsf{objs}(\rho)$. This is a contradiction, as the relation defined by containment in another resource's objs is well-founded, which is evident from its definition. Note that each element in $\mathsf{objs}(\rho)$ is reached by taking a non-zero number of steps through the resource graph of ρ, which must be a finitely constructable tree (since Res is an inductive data type). □

LEMMA F.15 (UNIQUE REACHABILITY ERASURE).

$$\rho_2(\ell) = \mathsf{unq}(\mathtt{w}) \Rightarrow \rho_1 \dashrightarrow \rho_2 \Rightarrow \checkmark\, \rho_1 \Rightarrow \mathsf{erase}(\rho_1)(\ell) = \mathtt{w}$$

PROOF. Suppose we have ρ_1 and ρ_2 such that

- $\rho_2(\ell) = \mathsf{unq}(\mathtt{w})^{(\mathrm{H1})}$
- $\rho_1 \dashrightarrow \rho_2{}^{(\mathrm{H2})}$
- $\checkmark\, \rho_1{}^{(\mathrm{H3})}$

To prove $\mathsf{erase}(\rho_1)(\ell) = \mathtt{w}$, by unfolding $\mathsf{erase}(-)$ of Res and Cell, it suffices to prove that

- $\ell \mapsto \mathsf{unq}(\mathtt{w}) \in \rho_1 \bullet \left(\bigodot_{(\ell', \rho_{\ell'}) \in \mathsf{objs}(\rho_1)} \rho_{\ell'}\right)^{(\mathrm{G1})}$.

Applying REACHABILITY OBJECT SUBRESOURCE with H2, we have either

- $\rho_2 \leq \rho_1{}^{(\mathrm{H4})}$, or
- $\exists\, (\ell', \rho') \in \mathsf{objs}(\rho_1).\ \rho_2 \leq \rho'^{(\mathrm{H5})}$

If $\rho_2 \leq \rho_1$, then $\rho_1(\ell) = \mathsf{unq}(\mathtt{w})$ by applying UNIQUE EXTENSION INVARIANCE with H1. Equivalently, $\ell \mapsto \mathsf{unq}(\mathtt{w}) \in \rho_1{}^{(\mathrm{H6})}$. Since the composition in G1 is defined due to H3, we know that $\ell \notin \mathrm{dom}(\rho_{\ell'})$ for any $(\ell', \rho_{\ell'}) \in \mathsf{objs}(\rho_1)$. If it were, then composing the two resources would require composing $\mathsf{unq}(\mathtt{w})$ with another cell, which cannot be done. This means composing the rest of ρ_1's objects does not change H6, proving G1.

If we instead have H5, then following the same reasoning from above, we deduce $\rho'(\ell) = \mathtt{w}$, or equivalently $\ell \mapsto \mathsf{unq}(\mathtt{w}) \in \rho'^{(\mathrm{H7})}$. Composing ρ' with ρ_1 and the other $(\ell', \rho_{\ell'}) \in \mathsf{objs}(\rho_1)$ does not change H7 like above, again proving G1. □

LEMMA F.16 (UNIQUE DOMAIN EXCLUSION).

$$\rho \,\sharp\, \ell \mapsto \mathsf{unq}(-) \Rightarrow \ell \notin \mathrm{dom}(\rho) \wedge \forall\, (\ell_1, \rho_1) \in \mathsf{objs}(\rho).\ \ell \notin \mathrm{dom}(\rho_1)$$

PROOF. Suppose we have ρ with $\rho \,\sharp\, \ell \mapsto \mathsf{unq}(-)$. Unfolding $\sharp$, the composition $\rho \bullet \ell \mapsto \mathsf{unq}(-) = \rho'$ must be defined and valid. From this, we deduce $\ell \notin \mathrm{dom}(\rho)$, since if it were, we would have to compose $\mathsf{unq}(-)$ with another cell, which cannot be done. Therefore, $\ell \notin \mathrm{dom}(\rho)$

Unfolding objs, we observe that $\mathsf{objs}(\rho') = \mathsf{objs}(\rho)$. This means for any $(\ell_1, \rho_1) \in \mathsf{objs}(\rho)$, we can instantiate $\checkmark\, \rho'$ to obtain $\rho' \sharp_{\mathsf{sh}} \rho_1$ If $\ell \in \mathrm{dom}(\rho_1)$, unfolding $\sharp_{\mathsf{sh}}$ would require $\rho'(\ell) \bullet \mathsf{unq}(-)$, which like above cannot be done. Therefore, $\ell \notin \mathrm{dom}(\rho_1)$ either. □

LEMMA F.17 (UNIQUE UPDATE COMPATIBILITY).

$$\rho \,\sharp\, \ell \mapsto \mathsf{unq}(-) \Rightarrow \rho \,\sharp\, \ell \mapsto \mathsf{unq}(\mathtt{w})$$

PROOF. Suppose we have ρ with $\rho \,\sharp\, \ell \mapsto \mathsf{unq}(-)$. Let us call their composition ρ', which is defined and valid by $\sharp$. Applying UNIQUE DOMAIN EXCLUSION tells us that

- $\ell \notin \mathrm{dom}(\rho)^{(\mathrm{H1})}$
- $\forall\, (\ell_1, \rho_1) \in \mathsf{objs}(\rho).\ \ell \notin \mathrm{dom}(\rho_1)^{(\mathrm{H2})}$

From H1, we deduce that $\rho \bullet \ell \mapsto \mathsf{unq}(\mathtt{w}) = \rho_{\mathtt{w}}$ is defined with $\rho_{\mathtt{w}} = \ell \uplus [\ell \mapsto \mathsf{unq}(\mathtt{w})]$.

To prove $\checkmark\, \rho'$, unfold $\checkmark$ and let $(\ell_1, \rho_1), (\ell_2, \rho_2) \in \mathsf{objs}(\rho_{\mathtt{w}})$. It suffices to prove that

- $\rho_{\mathtt{w}} \sharp_{\mathsf{sh}} \rho_1{}^{(\mathrm{G1})}$

- $(\ell_1 = \ell_2 \wedge \rho_1 = \rho_2) \vee (\ell_1 \neq \ell_2 \wedge \rho_1 \sharp_{\mathsf{sh}} \rho_2)^{(G2)}$

To do so, first observe $\mathsf{objs}(\rho_{\mathtt{w}}) = \mathsf{objs}(\rho) = \mathsf{objs}(\rho')$ by unfolding objs. This means that we can instantiate $\checkmark\, \rho'$ with (ℓ_1, ρ_1) and (ℓ_2, ρ_2) to solve G2.

To solve G1, we must prove that $\forall\, \ell' \in \mathrm{dom}(\rho_{\mathtt{w}}) \cap \mathrm{dom}(\rho_1)$ we have $\rho_{\mathtt{w}}(\ell') \sharp \rho_1(\ell')$. Applying H2, $\ell \notin \rho_1$ so any such ℓ' must be in $\mathrm{dom}(\rho)$ specifically. By observing $\rho_{\mathtt{w}}(\ell') = \rho(\ell')$ in this case, the proof obligation can be re-folded into $\rho \sharp_{\mathsf{sh}} \rho_1{}^{(G3)}$.

To solve this, we deduce $\checkmark\, \rho$ by applying Valid Extension Antitonicity with $\rho \leq \rho'$ and $\checkmark\, \rho'$. Instantiating this with (ℓ_1, ρ_1) solves G3 and completes the proof. □

Lemma F.18 (Unique Erasure Separability).

$$\rho \sharp \ell \mapsto \mathsf{unq}(\mathtt{w}) \Rightarrow \mathsf{erase}(\rho \bullet \ell \mapsto \mathsf{unq}(\mathtt{w})) = \mathsf{erase}(\rho) \uplus [\ell \mapsto \mathtt{w}]$$

Proof. Suppose we have ρ with $\rho \sharp \ell \mapsto \mathsf{unq}(\mathtt{w})$. Unfolding $\sharp$, the composition $\rho \bullet \ell \mapsto \mathsf{unq}(\mathtt{w})$ must be defined and valid; set this to be ρ'. Applying Unique Domain Exclusion tells us that $\ell \notin \mathrm{dom}(\rho)$ and $\forall\, (\ell_1, \rho_1) \in \mathsf{objs}(\rho).\ \ell \notin \mathrm{dom}(\rho_1)$.

With this, and the observation that $\mathsf{objs}(\rho') = \mathsf{objs}(\rho)$, which follows from unfolding objs, we can inspect $\mathsf{erase}(\rho \bullet \ell \mapsto \mathsf{unq}(\mathtt{w})) = \mathsf{erase}(\rho')$ to deduce

$$\begin{aligned}
\mathsf{erase}(\rho') &= \left[\ell \mapsto \mathsf{erase}(\chi) \mid \ell \mapsto \chi \in \rho' \bullet \left(\bigbullet_{(\ell_1,\rho_1) \in \mathsf{objs}(\rho')} \rho_1\right)\right] \\
&= \left[\ell \mapsto \mathsf{erase}(\chi) \mid \ell \mapsto \chi \in (\rho \bullet \ell \mapsto \mathsf{unq}(\mathtt{w})) \bullet \left(\bigbullet_{(\ell_1,\rho_1) \in \mathsf{objs}(\rho)} \rho_1\right)\right] \\
&= \left[\ell \mapsto \mathsf{erase}(\chi) \mid \ell \mapsto \chi \in \rho \bullet \left(\bigbullet_{(\ell_1,\rho_1) \in \mathsf{objs}(\rho)} \rho_1\right)\right] \uplus [\ell \mapsto \mathsf{erase}(\mathsf{unq}(\mathtt{w}))] \\
&= \mathsf{erase}(\rho) \uplus [\ell \mapsto \mathtt{w}]
\end{aligned}$$

□

Lemma F.19 (Object Composition).

$$\rho_1 \sharp \rho_2 \Rightarrow \mathsf{objs}(\rho_1 \bullet \rho_2) = \mathsf{objs}(\rho_1) \cup \mathsf{objs}(\rho_2)$$

Proof. Suppose we have ρ_1 and ρ_2 with $\rho_1 \sharp \rho_2$. To prove the equality above, we can do so in two steps:

- $\mathsf{objs}(\rho_1 \bullet \rho_2) \subseteq \mathsf{objs}(\rho_1) \cup \mathsf{objs}(\rho_2)^{(G1)}$
- $\mathsf{objs}(\rho_1 \bullet \rho_2) \supseteq \mathsf{objs}(\rho_1) \cup \mathsf{objs}(\rho_2)^{(G2)}$

To prove G2, let $(\ell, \rho_\ell) \in \mathsf{objs}(\rho_1) \cup \mathsf{objs}(\rho_2)$. without loss of generality, suppose $(\ell, \rho_\ell) \in \mathsf{objs}(\rho_1)$. Unfolding objs, this means $\rho_1 \twoheadrightarrow \ell \mapsto \mathsf{shr}(-, \rho_\ell)$. But since $\rho_1 \bullet \rho_2 \twoheadrightarrow \rho_1$ by $\twoheadrightarrow$-sub, $(\ell, \rho_\ell) \in \mathsf{objs}(\rho_1 \bullet \rho_2)$ by applying $\twoheadrightarrow$-trans.

To prove G1, let $(\ell, \rho_\ell) \in \mathsf{objs}(\rho_1 \bullet \rho_2)$. Unfolding objs, this means $\rho_1 \bullet \rho_2 \twoheadrightarrow \ell \mapsto \mathsf{shr}(-, \rho_\ell)$. It suffices to show that at least one of $\rho_1 \twoheadrightarrow \ell \mapsto \mathsf{shr}(-, \rho_\ell)$ or $\rho_2 \twoheadrightarrow \ell \mapsto \mathsf{shr}(-, \rho_\ell)$ must be true.

To do so, we can induct on $\twoheadrightarrow$ with a strengthened inductive hypothesis that will imply the property above. Specifically, we prove that $\rho_1 \bullet \rho_2 \twoheadrightarrow \rho$ implies $\rho_1 \twoheadrightarrow \rho$, $\rho_2 \twoheadrightarrow \rho$, or $\rho_1 \bullet \rho_2 \geq \rho$.

Case $\twoheadrightarrow$-jump

$$\frac{}{\rho_1 \bullet \rho_2 = \ell \mapsto \mathsf{shr}(-, \rho) \twoheadrightarrow \rho}\ (\twoheadrightarrow\text{-JUMP})$$

Unfolding $\bullet$, we have three slightly different cases to consider. Note that ℓ is the only location in $\mathrm{dom}(\rho_1) \cup \mathrm{dom}(\rho_2)$, since $\mathrm{dom}(\rho_1 \bullet \rho_2) = \{\ell\}$. If $\ell \in \mathrm{dom}(\rho_1)$ and $\ell \notin \mathrm{dom}(\rho_2)$, then $\rho_2 = \varnothing$ and $\rho_1 = \ell \mapsto \mathsf{shr}(n, \rho)$, so $\rho_1 \twoheadrightarrow \rho$ by $\twoheadrightarrow$-jump. Similarly, if $\ell \notin \mathrm{dom}(\rho_1)$ and $\ell \in \mathrm{dom}(\rho_2)$, we have $\rho_2 \twoheadrightarrow \rho$.

Finally, if $\ell \in \mathrm{dom}(\rho_1)$ and $\ell \in \mathrm{dom}(\rho_2)$, then $\mathsf{shr}(n, \rho) = \rho_1(\ell) \bullet \rho_2(\ell)$. This composition is defined, since $\rho_1 \sharp \rho_2$. Therefore $\rho_1 = \ell \mapsto \mathsf{shr}(n_1, \rho)$ and $\rho_2 = \ell \mapsto \mathsf{shr}(n_2, \rho)$ for some $n_1 + n_2 = n$, recalling that no other locations may be in their domains. In this case, both $\rho_1 \twoheadrightarrow \rho$ and $\rho_2 \twoheadrightarrow \rho$ by $\twoheadrightarrow$-JUMP.

Case $\twoheadrightarrow$-SUB

$$\text{($\twoheadrightarrow$-SUB)}\quad \frac{\rho_1 \bullet \rho_2 \geq \rho}{\rho_1 \bullet \rho_2 \twoheadrightarrow \rho}$$

By the premise, $\rho_1 \bullet \rho_2 \geq \rho$.

Case $\twoheadrightarrow$-TRANS

$$\text{($\twoheadrightarrow$-TRANS)}\quad \frac{\rho_1 \bullet \rho_2 \twoheadrightarrow \rho' \qquad \rho' \twoheadrightarrow \rho}{\rho_1 \bullet \rho_2 \twoheadrightarrow \rho}$$

Applying our inductive hypothesis on $\rho_1 \bullet \rho_2 \twoheadrightarrow \rho'$, we have one of

- $\rho_1 \twoheadrightarrow \rho'^{\,(\mathrm{H1})}$
- $\rho_2 \twoheadrightarrow \rho'^{\,(\mathrm{H2})}$
- $\rho_1 \bullet \rho_2 \geq \rho'^{\,(\mathrm{H3})}$

If we have H1, then $\rho_1 \twoheadrightarrow \rho' \twoheadrightarrow \rho$ and we are done by applying $\twoheadrightarrow$-TRANS. Similarly, if we have H2, $\rho_2 \twoheadrightarrow \rho' \twoheadrightarrow \rho$.

If we have H3, then by $\geq$ there must exist some ρ'' such that $\rho_1 \bullet \rho_2 = \rho' \bullet \rho''$. Now, apply Res Cross-Split to guarantee the existence of $\rho_1' \leq \rho_1$ and $\rho_2' \leq \rho_2$ such that $\rho' = \rho_1' \bullet \rho_2'$. This allows us to apply our inductive hypothesis on $\rho' = \rho_1' \bullet \rho_2' \twoheadrightarrow \rho$ to obtain one of

- $\rho_1' \twoheadrightarrow \rho^{(\mathrm{H4})}$
- $\rho_2' \twoheadrightarrow \rho^{(\mathrm{H5})}$
- $\rho_1' \bullet \rho_2' \geq \rho^{(\mathrm{H6})}$

If we have H4, then $\rho_1 \twoheadrightarrow \rho_1' \twoheadrightarrow \rho$, recalling that $\rho_1 \geq \rho_1'$ and applying $\twoheadrightarrow$-SUB. Similarly, if we have H5, then $\rho_2 \twoheadrightarrow \rho_2' \twoheadrightarrow \rho$. Finally, if we have H6, then combining it with H3 gives us $(\rho_1 \bullet \rho_2) \geq \rho' = \rho_1' \bullet \rho_2' \geq \rho$. By transitivity, $\rho_1 \bullet \rho_2 \geq \rho$, completing the case.

Since $\rho_1 \bullet \rho_2 \twoheadrightarrow \ell \mapsto \mathsf{shr}(-, \rho_\ell)$, we now have one of

- $\rho_1 \twoheadrightarrow \ell \mapsto \mathsf{shr}(-, \rho_\ell)^{(\mathrm{H7})}$
- $\rho_2 \twoheadrightarrow \ell \mapsto \mathsf{shr}(-, \rho_\ell)^{(\mathrm{H8})}$
- $\rho_1 \bullet \rho_2 \geq \ell \mapsto \mathsf{shr}(-, \rho_\ell)^{(\mathrm{H9})}$

If H7 holds, then $(\ell, \rho_\ell) \in \mathsf{objs}(\rho_1)$ by definition. Similarly, if H8 holds, then $(\ell, \rho_\ell) \in \mathsf{objs}(\rho_2)$. If $\rho_1 \bullet \rho_2 \geq \ell \mapsto \mathsf{shr}(-, \rho_\ell)$, then there exists some ρ' such that $\rho_1 \bullet \rho_2 = \ell \mapsto \mathsf{shr}(-, \rho_\ell) \bullet \rho'$ by $\geq$. Unfolding $\bullet$, we observe that ℓ must be in the domain of at least one of ρ_1 or ρ_2. By $\rho_1 \sharp \rho_2$ and unfolding $\checkmark$, such a location in either domain must be mapped to a cell of the form $\mathsf{shr}(-, \rho_\ell)$. This is exactly the condition for (ℓ, ρ_ℓ) to be in $\mathsf{objs}(\rho_1)$ or $\mathsf{objs}(\rho_2)$, depending on which domains ℓ is in. It is important to note that objs does not depend on the reference count of the shared cell. □

Lemma F.20 (Unique Shared Convertibility).

$$\rho_f \sharp (\ell \mapsto \mathsf{unq}(-) \bullet \rho) \Rightarrow \rho_f \sharp (\ell \mapsto \mathsf{shr}(-, \rho))$$

Proof. To prove $\rho_f \sharp (\ell \mapsto \mathsf{shr}(-, \rho))$, we must prove that the composition $\rho_f \bullet (\ell \mapsto \mathsf{shr}(-, \rho))$ is both defined and valid.

To prove that the composition is defined, we first rewrite $\rho_f \sharp (\ell \mapsto \mathsf{unq}(-) \bullet \rho)$ as $\rho_f \bullet \rho \sharp \ell \mapsto \mathsf{unq}(-)$ by unfolding and re-folding $\sharp$ (using both Res Composition Associative and Res

Composition Commutative). From Unique Domain Exclusion, this means $\ell \notin \mathrm{dom}(\rho_f \bullet \rho)$ and therefore is not in $\mathrm{dom}(\rho_f)$. Thus, $\rho_f \bullet (\ell \mapsto \mathsf{shr}(-, \rho))$ is defined.

To prove $\checkmark\, (\rho_f \bullet (\ell \mapsto \mathsf{shr}(-, \rho)))$, we must prove for arbitrary $(\ell_1, \rho_1), (\ell_2, \rho_2) \in \mathsf{objs}(\rho_f \bullet \ell \mapsto \mathsf{shr}(-, \rho))$, that

- $\rho_f \bullet (\ell \mapsto \mathsf{shr}(-, \rho)) \sharp_{\mathsf{sh}} \rho_1{}^{(\mathrm{G1})}$
- $(\ell_1 = \ell_2 \wedge \rho_1 = \rho_2) \vee (\ell_1 \neq \ell_2 \wedge \rho_1 \sharp_{\mathsf{sh}} \rho_2)^{(\mathrm{G2})}$

To do so, we would like to use $\checkmark\, (\rho_f \bullet (\ell \mapsto \mathsf{unq}(-) \bullet \rho))$, which we will denote ρ'. Note first

$$\begin{aligned} \mathsf{objs}(\rho') &= \mathsf{objs}(\rho_f \bullet \ell \mapsto \mathsf{unq}(-) \bullet \rho) \\ &= \mathsf{objs}(\rho_f \bullet \rho) \end{aligned}$$

Next, observe that $\mathsf{objs}(\ell \mapsto \mathsf{shr}(-, \rho)) = \mathsf{objs}(\rho) \cup (\ell, \rho)$. We have $(\ell, \rho) \in \mathsf{objs}(\ell \mapsto \mathsf{shr}(-, \rho))$ by definition, and all other reachable objects must pass through ρ itself, so are therefore in $\mathsf{objs}(\rho)$. Using Object Composition, we thus have

$$\begin{aligned} \mathsf{objs}(\rho_f \bullet \ell \mapsto \mathsf{shr}(-, \rho)) &= \mathsf{objs}(\rho_f) \cup \mathsf{objs}(\rho) \cup (\ell, \rho) \\ &= \mathsf{objs}(\rho_f \bullet \rho) \cup (\ell, \rho) \\ &= \mathsf{objs}(\rho') \cup (\ell, \rho) \end{aligned}$$

We first prove G2. Observe that if $(\ell_1, \rho_1), (\ell_2, \rho_2) \in \mathsf{objs}(\rho')$, then instantiating $\checkmark\, \rho'$ solves the goal. Similarly, if $(\ell_1, \rho_1) = (\ell_2, \rho_2) = (\ell, \rho)$, we are done by definition.

Otherwise, without loss of generality let $(\ell_1, \rho_1) = (\ell, \rho)$ and $(\ell_2, \rho_2) \in \mathsf{objs}(\rho')$. From Unique Domain Exclusion with $\rho', \ell \neq \ell_2$, so it remains to prove $\rho \sharp_{\mathsf{sh}} \rho_2$. To do so, instantiate $\checkmark\, \rho'$ with (ℓ_2, ρ_2) to get $\rho' \sharp_{\mathsf{sh}} \rho_2$. Since $\rho \leq \rho'$, applying Compatability Extension Antitonicity solves G2.

Next, we prove G1. Like above, we consider the case where $(\ell_1, \rho_1) \in \mathsf{objs}(\rho')$ and $(\ell_1, \rho_1) = (\ell, \rho)$ separately. First, suppose $(\ell_1, \rho_1) \in \mathsf{objs}(\rho')$. Unfolding $\sharp_{\mathsf{sh}}$, we must prove

- $\forall\, \ell' \in \mathrm{dom}(\rho_f \bullet \ell \mapsto \mathsf{shr}(-, \rho)) \cap \mathrm{dom}(\rho_1).\ (\rho_f \bullet \ell \mapsto \mathsf{shr}(-, \rho))(\ell') \sharp_{\mathsf{sh}} \rho_1(\ell)^{(\mathrm{G3})}$

Since $\ell \notin \mathrm{dom}(\rho_1)$ from Unique Domain Exclusion, any such ℓ' must be in $\mathrm{dom}(\rho_f)$ as well. Also, for such ℓ', $(\rho_f \bullet \ell \mapsto \mathsf{shr}(-, \rho))(\ell') = \rho_f(\ell')$. Therefore, the condition above reduces to proving $\rho_f \sharp_{\mathsf{sh}} \rho_1$. To prove this, instantiate $\checkmark\, \rho'$ with (ℓ_1, ρ_1) to obtain $\rho' \sharp_{\mathsf{sh}} \rho_1$, and use Compatability Extension Antitonicity with $\rho_f \leq \rho'$.

Finally, if $(\ell_1, \rho_1) = (\ell, \rho)$, it remains to prove that $\rho_f \bullet \ell \mapsto \mathsf{shr}(-, \rho) \sharp_{\mathsf{sh}} \rho$. Following similar reasoning to above, noting that $\ell \notin \mathrm{dom}(\rho)$, this reduces to $\rho_f \sharp_{\mathsf{sh}} \rho$. Since $\rho_f \sharp (\ell \mapsto \mathsf{unq}(-) \bullet \rho)$, we have $\rho_f \sharp \rho$ as well by unfolding and re-folding $\sharp$. This implies $\rho_f \sharp_{\mathsf{sh}} \rho$, since their composition can only be defined when $\rho_f(\ell') \sharp \rho(\ell')$ for any ℓ' in both domains. □

Lemma F.21 (Shared Object Erasure).

$$\begin{aligned} &\checkmark\, \rho \Rightarrow (\ell_1, \rho_1) \in \mathsf{objs}(\rho) \Rightarrow \rho_1(\ell) = \mathsf{shr}(n, \rho_\ell) \Rightarrow \\ &\quad (\mathsf{erase}(\rho)(\ell) = \mathtt{n} \wedge \ell \notin \mathrm{dom}(\rho) \wedge (\forall\, (\ell', \rho') \in \mathsf{objs}(\rho).\ (\ell', \rho') \neq (\ell_1, \rho_1) \Rightarrow \ell \notin \mathrm{dom}(\rho'))) \\ &\ \vee (\mathsf{erase}(\rho)(\ell) > \mathtt{n} \wedge (\ell \in \mathrm{dom}(\rho) \vee (\exists\, (\ell', \rho') \in \mathsf{objs}(\rho).\ (\ell', \rho') \neq (\ell_1, \rho_1) \wedge \ell \in \mathrm{dom}(\rho')))) \end{aligned}$$

Proof. Suppose we have ρ, ρ_1, and ℓ such that

- $\checkmark\, \rho^{(\mathrm{H1})}$
- $(\ell_1, \rho_1) \in \mathsf{objs}(\rho)^{(\mathrm{H2})}$
- $\rho_1(\ell) = \mathsf{shr}(n, \rho_\ell)^{(\mathrm{H3})}$

To prove the disjunction above, we can unfold $\mathsf{erase}(\rho)$ and study the underlying map:

$$\mathsf{erase}(\rho) = \left[\ell_0 \mapsto \mathsf{erase}(\chi) \mid \ell_0 \mapsto \chi \in \rho \bullet \left(\textstyle\bigodot_{(\ell', \rho') \in \mathsf{objs}(\rho)} \rho'\right)\right]$$

Specifically, we can study the composition $\rho \bullet \left(\bigodot_{(\ell',\rho') \in \mathsf{objs}(\rho)} \rho'\right)$, which we denote ρ_{flat}. Since we have $\checkmark\ \rho$, this composition must be defined. From H2 and H3, we must have $\rho_{\mathsf{flat}}(\ell)$ of the form $\mathsf{shr}(n', \rho_\ell)$.

Whenever we have $\ell \in \mathrm{dom}(\rho)$, we must have $\rho(\ell) = \mathsf{shr}(n_\rho, \rho_\ell)$, where $n_\rho \in \mathbb{N}^+$. Similarly, for any $(\ell', \rho') \in \mathsf{objs}(\rho)$ we have $\rho(\ell) = \mathsf{shr}(n_{\rho'}, \rho_\ell)$ with $n_{\rho'} \in \mathbb{N}^+$. Otherwise, the composition would not be defined.

Note that $(\ell_1, \rho_1) \in \mathsf{objs}(\rho)$ by H2. If ℓ is in $\mathrm{dom}(\rho)$ or in $\mathrm{dom}(\rho')$ for some $(\ell', \rho') \neq (\ell_1, \rho_1)$ from $\mathsf{objs}(\rho)$, then when we compose everything together to get ρ_{flat}, we have $n' > n$, since we start with $\mathsf{shr}(n, \rho_\ell)$ from ρ_1 and add some positive integer when we compose the relevant resource. This proves the right disjunct, since we get $\mathsf{erase}(\rho)(\ell) = \mathtt{n'} > \mathtt{n}$ when we erase.

Otherwise, $\ell \notin \mathrm{dom}(\rho)$, and the only $(\ell', \rho') \in \mathsf{objs}(\rho)$ with $\ell \in \mathrm{dom}(\rho')$ is exactly (ℓ_1, ρ_1). This means that when we compose everything, ℓ never changes from $\mathsf{shr}(n, \rho_\ell)$. When we erase the resulting ρ_{flat}, we therefore must get $\mathsf{erase}(\rho)(\ell) = \mathtt{n'} = \mathtt{n}$, which proves the left disjunct. □

Lemma F.22 (Shared Subresource Erasure).

$$\begin{aligned}
&\checkmark\ \rho \Rightarrow \rho = \rho_1 \bullet \rho_2 \Rightarrow \rho_1(\ell) = \mathsf{shr}(n, \rho_\ell) \Rightarrow \\
&\quad (\mathsf{erase}(\rho)(\ell) = \mathtt{n} \land \ell \notin \mathrm{dom}(\rho_2) \land (\forall\, (\ell', \rho') \in \mathsf{objs}(\rho).\ \ell \notin \mathrm{dom}(\rho'))) \\
&\ \lor (\mathsf{erase}(\rho)(\ell) > \mathtt{n} \land (\ell \in \mathrm{dom}(\rho_2) \lor (\exists\, (\ell', \rho') \in \mathsf{objs}(\rho).\ \ell \in \mathrm{dom}(\rho'))))
\end{aligned}$$

Proof. The proof proceeds similarly to that of Shared Object Erasure above. Suppose we have ρ, ρ_1, ρ_2, and ℓ such that

- $\checkmark\ \rho^{(\mathrm{H1})}$
- $\rho_1 \bullet \rho_2 = \rho^{(\mathrm{H2})}$
- $\rho_1(\ell) = \mathsf{shr}(n, \rho_\ell)^{(\mathrm{H3})}$

Unfold $\mathsf{erase}(\rho)$ and denote the underlying composition $\rho_1 \bullet \rho_2 \bullet \left(\bigodot_{(\ell',\rho') \in \mathsf{objs}(\rho)} \rho'\right)$ as ρ_{flat}. This composition must be defined, by H1.

Since $\rho_1(\ell) = \mathsf{shr}(n, \rho_\ell)$, we must have $\rho_{\mathsf{flat}}(\ell)$ of the form $\mathsf{shr}(\mathtt{n'}, \rho_\ell)$ for some $n' \in NN^+$. If $\ell \notin \mathrm{dom}(\rho_2)$, and for all $(\ell', \rho') \in \mathsf{objs}(\rho)$, $\ell \notin \mathrm{dom}(\rho')$, then composing ρ_1 with all of $\rho_2 \bullet \left(\bigodot_{(\ell',\rho') \in \mathsf{objs}(\rho)} \rho'\right)$ leaves ℓ untouched, meaning $\mathtt{n'} = \mathtt{n}$. In this scenario, left disjunct holds.

Otherwise, we either have $\ell \in \mathrm{dom}(\rho_2)$, or there must be some $(\ell', \rho') \in \mathsf{objs}(\rho)$ where $\ell \in \mathrm{dom}(\rho')$. In that case, $\mathtt{n'} > \mathtt{n}$, since when we compose ρ_1 with all of $\rho_2 \bullet \left(\bigodot_{(\ell',\rho') \in \mathsf{objs}(\rho)} \rho'\right)$, the reference count of the shared resource is incremented at least once by some positive integer. In this scenario, the right disjunct holds. □

Lemma F.23 (Shared Reachability Erasure).

$$\rho_2(\ell) = \mathsf{shr}(n_2, \rho_\ell) \Rightarrow \rho_1 \twoheadrightarrow \rho_2 \Rightarrow \checkmark\ \rho_1 \Rightarrow \exists\, n_1 \geq n_2.\ \mathsf{erase}(\rho_1)(\ell) = \mathtt{n_1}$$

Proof. By using Reachability Object Subresource, we can apply Shared Object Erasure and Shared Subresource Erasure to characterize the the erasure of reachable objects. This proof does not use those lemmas to their full strength, as the information provided about domains is not necessary here.

Suppose we have ρ_1, ρ_2 such that

- $\rho_2(\ell) = \mathsf{shr}(n_2, \rho_\ell)^{(\mathrm{H1})}$
- $\rho_1 \twoheadrightarrow \rho_2{}^{(\mathrm{H2})}$
- $\checkmark\ \rho_1{}^{(\mathrm{H3})}$

Instantiate Reachability Object Subresource with H2 to give us either

- $\rho_2 \preceq \rho_1{}^{(\mathrm{H4})}$
- $\rho_2 \preceq \rho^{(\mathrm{H5})}$ where $(\ell, \rho) \in \mathsf{objs}(\rho_1)$

If we have H4, instantiate Shared Subresource Erasure using H3, H4, and H1, noting that $\rho_2 \leq \rho_1$ guarantees the existence of some ρ_3 such that $\rho_1 = \rho_2 \bullet \rho_3$ as required. Set $n_1 = \mathsf{erase}(\rho)(\ell)$; we are done, since in either case, $n_1 \geq n_2$.

Alternatively, if we have H5, then from $\rho_2 \leq \rho$ and H1, we note $\ell \in \mathsf{dom}(\rho)$. Unfolding $\bullet$, $\rho(\ell)$ is of the form $\mathsf{shr}(n', \rho_\ell)$ where $n' \geq n_2$. Now, we apply Shared Object Erasure with H3, H5, and the prior remark. Set $n_1 = \mathsf{erase}(\rho)(\ell)$; we are done, since in either case, $n_1 \geq n' \geq n_2$. □

Lemma F.24 (Shared Reachability Incrementability).

$$\rho_2(\ell) = \mathsf{shr}(-, \rho_\ell) \Rightarrow \rho_1 \twoheadrightarrow \rho_2 \Rightarrow \checkmark\, \rho_1 \Rightarrow \rho_1 \sharp (\ell \mapsto \mathsf{shr}(n, \rho_\ell))$$

Proof. Suppose we have ρ_1, ρ_2, and ℓ such that

- $\rho_2(\ell) = \mathsf{shr}(-, \rho_\ell)^{(H1)}$
- $\rho_1 \twoheadrightarrow \rho_2{}^{(H2)}$
- $\checkmark\, \rho_1{}^{(H3)}$

To prove $\rho_1 \sharp (\ell \mapsto \mathsf{shr}(n, \rho_\ell))$, we must prove that their composition is both defined and valid. First, we prove $\rho_1 \sharp (\ell \mapsto \mathsf{shr}(n, \rho_\ell))$ is defined. If $\ell \notin \mathsf{dom}(\rho_1)$, the composition is defined trivially. Otherwise, by Reachability Object Subresource, we either have

- $\rho_2 \leq \rho_1{}^{(H4)}$, or
- $\rho_2 \leq \rho_0{}^{(H5)}$ for some $(\ell_0, \rho_0) \in \mathsf{objs}(\rho_1)$

If we have H4, then applying Shared Extension Monotonicity tells us $\rho_1(\ell) = \mathsf{shr}(-, \rho_\ell)$. This form ensures the composition is defined.

Otherwise, we have H4. Apply Shared Extension Monotonicity again to obtain $\rho_0(\ell) = \mathsf{shr}(-, \rho_\ell)$. Now, instantiating H3 with (ℓ_0, ρ_0) tells us $\rho_0 \sharp_{\mathsf{sh}} \rho_1$. Unfolding $\sharp_{\mathsf{sh}}$, since $\ell \in \mathsf{dom}(\rho_1)$ and $\ell_0(\ell) = \mathsf{shr}(-, \rho_\ell)$, we have $\rho_0(\ell) \sharp \rho_1(\ell)$. This can only be the case when $\rho_1(\ell)$ is also of the form $\mathsf{shr}(-, \rho_\ell)$, meaning the composition is defined in this case too.

Now, we prove the composition is valid. To do so, take two arbitrary $(\ell', \rho'), (\ell'', \rho'') \in \mathsf{objs}(\rho_1 \bullet \ell \mapsto \mathsf{shr}(n, \rho_\ell))$. We must prove the following:

- $\rho' \sharp_{\mathsf{sh}} \rho_1 \bullet \ell \mapsto \mathsf{shr}(n, \rho_\ell)^{(G1)}$
- $(\ell' = \ell'' \land \rho' = \rho'') \lor (\ell' \neq \ell'' \land \rho' \sharp_{\mathsf{sh}} \rho'')^{(G2)}$

From Object Composition, $\mathsf{objs}(\rho_1 \bullet \ell \mapsto \mathsf{shr}(n, \rho_\ell)) = \mathsf{objs}(\rho_1) \cup \mathsf{objs}(\ell \mapsto \mathsf{shr}(n, \rho_\ell))$. Unfolding objs, we observe $(\ell, \rho_\ell) \in \mathsf{objs}(\ell \mapsto \mathsf{shr}(n, \rho_\ell))$ unsurprisingly. Every other object reachable from $\ell \mapsto \mathsf{shr}(n, \rho_\ell)$ must necessarily pass through ρ_ℓ.

We now prove $\mathsf{objs}(\rho_1) \cup \mathsf{objs}(\ell \mapsto \mathsf{shr}(n, \rho_\ell)) = \mathsf{objs}(\rho_1)$ by proving $\mathsf{objs}(\ell \mapsto \mathsf{shr}(n, \rho_\ell)) \subseteq \mathsf{objs}(\rho_1)$. Take some $(\ell_0, \rho_0) \in \mathsf{objs}(\ell \mapsto \mathsf{shr}(n, \rho_\ell))$. By the observations above, there are only two cases to consider:

(1) If $(\ell_0, \rho_0) = (\ell, \rho_\ell)$, then we have $\rho_1 \twoheadrightarrow \rho_2 \twoheadrightarrow \ell \mapsto \mathsf{shr}(-, \rho_\ell)$ and $(\ell_0, \rho_0) \in \mathsf{objs}(\rho_1)$
(2) If $(\ell_0, \rho_0) \in \mathsf{objs}(\rho_\ell)$, then we have similarly have $\rho_1 \twoheadrightarrow \rho_2 \twoheadrightarrow \rho_\ell \twoheadrightarrow \ell_0 \mapsto \mathsf{shr}(-, \rho_0)$ and $(\ell_0, \rho_0) \in \mathsf{objs}(\rho_1)$

This allows us to instantiate $\checkmark\, \rho_1$ with $(\ell', \rho'), (\ell'', \rho'')$ which solves G2. Furthermore, we learn $\rho' \sharp_{\mathsf{sh}} \rho_1{}^{(H6)}$, which we will use to prove G1. To do so, unfold $\sharp_{\mathsf{sh}}$ and consider an arbitrary location ℓ_d in $\mathsf{dom}(\rho') \cap \mathsf{dom}(\rho_1 \bullet \ell \mapsto \mathsf{shr}(n, \rho_\ell))$. If $\ell \in \mathsf{dom}(\rho_1)$, then $\rho'(\ell_d) \sharp (\rho_1 \bullet \ell \mapsto \mathsf{shr}(n, \rho_\ell))(\ell_d)$ follows from H6, with $\rho_1 \sharp (\ell \mapsto \mathsf{shr}(n, \rho_\ell))$.

The only remaining location that may not be in $\mathsf{dom}(\rho_1)$ is ℓ itself. If $\ell \in \mathsf{dom}(\rho')$ but $\ell \notin \mathsf{dom}(\rho_1)$, it suffices to show $\rho'(\ell) \sharp \mathsf{shr}(n, \rho_\ell)$ to complete the proof. This holds exactly when $\rho'(\ell)$ is of the form $\mathsf{shr}(-, \rho_\ell)$ Apply Reachability Object Subresource with $\rho_1 \twoheadrightarrow \rho_2$ again, but note $\rho_2 \leq \rho_1$ is not possible since $\ell \notin \mathsf{dom}(\rho_1)$. This guarantees the existence of some $(\ell_3, \rho_3) \in \mathsf{objs}(\rho_1)$

such that $\rho_2 \leq \rho_3$. By Shared Extension Monotonicity, $\rho_3(\ell) = \mathsf{shr}(-, \rho_\ell)$. Instantiating $\checkmark\ \rho_1$ with (ℓ', ρ') and (ℓ_3, ρ_3) gives us either

- $\ell' = \ell_3 \wedge \rho' = \rho_3{}^{(\mathrm{H8})}$ or
- $\ell' \neq \ell_3 \wedge \rho' \ \sharp_{\mathsf{sh}}\ \rho_3{}^{(\mathrm{H8})}$

If we have H8, then $\rho'(\ell) = \rho_3(\ell) = \mathsf{shr}(-, \rho_\ell)$ and $\rho'(\ell)$ is of the proper form. Otherwise, $\rho' \ \sharp_{\mathsf{sh}}\ \rho_3$ guarantees $\rho'(\ell)$ is of the proper form as well, by unfolding $\sharp_{\mathsf{sh}}$ and noting $\ell \in \mathrm{dom}(\rho') \cap \mathrm{dom}(\rho_3)$. □

F.2 Logic

Lemma F.25 (Predicate Monotonicity). *For all P defined in Fig. D.3,*

$$P(\omega, \rho) \Rightarrow \omega \sqsubseteq \omega^+ \Rightarrow P(\omega^+, \rho)$$

Proof. Note that the definition of *Prd* imposes a monotonicity requirement; this lemma ensures the atomics and connectives defined are in fact predicates. To do so, we prove that each atomic is monotone, then prove that each connective is monotone, assuming its composite predicates are already. Most of the atomic cases are trivial, with the monotonicity of most connectives following either from the monotonicity of the connected predicates, or by definition. We highlight a variety of cases below:

Case $size\,(\ell,\ n)$ From $size\,(\ell,\ n)(\omega, \rho)$, we have $\rho = \varnothing$, so it suffices to prove $\exists\, b.\ \ell = \langle b, 0\rangle \wedge \omega^+.\mathsf{sizes}(b) = n$. Unfolding $size\,(\ell,\ n)$, there exists $\ell = \langle b, 0\rangle$ with $\omega.\mathsf{sizes}(b) = n$; by $\omega.\mathsf{sizes} \subseteq \omega^+.\mathsf{sizes}$, we are done.

Case $\diamond P$ From $\diamond P$, we have $\exists\, \rho_p.\ \rho \dashrightarrow \rho_p$, so it suffices to prove $P(\omega^+, \rho_p)$. Unfolding $\diamond$, we have $P(\omega, \rho_p)$; P's monotonicity completes the proof.

Case $!\,P$ Unfolding $!$, we have $\rho = \varnothing \wedge P(\omega, \varnothing)$. To prove $!\,P(\omega^+, \rho)$, it suffices to prove $P(\omega^+, \varnothing)$, since $\rho = \varnothing$. This follows immediately from the monotonicity of P.

Case $\triangleright P$ Unfolding $\triangleright$, we have $\omega.\mathsf{step} = 0 \vee (\omega.\mathsf{step} > 0 \wedge P(\blacktriangleright\omega, \rho))$. If $\omega^+.\mathsf{step} = 0$, we are done. Otherwise, it suffices to prove $P(\blacktriangleright\omega^+, \rho)$.
Note that if $\omega^+.\mathsf{step} > 0$, then $\omega.\mathsf{step} > 0$ as well, since $\omega.\mathsf{step} \geq \omega^+.\mathsf{step} > 0$. This means we know $P(\blacktriangleright\omega, \rho)$. $P(\blacktriangleright\omega^+, \rho)$ follows from the monotonicity of P after observing that $\blacktriangleright\omega \sqsubseteq \blacktriangleright\omega^+$ by definition alongside $\omega \sqsubseteq \omega^+$.

Case $P \star Q$ Similarly to $\diamond P$, unfolding $\star$ tells us that $\exists\, \rho_p, \rho_q.\ \rho = \rho_p \bullet \rho_q$, so it suffices to prove $P(\omega^+, \rho_p)$ and $Q(\omega^+, \rho_p)$, which follow from the monotonicity of P and Q respectively.

Case $P \mathrel{-\!\!\star} Q$ Unfolding $-\!\!\star$ in the goal, take arbitrary ω^{++}, $\rho_p \ \sharp\ \rho$, and ρ_q where $\omega^{++} \sqsupseteq \omega^+$ and $\rho \bullet \rho_p = \rho_q$. Since $\omega^{++} \sqsupseteq \omega^+ \sqsupseteq \omega$, by Wld Extension Partial Order, we can instantiate $(P \mathrel{-\!\!\star} Q)\,(\omega, \rho)$ with ω^{++}, ρ_p, and ρ_q to complete the proof.

Case $wp\,(\mathsf{e})\,\{\hat{Q}\}$ We proceed similarly to the $-\!\!\star$ case, since the definition of $wp\,(-)\,\{-\}$ involves a similar universal quantification over future worlds. It is worth noting that the weakest precondition is only defined when $\checkmark\ \rho$; the $\rho_f \ \sharp\ \rho$ constraint implicitly gives us this needed validity, by the definition of $\sharp$ paired with Valid Extension Antitonicity. Instantiating $wp\,(\mathsf{e})\,\{\hat{Q}\}(\omega, \rho)$ with all relevant values will therefore suffice.

□

F.2.1 *Selected Separation Logic Rules.*

Lemma F.26 ($\equiv$-refl).

$$\frac{(\equiv\text{-}\mathit{REFL})}{\vDash P \equiv P}$$

Proof. Immediate after unfolding $\equiv$ and $!$ with $-\!\!\star$-self. □

Lemma F.27 ($\equiv$-sym).

$$(\equiv\text{-com})\quad P \equiv Q \dashv\vDash Q \equiv P$$

Proof. Immediate after unfolding $\equiv$ with $\star$-com. □

Lemma F.28 ($\equiv$-trans).

$$(\equiv\text{-trans})\quad \frac{\vDash P \equiv Q \qquad \vDash Q \equiv R}{\vDash P \equiv R}$$

Proof. Immediate after unfolding $\equiv$ using the premises and $!$-drop. □

Lemma F.29 ($\equiv$-L).

$$(\equiv\text{-L})\quad P \star (P \equiv Q) \vDash Q$$

Proof. Unfolding $\equiv$ and applying $!$-drop, it suffices if

$$P \star !\ (P -\!\!\star Q) \vDash Q$$

which, after applying $!$-L, is exactly $-\!\!\star$-L. □

F.2.2 Unrestricted Modality Rules.

Lemma F.30 ($!$-unr).

$$(!\text{-unr})\quad !P \dashv\vDash !P \star !P$$

Proof. Unfolding $\vDash$, suppose we have ω and ρ such that $\checkmark\ \rho$. We must prove $!P(\omega, \rho) \Leftrightarrow (!P \star !P)\ (\omega, \rho)$. Unfolding $!$ and $\star$, this is

$$\begin{aligned} &\rho = \varnothing \wedge P(\omega, \varnothing) \\ \Leftrightarrow\ &\rho = \rho_p \bullet \rho_q \wedge \left(\rho_p = \varnothing \wedge P(\omega, \varnothing)\right) \wedge \left(\rho_q = \varnothing \wedge P(\omega, \varnothing)\right) \end{aligned}$$

where $\rho_p \bullet \rho_q = \varnothing = \rho$. This holds by inspection. □

Lemma F.31 ($!$-$\wedge$-emp).

$$(!\text{-}\wedge\text{-}emp)\quad !P \dashv\vDash emp \wedge P$$

Proof. Immediate after unfolding $!$, emp, and $\wedge$. □

Lemma F.32 ($!$-L).

$$(!\text{-L})\quad !P \vDash P$$

Proof. Immediate from $!$-$\wedge$-emp and $\wedge$-L. □

Lemma F.33 ($!$-drop).

$$(!\text{-drop})\quad !P \vDash emp$$

Proof. Immediate from $!$-$\wedge$-emp and $\wedge$-L. □

Lemma F.34 ($!$-idem).

$$\frac{(!\text{-IDEM})}{!\,P \dashv\vDash !\,!\,P}$$

Proof. Using $!$-$\wedge$-*emp*, the following sequence of $\dashv\vDash$ completes the proof:

$$!\,P \dashv\vDash emp \wedge P \dashv\vDash emp \wedge emp \wedge P \dashv\vDash emp \wedge !\,P \dashv\vDash !\,!\,P$$

□

Lemma F.35 ($!$-mono).

$$\frac{P \vDash Q}{!\,P \vDash !\,Q}\ (!\text{-MONO})$$

Proof. Unfolding $\vDash$ and $!$, suppose we have ω, ρ such that

- $\rho = \varnothing^{(\mathrm{H1})}$
- $P(\omega, \varnothing)^{(\mathrm{H2})}$

and assume $P \vDash Q^{(\mathrm{H3})}$. Unfolding $!$ in the goal, it suffices to prove $\rho = \varnothing \wedge Q(\omega, \varnothing)$. This follows from H1 and H3, instantiated with H2 since $\checkmark\,\varnothing$ holds trivially. □

Lemma F.36 ($!$-*emp*).

$$\frac{(!\text{-}emp)}{emp \vDash !\,emp}$$

Proof. Using $!$-$\wedge$-*emp*, it suffices to prove $emp \vDash emp \wedge emp$, which holds by unfolding $\wedge$. □

Lemma F.37 ($!$-$\ulcorner - \urcorner$).

$$\frac{(!\text{-}\ulcorner - \urcorner)}{\ulcorner P \urcorner \vDash !\,\ulcorner P \urcorner}$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that $\checkmark\,\rho^{(\mathrm{H1})}$ and $\ulcorner P \urcorner(\omega, \rho)^{(\mathrm{H2})}$. $!\,\ulcorner P \urcorner(\omega, \rho)$ follows immediately from unfolding $!$ and $\ulcorner - \urcorner$, as H2 tells us that $\rho = \varnothing$ and P holds. □

Lemma F.38 ($!$-*size* $(-, -)$).

$$\frac{(!\text{-}size\,(-, -))}{size\,(\ell,\ n) \vDash !\,size\,(\ell,\ n)}$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that $\checkmark\,\rho^{(\mathrm{H1})}$ and $size\,(\ell,\ n)(\omega, \rho)^{(\mathrm{H2})}$. Then, $!\,size\,(\ell,\ n)(\omega, \rho)$ follows immediately from unfolding $!$ and $size\,(-, -)$, since $\rho = \varnothing$ necessarily.

□

Lemma F.39 ($!$-$\{-\} - \{-\}$).

$$\frac{(!\text{-}\{-\} - \{-\})}{\{P\}\ \mathsf{e}\ \{\hat{Q}\} \vDash !\,\{P\}\ \mathsf{e}\ \{\hat{Q}\}}$$

Proof. Immediate from unfolding $\{-\} - \{-\}$, $!$-idem, and refolding $\{-\} - \{-\}$. □

Lemma F.40 ($!$-$\equiv$).

$$\frac{(!\text{-}\equiv)}{P \equiv Q \vDash !\ (P \equiv Q)}$$

Proof. Immediate from unfolding $\equiv$, $!$-$\star$, $!$-idem, and refolding $\equiv$. □

Lemma F.41 ($!$-$\star$).

$$\frac{(!\text{-}\star)}{!\ (P \star Q) \dashv\vDash !\,P \star !\,Q}$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that $\checkmark\ \rho^{(H1)}$. Unfolding $!$ and $\star$, we must prove

$$\begin{aligned} &\rho = \varnothing \wedge P(\omega, \varnothing) \wedge Q(\omega, \varnothing) \\ \Leftrightarrow\ &\rho = \rho_p \bullet \rho_q \wedge \big(\rho_p = \varnothing \wedge P(\omega, \varnothing)\big) \wedge \big(\rho_q = \varnothing \wedge P(\omega, \varnothing)\big) \end{aligned}$$

where $\rho_p \bullet \rho_q = \varnothing = \rho$. This holds by inspection. □

Lemma F.42 ($!$-$\wedge$).

$$(!\text{-}\wedge)\qquad !\ (P \wedge Q) \dashv\vDash\ !P \wedge\ !Q$$

Proof. Using $!$-$\wedge$-*emp*, the following sequence of $\dashv\vDash$ completes the proof

$$!\ (P \wedge Q) \dashv\vDash emp \wedge P \wedge Q \dashv\vDash emp \wedge P \wedge emp \wedge Q \dashv\vDash\ !P \wedge\ !Q$$

since $emp \dashv\vDash emp \wedge emp$ by definition. □

Lemma F.43 ($!$-$\wedge_1$).

$$(!\text{-}(- \wedge -))\qquad !P \wedge Q \dashv\vDash\ !\ (P \wedge Q)$$

Proof. Follows from $!$-$\wedge$-*emp* using the associativity of $\wedge$. □

Lemma F.44 ($!$-$\wedge/\star$).

$$(!\text{-}\wedge/\star)\qquad !\ (P \wedge Q) \dashv\vDash\ !\ (P \star Q)$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that $\checkmark\ \rho^{(H1)}$. Unfolding $!$, $\star$, and $\wedge$, we must prove

$$\rho = \varnothing \wedge P(\omega, \varnothing) \wedge Q(\omega, \varnothing) \Leftrightarrow \rho = \varnothing \wedge P(\omega, \varnothing) \wedge Q(\omega, \varnothing)$$

since $!$ ensures that $\rho = \varnothing$ on both sides, meaning ρ_p and ρ_q must be exactly $\varnothing$ as well. This holds trivially. □

Lemma F.45 ($!$-$\forall$).

$$(!\text{-}\forall)\qquad \frac{\hat{P} \in Prd\,(X) \qquad X \textit{ is inhabited}}{!\forall\ \hat{P} \dashv\vDash \forall\ !\hat{P}}$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that $\checkmark\ \rho^{(H1)}$. Also, assume X is inhabited. We must prove $!\forall\ \hat{P}(\omega, \rho) \Leftrightarrow \forall\ !\hat{P}(\omega, \rho)$. Unfolding $!$ and $\forall$, this is

$$\rho = \varnothing \wedge \Big(\forall x \in X.\ \hat{P}(x)(\omega, \varnothing)\Big) \Leftrightarrow \forall x \in X.\ \Big(\rho = \varnothing \wedge \hat{P}(x)(\omega, \varnothing)\Big)$$

Selecting arbitrary elements on each side and instantiating as appropriate completes the proof. Crucially, since X is inhabited, we can take arbitrary $x \in X$ to get $\rho = \varnothing$, which is necessary for the backward direction. □

Lemma F.46 ($!$-$\triangleright$).

$$(!\text{-}\triangleright)\qquad !\triangleright P \vDash \triangleright\ !P$$

Proof. Unfolding $\vDash$ and $!$, suppose we have ω, ρ such that

- $\checkmark\ \rho^{(H1)}$
- $\rho = \varnothing^{(H2)}$
- $\triangleright P(\omega, \varnothing)^{(H3)}$

Unfolding $\triangleright$ in the goal, we must either prove

- $\omega.\mathsf{step} = 0^{(G1)}$, or
- $\omega.\mathsf{step} > 0 \wedge\, !\, P(\blacktriangleright\omega, \rho)^{(G2)}$

If $\omega.\mathsf{step} = 0$, then G1 is satisfied trivially. Otherwise, $\omega.\mathsf{step} > 0$ and by unfolding $!$ in G2 it remains to prove

- $\rho = \varnothing^{(G3)}$
- $P(\blacktriangleright\omega, \varnothing)^{(G4)}$

G3 follows from H2. Since $\omega.\mathsf{step} > 0$, unfolding $\triangleright$ in H3 must give us exactly $P(\blacktriangleright\omega, \varnothing)$, which proves G4. □

Lemma F.47 ($\triangleright$ -!).

$$\frac{(! \text{-}\triangleright)}{emp \wedge \triangleright\, !\, P \vDash\, !\, \triangleright P}$$

Proof. Unfolding $\vDash$, $\wedge$, and emp, suppose we have ω, ρ such that

- $\checkmark\, \rho^{(H1)}$
- $\rho = \varnothing^{(H2)}$
- $\triangleright\, !\, P(\omega, \varnothing)^{(H3)}$

Unfolding $!$ and $\triangleright$ in the goal, it suffices to prove

- $\rho = \varnothing^{(G1)}$
- $\omega.\mathsf{step} = 0 \vee (\omega.\mathsf{step} > 0 \wedge \triangleright P(\omega, \varnothing))^{(G2)}$

H2 solves G1. Unfolding $\triangleright$ and $!$ in H3, we either have

- $\omega.\mathsf{step} = 0$, which would solve G2, or
- $\omega.\mathsf{step} > 0^{(H4)}$ and $P(\blacktriangleright\omega, \varnothing)^{(H5)}$

In the latter case, to prove G2 it suffices to show $\triangleright P(\omega, \varnothing)$, or equivalently $P(\blacktriangleright\omega, \varnothing)$ with H4. This is solved by H5 exactly, completing the proof. □

F.2.3 Later Modality Rules.

Lemma F.48 ($\triangleright$ -R).

$$\frac{(\triangleright\text{-}R)}{P \vDash \triangleright P}$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that $\checkmark\, \rho^{(H1)}$ and $P(\omega, \rho)^{(H2)}$. If $\omega.\mathsf{step} = 0$, the claim holds trivially. Otherwise, unfolding $\triangleright$, we must prove that $P(\blacktriangleright\omega, \rho)$ holds, which immediately follows from the definition of Prd, since $\omega \sqsubseteq \blacktriangleright\omega$. □

Lemma F.49 ($\triangleright$ -IND).

$$(\triangleright\text{-IND})\quad \frac{P \wedge \triangleright Q \vDash Q}{P \vDash Q}$$

Proof. Unfolding $\vDash$, suppose we have

- $\checkmark\, \rho^{(H1)}$
- $P(\omega, \rho)^{(H2)}$

By the premise and H1, to prove $Q(\omega, \rho)$ it suffices to prove $(P \wedge \triangleright Q)\ (\omega, \rho)$, or equivalently

- $P(\omega, \rho)^{(G1)}$
- $\triangleright Q(\omega, \rho)^{(G2)}$

Clearly G1 holds by H2. Let us first restate the premise for convenience, unfolding $\wedge$ to obtain $\forall\, \rho, \omega.\ \checkmark\ \rho \Rightarrow P(\omega, \rho) \wedge \triangleright Q(\omega, \rho) \Rightarrow Q(\omega, \rho)^{(\mathrm{H3})}$. This is a meta-level statement that always holds.

Now, to prove G2, we will use induction. Specifically, let $\omega_k = \langle \mathsf{step} : k, \mathsf{sizes} : \omega.\mathsf{sizes}\rangle$; we will prove $\triangleright Q(\omega_k, \rho)$ for all $k \le \omega.\mathsf{step}$. When $k = \omega.\mathsf{step}$, then $\omega_k = \omega$ and the proof will be complete.

Case: $k = 0$ The proof of $\triangleright Q(\omega_0, \rho)$ holding follows immediately from the definition of $\triangleright$.

Case: $k = n + 1$ The inductive hypothesis is $\triangleright Q(\omega_n, \rho)^{(\mathrm{H4})}$, and we must prove $\triangleright Q(\omega_{n+1}, \rho)$, where $n + 1 \le \omega.\mathsf{step}^{(\mathrm{H5})}$. Unfolding $\triangleright$, it suffices to prove $Q(\blacktriangleright\omega_{n+1}, \rho) = Q(\omega_n, \rho)$. To do so, we instantiate H3 with ω_n and ρ. With H1, H2 (invoking the monotonicity of *Prd*, since $\omega \sqsubseteq \omega_k$ using H5), and H4, the proof is complete.

□

Lemma F.50 ($\triangleright$ -mono).

$$\frac{P \vDash Q}{\triangleright P \vDash \triangleright Q}\ (\triangleright\text{-MONO})$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that

- $\checkmark\ \rho^{(\mathrm{H1})}$
- $\triangleright P(\omega, \rho)^{(\mathrm{H2})}$

and assume $P \vDash Q^{(\mathrm{H3})}$. If $\omega.\mathsf{step} = 0$, the claim holds trivially. Otherwise, unfolding $\triangleright$, we have $P(\blacktriangleright\omega, \rho)^{(\mathrm{H4})}$ and must prove $Q(\blacktriangleright\omega, \rho)^{(\mathrm{G1})}$. This follows by instantiating H3 with H1 and H4. □

Lemma F.51 ($\triangleright$ -$\wedge$).

$$(\triangleright\text{-}\wedge)\quad \triangleright\ (P \wedge Q) \dashv\vDash \triangleright P \wedge \triangleright Q$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that $\checkmark\ \rho$. Unfolding $\wedge$, we must prove that

$$\triangleright\ (P \wedge Q)\ (\omega, \rho) \Leftrightarrow \triangleright P(\omega, \rho) \wedge \triangleright Q(\omega, \rho)$$

Begin by unfolding $\triangleright$. If $\omega.\mathsf{step} = 0$, the claim holds trivially. Otherwise, $\omega.\mathsf{step} > 0$ and we rewrite as

$$(P \wedge Q)\ (\blacktriangleright\omega, \rho) \Leftrightarrow P(\blacktriangleright\omega, \rho) \wedge Q(\blacktriangleright\omega, \rho)$$

which is immediate with the definition of $\wedge$. □

Lemma F.52 ($\triangleright$ -$\star$).

$$(\triangleright\text{-}\star)\quad \triangleright\ (P \star Q) \dashv\vDash \triangleright P \star \triangleright Q$$

Proof. Unfolding $\vDash$ in the goal, suppose we have ω, ρ such that $\checkmark\ \rho$. We must prove that $\triangleright\ (P \star Q)\ (\omega, \rho) \Leftrightarrow (\triangleright P \star \triangleright Q)\ (\omega, \rho)$. We prove each direction separately.

For the forward direction, begin by unfolding $\triangleright$. If $\omega.\mathsf{step} = 0$, the claim holds trivially. Otherwise, we may assume $(P \star Q)\ (\blacktriangleright\omega, \rho)^{(\mathrm{H1})}$ and must prove the existence of ρ_p and ρ_q such that

- $\rho_p \bullet \rho_q = \rho^{(\mathrm{G1})}$
- $\triangleright P(\omega, \rho_p)^{(\mathrm{G2})}$
- $\triangleright Q(\omega, \rho_q)^{(\mathrm{G3})}$

Unfolding $\star$ in H1, there must exist ρ_p and ρ_q with $\rho_p \bullet \rho_q = \rho$ such that $P(\blacktriangleright\omega, \rho_p)$ and $Q(\blacktriangleright\omega, \rho_q)$ hold, which solves all three goals after unfolding $\triangleright$ in G2 and G3.

For the backward direction, we similarly begin by unfolding $\star$ and $\triangleright$ (handling the trivial $\omega.\mathsf{step} = 0$ case, as above) to obtain $P(\blacktriangleright\omega, \rho_p)$ and $Q(\blacktriangleright\omega, \rho_q)$ for some $\rho_p \bullet \rho_q = \rho$. Unfolding $\triangleright$ and $\star$ in the goal as above, these are exactly the ρ_p and ρ_q that must exist. □

Lemma F.53 ($\triangleright$ -$\multimap$).

$$\text{($\triangleright$ -$\multimap$)}\qquad \triangleright\ (P \mathrel{-\!\!\star} Q) \vDash \triangleright P \mathrel{-\!\!\star} \triangleright Q$$

Proof. By $-\!\!\star$-R, it suffices to prove that

$$\triangleright\ (P \mathrel{-\!\!\star} Q) \star \triangleright P \vDash \triangleright Q$$

By $\triangleright$ -$\star$ and $\triangleright$ -mono, it suffices if

$$(P \mathrel{-\!\!\star} Q) \star P \vDash Q$$

which is exactly $-\!\!\star$-L. □

F.2.4 Non-Standard Entailments.

Lemma F.54 (@ -mono).

$$\text{(@ -MONO)}\qquad \frac{P \vDash Q}{@_\ell\, P \vDash @_\ell\, Q}$$

Proof. Unfolding $\vDash$ in the goal, suppose we have ω, ρ such that

- $\checkmark\ \rho^{(\mathrm{H1})}$
- $@_\ell\, P(\omega, \rho)^{(\mathrm{H2})}$

Unfolding $@_\ell$ in the goal, we must prove the existence of some ρ_q such that

- $\rho = \ell \mapsto \mathsf{shr}(1, \rho_q)^{(\mathrm{G1})}$
- $Q(\omega, \rho_q)^{(\mathrm{G2})}$

Unfolding $@_\ell$ in H2, there exists some ρ_p with

- $\rho = \ell \mapsto \mathsf{shr}(1, \rho_p)^{(\mathrm{H3})}$
- $P(\omega, \rho_p)^{(\mathrm{H4})}$

Choose ρ_q to be ρ_p. H3 therefore solves G1.

Applying $\dashrightarrow$-jump, we have $\rho \dashrightarrow \rho_p$, so we can apply Valid Reachability Monotonicity with H1 to obtain $\checkmark\ \rho_p$. Now, we instantiate the premise $P \vDash Q$ with $\checkmark\ \rho_p$ and H4 to derive $Q(\omega, \rho_p)$, solving G2. □

Lemma F.55 (@ -!).

$$\text{(@ -!)}\qquad @_\ell\, P \star !\, Q \dashv\vDash @_\ell\ (P \star !\, Q)$$

Proof. Unfolding $\dashv\vDash$ in the goal, suppose we have ω, ρ such that $\checkmark\ \rho$. We must prove that $(@_\ell\, P \star !\, Q)\ (\omega, \rho) \Leftrightarrow @_\ell\ (P \star !\, Q)\ (\omega, \rho)$. Unfolding $@_\ell$, $\star$, and $!$, we must prove

$$\begin{gathered}\big(\exists\, \rho_p.\ \rho = \ell \mapsto \mathsf{shr}(1, \rho_p) \wedge P(\omega, \rho_p)\big) \wedge Q(\omega, \varnothing)\\ \Leftrightarrow \exists\, \rho_p.\ \rho = \ell \mapsto \mathsf{shr}(1, \rho_p) \wedge \big(P(\omega, \rho_p) \wedge Q(\omega, \varnothing)\big)\end{gathered}$$

after noting that separating a resource into one that satisfies an unrestricted predicate means the separation must be trivial. These are both equivalent to $\exists\, \rho_p.\ \rho = \ell \mapsto \mathsf{shr}(1, \rho_p) \wedge P(\omega, \rho_p) \wedge Q(\omega^+, \varnothing)$. Note that if there exists no such ρ_p, both equivalent statements do not hold. □

Lemma F.56 ($@$ -$\vee$).

$$(@\text{ -}\vee)$$
$$@_\ell\ (P \vee Q) \dashv\vDash @_\ell P \vee @_\ell Q$$

Proof. Unfolding $\dashv\vDash$ in the goal, suppose we have ω, ρ such that $\checkmark\rho$. We must prove that $@_\ell\ (P \vee Q)\ (\omega,\rho) \Leftrightarrow @_\ell P \vee @_\ell Q(\omega,\rho)$. Unfolding $@_\ell$ and $\vee$, we must prove

$$\begin{aligned}&\exists\,\rho_{pq}.\ \rho = \ell \mapsto \mathsf{shr}(1,\rho_{pq}) \wedge \left(\hat{P}(x)(\omega,\rho_{pq}) \vee \hat{Q}(x)(\omega,\rho_{pq})\right)\\ \Leftrightarrow\ &\left(\exists\,\rho_p.\ \rho = \ell \mapsto \mathsf{shr}(1,\rho_p) \wedge \hat{P}(x)(\omega,\rho_p)\right) \vee \left(\exists\,\rho_q.\ \rho = \ell \mapsto \mathsf{shr}(1,\rho_q) \wedge \hat{Q}(x)(\omega,\rho_q)\right)\end{aligned}$$

We prove each direction of the implication separately. For the forward direction, suppose we have $\rho = \ell \mapsto \mathsf{shr}(1,\rho_{pq})$. If $\hat{P}(x)(\omega,\rho_{pq})$ holds, then $\exists\,\rho_p.\ \rho = \ell \mapsto \mathsf{shr}(1,\rho_p) \wedge \hat{P}(x)(\omega,\rho_{pq})$, where $\rho_p = \rho_{pq}$. Otherwise, $\hat{Q}(x)(\omega,\rho_{pq})$ holds, and thus $\exists\,\rho_q.\ \rho = \ell \mapsto \mathsf{shr}(1,\rho_q) \wedge \hat{Q}(x)(\omega,\rho_{pq})$ does as well where $\rho_q = \rho_{pq}$.

For the backward direction, we proceed similarly. If the left disjunct holds, and we assert $\rho_{pq} = \rho_p$; otherwise, the right disjunct must hold and we assert $\rho_{pq} = \rho_p$ to complete the proof. □

Lemma F.57 ($@$ -$\exists$).

$$(@\text{ -}\exists\ )$$
$$@_\ell \exists\ \hat{P} \dashv\vDash \exists\ @_\ell \hat{P}$$

Proof. Unfolding $\dashv\vDash$ in the goal, suppose we have ω, ρ such that $\checkmark\rho$. We must prove that $@_\ell \exists\ \hat{P}(\omega,\rho) \Leftrightarrow \exists\ @_\ell \hat{P}(\omega,\rho)$. Unfolding $@_\ell$ and $\exists$, we must prove

$$\begin{aligned}&\exists\,\rho_p.\ \rho = \ell \mapsto \mathsf{shr}(1,\rho_p) \wedge \left(\exists\,x.\ \hat{P}(x)(\omega,\rho_p)\right)\\ \Leftrightarrow\ &\exists\,x.\ \left(\exists\,\rho_p.\ \rho = \ell \mapsto \mathsf{shr}(1,\rho_p) \wedge \hat{P}(x)(\omega,\rho_p)\right)\end{aligned}$$

These are both equivalent to $\exists\,\rho_p, x.\ \rho = \ell \mapsto \mathsf{shr}(1,\rho_p) \wedge \hat{P}(x)(\omega,\rho_p)$, noting that reordering of the existential quantifiers makes no difference, and the resource ρ_p is dependent on the structure of ρ only. If the domain of either existential is uninhabited, the statements are still equivalent, since would both be false. □

Lemma F.58 ($@$ -$\triangleright$).

$$(@\text{ -}\triangleright\ )$$
$$@_\ell \triangleright P \vDash \triangleright @_\ell P$$

Proof. Unfolding $\vDash$ in the goal, suppose we have ω, ρ, and ℓ such that

- $\checkmark\rho^{(\mathrm{H1})}$
- $@_\ell \triangleright P(\omega,\rho)^{(\mathrm{H2})}$

Unfolding $@_\ell$ and $\triangleright$ in the goal, we must prove either

- $\omega.\mathsf{step} = 0^{(\mathrm{G1})}$ or
- $\omega.\mathsf{step} > 0 \wedge \exists\,\rho_p.\ \rho = \ell \mapsto \mathsf{shr}(1,\rho_p) \wedge P(\omega,\rho_p)^{(\mathrm{G2})}$

Unfolding $@_\ell$ and $\triangleright$ in H2, there exists some ρ' with

- $\rho = \ell \mapsto \mathsf{shr}(1,\rho')^{(\mathrm{H3})}$
- $\omega.\mathsf{step} = 0 \vee (\omega.\mathsf{step} > 0 \wedge P(\omega,\rho'))^{(\mathrm{H4})}$

We proceed by cases on H4. If $\omega.\mathsf{step} = 0$, then G1 holds and we are done. Otherwise, we have $(\omega.\mathsf{step} > 0 \wedge P(\omega,\rho'))$, which proves G2 after asserting ρ' is the resource ρ_p which must exist. □

Lemma F.59 ($@$ -$\bot$).

$$\frac{(@\text{-}\bot)}{@_\ell \bot \vDash \bot}$$

Proof. Unfolding $\vDash$ in the goal, suppose we have ω, ρ such that $\checkmark\ \rho^{(H1)}$ and $(@_\ell \bot)\ (\omega, \rho)^{(H2)}$. Unfolding $@_\ell$ and $\bot$, we must prove

$$\exists\, \rho_p.\ \rho = \ell \mapsto \mathsf{shr}(1, \rho_p) \wedge \bot \Rightarrow \bot$$

which follows using standard intuitionistic logic rules. □

Lemma F.60 ($\diamond$ -R).

$$\frac{(\diamond\text{-R})}{P \vDash \diamond P}$$

Proof. Unfolding $\vDash$ in the goal, suppose we have ω, ρ such that $\checkmark\ \rho^{(H1)}$ and $P(\omega, \rho)^{(H2)}$. Since $\rho \twoheadrightarrow \rho$ (as $\rho \leq \rho$), the result immediately follows after unfolding $\diamond$. □

Lemma F.61 ($\diamond$ -mono).

$$(\diamond\text{-mono})\quad \frac{P \vDash Q}{\diamond P \vDash \diamond Q}$$

Proof. Unfolding $\vDash$ in the goal, suppose we have ω, ρ such that

- $\checkmark\ \rho^{(H1)}$
- $\diamond P(\omega, \rho)^{(H2)}$

Unfolding $\diamond$, we must prove the existence of some ρ_q such that

- $\rho \twoheadrightarrow \rho_q{}^{(G1)}$
- $Q(\omega, \rho_q)^{(G2)}$

Unfolding $\diamond$ in H2, there exists some ρ_p with

- $\rho \twoheadrightarrow \rho_p{}^{(H3)}$
- $P(\omega, \rho_p)^{(H4)}$

We claim that the ρ_q is exactly the ρ_p that we are searching for. H3 therefore solves G1.

Applying Valid Reachability Monotonicity with H1 and H3 yields $\checkmark\ \rho_p$. Now, we instantiate the premise $P \vDash Q$ with $\checkmark\ \rho_p$ and H4 to derive $Q(\omega, \rho_p)$, solving G2. □

Lemma F.62 ($\diamond$ -bind).

$$(\diamond\text{-bind})\quad \frac{P \vDash \diamond Q}{\diamond P \vDash \diamond Q}$$

Proof. Unfolding $\vDash$ in the goal, suppose we have ω, ρ such that

- $\checkmark\ \rho^{(H1)}$
- $\diamond P(\omega, \rho)^{(H2)}$

Unfolding $\diamond$, we must prove the existence of some ρ_q such that

- $\rho \twoheadrightarrow \rho_q{}^{(G1)}$
- $Q(\omega, \rho_q)^{(G2)}$

Unfolding $\diamond$ in H2, there exists some ρ_p with

- $\rho \twoheadrightarrow \rho_p{}^{(H3)}$

- $P(\omega, \rho_p)^{(\mathrm{H4})}$

Applying Valid Reachability Monotonicity with H1 and H3 gives us $\checkmark\, \rho_p$; instantiating $P \vDash \diamond Q$ with this and H4 gives us $\diamond Q(\omega, \rho_p)$. Unfolding $\diamond$, there must exist some ρ' with

- $\rho_p \twoheadrightarrow \rho'^{(\mathrm{H5})}$
- $Q(\omega, \rho')^{(\mathrm{H6})}$

ρ' is the ρ_q that we are searching for. H6 instantly solves G2. G1 is solved by applying $\twoheadrightarrow$-trans with H3 and H5. □

Lemma F.63 ($\diamond$-idem).

$$(\diamond\text{-}\mathit{IDEM})$$
$$\diamond \diamond P \vDash \diamond P$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that

- $\checkmark\, \rho^{(\mathrm{H1})}$
- $\diamond \diamond P(\omega, \rho)^{(\mathrm{H2})}$

Unfolding $\diamond$, we must prove the existence of some ρ_p such that

- $\rho \twoheadrightarrow \rho_p{}^{(\mathrm{G1})}$
- $P(\omega, \rho_p)^{(\mathrm{G2})}$

Unfolding $\diamond$ in H2, there exists some ρ_1 with

- $\rho \twoheadrightarrow \rho_1{}^{(\mathrm{H3})}$
- $\diamond P(\omega, \rho_1)^{(\mathrm{H4})}$

Unfolding $\diamond$ in H4, there exists some ρ_2 with

- $\rho_1 \twoheadrightarrow \rho_2{}^{(\mathrm{H5})}$
- $P(\omega, \rho_2)^{(\mathrm{H6})}$

ρ_2 is the ρ_p that we are searching for. H6 instantly solves G2. G1 is solved by applying $\twoheadrightarrow$-trans with H3 and H5. □

Lemma F.64 ($\diamond$-@).

$$(\diamond\text{-}@)$$
$$@_\ell\, P \vDash \diamond P$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that

- $\checkmark\, \rho^{(\mathrm{H1})}$
- $@_\ell\, P(\omega, \rho)^{(\mathrm{H2})}$

Unfolding $\diamond$, we must prove the existence of some ρ_p such that

- $\rho \twoheadrightarrow \rho_p{}^{(\mathrm{G1})}$
- $P(\omega, \rho_p)^{(\mathrm{G2})}$

Unfolding $@_\ell$ in H2, there exists some ρ' with

- $\rho = \ell \mapsto \mathsf{shr}(1, \rho')^{(\mathrm{H3})}$
- $P(\omega, \rho')^{(\mathrm{H4})}$

ρ' is the ρ_p that we are searching for. H4 instantly solves G2. G1 is solved by applying $\twoheadrightarrow$-jump with H3. □

Lemma F.65 ($\diamond$-drop).

$$(\diamond\text{-}\mathit{DROP})$$
$$\diamond\ (P \star Q) \vDash \diamond P$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that

- $\checkmark\ \rho^{(H1)}$
- $\diamond\ (P \star Q)\ (\omega, \rho)^{(H2)}$

Unfolding $\diamond$ in the goal, we must prove the existence of some ρ_p such that

- $\rho \dashrightarrow \rho_p{}^{(G1)}$
- $P(\omega, \rho_p)^{(G2)}$

Unfolding $\diamond$ in H2, there exists some ρ' with

- $\rho \dashrightarrow \rho'^{(H3)}$
- $(P \star Q)\ (\omega, \rho')^{(H4)}$

Unfolding $\star$ in H4, there exist ρ'_p and ρ'_q such that

- $\rho' = \rho'_p \bullet \rho'_q{}^{(H5)}$
- $P(\omega, \rho'_p)^{(H6)}$
- $Q(\omega, \rho'_q)^{(H7)}$

ρ'_p is the ρ_p that we are searching for. H6 instantly solves G2.

Now, note that $\rho'_p \leq \rho'$ from H5, meaning $\rho' \dashrightarrow \rho'_p$ by $\dashrightarrow$-sub. Applying $\dashrightarrow$-trans with this and H3 solves G1. □

Lemma F.66 ($\diamond$-!).

$$\frac{P \vDash \diamond\,!\,Q}{P \vDash P \star !\,Q}\ (\diamond\text{-}!)$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that

- $\checkmark\ \rho^{(H1)}$
- $P(\omega, \rho)^{(H2)}$

Unfolding $\star$ and ! and simplifying, we must prove $P(\omega, \rho) \wedge Q(\omega, \varnothing)$, noting the separation of ρ must be trivial to satisfy the emptiness condition of !. With H2, it remains to show $Q(\omega, \varnothing)^{(G1)}$.

Now, instantiate $P \vDash \diamond\,!\,Q$ with H1 and H2 to obtain $\diamond\,!\,Q$. Unfolding $\diamond$ and !, this tells us that $\rho \dashrightarrow \varnothing \wedge Q(\omega, \varnothing)$, solving G1. □

F.2.5 Weakest Preconditions.

Lemma F.67 (wp-ramify).

$$\left(\forall\ \mathtt{w}.\ \hat{P}(\mathtt{w}) \mathrel{-\!\!\star} \hat{Q}(\mathtt{w})\right) \star wp\ (\mathtt{e})\ \{\hat{P}\} \vDash wp\ (\mathtt{e})\ \{\hat{Q}\}\quad (\text{wp-ramify})$$

Proof. Unfolding $\vDash$ and $\star$, suppose we have $\omega, \rho, \rho_1, \rho_2$ such that

- $\checkmark\ \rho^{(H1)}$
- $\rho = \rho_1 \bullet \rho_2{}^{(H2)}$
- $\left(\forall\ \mathtt{w}.\ \hat{P}(\mathtt{w}) \mathrel{-\!\!\star} \hat{Q}(\mathtt{w})\right)(\omega, \rho_1)^{(H3)}$
- $wp\ (\mathtt{e})\ \{\hat{P}\}(\omega, \rho_2)^{(H4)}$

Unfolding $wp\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(H5)}$
- $\rho_f \sharp \rho^{(H6)}$

- $\psi = \omega^+.\mathsf{sizes}^{(\mathrm{H7})}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(\mathrm{H8})}$
- $k < \omega^+.\mathsf{step}^{(\mathrm{H9})}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(\mathrm{H10})}$
- $(\psi, \mu, \mathtt{e}) \rightarrow^k (\psi', \mu', \mathtt{e}') \nrightarrow^{(\mathrm{H11})}$

We must show, for some $\rho'^{(\mathrm{G1})}$,

- $\rho_f \,\sharp\, \rho'^{(\mathrm{G2})}$
- $\psi' \supseteq \psi^{(\mathrm{G3})}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(\mathrm{G4})}$
- $\mathtt{e}' \in \mathtt{Word}^{(\mathrm{G5})}$
- $\hat{Q}(\mathtt{e}')(\omega', \rho')^{(\mathrm{G6})}$

Now, note that $\mu = \mathsf{erase}(\rho \bullet \rho_f) = \mathsf{erase}((\rho_1 \bullet \rho_2) \bullet \rho_f) = \mathsf{erase}(\rho_2 \bullet (\rho_1 \bullet \rho_f))$ by H2, Res Composition Associative, and Res Composition Commutative. Also note that $\rho_2 \,\sharp\, (\rho_1 \bullet \rho_f)$, since their composition is defined and valid by unfolding $\sharp$ in H6.

This means that we can instantiate $wp\ (\mathtt{e})\ \{\hat{P}\}(\omega, \rho_2)$ with $\rho_2 \,\sharp\, (\rho_1 \bullet \rho_f)$, $\mu = \mathsf{erase}(\rho_2 \bullet (\rho_1 \bullet \rho_f))$, and $(\psi, \mu, \mathtt{e}) \rightarrow^k (\psi', \mu', \mathtt{e}') \nrightarrow$, using additional hypotheses and worlds from above as appropriate. This guarantees the existence of some ρ_2' such that

- $(\rho_1 \bullet \rho_f) \,\sharp\, \rho_2'^{(\mathrm{H12})}$
- $\psi' \supseteq \psi^{(\mathrm{H13})}$
- $\mu' = \mathsf{erase}(\rho_2' \bullet (\rho_1 \bullet \rho_f))^{(\mathrm{H14})}$
- $\mathtt{e}' \in \mathtt{Word}^{(\mathrm{H15})}$
- $\hat{P}(\mathtt{e}')(\omega', \rho_2')^{(\mathrm{H16})}$

H13 and H15 immediately solve G3 and G5 respectively.

We assert that $\rho' = \rho_1 \bullet \rho_2'$. H14 solves G4 using Res Composition Commutative. To prove G2, the composition $\rho_f \bullet (\rho_1 \bullet \rho_2')$ must be defined and valid. This follows from H12 by unfolding $\bullet$ and applying Res Composition Commutative as appropriate.

It remains to prove G6, and we have not yet used H16 nor H3. Unfolding $\forall$ and $-\!\!\star$, then instantiating $\left(\forall\ \mathtt{w}.\ \hat{P}(\mathtt{w}) -\!\!\star \hat{Q}(\mathtt{w})\right)(\omega, \rho_1)$ with $\omega' \sqsupseteq \omega^+ \sqsupseteq \omega$ and $\mathtt{e}'$ gives us

- $\forall\, \rho_p \,\sharp\, \rho, \rho_q.\ \rho_1 \bullet \rho_p = \rho_q \Rightarrow \hat{P}(\mathtt{e}')(\omega', \rho_p) \Rightarrow \hat{Q}(\mathtt{e}')(\omega', \rho_q)^{(\mathrm{H17})}$

Now, let $\rho_p = \rho_2'$ and $\rho_q = \rho' = \rho_1 \bullet \rho_2'$. Instantiating H17 using these resources and H16 solves G6, completing the proof. □

Lemma F.68 (wp-frame).

$$\frac{(\textit{WP-FRAME})}{P \star wp\ (\mathtt{e})\ \{\hat{Q}\} \vDash wp\ (\mathtt{e})\ \{\mathtt{w}.\ P \star \hat{Q}(\mathtt{w})\}}$$

Proof. By wp-ramify, it suffices if

$$P \star wp\ (\mathtt{e})\ \{\hat{Q}\} \vDash \left(\forall\ \mathtt{w}.\ \hat{Q}(\mathtt{w}) -\!\!\star \left(P \star \hat{Q}(\mathtt{w})\right)\right) \star wp\ (\mathtt{e})\ \{\hat{Q}\}$$

By $\star$-mono and $\forall$ -R, it suffices if

$$P \vDash \hat{Q}(\mathtt{w}) -\!\!\star \left(P \star \hat{Q}(\mathtt{w})\right)$$

for arbitrary $\mathtt{w}$. This follows from $-\!\!\star$-R and refl. □

Lemma F.69 (wp-mono).

$$\frac{\forall\, \mathtt{w}.\ \hat{P}(\mathtt{w}) \vDash \hat{Q}(\mathtt{w})}{wp\ (\mathtt{e})\ \{\hat{P}\} \vDash wp\ (\mathtt{e})\ \{\hat{Q}\}}\ \textit{(wp-mono)}$$

Proof. By wp-ramify, it suffices if

$$wp\ (\mathtt{e})\ \{\hat{P}\} \vDash \left(\forall\ \mathtt{w}.\ \hat{P}(\mathtt{w}) \mathrel{-\!\!\star} \hat{Q}(\mathtt{w})\right) \star wp\ (\mathtt{e})\ \{\hat{P}\}$$

By $\star$-mono and $\forall$ -R, it suffices if

$$\vDash \hat{P}(\mathtt{w}) \mathrel{-\!\!\star} \hat{Q}(\mathtt{w})$$

for arbitrary $\mathtt{w}$, which follows from $\mathrel{-\!\!\star}$-R and the premise. □

Lemma F.70 (wp-val).

$$\textit{(wp-val)}\quad \hat{Q}(\mathtt{w}) \vDash wp\ (\mathtt{w})\ \{\hat{Q}\}$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that

- $\checkmark\ \rho^{(H1)}$
- $\hat{Q}(\mathtt{w})(\omega, \rho)^{(H2)}$

Unfolding $wp\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(H3)}$
- $\rho_f \ \sharp\ \rho^{(H4)}$
- $\psi = \omega^+.\mathsf{sizes}^{(H5)}$
- $k < \omega^+.\mathsf{step}^{(H6)}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(H7)}$
- $(\psi, \mathsf{erase}(\rho \bullet \rho_f), \mathtt{w}) \to^k (\psi', \mu', \mathtt{e}') \not\to^{(H8)}$

We must show, for some $\rho'^{(G1)}$,

- $\rho_f \ \sharp\ \rho'^{(G2)}$
- $\psi' \supseteq \psi^{(G3)}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(G4)}$
- $\mathtt{e}' \in \mathtt{Word}^{(G5)}$
- $\hat{Q}(\mathtt{e}')(\omega', \rho')^{(G6)}$

Let $\rho' = \rho$. H4 subsequently solves G2. By the operational semantics, $(\psi, \mathsf{erase}(\rho \bullet \rho_f), \mathtt{w})$ cannot take any steps, meaning we must have

- $\psi' = \psi$, solving G3
- $\mu' = \mathsf{erase}(\rho \bullet \rho_f)$, solving G4
- $\mathtt{e}' = \mathtt{w}$, solving G5
- $k = 0$

Since $k = 0$, we have $\omega' = \omega^+$. Applying the monotonicity of *Prd* to H2 with H3 solves G6. □

Lemma F.71 (wp-bind).

$$\textit{(wp-bind)}\quad wp\ (\mathtt{e})\ \{\mathtt{w}.\ wp\ (\mathtt{K}[\mathtt{w}])\ \{\hat{Q}\}\} \vDash wp\ (\mathtt{K}[\mathtt{e}])\ \{\hat{Q}\}$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that

- $\checkmark\ \rho^{(H1)}$

- $\mathit{wp}\ (\mathtt{e})\ \{\mathtt{w}.\ \mathit{wp}\ (\mathtt{K}[\mathtt{w}])\ \{\hat{Q}\}\}(\omega, \rho)^{(\mathrm{H2})}$

Unfolding $\mathit{wp}\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(\mathrm{H3})}$
- $\rho_f \sharp \rho^{(\mathrm{H4})}$
- $\psi = \omega^+.\mathsf{sizes}^{(\mathrm{H5})}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(\mathrm{H6})}$
- $k < \omega^+.\mathsf{step}^{(\mathrm{H7})}$
- $\omega_2 = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi_2 \rangle^{(\mathrm{H8})}$
- $(\psi, \mu, \mathtt{K}[\mathtt{e}]) \longrightarrow^k (\psi_2, \mu_2, \mathtt{e}') \not\rightarrow^{(\mathrm{H9})}$

We must show, for some $\rho'^{(\mathrm{G1})}$,

- $\rho_f \sharp \rho'^{(\mathrm{G2})}$
- $\psi_2 \supseteq \psi^{(\mathrm{G3})}$
- $\mu_2 = \mathsf{erase}(\rho' \bullet \rho_f)^{(\mathrm{G4})}$
- $\mathtt{e}' \in \mathtt{Word}^{(\mathrm{G5})}$
- $\hat{Q}(\mathtt{e}')(\omega_2, \rho')^{(\mathrm{G6})}$

It follows from H9 by inspection of the operational semantics that there exist ψ_1, μ_1, $\mathtt{e}_\circ$, and $0 \le j \le k$ such that

- $(\psi, \mu, \mathtt{e}) \longrightarrow^j (\psi_1, \mu_1, \mathtt{e}_\circ) \not\rightarrow^{(\mathrm{H10})}$
- $(\psi, \mu, \mathtt{K}[\mathtt{e}]) \longrightarrow^j (\psi_1, \mu_1, \mathtt{K}[\mathtt{e}_\circ]) \longrightarrow^{k-j} (\psi_2, \mu_2, \mathtt{e}') \not\rightarrow^{(\mathrm{H11})}$

Now, instantiate $\mathit{wp}\ (\mathtt{e})\ \{\mathtt{w}.\ \mathit{wp}\ (\mathtt{K}[\mathtt{w}])\ \{\hat{Q}\}\}(\omega, \rho)$ with H3, H4, H5, H6, $j \le k < \omega^+.\mathsf{step}$ and $\omega_1 = \langle \mathsf{step} : \omega^+.\mathsf{step} - j, \mathsf{sizes} : \psi_1 \rangle$. By providing H10, we conclude that for some ρ_1',

- $\rho_f \sharp \rho_1'^{(\mathrm{H12})}$
- $\psi_1 \supseteq \psi^{(\mathrm{H13})}$
- $\mu_1 = \mathsf{erase}(\rho_1' \bullet \rho_f)^{(\mathrm{H14})}$
- $\mathtt{e}_\circ \in \mathtt{Word}^{(\mathrm{H15})}$
- $\mathit{wp}\ (\mathtt{K}[\mathtt{e}_\circ])\ \{\hat{Q}\}(\omega_1, \rho_1')^{(\mathrm{H16})}$

Now, instantiate $\mathit{wp}\ (\mathtt{K}[\mathtt{e}_\circ])\ \{\hat{Q}\}(\omega_1, \rho_1')$ with $\omega_1 \sqsupseteq \omega_1$, $\rho_f \sharp \rho_1'$, $\psi_1 = \omega_1.\mathsf{sizes}$, $k - j < \omega_1.\mathsf{step}$, and $\omega_2 = \langle \mathsf{step} : \omega_1.\mathsf{step} - (k - j), \mathsf{sizes} : \psi_2 \rangle$. Note that this ω_2 is exactly the ω_2 from H8, since $\omega_1.\mathsf{step} - (k-j) = (\omega^+.\mathsf{step} - j) - (k-j) = \omega^+.\mathsf{step} - k$. For this same reason, we know $k - j < \omega_1.\mathsf{step}$. By providing $(\psi_1, \mu_1, \mathtt{K}[\mathtt{e}_\circ]) \longrightarrow^{k-j} (\psi_2, \mu_2, \mathtt{e}') \not\rightarrow$ from H11, we conclude that for some ρ_2',

- $\rho_f \sharp \rho_2'^{(\mathrm{H17})}$
- $\psi_2 \supseteq \psi_1^{(\mathrm{H18})}$
- $\mu_2 = \mathsf{erase}(\rho_2' \bullet \rho_f)^{(\mathrm{H19})}$
- $\mathtt{e}' \in \mathtt{Word}^{(\mathrm{H20})}$
- $\hat{Q}(\mathtt{e}')(\omega_2, \rho_2')^{(\mathrm{H21})}$

We set $\rho' = \rho_2'$. H17, H19, H20, and H21 instantly solve G2, G4, G5, G6, respectively. H18 and H13 together prove G3. □

Lemma F.72 (wp-let).

$$\frac{(\textit{wp-let})}{\triangleright\ \mathit{wp}\ (\mathtt{e}[\mathtt{w}/\mathtt{x}])\ \{\hat{Q}\} \vDash \mathit{wp}\ (\mathtt{const\ x = w;\ e})\ \{\hat{Q}\}}$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that

- $\checkmark\, \rho^{(\mathrm{H1})}$
- $\triangleright\, wp\ (\mathtt{e}[\mathtt{w}/\mathtt{x}])\ \{\hat{Q}\}(\omega, \rho)^{(\mathrm{H2})}$

Unfolding $\triangleright$, this tells us that either

- $\omega.\mathsf{step} = 0^{(\mathrm{H3})}$, or
- $\omega.\mathsf{step} > 0 \wedge wp\ (\mathtt{e}[\mathtt{w}/\mathtt{x}])\ \{\hat{Q}\}(\blacktriangleright\omega, \rho)^{(\mathrm{H4})}$

Unfolding $wp\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(\mathrm{H5})}$
- $\rho_f \sharp \rho^{(\mathrm{H6})}$
- $\psi = \omega^+.\mathsf{sizes}^{(\mathrm{H7})}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(\mathrm{H8})}$
- $k < \omega^+.\mathsf{step}^{(\mathrm{H9})}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(\mathrm{H10})}$
- $(\psi, \mu, \mathtt{const\ x = w;\ e}) \rightarrow^k (\psi', \mu', \mathtt{e}') \not\rightarrow^{(\mathrm{H11})}$

If we have H3, then for any $\omega^+ \sqsupseteq \omega$, there exist no non-negative $k < \omega^+.\mathsf{step}$, meaning that $wp\ (\mathtt{const\ x = w;\ e})\ \{\hat{Q}\}(\omega, \rho)$ holds vacuously. Otherwise, we may use H4 and must prove the existence of some ρ' such that

- $\rho_f \sharp \rho'^{(\mathrm{G1})}$
- $\psi' \supseteq \psi^{(\mathrm{G2})}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(\mathrm{G3})}$
- $\mathtt{e}' \in \mathtt{Word}^{(\mathrm{G4})}$
- $\hat{Q}(\mathtt{e}')(\omega', \rho')^{(\mathrm{G5})}$

By inspecting the operational semantics, we observe that the evaluation in H11 must proceed as $(\psi, \mu, \mathtt{const\ x = w;\ e}) \rightarrow (\psi, \mu, \mathtt{e}[\mathtt{w}/\mathtt{x}]) \rightarrow^{k-1} (\psi', \mu', \mathtt{e}') \not\rightarrow^{(\mathrm{H12})}$, noting that this first step must always be taken before reaching an irreducible configuration.

Now, instantiate $wp\ (\mathtt{e}[\mathtt{w}/\mathtt{x}])\ \{\hat{Q}\}(\blacktriangleright\omega, \rho)$ from H4 with

- $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$
- $\rho_f \sharp \rho$, from H6
- $\psi = \blacktriangleright\omega^+.\mathsf{sizes} = \omega^+.\mathsf{sizes}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)$, from H8
- $k - 1 < \blacktriangleright\omega^+.\mathsf{step}$
- $\omega' = \langle \mathsf{step} : \blacktriangleright\omega^+.\mathsf{step} - (k-1), \mathsf{sizes} : \psi' \rangle = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle$

Note that $\blacktriangleright\omega^+$ is defined, since $k < \omega^+.\mathsf{step}$ must be at least one in order to take the step in H12. Also, $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$ and $k - 1 < \blacktriangleright\omega^+.\mathsf{step}$ by unfolding $\blacktriangleright$ in H5 and H9 respectively, so the instantiation is valid. Providing $(\psi, \mu, \mathtt{e}[\mathtt{w}/\mathtt{x}]) \rightarrow^{k-1} (\psi', \mu', \mathtt{e}') \not\rightarrow$ from H12 guarantees the existence of some ρ' that meets the conditions from above, solving all remaining goals. □

Lemma F.73 (wp-seq).

(wp-seq)

$$wp\ (\mathtt{e}_1)\ \{\_.\ \triangleright\, wp\ (\mathtt{e}_2)\ \{\hat{Q}\}\} \vDash wp\ (\mathtt{e}_1; \mathtt{e}_2)\ \{\hat{Q}\}$$

Proof. After desugaring $\mathtt{e}_1; \mathtt{e}_2$, it suffices to prove

$$wp\ (\mathtt{e}_1)\ \{\_.\ \triangleright\, wp\ (\mathtt{e}_2)\ \{\hat{Q}\}\} \vDash wp\ (\mathtt{const\ x = e_1;\ e_2})\ \{\hat{Q}\}$$

where $\mathtt{x}$ does not appear free in $\mathtt{e}_2$. By wp-bind, it suffices if

$$wp\ (\mathtt{e}_1)\ \{\_.\ \triangleright\, wp\ (\mathtt{e}_2)\ \{\hat{Q}\}\} \vDash wp\ (\mathtt{e}_1)\ \{\mathtt{w}.\ wp\ (\mathtt{const\ x = w;\ e_2})\ \{\hat{Q}\}\}$$

Now, since $\triangleright\, wp\ (\mathtt{e}_2[\mathtt{w}/\mathtt{x}])\ \{\hat{Q}\} \vDash wp\ (\mathtt{const\ x = w;\ e}_2)\ \{\hat{Q}\}$ for arbitrary $\mathtt{w}$ by WP-LET, applying WP-MONO leaves us with

$$\triangleright\, wp\ (\mathtt{e}_2[\mathtt{w}/\mathtt{x}])\ \{\hat{Q}\} \vDash \triangleright\, wp\ (\mathtt{e}_2)\ \{\hat{Q}\}$$

as a proof obligation. This follows from REFL, as $\mathtt{x}$ does not appear free in $\mathtt{e}_2$ ☐

LEMMA F.74 (WP-BOP).

$$\text{(WP-BOP)}\quad \frac{\mathtt{w} = [\![\oplus]\!](\mathtt{w}_1, \mathtt{w}_2)}{\triangleright\, \hat{Q}(\mathtt{w}) \vDash wp\ (\mathtt{w}_1 \oplus \mathtt{w}_2)\ \{\hat{Q}\}}$$

PROOF. Unfolding $\vDash$, suppose we have ω, ρ such that

- $\checkmark\ \rho^{(\mathrm{H1})}$
- $\triangleright\, \hat{Q}(\mathtt{w})(\omega, \rho)^{(\mathrm{H2})}$

Unfolding $\triangleright$, this tells us that either

- $\omega.\mathsf{step} = 0^{(\mathrm{H3})}$, or
- $\omega.\mathsf{step} > 0 \land \hat{Q}(\mathtt{w})(\blacktriangleright\omega, \rho)^{(\mathrm{H4})}$

Unfolding $wp\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(\mathrm{H5})}$
- $\rho_f \ \sharp\ \rho^{(\mathrm{H6})}$
- $\psi = \omega^+.\mathsf{sizes}^{(\mathrm{H7})}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(\mathrm{H8})}$
- $k < \omega^+.\mathsf{step}^{(\mathrm{H9})}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(\mathrm{H10})}$
- $(\psi, \mu, \mathtt{w}_1 \oplus \mathtt{w}_2) \rightarrow^k (\psi', \mu', \mathtt{e}') \not\rightarrow^{(\mathrm{H11})}$

If we have H3, then for any $\omega^+ \sqsupseteq \omega$, there exist no non-negative $k < \omega^+.\mathsf{step}$, meaning that $wp\ (\mathtt{w}_1 \oplus \mathtt{w}_2)\ \{\hat{Q}\}(\omega, \rho)$ holds vacuously. Otherwise, we may use H4 and must prove the existence of some ρ' such that

- $\rho_f \ \sharp\ \rho'^{(\mathrm{G1})}$
- $\psi' \supseteq \psi^{(\mathrm{G2})}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(\mathrm{G3})}$
- $\mathtt{e}' \in \mathtt{Word}^{(\mathrm{G4})}$
- $\hat{Q}(\mathtt{e}')(\omega', \rho')^{(\mathrm{G5})}$

By inspecting the operational semantics, using the premise, we observe that the evaluation in H11 must proceed as $(\psi, \mu, \mathtt{w}_1 \oplus \mathtt{w}_2) \rightarrow (\psi, \mu, \mathtt{w}) \not\rightarrow^{(\mathrm{H12})}$, where

- $\psi' = \psi$, solving G2
- $\mathtt{e}' = \mathtt{w} \in \mathtt{Word}$, solving G4
- $\mu = \mu'$
- $k = 1$, so $\omega' = \blacktriangleright\omega^+$

We set $\rho' = \rho$; G1 and G3 follow from H6 and H8. It remains to show $\hat{Q}(\mathtt{e}')(\omega', \rho') = \hat{Q}(\mathtt{w})(\blacktriangleright\omega^+, \rho)$, which follows from H4 with with definition of *Prd*. ☐

LEMMA F.75 (WP-FUNPTR).

$$\text{(WP-FUNPTR)}\quad \frac{\mathtt{F} \ni \mathtt{f}\ (\overline{\mathtt{x}})\ \{\mathtt{e}\}}{\triangleright\, \hat{Q}(\langle \mathtt{f} \rangle_{\mathtt{F}}) \vDash wp_{\mathtt{F}}\ (\mathtt{f})\ \{\hat{Q}\}}$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that

- $\checkmark\ \rho^{(H1)}$
- $\triangleright\ \hat{Q}(\langle \mathtt{f} \rangle_{\mathtt{F}})(\omega, \rho)^{(H2)}$

Unfolding $\triangleright$, this tells us that either

- $\omega.\mathsf{step} = 0^{(H3)}$, or
- $\omega.\mathsf{step} > 0 \land \hat{Q}(\langle \mathtt{f} \rangle_{\mathtt{F}})(\blacktriangleright\omega, \rho)^{(H4)}$

Unfolding $wp\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(H5)}$
- $\rho_f \sharp \rho^{(H6)}$
- $\psi = \omega^+.\mathsf{sizes}^{(H7)}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(H8)}$
- $k < \omega^+.\mathsf{step}^{(H9)}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(H10)}$
- $(\psi, \mu, \mathtt{f}) \longrightarrow^k (\psi', \mu', \mathtt{e}') \not\rightarrow^{(H11)}$

If we have H3, then for any $\omega^+ \sqsupseteq \omega$, there exist no non-negative $k < \omega^+.\mathsf{step}$, meaning that $wp_{\mathtt{F}}\ (\mathtt{f})\ \{\hat{Q}\}(\omega, \rho)$ holds vacuously. Otherwise, we may use H4 and must prove the existence of some ρ' such that

- $\rho_f \sharp \rho'^{(G1)}$
- $\psi' \supseteq \psi^{(G2)}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(G3)}$
- $\mathtt{e}' \in \mathtt{Word}^{(G4)}$
- $\hat{Q}(\mathtt{e}')(\omega', \rho')^{(G5)}$

By inspecting the operational semantics, using the premise, we observe that the evaluation in H11 must proceed as $(\psi, \mu, \mathtt{f}) \longrightarrow (\psi, \mu, \langle \mathtt{f} \rangle_{\mathtt{F}}) \not\rightarrow^{(H12)}$, where

- $\psi' = \psi$, solving G2
- $\mathtt{e}' = \langle \mathtt{f} \rangle_{\mathtt{F}} \in \mathtt{Word}$, solving G4
- $\mu = \mu'$
- $k = 1$, so $\omega' = \blacktriangleright\omega^+$

We assert $\rho' = \rho$; G1 and G3 follow from H6 and H8. It remains to show $\hat{Q}(\mathtt{e}')(\omega', \rho') = \hat{Q}(\langle \mathtt{f} \rangle_{\mathtt{F}})(\blacktriangleright\omega^+, \rho)$, which follows from H4 with the definition of *Prd*. □

Lemma F.76 (wp-app).

$$\frac{\mathtt{F} \ni \mathtt{f}\ (\overline{\mathtt{x}})\ \{\mathtt{e}\}}{\triangleright\ wp_{\mathtt{F}}\left(\mathtt{e}[\overline{\mathtt{w}/\mathtt{x}}]\right)\{\hat{Q}\} \vDash wp_{\mathtt{F}}\ (\langle \mathtt{f} \rangle_{\mathtt{F}}\ (\overline{\mathtt{w}}))\ \{\hat{Q}\}}\ (\textsc{wp-app})$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that

- $\checkmark\ \rho^{(H1)}$
- $\triangleright\ wp_{\mathtt{F}}\left(\mathtt{e}[\overline{\mathtt{w}/\mathtt{x}}]\right)\{\hat{Q}\}(\omega, \rho)^{(H2)}$

Unfolding $\triangleright$, this tells us that either

- $\omega.\mathsf{step} = 0^{(H3)}$, or

- $\omega.\mathsf{step} > 0 \wedge \mathit{wp}_{\mathtt{F}}\left(\mathtt{e}[\overline{\mathtt{w}/\mathtt{x}}]\right)\{\hat{Q}\}(\blacktriangleright\omega, \rho)^{(\mathrm{H4})}$

Unfolding $\mathit{wp}\,(-)\,\{-\}$, suppose

- $\omega^{+} \sqsupseteq \omega^{(\mathrm{H5})}$
- $\rho_f \sharp \rho^{(\mathrm{H6})}$
- $\psi = \omega^{+}.\mathsf{sizes}^{(\mathrm{H7})}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(\mathrm{H8})}$
- $k < \omega^{+}.\mathsf{step}^{(\mathrm{H9})}$
- $\omega' = \langle \mathsf{step} : \omega^{+}.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(\mathrm{H10})}$
- $\mathtt{F} \vdash (\psi, \mu, \langle \mathtt{f} \rangle_{\mathtt{F}}\,(\overline{\mathtt{w}})) \longrightarrow^{k} (\psi', \mu', \mathtt{e}') \nrightarrow^{(\mathrm{H11})}$

If we have H3, then for any $\omega^{+} \sqsupseteq \omega$, there exist no non-negative $k < \omega^{+}.\mathsf{step}$, meaning that $\mathit{wp}_{\mathtt{F}}\,(\langle \mathtt{f} \rangle_{\mathtt{F}}\,(\overline{\mathtt{w}}))\,\{\hat{Q}\}(\omega, \rho)$ holds vacuously. Otherwise, we may use H4 and must prove the existence of some ρ' such that

- $\rho_f \sharp \rho'^{(\mathrm{G1})}$
- $\psi' \supseteq \psi^{(\mathrm{G2})}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(\mathrm{G3})}$
- $\mathtt{e}' \in \mathtt{Word}^{(\mathrm{G4})}$
- $\hat{Q}(\mathtt{e}')(\omega', \rho')^{(\mathrm{G5})}$

By inspecting the operational semantics, using $\mathtt{F} \ni \mathtt{f}\,(\overline{\mathtt{x}})\,\{\mathtt{e}\}$ we observe that the evaluation in H11 must proceed as $\mathtt{F} \vdash (\psi, \mu, \langle \mathtt{f} \rangle_{\mathtt{F}}\,(\overline{\mathtt{w}})) \longrightarrow (\psi, \mu, \mathtt{e}[\overline{\mathtt{w}/\mathtt{x}}]) \longrightarrow^{k-1} (\psi', \mu', \mathtt{e}') \nrightarrow^{(\mathrm{H12})}$. This first substitution step must always be taken before reaching an irreducible configuration.

Now, instantiate $\mathit{wp}_{\mathtt{F}}\left(\mathtt{e}[\overline{\mathtt{w}/\mathtt{x}}]\right)\{\hat{Q}\}(\blacktriangleright\omega, \rho)$ from H4 with

- $\blacktriangleright\omega^{+} \sqsupseteq \blacktriangleright\omega$
- $\rho_f \sharp \rho$, from H6
- $\psi = \blacktriangleright\omega^{+}.\mathsf{sizes} = \omega^{+}.\mathsf{sizes}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)$, from H8
- $k - 1 < \blacktriangleright\omega^{+}.\mathsf{step}$
- $\omega' = \langle \mathsf{step} : \blacktriangleright\omega^{+}.\mathsf{step} - (k-1), \mathsf{sizes} : \psi' \rangle = \langle \mathsf{step} : \omega^{+}.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle$

Note that $\blacktriangleright\omega^{+}$ is defined, since $k < \omega^{+}.\mathsf{step}$ must be at least one in order to take the step in H12. Also, $\blacktriangleright\omega^{+} \sqsupseteq \blacktriangleright\omega$ and $k - 1 < \blacktriangleright\omega^{+}.\mathsf{step}$ by unfolding $\blacktriangleright$ in H5 and H9 respectively, so the instantiation is valid. Providing $\mathtt{F} \vdash (\psi, \mu, \mathtt{e}[\overline{\mathtt{w}/\mathtt{x}}]) \longrightarrow^{k-1} (\psi', \mu', \mathtt{e}') \nrightarrow$ from H12 guarantees the existence of some ρ' that meets the conditions from above, solving all remaining goals. □

Lemma F.77 (wp-if-t).

$$\frac{\mathtt{w} \notin \{\mathtt{null}, 0, ☣\}}{\triangleright\, \mathit{wp}\,(\mathtt{e}_1)\,\{\hat{Q}\} \vDash \mathit{wp}\,(\mathtt{if}\ (\mathtt{w})\ \{\mathtt{e}_1\}\ \mathtt{else}\ \{\mathtt{e}_2\})\,\{\hat{Q}\}}\ (\textit{wp-if-t})$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that

- $\checkmark\, \rho^{(\mathrm{H1})}$
- $\triangleright\, \mathit{wp}\,(\mathtt{e}_1)\,\{\hat{Q}\}(\omega, \rho)^{(\mathrm{H2})}$

Unfolding $\triangleright$, this tells us that either

- $\omega.\mathsf{step} = 0^{(\mathrm{H3})}$, or
- $\omega.\mathsf{step} > 0 \wedge \mathit{wp}\,(\mathtt{e}_1)\,\{\hat{Q}\}(\blacktriangleright\omega, \rho)^{(\mathrm{H4})}$

Unfolding $\mathit{wp}\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(\mathrm{H5})}$
- $\rho_f \sharp \rho^{(\mathrm{H6})}$
- $\psi = \omega^+.\mathsf{sizes}^{(\mathrm{H7})}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(\mathrm{H8})}$
- $k < \omega^+.\mathsf{step}^{(\mathrm{H9})}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(\mathrm{H10})}$
- $(\psi, \mu, \mathtt{if}\ (\mathtt{w})\ \{\mathtt{e_1}\}\ \mathtt{else}\ \{\mathtt{e_2}\}) \to^k (\psi', \mu', \mathtt{e}') \not\to^{(\mathrm{H11})}$

If we have H3, then for any $\omega^+ \sqsupseteq \omega$, there exist no non-negative $k < \omega^+.\mathsf{step}$, meaning that $\mathit{wp}\ (\mathtt{if}\ (\mathtt{w})\ \{\mathtt{e_1}\}\ \mathtt{else}\ \{\mathtt{e_2}\})\ \{\hat{Q}\}(\omega, \rho)$ holds vacuously. Otherwise, we may use H4 and must prove the existence of some ρ' such that

- $\rho_f \sharp \rho'^{(\mathrm{G1})}$
- $\psi' \supseteq \psi^{(\mathrm{G2})}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(\mathrm{G3})}$
- $\mathtt{e}' \in \mathtt{Word}^{(\mathrm{G4})}$
- $\hat{Q}(\mathtt{e}')(\omega', \rho')^{(\mathrm{G5})}$

By inspecting the operational semantics, using $\mathtt{w} \notin \{\mathtt{null}, \mathtt{0}, ☣\}$ we observe that the evaluation in H11 must proceed as $(\psi, \mu, \mathtt{if}\ (\mathtt{w})\ \{\mathtt{e_1}\}\ \mathtt{else}\ \{\mathtt{e_2}\}) \to (\psi, \mu, \mathtt{e_1}) \to^{k-1} (\psi', \mu', \mathtt{e}') \not\to^{(\mathrm{H12})}$. This first step must always be taken before reaching an irreducible configuration.

Now, instantiate $\mathit{wp}\ (\mathtt{e_1})\ \{\hat{Q}\}(\blacktriangleright\omega, \rho)$ from H4 with

- $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$
- $\rho_f \sharp \rho$, from H6
- $\psi = \blacktriangleright\omega^+.\mathsf{sizes} = \omega^+.\mathsf{sizes}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)$, from H8
- $k - 1 < \blacktriangleright\omega^+.\mathsf{step}$
- $\omega' = \langle \mathsf{step} : \blacktriangleright\omega^+.\mathsf{step} - (k-1), \mathsf{sizes} : \psi' \rangle = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle$

Note that $\blacktriangleright\omega^+$ is defined, since $k < \omega^+.\mathsf{step}$ must be at least one in order to take the step in H12. Also, $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$ and $k - 1 < \blacktriangleright\omega^+.\mathsf{step}$ by unfolding $\blacktriangleright$ in H5 and H9 respectively, so the instantiation is valid. Providing $(\psi, \mu, \mathtt{e_1}) \to^{k-1} (\psi', \mu', \mathtt{e}') \not\to$ from H12 guarantees the existence of some ρ' that meets the conditions from above, solving all remaining goals. □

Lemma F.78 (wp-if-f).

$$\textit{(wp-if-f)}\quad \frac{\mathtt{w} \in \{\mathtt{null}, \mathtt{0}\}}{\triangleright\ \mathit{wp}\ (\mathtt{e_2})\ \{\hat{Q}\} \vDash \mathit{wp}\ (\mathtt{if}\ (\mathtt{w})\ \{\mathtt{e_1}\}\ \mathtt{else}\ \{\mathtt{e_2}\})\ \{\hat{Q}\}}$$

Proof. Unfolding $\vDash$, suppose we have ω, ρ such that

- $\checkmark\ \rho^{(\mathrm{H1})}$
- $\triangleright\ \mathit{wp}\ (\mathtt{e_2})\ \{\hat{Q}\}(\omega, \rho)^{(\mathrm{H2})}$

Unfolding $\triangleright$, this tells us that either

- $\omega.\mathsf{step} = 0^{(\mathrm{H3})}$, or
- $\omega.\mathsf{step} > 0 \wedge \mathit{wp}\ (\mathtt{e_2})\ \{\hat{Q}\}(\blacktriangleright\omega, \rho)^{(\mathrm{H4})}$

Unfolding $\mathit{wp}\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(\mathrm{H5})}$

- $\rho_f \sharp \rho^{(H6)}$
- $\psi = \omega^+.\mathsf{sizes}^{(H7)}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(H8)}$
- $k < \omega^+.\mathsf{step}^{(H9)}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(H10)}$
- $(\psi, \mu, \texttt{if (w) \{e}_1\texttt{\} else \{e}_2\texttt{\}}) \rightarrow^k (\psi', \mu', \texttt{e}') \not\rightarrow^{(H11)}$

If we have H3, then for any $\omega^+ \sqsupseteq \omega$, there exist no non-negative $k < \omega^+.\mathsf{step}$, meaning that $\mathit{wp}\ (\texttt{if (w) \{e}_1\texttt{\} else \{e}_2\texttt{\}})\ \{\hat{Q}\}(\omega, \rho)$ holds vacuously. Otherwise, we may use H4 and must prove the existence of some ρ' such that

- $\rho_f \sharp \rho'^{(G1)}$
- $\psi' \supseteq \psi^{(G2)}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(G3)}$
- $\texttt{e}' \in \texttt{Word}^{(G4)}$
- $\hat{Q}(\texttt{e}')(\omega', \rho')^{(G5)}$

By inspecting the operational semantics, using $\texttt{w} \in \{\texttt{null}, \texttt{0}\}$ we observe that the evaluation in H11 must proceed as $(\psi, \mu, \texttt{if (w) \{e}_1\texttt{\} else \{e}_2\texttt{\}}) \rightarrow (\psi, \mu, \texttt{e}_2) \rightarrow^{k-1} (\psi', \mu', \texttt{e}') \not\rightarrow^{(H12)}$. This first step must always be taken before reaching an irreducible configuration.

Now, instantiate $\mathit{wp}\ (\texttt{e}_2)\ \{\hat{Q}\}(\blacktriangleright\omega, \rho)$ from H4 with

- $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$
- $\rho_f \sharp \rho$, from H6
- $\psi = \blacktriangleright\omega^+.\mathsf{sizes} = \omega^+.\mathsf{sizes}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)$, from H8
- $k - 1 < \blacktriangleright\omega^+.\mathsf{step}$
- $\omega' = \langle \mathsf{step} : \blacktriangleright\omega^+.\mathsf{step} - (k-1), \mathsf{sizes} : \psi' \rangle = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle$

Note that $\blacktriangleright\omega^+$ is defined, since $k < \omega^+.\mathsf{step}$ must be at least one in order to take the step in H12. Also, $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$ and $k - 1 < \blacktriangleright\omega^+.\mathsf{step}$ by unfolding $\blacktriangleright$ in H5 and H9 respectively, so the instantiation is valid. Providing $(\psi, \mu, \texttt{e}_2) \rightarrow^{k-1} (\psi', \mu', \texttt{e}') \not\rightarrow$ from H12 guarantees the existence of some ρ' that meets the conditions from above, solving all remaining goals. □

Lemma F.79 (wp-malloc).

(wp-malloc)

$$\frac{n > 0}{\triangleright \left(\forall\ \ell \in \mathsf{Loc}_{\mathbb{N}^+}.\ \left(\bigstar_{i<n} (\ell + i) \mapsto ☣\right) \mathrel{-\!\!\star} \mathit{size}\,(\ell,\ n) \mathrel{-\!\!\star} \hat{Q}(\ell)\right) \vDash \mathit{wp}\ (\texttt{malloc (n)})\ \{\hat{Q}\}}$$

Proof. Unfolding $\vDash$ and $\star$, suppose we have ω and ρ such that

- $\checkmark\ \rho^{(H1)}$
- $\triangleright \left(\forall\ \ell \in \mathsf{Loc}_{\mathbb{N}^+}.\ (\bigstar_{i<n} (\ell + i) \mapsto ☣) \mathrel{-\!\!\star} \mathit{size}\,(\ell,\ n) \mathrel{-\!\!\star} \hat{Q}(\ell)\right)(\omega, \rho)^{(H2)}$

Unfolding $\triangleright$, this tells us that either

- $\omega.\mathsf{step} = 0^{(H3)}$, or
- $\omega.\mathsf{step} > 0 \land \left(\forall\ \ell \in \mathsf{Loc}_{\mathbb{N}^+}.\ (\bigstar_{i<n} (\ell + i) \mapsto ☣) \mathrel{-\!\!\star} \mathit{size}\,(\ell,\ n) \mathrel{-\!\!\star} \hat{Q}(\ell)\right)(\blacktriangleright\omega, \rho)^{(H4)}$

Unfolding $\mathit{wp}\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(H5)}$
- $\rho_f \sharp \rho^{(H6)}$

- $\psi = \omega^+.\mathsf{sizes}^{(\mathrm{H7})}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(\mathrm{H8})}$
- $k < \omega^+.\mathsf{step}^{(\mathrm{H9})}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(\mathrm{H10})}$
- $(\psi, \mu, \mathtt{malloc}\,(\mathtt{n})) \to^k (\psi', \mu', \mathtt{e}') \not\to^{(\mathrm{H11})}$

If we have H3, then for any $\omega^+ \sqsupseteq \omega$, there exist no non-negative $k < \omega^+.\mathsf{step}$, meaning that $\mathit{wp}\,(\mathtt{malloc}\,(\mathtt{n}))\,\{\hat{Q}\}(\omega, \rho)$ holds vacuously. Otherwise, we may use H4 and must prove the existence of some ρ' such that

- $\rho_f \,\sharp\, \rho'^{(\mathrm{G1})}$
- $\psi' \supseteq \psi^{(\mathrm{G2})}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(\mathrm{G3})}$
- $\mathtt{e}' \in \mathtt{Word}^{(\mathrm{G4})}$
- $\hat{Q}(\mathtt{e}')(\omega', \rho')^{(\mathrm{G5})}$

Let $b \in \mathbb{N}^+ \setminus \mathrm{dom}(\psi)$. By inspecting the operational semantics, using this and $n > 0$, we observe that the evaluation in H11 must proceed as exactly $(\psi, \mu, \mathtt{malloc}\,(\mathtt{n})) \to (\psi', \mu', \ell) \not\to^{(\mathrm{H12})}$, where

- $\psi' = \psi[b \mapsto n]^{(\mathrm{H13})}$
- $\mu' = \mu[\langle b, i \rangle \mapsto ☣ \mid i < n]^{(\mathrm{H14})}$
- $\ell = \langle b, 0 \rangle^{(\mathrm{H15})}$
- $\ell \in \mathtt{Word}$, solving G4
- $k = 1$, so $\omega' = \langle \mathsf{step} : \blacktriangleright \omega^+.\mathsf{step}, \mathsf{sizes} : \psi' \rangle^{(\mathrm{H16})}$

Since $b \notin \mathrm{dom}(\psi)$, $\psi' \supseteq \psi$, solving G2. Now, instantiate H4 with $\ell \in \mathsf{Loc}_{\mathbb{N}^+}$, since $b \in \mathbb{N}^+ \setminus \mathrm{dom}(\psi)$. Instantiate the $-\!\!\star$ with $\omega' \sqsupseteq \blacktriangleright \omega^+ \sqsupseteq \blacktriangleright \omega$. Observe that

$$\left(\bigstar_{i<n} (\ell + i) \mapsto ☣\right)(\omega', \bullet_{i<n} (\ell + i) \mapsto \mathsf{unq}(☣))$$

holds, by unfolding $\star$ and $\mapsto$. From H15, $\mathit{size}\,(\ell,\ n)(\omega', \varnothing)$ holds; supplying both of these gives us $\hat{Q}(\ell)(\rho \bullet \bullet_{i<n}(\ell + i) \mapsto \mathsf{unq}(☣))$. This composition of resources is defined and valid, since the location ℓ is at a fresh block b, appearing in neither ψ nor μ

We assert $\rho' = \rho \bullet \bullet_{i<n}(\ell + i) \mapsto \mathsf{unq}(☣)$, which solves G5. Note that unfolding $\to$ in H12 tells us $\mathrm{dom}(\mu) \subseteq \mathsf{span}(\psi)$. For any $\ell + i = \langle b, i \rangle$, we know $\ell + i$ is not in $\mathsf{span}(\psi)$, as we selected $b \notin \mathrm{dom}(\psi)$. If $\ell + i$ were in $\mathrm{dom}(\rho)$, then $\ell + i$ would be in $\mathrm{dom}(\mu) = \mathrm{dom}(\mathsf{erase}(\rho \bullet \rho_f))$, which is a contradiction. ρ' is thus well-defined.

Furthermore, from the argument above, $\rho' \bullet \rho_f$ must be defined as well, emphasizing that μ is composed of ρ and ρ_f. Its validity follows immediately from H6, since $\mathsf{objs}(\rho' \bullet \rho_f) = \mathsf{objs}(\rho \bullet \rho_f)$; adding the extra $\bullet_{i<n}(\ell+i) \mapsto \mathsf{unq}(☣)$ does not change the reachable objects. Thus, G1 holds. Finally, applying Unique Erasure Separability n times gives us $\mathsf{erase}(\rho' \bullet \rho_f) = \mathsf{erase}(\rho \bullet \rho_f)[\langle b, i \rangle \mapsto ☣ \mid i < n] = \mu[\langle b, i \rangle \mapsto ☣ \mid i < n]$, solving G3. □

Lemma F.80 (wp-free).

(wp-free)

$$\left(\bigstar_{i<n} (\ell + i) \mapsto \mathtt{w_i}\right) \star \mathit{size}\,(\ell,\ n) \star \triangleright\, \mathit{wp}\,(\mathtt{e})\,\{\hat{Q}\} \vDash \mathit{wp}\,(\mathtt{free}\,(\ell)\,;\ \mathtt{e})\,\{\hat{Q}\}$$

Proof. Unfolding $\vDash$, $\star$, $\mapsto$, and $\mathit{size}\,(-,\ -)$, suppose we have ω, ρ, ℓ, ρ_e, and a collections of n resources ρ_i such that

- $\checkmark\, \rho^{(\mathrm{H1})}$
- $\rho = (\bullet_{i<n}\rho_i) \bullet \rho_e^{(\mathrm{H2})}$

- $\rho_i = (\ell + i) \mapsto \mathsf{unq}(\mathtt{w_i})^{(H3)}$
- $\ell = \langle b, 0\rangle^{(H4)}$
- $\omega.\mathsf{sizes}(b) = n^{(H5)}$
- $\triangleright\ wp\ (\mathtt{e})\ \{\hat{Q}\}(\omega, \rho_e)^{(H6)}$

Unfolding $\triangleright$, this tells us that either

- $\omega.\mathsf{step} = 0^{(H7)}$, or
- $\omega.\mathsf{step} > 0 \land wp\ (\mathtt{e})\ \{\hat{Q}\}(\blacktriangleright\omega, \rho_e)^{(H8)}$

Unfolding $wp\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(H9)}$
- $\rho_f \,\sharp\, \rho^{(H10)}$
- $\psi = \omega^+.\mathsf{sizes}^{(H11)}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(H12)}$
- $k < \omega^+.\mathsf{step}^{(H13)}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi'\rangle^{(H14)}$
- $(\psi, \mu, \mathtt{free}\ (\ell)\ ;\ \mathtt{e}) \longrightarrow^k (\psi', \mu', \mathtt{e}') \not\rightarrow^{(H15)}$

If we have H7, then for any $\omega^+ \sqsupseteq \omega$, there exist no non-negative $k < \omega^+.\mathsf{step}$, meaning that $wp\ (\mathtt{free}\ (\ell)\ ;\ \mathtt{e})\ \{\hat{Q}\}(\omega, \rho)$ holds vacuously. Otherwise, we may use H8 and must prove the existence of some ρ' such that

- $\rho_f \,\sharp\, \rho'^{(G1)}$
- $\psi' \supseteq \psi^{(G2)}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(G3)}$
- $\mathtt{e}' \in \mathtt{Word}^{(G4)}$
- $\hat{Q}(\mathtt{e}')(\omega', \rho')^{(G5)}$

Unfolding $\sqsupseteq$ in H9 and pairing it with H11 and H5 ensures $\psi(b) = n$. Consider $\mathsf{span}(b \mapsto n)$; by definition, this is exactly $[\langle b, i\rangle \mid i < n]$. Now, apply Unique Erasure Separability n times with $\mu = \mathsf{erase}((\bullet_{i<n}\rho_i) \bullet \rho_e \bullet \rho_f)$ to get $\mu = \mathsf{erase}(\rho_e \bullet \rho_f) \uplus [(l + i) \mapsto \mathtt{w_i} \mid i < n]^{(H16)}$. Thus, $\mathsf{span}(b \mapsto n) \subseteq \mathrm{dom}(\mu)$.

By inspecting the operational semantics, using the remarks above, we observe that the evaluation in H15 must proceed as exactly

- $(\psi, \mu, \mathtt{free}\ (\ell)\ ;\ \mathtt{e}) \longrightarrow (\psi, \mu \setminus \mathsf{span}(b \mapsto n), \mathtt{e}) \longrightarrow^{k-1} (\psi', \mu', \mathtt{e}') \not\rightarrow^{(H17)}$

Now, instantiate $wp\ (\mathtt{e})\ \{\hat{Q}\}(\blacktriangleright\omega, \rho_e)$ from H8 with

- $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$
- $\rho_f \,\sharp\, \rho_e$, from H10
- $\psi = \blacktriangleright\omega^+.\mathsf{sizes} = \omega^+.\mathsf{sizes}$
- $\mu \setminus \mathsf{span}(b \mapsto n) = \mathsf{erase}(\rho_e \bullet \rho_f)$, from H16
- $k - 1 < \blacktriangleright\omega^+.\mathsf{step}$
- $\omega' = \langle \mathsf{step} : \blacktriangleright\omega^+.\mathsf{step} - (k-1), \mathsf{sizes} : \psi'\rangle = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi'\rangle$

Note that $\blacktriangleright\omega^+$ is defined, since $k < \omega^+.\mathsf{step}$ must be at least one in order to take the step in H17. Also, $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$ and $k - 1 < \blacktriangleright\omega^+.\mathsf{step}$ by unfolding $\blacktriangleright$ in H9 and H13 respectively, so the instantiation is valid. Providing $(\psi, \mu \setminus \mathsf{span}(b \mapsto n), \mathtt{e}) \longrightarrow^{k-1} (\psi', \mu', \mathtt{e}') \not\rightarrow$ from H17 guarantees the existence of some ρ' that meets the conditions from above, solving all remaining goals. □

Lemma F.81 (wp-load).

$$\frac{P \vDash \Diamond\, \ell \mapsto \mathtt{w}}{P \star \triangleright \left(P \mathrel{-\!\!\star} \hat{Q}(\mathtt{w})\right) \vDash wp\ (*\ell)\ \{\hat{Q}\}}\ (\textsc{wp-load})$$

Proof. Unfolding $\vDash$ and $\star$, suppose we have $\omega, \rho, \rho_1, \rho_2$ such that

- $\checkmark\ \rho^{(H1)}$
- $\rho = \rho_1 \bullet \rho_2{}^{(H2)}$
- $P(\omega, \rho_1)^{(H3)}$
- $\triangleright \left(P \mathrel{-\!\!\star} \hat{Q}(\mathtt{w})\right)(\omega, \rho_2)^{(H4)}$

Applying Valid Extension Antitonicity with ρ to get $\checkmark\ \rho_1$, so we can instantiate the premise $P \vDash \Diamond\, \ell \mapsto \mathtt{w}$ with H3 to get $(\Diamond\, \ell \mapsto \mathtt{w})\ (\omega, \rho_1)$. Unfolding $\Diamond$ and $\mapsto$ gives us $\rho_1 \dashrightarrow \ell \mapsto \mathsf{unq}(\mathtt{w})^{(H5)}$. Unfolding $\triangleright$ in H4, we also have either

- $\omega.\mathsf{step} = 0^{(H6)}$, or
- $\omega.\mathsf{step} > 0 \wedge \left(P \mathrel{-\!\!\star} \hat{Q}(\mathtt{w})\right)(\blacktriangleright\omega, \rho_2)^{(H7)}$

Now, unfolding $wp\ (-)\ \{-\}$ in our goal $wp\ (*\ell)\ \{\hat{Q}\}(\omega, \rho)$, suppose

- $\omega^+ \sqsupseteq \omega^{(H8)}$
- $\rho_f \sharp \rho^{(H9)}$
- $\psi = \omega^+.\mathsf{sizes}^{(H10)}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(H11)}$
- $k < \omega^+.\mathsf{step}^{(H12)}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(H13)}$
- $(\psi, \mu, *\ell) \to^k (\psi', \mu', \mathtt{e}') \not\to^{(H14)}$

If we have H6, then for any $\omega^+ \sqsupseteq \omega$, there exist no non-negative $k < \omega^+.\mathsf{step}$, meaning that $wp\ (*\ell)\ \{\hat{Q}\}(\omega, \rho)$ holds vacuously. Otherwise, we may use H7 and must prove the existence of some ρ' such that

- $\rho_f \sharp \rho'^{(G1)}$
- $\psi' \supseteq \psi^{(G2)}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(G3)}$
- $\mathtt{e}' \in \mathtt{Word}^{(G4)}$
- $\hat{Q}(\mathtt{e}')(\omega', \rho')^{(G5)}$

Now, note that $(\rho \bullet \rho_f) \dashrightarrow \rho \dashrightarrow \rho_1 \dashrightarrow \ell \mapsto \mathsf{unq}(\mathtt{w})$ from H2 and H5. Additionally, $\checkmark\ (\rho \bullet \rho_f)$ by unfolding $\sharp$ in H9. Together with Unique Reachability Erasure, these imply that $\mathsf{erase}(\rho \bullet \rho_f)(\ell) = \mu(\ell) = \mathtt{w}$.

By inspecting the operational semantics, using $\mu(\ell) = \mathtt{w}$ we observe that the evaluation in H14 must proceed as exactly $(\psi, \mu, *\ell) \to (\psi', \mu', \mathtt{w}) \not\to^{(H15)}$, where

- $\psi = \psi'$, solving G2
- $\mathtt{e}' = \mathtt{w} \in \mathtt{Word}$, solving G4
- $\mu = \mu'^{(H16)}$
- $k = 1$, so $\omega' = \blacktriangleright\omega^{+(H17)}$

We assert that $\rho' = \rho$. H9 and H16 therefore solve G1 and G3 respectively. To solve G5, or equivalently to prove $\hat{Q}(\mathtt{w})(\blacktriangleright\omega^+, \rho)$ we instantiate $\left(P \mathrel{-\!\!\star} \hat{Q}(\mathtt{w})\right)(\blacktriangleright\omega, \rho_2)$ from H7 with $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$.

Providing $P(\blacktriangleright\omega^+, \rho_1)$ from H3 using the definition of Prd (as $\blacktriangleright\omega^+ \sqsupseteq \omega$) gives us $\hat{Q}(\mathtt{w})(\blacktriangleright\omega^+, \rho_1 \bullet \rho_2) = \hat{Q}(\mathtt{w})(\blacktriangleright\omega^+, \rho)$, using H1, solving G5, and completing the proof. $\square$

Lemma F.82 (wp-store).

$$\text{(wp-store)} \quad \ell \mapsto - \star \triangleright \left(\ell \mapsto \mathtt{w} \mathrel{-\!\!\star} wp\ (\mathtt{e})\ \{\hat{Q}\}\right) \vDash wp\ (*\ell = \mathtt{w};\ \mathtt{e})\ \{\hat{Q}\}$$

Proof. Unfolding $\vDash$, $\star$, and $\mapsto$, suppose we have $\omega, \rho, \rho_1, \rho_2$ such that

- $\checkmark\ \rho^{(\mathrm{H1})}$
- $\rho = \rho_1 \bullet \rho_2{}^{(\mathrm{H2})}$
- $\rho_1 = \ell \mapsto \mathsf{unq}(-)^{(\mathrm{H3})}$
- $\triangleright \left(\ell \mapsto \mathtt{w} \mathrel{-\!\!\star} wp\ (\mathtt{e})\ \{\hat{Q}\}\right)(\omega, \rho_2)^{(\mathrm{H6})}$

Unfolding $\triangleright$, this tells us that either

- $\omega.\mathsf{step} = 0^{(\mathrm{H5})}$, or
- $\omega.\mathsf{step} > 0 \land \left(\ell \mapsto \mathtt{w} \mathrel{-\!\!\star} wp\ (\mathtt{e})\ \{\hat{Q}\}\right)(\blacktriangleright\omega, \rho_2)^{(\mathrm{H6})}$

Unfolding $wp\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(\mathrm{H7})}$
- $\rho_f \mathrel{\sharp} \rho^{(\mathrm{H8})}$
- $\psi = \omega^+.\mathsf{sizes}^{(\mathrm{H9})}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(\mathrm{H10})}$
- $k < \omega^+.\mathsf{step}^{(\mathrm{H11})}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(\mathrm{H12})}$
- $(\psi, \mu, *\ell = \mathtt{w};\ \mathtt{e}) \to^k (\psi', \mu', \mathtt{e}') \not\to^{(\mathrm{H13})}$

If we have H5, then for any $\omega^+ \sqsupseteq \omega$, there exist no non-negative $k < \omega^+.\mathsf{step}$, meaning that $wp\ (*\ell = \mathtt{w};\ \mathtt{e})\ \{\hat{Q}\}(\omega, \rho)$ holds vacuously. Otherwise, we may use H6 and must prove the existence of some ρ' such that

- $\rho_f \mathrel{\sharp} \rho'^{(\mathrm{G1})}$
- $\psi' \supseteq \psi^{(\mathrm{G2})}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(\mathrm{G3})}$
- $\mathtt{e}' \in \mathtt{Word}^{(\mathrm{G4})}$
- $\hat{Q}(\mathtt{e}')(\omega', \rho')^{(\mathrm{G5})}$

Now, note that $(\rho \bullet \rho_f) \dashrightarrow \rho \dashrightarrow \ell \mapsto \mathsf{unq}(-)$ from H2 and H3. Additionally, $\checkmark\ (\rho \bullet \rho_f)$ by unfolding $\sharp$ in H8. Together with Unique Reachability Erasure, these imply that $\ell \in \mathrm{dom}(\mathsf{erase}(\rho \bullet \rho_f)) = \mathrm{dom}(\mu)$.

By inspecting the operational semantics, using $\ell \in \mathrm{dom}(\mu)$ we observe that the evaluation in H13 must proceed as $(\psi, \mu, *\ell = \mathtt{w};\ \mathtt{e}) \to (\psi, \mu[\ell \mapsto \mathtt{w}], \mathtt{e}) \to^{k-1} (\psi', \mu', \mathtt{e}') \not\to^{(\mathrm{H14})}$. This first step must always be taken before reaching an irreducible configuration.

Note that $\rho_2 \mathrel{\sharp} \rho_1 = \rho_2 \mathrel{\sharp} \ell \mapsto \mathsf{unq}(-)$, since their composition is defined and valid as exactly ρ. Applying Unique Update Compatibility gives us $\rho_2 \mathrel{\sharp} \ell \mapsto \mathsf{unq}(\mathtt{w})$. Let us call this valid composition $\rho_{\mathtt{w}}$; we use it below.

Now, instantiate $\left(\ell \mapsto \mathtt{w} \mathrel{-\!\!\star} wp\ (\mathtt{e})\ \{\hat{Q}\}\right)(\blacktriangleright\omega, \rho_2)$ with $\blacktriangleright\omega$ and $(\ell \mapsto \mathtt{w})(\blacktriangleright\omega, \ell \mapsto \mathsf{unq}(\mathtt{w}))$, which holds by $\mapsto$ definition, to obtain $wp\ (\mathtt{e})\ \{\hat{Q}\}(\blacktriangleright\omega, \rho_{\mathtt{w}})^{(\mathrm{H15})}$.

Before instantiating this, first observe $(\rho_2 \bullet \rho_f) \sharp \ell \mapsto \mathsf{unq}(-)$ by unfolding $\sharp$ in H8. Applying Unique Update Compatibility using this gives us $(\rho_2 \bullet \rho_f) \sharp \ell \mapsto \mathsf{unq}(\mathtt{w})^{(H16)}$ as well. Now, apply Unique Erasure Separability using these facts to obtain

- $\mu = \mathsf{erase}(\rho \bullet \rho_f) = \mathsf{erase}(\rho_1 \bullet (\rho_2 \bullet \rho_f)) = \mathsf{erase}(\rho_2 \bullet \rho_f) \uplus [\ell \mapsto -]^{(H17)}$
- $\mathsf{erase}(\rho_{\mathtt{w}} \bullet \rho_f) = \mathsf{erase}(\ell \mapsto \mathsf{unq}(\mathtt{w}) \bullet (\rho_2 \bullet \rho_f)) = \mathsf{erase}(\rho_2 \bullet \rho_f) \uplus [\ell \mapsto \mathtt{w}]^{(H18)}$

Together, these observations let us deduce that $\mathsf{erase}(\rho_{\mathtt{w}} \bullet \rho_f) = \mu[\ell \mapsto \mathtt{w}]$.

We are finally ready to instantiate H15 with

- $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$
- $\rho_f \sharp \rho_{\mathtt{w}}$, by unfolding $\sharp$ in H16
- $\psi = \blacktriangleright\omega^+.\mathsf{sizes} = \omega^+.\mathsf{sizes}$
- $\mathsf{erase}(\rho_{\mathtt{w}} \bullet \rho_f) = \mu[\ell \mapsto \mathtt{w}]$
- $k - 1 < \blacktriangleright\omega^+.\mathsf{step}$
- $\omega' = \langle \mathsf{step} : \blacktriangleright\omega^+.\mathsf{step} - (k-1), \mathsf{sizes} : \psi' \rangle = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle$

Note that $\blacktriangleright\omega^+$ is defined, since $k < \omega^+.\mathsf{step}$ must be at least one in order to take the step in H14. Also, $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$ and $k - 1 < \blacktriangleright\omega^+.\mathsf{step}$ by unfolding $\blacktriangleright$ in H7 and H11 respectively, so the instantiation is valid. Providing $(\psi, \mu[\ell \mapsto \mathtt{w}], \mathtt{e}) \rightarrow^{k-1} (\psi', \mu', \mathtt{e}') \nrightarrow$ from H14 guarantees the existence of some ρ' that meets the conditions from above, solving all remaining goals. □

Lemma F.83 (wp-incr-own).

$$\text{(WP-INCR-OWN)}\quad \frac{n' = n + 1}{\ell \mapsto \mathtt{n} \star \triangleright \left(\ell \mapsto \mathtt{n}' \mathrel{-\!\!\star} \hat{Q}(\mathtt{n}')\right) \vDash wp\ ({+}{+}\ell)\ \{\hat{Q}\}}$$

Proof. Unfolding $\vDash$, $\star$, and $\mapsto$, suppose we have $\omega, \rho, \rho_1, \rho_2$ such that

- $\checkmark\ \rho^{(H1)}$
- $\rho = \rho_1 \bullet \rho_2^{(H2)}$
- $\rho_1 = \ell \mapsto \mathsf{unq}(\mathtt{n})^{(H3)}$
- $\triangleright \left(\ell \mapsto \mathtt{n}' \mathrel{-\!\!\star} \hat{Q}(\mathtt{n}')\right)(\omega, \rho_2)^{(H4)}$

Unfolding $\triangleright$, this tells us that either

- $\omega.\mathsf{step} = 0^{(H5)}$, or
- $\omega.\mathsf{step} > 0 \wedge \left(\ell \mapsto \mathtt{n}' \mathrel{-\!\!\star} \hat{Q}(\mathtt{n}')\right)(\blacktriangleright\omega, \rho_2)^{(H6)}$

Unfolding $wp\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(H7)}$
- $\rho_f \sharp \rho^{(H8)}$
- $\psi = \omega^+.\mathsf{sizes}^{(H9)}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(H10)}$
- $k < \omega^+.\mathsf{step}^{(H11)}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(H12)}$
- $(\psi, \mu, {+}{+}\ell) \rightarrow^k (\psi', \mu', \mathtt{e}') \nrightarrow^{(H13)}$

If we have H5, then for any $\omega^+ \sqsupseteq \omega$, there exist no non-negative $k < \omega^+.\mathsf{step}$, meaning that $wp\ ({+}{+}\ell)\ \{\hat{Q}\}(\omega, \rho)$ holds vacuously. Otherwise, we may use H4 and must prove the existence of some ρ' such that

- $\rho_f \sharp \rho'^{(G1)}$

- $\psi' \supseteq \psi^{(G2)}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(G3)}$
- $e' \in \mathtt{Word}^{(G4)}$
- $\hat{Q}(e')(\omega', \rho')^{(G5)}$

Now, note that $(\rho \bullet \rho_f) \twoheadrightarrow \rho \twoheadrightarrow \ell \mapsto \mathsf{unq}(n)$ from H2 and H3. Additionally, $\checkmark\, (\rho \bullet \rho_f)$ by unfolding $\sharp$ in H8. Together with Unique Reachability Erasure, these imply that $\mathsf{erase}(\rho \bullet \rho_f)(\ell) = \mu(\ell) = n$.

By inspecting the operational semantics, using $\mu(\ell) = n$ and $n' = n + 1$, we observe that the evaluation in H13 must proceed as exactly $(\psi, \mu, {++}\ell) \longrightarrow (\psi', \mu', n') \not\rightarrow^{(H14)}$, where

- $\psi = \psi'$, solving G2
- $n' \in \mathtt{Word}$, solving G4
- $\mu' = \mu[\ell \mapsto n']^{(H15)}$
- $k = 1$, so $\omega' = \blacktriangleright\omega^{+(H16)}$

We assert that $\rho' = \rho_2 \bullet \ell \mapsto \mathsf{unq}(n')$. Observe that $(\rho_2 \bullet \rho_f) \,\sharp\, \ell \mapsto \mathsf{unq}(n)$ by unfolding $\sharp$ in H8. Applying Unique Update Compatibility using this gives us $(\rho_2 \bullet \rho_f) \,\sharp\, \ell \mapsto \mathsf{unq}(n')$ as well. By $\sharp$ definition, this solves G1.

Now, apply Unique Erasure Separability to the compatibility observations above to obtain

- $\mathsf{erase}(\rho \bullet \rho_f) = \mathsf{erase}(\rho_1 \bullet (\rho_2 \bullet \rho_f)) = \mathsf{erase}(\rho_2 \bullet \rho_f) \uplus [\ell \mapsto n]^{(H17)}$
- $\mathsf{erase}(\rho' \bullet \rho_f) = \mathsf{erase}(\ell \mapsto \mathsf{unq}(n') \bullet (\rho_2 \bullet \rho_f)) = \mathsf{erase}(\rho_2 \bullet \rho_f) \uplus [\ell \mapsto n']^{(H18)}$

Together, these observations let us deduce that $\mu' = \mu[\ell \mapsto n'] = \mathsf{erase}(\rho' \bullet \rho_f)$, solving G3.

To solve G5, or equivalently to prove $\hat{Q}(n')(\blacktriangleright\omega^+, \rho')$ we instantiate $\left(\ell \mapsto n' \mathrel{-\!\!\star} \hat{Q}(n')\right)(\blacktriangleright\omega, \rho_2)$ from H6 with $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$. Providing $(\ell \mapsto n')\,(\blacktriangleright\omega^+, \ell \mapsto \mathsf{unq}(n'))$, which holds by $\mapsto$ definition, gives us $\hat{Q}(n')(\blacktriangleright\omega^+, \rho_2 \bullet \ell \mapsto \mathsf{unq}(n')) = \hat{Q}(n')(\blacktriangleright\omega^+, \rho')$, solving G5 and completing the proof. □

Lemma F.84 (wp-decr-own).

$$\frac{n' = n - 1}{\ell \mapsto n \star \triangleright \left(\ell \mapsto n' \mathrel{-\!\!\star} \hat{Q}(n')\right) \vDash wp\ ({-}{-}\ell)\ \{\hat{Q}\}}\ (\textsc{wp-decr-own})$$

Proof. Unfolding $\vDash$, $\star$, and $\mapsto$, suppose we have $\omega, \rho, \rho_1, \rho_2$ such that

- $\checkmark\, \rho^{(H1)}$
- $\rho = \rho_1 \bullet \rho_2^{(H2)}$
- $\rho_1 = \ell \mapsto \mathsf{unq}(n)^{(H3)}$
- $\triangleright \left(\ell \mapsto n' \mathrel{-\!\!\star} \hat{Q}(n')\right)(\omega, \rho_2)^{(H4)}$

Unfolding $\triangleright$, this tells us that either

- $\omega.\mathsf{step} = 0^{(H5)}$, or
- $\omega.\mathsf{step} > 0 \wedge \left(\ell \mapsto n' \mathrel{-\!\!\star} \hat{Q}(n')\right)(\blacktriangleright\omega, \rho_2)^{(H6)}$

Unfolding $wp\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(H7)}$
- $\rho_f \,\sharp\, \rho^{(H8)}$
- $\psi = \omega^+.\mathsf{sizes}^{(H9)}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(H10)}$

- $k < \omega^+.\mathsf{step}^{(H11)}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(H12)}$
- $(\psi, \mu, {-}{-}\ell) \rightarrow^k (\psi', \mu', \mathtt{e}') \not\rightarrow^{(H13)}$

If we have H5, then for any $\omega^+ \sqsupseteq \omega$, there exist no non-negative $k < \omega^+.\mathsf{step}$, meaning that $wp\ ({-}{-}\ell)\ \{\hat{Q}\}(\omega, \rho)$ holds vacuously. Otherwise, we may use H4 and must prove the existence of some ρ' such that

- $\rho_f \sharp \rho'^{(G1)}$
- $\psi' \supseteq \psi^{(G2)}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(G3)}$
- $\mathtt{e}' \in \mathtt{Word}^{(G4)}$
- $\hat{Q}(\mathtt{e}')(\omega', \rho')^{(G5)}$

Now, note that $(\rho \bullet \rho_f) \twoheadrightarrow \rho \twoheadrightarrow \ell \mapsto \mathsf{unq}(\mathtt{n})$ from H2 and H3. Additionally, $\checkmark (\rho \bullet \rho_f)$ by unfolding $\sharp$ in H8. Together with Unique Reachability Erasure, these imply that $\mathsf{erase}(\rho \bullet \rho_f)(\ell) = \mu(\ell) = \mathtt{n}$.

By inspecting the operational semantics, using $\mu(\ell) = \mathtt{n}$ and $n' = n - 1$, we observe that the evaluation in H13 must proceed as exactly $(\psi, \mu, {-}{-}\ell) \rightarrow (\psi', \mu', \mathtt{n}') \not\rightarrow^{(H14)}$, where

- $\psi = \psi'$, solving G2
- $\mathtt{n}' \in \mathtt{Word}$, solving G4
- $\mu' = \mu[\ell \mapsto n']^{(H15)}$
- $k = 1$, so $\omega' = \blacktriangleright\omega^{+(H16)}$

We assert that $\rho' = \rho_2 \bullet \ell \mapsto \mathsf{unq}(\mathtt{n}')$. Observe that $(\rho_2 \bullet \rho_f) \sharp \ell \mapsto \mathsf{unq}(\mathtt{n})$ by unfolding $\sharp$ in H8. Applying Unique Update Compatibility using this gives us $(\rho_2 \bullet \rho_f) \sharp \ell \mapsto \mathsf{unq}(\mathtt{n}')$ as well. By $\sharp$ definition, this solves G1.

Now, apply Unique Erasure Separability to the compatibility observations above to obtain

- $\mathsf{erase}(\rho \bullet \rho_f) = \mathsf{erase}(\rho_1 \bullet (\rho_2 \bullet \rho_f)) = \mathsf{erase}(\rho_2 \bullet \rho_f) \uplus [\ell \mapsto \mathtt{n}]^{(H17)}$
- $\mathsf{erase}(\rho' \bullet \rho_f) = \mathsf{erase}(\ell \mapsto \mathsf{unq}(\mathtt{n}') \bullet (\rho_2 \bullet \rho_f)) = \mathsf{erase}(\rho_2 \bullet \rho_f) \uplus [\ell \mapsto \mathtt{n}']^{(H18)}$

Together, these observations let us deduce that $\mu' = \mu[\ell \mapsto \mathtt{n}'] = \mathsf{erase}(\rho' \bullet \rho_f)$, solving G3.

To solve G5, or equivalently to prove $\hat{Q}(\mathtt{n}')(\blacktriangleright\omega^+, \rho')$ we instantiate $\left(\ell \mapsto \mathtt{n}' \twoheadrightarrow\!\!\star\ \hat{Q}(\mathtt{n}')\right)(\blacktriangleright\omega, \rho_2)$ from H6 with $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$. Providing $(\ell \mapsto \mathtt{n}')\ (\blacktriangleright\omega^+, \ell \mapsto \mathsf{unq}(\mathtt{n}'))$, which holds by $\mapsto$ definition, gives us $\hat{Q}(\mathtt{n}')(\blacktriangleright\omega^+, \rho_2 \bullet \ell \mapsto \mathsf{unq}(\mathtt{n}')) = \hat{Q}(\mathtt{n}')(\blacktriangleright\omega^+, \rho')$, solving G5 and completing the proof. ◻

Lemma F.85 (wp-incr-share).

$$\frac{P \vDash \Diamond @_\ell\, Q}{P \star \triangleright \left(\forall\ n > 1.\ P \twoheadrightarrow\!\!\star\ @_\ell\, Q \twoheadrightarrow\!\!\star\ \hat{R}(\mathtt{n})\right) \vDash wp\ ({+}{+}\ell)\ \{\hat{R}\}}\ (\textit{wp-incr-share})$$

Proof. Unfolding $\vDash$ and $\star$, suppose we have $\omega, \rho, \rho_1, \rho_2$ such that

- $\checkmark \rho^{(H1)}$
- $\rho = \rho_1 \bullet \rho_2^{(H2)}$
- $P(\omega, \rho_1)^{(H3)}$
- $\triangleright \left(\forall\ n > 1.\ P \twoheadrightarrow\!\!\star\ @_\ell\, Q \twoheadrightarrow\!\!\star\ \hat{R}(\mathtt{n})\right)(\omega, \rho_2)^{(H4)}$

Unfolding $\triangleright$, this tells us that either

- $\omega.\mathsf{step} = 0^{(\mathrm{H5})}$, or
- $\omega.\mathsf{step} > 0 \land \left(\forall\ n > 1.\ P \mathrel{-\!\!\star} @_\ell\, Q \mathrel{-\!\!\star} \hat{R}(\mathtt{n})\right)(\blacktriangleright\omega, \rho_2)^{(\mathrm{H6})}$

Unfolding $wp\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(\mathrm{H7})}$
- $\rho_f \sharp \rho^{(\mathrm{H8})}$
- $\psi = \omega^+.\mathsf{sizes}^{(\mathrm{H9})}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(\mathrm{H10})}$
- $k < \omega^+.\mathsf{step}^{(\mathrm{H11})}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(\mathrm{H12})}$
- $(\psi, \mu, \mathtt{++}\ell) \rightarrow^k (\psi', \mu', \mathtt{e}') \not\rightarrow^{(\mathrm{H13})}$

If we have H5, then for any $\omega^+ \sqsupseteq \omega$, there exist no non-negative $k < \omega^+.\mathsf{step}$, meaning that $wp\ (\mathtt{++}\ell)\ \{\hat{R}\}(\omega, \rho)$ holds vacuously. Otherwise, we may use H6 and must prove the existence of some ρ' such that

- $\rho_f \sharp \rho'^{(\mathrm{G1})}$
- $\psi' \supseteq \psi^{(\mathrm{G2})}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(\mathrm{G3})}$
- $\mathtt{e}' \in \mathtt{Word}^{(\mathrm{G4})}$
- $\hat{R}(\mathtt{e}')(\omega', \rho')^{(\mathrm{G5})}$

Now, instantiate the premise $P \vDash \diamond\, @_\ell\, Q$ with with H3 (noting $\checkmark\ \rho_1$ using Valid Extension Antitonicity with H1) to obtain $\diamond\, @_\ell\, Q(\omega, \rho_1)$. Unfolding $\diamond$ and $@_\ell$, this guarantees the existence of some ρ_q such that $\rho_1 \dashrightarrow \ell \mapsto \mathsf{shr}(1, \rho_q) \land Q(\omega, \rho_q)^{(\mathrm{H14})}$.

Now, we use $\rho \bullet \rho_f \dashrightarrow \rho_1 \dashrightarrow \ell \mapsto \mathsf{shr}(1, \rho_q)$ with Shared Reachability Erasure (since $\rho \bullet \rho_f$ is valid by H8) to obtain $\mathsf{erase}(\rho \bullet \rho_f)(\ell) = \mu(\ell) = \mathtt{n}^{(\mathrm{H15})}$ for some $\mathtt{n} \geq \mathtt{1}$.

Now, let $n' = n + 1$. By inspecting the operational semantics, using $\mu(\ell) = \mathtt{n}$, we observe that the evaluation in H13 must proceed as exactly $(\psi, \mu, \mathtt{++}\ell) \rightarrow (\psi', \mu', \mathtt{n}') \not\rightarrow^{(\mathrm{H16})}$, where

- $\psi = \psi'$, solving G2
- $\mathtt{n}' \in \mathtt{Word}$, solving G4
- $\mu' = \mu[\ell \mapsto n']^{(\mathrm{H17})}$
- $k = 1$, so $\omega' = \blacktriangleright\omega^{+(\mathrm{H18})}$

To solve $\hat{R}(\mathtt{e}')(\omega', \rho') = \hat{R}(\mathtt{n}')(\blacktriangleright\omega^+, \rho')$, we will want to use H6 with H3 and H14. This motivates the assertion that $\rho' = \rho \bullet \ell \mapsto \mathsf{shr}(1, \rho_q)$. Instantiating H6 with $n' > 1$, $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$, $P(\blacktriangleright\omega^+, \rho_1)$, and $Q(\blacktriangleright\omega^+, \rho_q)$ (invoking the monotonicity of Prd as appropriate) gives us $\hat{R}(\mathtt{n}')(\blacktriangleright\omega^+, \rho_1 \bullet \rho_2 \bullet \rho_q)$, solving G5 with the choice of ρ'.

To prove G1, we can unfold and re-fold $\sharp$ to equivalently obtain $\rho \bullet \rho_f \sharp \ell \mapsto \mathsf{shr}(1, \rho_q)$ as a goal. Since $\rho \bullet \rho_f \dashrightarrow \ell \mapsto \mathsf{shr}(1, \rho_q)$ and $\checkmark\ (\rho \bullet \rho_f)$, as noted above, applying Shared Reachability Incrementability solves G1.

Finally, we must show $\mu' = \mu[\ell \mapsto n'] = \mathsf{erase}(\rho' \bullet \rho_f)$. To do so, note that $\mathsf{objs}(\rho' \bullet \rho_f) = \mathsf{objs}(\rho \bullet \rho_f)$, by applying Object Composition with the observation that any object of $\ell \mapsto \mathsf{shr}(1, \rho_q)$ is already included in $\mathsf{objs}(\rho \bullet \rho_f)$, since $\rho \bullet \rho_f \dashrightarrow \ell \mapsto \mathsf{shr}(1, \rho_q)$. Therefore,

$$\begin{aligned}
\mathsf{erase}(\rho' \bullet \rho_f) &= \left[\ell' \mapsto \mathsf{erase}(\chi) \mid \ell' \mapsto \chi \in \rho' \bullet \rho_f \bullet \left(\bigbullet_{(\ell_0,\rho_0) \in \mathsf{objs}(\rho' \bullet \rho_f)} \rho_0\right)\right] \\
&= \left[\ell' \mapsto \mathsf{erase}(\chi) \mid \ell' \mapsto \chi \in \ell \mapsto \mathsf{shr}(1, \rho_q) \bullet \rho \bullet \rho_f \bullet \left(\bigbullet_{(\ell_0,\rho_0) \in \mathsf{objs}(\rho \bullet \rho_f)} \rho_0\right)\right]
\end{aligned}$$

But we know $\rho \bullet \rho_f \bullet \left(\bigodot_{(\ell_0,\rho_0)\in\mathsf{objs}(\rho\bullet\rho_f)}\rho_0\right)$ maps ℓ to $\mathsf{shr}(n,\rho_q)$ from H15 (noting the resource that is shared must be ρ_q for the composition to be defined, which it is by $\checkmark$'s definition), so composing another $\mathsf{shr}(1,\rho_q)$ increments the reference count by one, while changing nothing else. Therefore, $\mathsf{erase}(\rho' \bullet \rho_f) = \mu[\ell \mapsto n'] = \mu'$, completing the proof. $\square$

Lemma F.86 (wp-decr-share).

(wp-decr-share)

$$@_\ell\, P \star \triangleright \left(\forall\, n.\ (\ulcorner n > 0 \urcorner \vee (\ulcorner n = 0 \urcorner \star \ell \mapsto 0 \star P)) \mathrel{-\!\!\star} \hat{Q}(\mathtt{n})\right) \vDash wp\ (-\!-\ell)\ \{\hat{Q}\}$$

Proof. Unfolding $\vDash$ and $\star$, suppose we have $\omega, \rho, \rho_1, \rho_2$ such that

- $\checkmark\, \rho$ (H1)
- $\rho = \rho_1 \bullet \rho_2$ (H2)
- $@_\ell\, P(\omega, \rho_1)$ (H3)
- $\triangleright \left(\forall\, n.\ (\ulcorner n > 0 \urcorner \vee (\ulcorner n = 0 \urcorner \star \ell \mapsto 0 \star P)) \mathrel{-\!\!\star} \hat{Q}(\mathtt{n})\right)(\omega, \rho_2)$ (H4)

Unfolding $\triangleright$, this tells us that either

- $\omega.\mathsf{step} = 0$ (H5), or
- $\omega.\mathsf{step} > 0 \wedge \left(\forall\, n.\ (\ulcorner n > 0 \urcorner \vee (\ulcorner n = 0 \urcorner \star \ell \mapsto 0 \star P)) \mathrel{-\!\!\star} \hat{Q}(\mathtt{n})\right)(\blacktriangleright\omega, \rho_2)$ (H6)

Unfolding $wp\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega$ (H7)
- $\rho_f \sharp \rho$ (H8)
- $\psi = \omega^+.\mathsf{sizes}$ (H9)
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)$ (H10)
- $k < \omega^+.\mathsf{step}$ (H11)
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle$ (H12)
- $(\psi, \mu, -\!-\ell) \to^k (\psi', \mu', \mathtt{e}') \not\to$ (H13)

If we have H5, then for any $\omega^+ \sqsupseteq \omega$, there exist no non-negative $k < \omega^+.\mathsf{step}$, meaning that $wp\ (-\!-\ell)\ \{\hat{Q}\}(\omega, \rho)$ holds vacuously. Otherwise, we may use H6 and must prove the existence of some ρ' such that

- $\rho_f \sharp \rho'$ (G1)
- $\psi' \supseteq \psi$ (G2)
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)$ (G3)
- $\mathtt{e}' \in \mathtt{Word}$ (G4)
- $\hat{Q}(\mathtt{e}')(\omega', \rho')$ (G5)

Now, unfold $@_\ell$ in H3 to obtain $\rho_1 = \ell \mapsto \mathsf{shr}(1, \rho_p) \wedge P(\omega, \rho_p)$ (H14). for some ρ_p. This means we can instantiate Shared Subresource Erasure with $\checkmark\, \rho \bullet \rho_f$ from H8, along with $\rho \bullet \rho_f = \rho_1 \bullet (\rho_2 \bullet \rho_f)$ where $\rho_1(\ell) = \mathsf{shr}(1, \rho_p)$. Noting $\mathsf{erase}(\rho \bullet \rho_f) = \mu$ gives us one of the two following cases:

- $\mu(\ell) = 1$ (H15), with
  - $\ell \notin \mathrm{dom}(\rho_2 \bullet \rho_f)$ (H16) and
  - $\forall\, (\ell_0, \rho_0) \in \mathsf{objs}(\rho \bullet \rho_f).\ \ell \notin \mathrm{dom}(\rho_0)$ (H17)
- $\mu(\ell) > 1$ (H18), with
  - $\ell \in \mathrm{dom}(\rho_2 \bullet \rho_f)$ (H19) or
  - $\exists\, (\ell_0, \rho_0) \in \mathsf{objs}(\rho_2 \bullet \rho_f).\ \ell \in \mathrm{dom}(\rho_0)$ (H20)

In either case, let $n' = \mu(\ell) - 1$. By inspecting the operational semantics, we observe that the evaluation in H13 must proceed as exactly $(\psi, \mu, \texttt{--}\ell) \rightarrow (\psi', \mu', \texttt{n}') \nrightarrow^{(H21)}$, where

- $\psi = \psi'$, solving G2
- $\texttt{n}' \in \texttt{Word}$, solving G4
- $\mu' = \mu[\ell \mapsto n']^{(H22)}$
- $k = 1$, so $\omega' = \blacktriangleright\omega^{+(H23)}$

We now consider each of the two cases above separately, based on the resulting n' value:

Case: $n' > 0$**.** Note that $n' > 0$ exactly when $\mu(\ell) > \texttt{1}$, giving us H19 and H20 to work with. Instantiate H6 with n'. Since $n' > 0$ holds, we can instantiate the resulting $\mathrel{-\!\!\star}$ with $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$ to obtain $\hat{Q}(\texttt{n})(\blacktriangleright\omega^+, \rho_2)$.

We assert $\rho' = \rho_2$. With H23 and the observation above, we solve G5. Since $\rho \sharp \rho_f$ and $\rho = \rho_1 \bullet \rho_2$, we have $\rho_2 \sharp \rho_f$ by unfolding $\sharp$ and appealing to Valid Extension Antitonicity. This solves G1.

To solve G3, we must prove $\mathsf{erase}(\rho_2 \bullet \rho_f) = \mu[\ell \mapsto n']$. Unfolding $\mathsf{erase}(-)$, we have

$$\mathsf{erase}(\rho_2 \bullet \rho_f) = \left[\ell' \mapsto \mathsf{erase}(\chi) \mid \ell' \mapsto \chi \in \rho_2 \bullet \rho_f \bullet \left(\bigodot_{(\ell_0,\rho_0) \in \mathsf{objs}(\rho_2 \bullet \rho_f)} \rho_0\right)\right]$$

If we have H19, then $(\rho_2 \bullet \rho_f)(\ell) = \mathsf{shr}(-, \rho_p)$, since ℓ is in the domain. If ℓ mapped to a cell of any other form, that would contradict $\rho \sharp \rho_f$. Similarly, if we have H20 then we have $\rho_2 \bullet \rho_f \dashrightarrow \rho_0 \dashrightarrow \ell \mapsto \mathsf{shr}(-, \rho_p)$ by unfolding objs. In either case, $\rho_2 \bullet \rho_f \dashrightarrow \rho_p$ and $(\ell, \rho_p) \in \mathsf{objs}(\rho_2 \bullet \rho_f)$.

With this, we deduce $\mathsf{objs}(\rho \bullet \rho_f) = \mathsf{objs}(\rho_2 \bullet \rho_f)$. By Object Composition, we have $\mathsf{objs}(\rho \bullet \rho_f) = \mathsf{objs}(\rho_1) \cup \mathsf{objs}(\rho_2 \bullet \rho_f)$. Since $\rho_1 = \ell \mapsto \mathsf{shr}(1, \rho_p)$, unfolding objs reveals $\mathsf{objs}(\rho_1) = (\ell, \rho_p) \cup \mathsf{objs}(\rho_p)$. But both of these are contained in $\mathsf{objs}(\rho_2 \bullet \rho_f)$ by the argument above.

With this, we can now unfold $\mu = \mathsf{erase}(\rho \bullet \rho_f)$ and compare with the erasure above:

$$\begin{aligned}\mathsf{erase}(\rho \bullet \rho_f) &= \left[\ell' \mapsto \mathsf{erase}(\chi) \mid \ell' \mapsto \chi \in \rho_1 \bullet \rho_2 \bullet \rho_f \bullet \left(\bigodot_{(\ell_0,\rho_0) \in \mathsf{objs}(\rho \bullet \rho_f)} \rho_0\right)\right] \\ &= \left[\ell' \mapsto \mathsf{erase}(\chi) \mid \ell' \mapsto \chi \in \rho_1 \bullet \rho_2 \bullet \rho_f \bullet \left(\bigodot_{(\ell_0,\rho_0) \in \mathsf{objs}(\rho_2 \bullet \rho_f)} \rho_0\right)\right]\end{aligned}$$

This looks exactly like the erasure above. The only difference is that here, there is an extra $\rho_1 = \ell \mapsto \mathsf{shr}(n, \rho_p)$ in the underlying composition. Observe that erasing a shared cell yields its reference count, removing ρ_1 from the composition will decrease the reference count by 1, and the resulting composition will still contain some $\ell \mapsto \mathsf{shr}(n', \rho_p)$. This means that $\mathsf{erase}(\rho_2 \bullet \rho_f)$ is exactly $\mathsf{erase}(\rho \bullet \rho_f) = \mu$, but with $\ell \mapsto n'$ where $n' = n - 1$, completing this case.

Case: $n' = 0$**.** Note that $n' = 0$ exactly when $\mu(\ell) = \texttt{1}$, giving us H16 and H17 to work with. Instantiate H6 with $n' = 0$ to get $\left(\ulcorner 0 > 0 \urcorner \vee (\ulcorner 0 = 0 \urcorner \star \ell \mapsto \texttt{0} \star P) \mathrel{-\!\!\star} \hat{Q}(\texttt{n}')\right)(\blacktriangleright\omega, \rho_2)$. Observe $\ell \mapsto \mathsf{unq}(\texttt{0})$ satisfies $\ell \mapsto \texttt{0}$ in any world, and $P(\blacktriangleright\omega^+, \rho_p)$ holds from H14 and the definition of *Prd*. This means we can instantiate the $\mathrel{-\!\!\star}$ with $\blacktriangleright\omega^+ \sqsupseteq \blacktriangleright\omega$ and supply $\ell \mapsto \mathsf{unq}(\texttt{0}) \bullet \rho_p$ to obtain $\hat{Q}(\texttt{n}')(\blacktriangleright\omega^+, \rho_2 \bullet \ell \mapsto \mathsf{unq}(\texttt{0}) \bullet \rho_p)$.

We assert $\rho' = \rho_2 \bullet \ell \mapsto \mathsf{unq}(\texttt{0}) \bullet \rho_p$. With H23 and the observation above, we solve G5. It remains to prove $\rho' \sharp \rho_f$ and that $\mathsf{erase}(\rho' \bullet \rho_f) = \mu[\ell \mapsto n']$.

Following the argument in the $n' > 0$ case, observe $\mathsf{objs}(\rho \bullet \rho_f) = (\ell, \rho_p) \cup (\rho_2 \bullet \rho_p \bullet \rho_f)$. Since, $\ell \mapsto \mathsf{unq}(\texttt{0})$ has no reachable objects, this is equivalent to stating

- $\mathsf{objs}(\rho \bullet \rho_f) = (\ell, \rho_p) \cup \mathsf{objs}(\rho' \bullet \rho_f)^{(H24)}$

To prove $\rho' \sharp \rho_f$, take arbitrary $(\ell_3, \rho_3), (\ell_4, \rho_4) \in \mathsf{objs}(\rho' \bullet \rho_f)$. We must prove

- $\rho_3 \sharp_{\mathsf{sh}} \rho' \sharp \rho_f{}^{(G6)}$
- $(\ell_3 = \ell_4 \wedge \rho_3 = \rho_4) \vee (\ell_3 \neq \ell_4 \wedge \rho_3 \sharp_{\mathsf{sh}} \rho_4)^{(G7)}$

Since $(\ell_3, \rho_3), (\ell_4, \rho_4) \in \mathsf{objs}(\rho \bullet \rho_f)$ by H24, and $\checkmark\, \rho \bullet \rho_f$ from H8, we can instantiate to instantly solve G7 as well as obtain $\rho_3 \sharp_{\mathsf{sh}} \rho_1 \bullet \rho_2 \bullet \rho_f{}^{(H25)}$.

To prove G6, we can reduce the proof obligation from $\rho_3 \sharp_{\mathsf{sh}} \rho' \sharp \rho_f$ to $\rho_3 \sharp_{\mathsf{sh}} \rho_2 \rho_p \sharp \rho_f$ by using H17, to deduce $\ell \notin \mathrm{dom}(\rho_3)$. Similarly, we can rewrite H25 as $\rho_3 \sharp_{\mathsf{sh}} \rho_2 \bullet \rho_f{}^{(H26)}$ by the same logic.

Unfolding $\sharp_{\mathsf{sh}}$, we must prove $\rho_3(\ell') \sharp \rho_2 \bullet \rho_p \bullet \rho_f(\ell')$ for all ℓ' in both domains. If $\ell' \in \mathrm{dom}(\rho_2 \bullet \rho_f)$, we can instantiate H26 to obtain the needed compatibility. Otherwise, $\ell' \in \mathrm{dom}(\rho_3) \cap \mathrm{dom}(\rho_p)$. Instantiating $\checkmark\, \rho \bullet \rho_f$ with (ℓ_3, ρ_3) and (ℓ, ρ_p), gives us exactly $\rho_3 \sharp_{\mathsf{sh}} \rho_p$ (since $\ell_3 \neq \ell$ by H17), from which the final case follows.

Now, we turn to prove $\mathsf{erase}(\rho' \bullet \rho_f) = \mu[\ell \mapsto n']$. To do so, we will unfold $\mathsf{erase}(-)$ with the goal of meeting in the middle with $\mu = \mathsf{erase}(\rho \bullet \rho_f)$:

$$\begin{aligned}
\mathsf{erase}(\rho' \bullet \rho_f) &= \left[\ell' \mapsto \mathsf{erase}(\chi) \mid \ell' \mapsto \chi \in \rho' \bullet \rho_f \bullet \left(\textstyle\bigodot_{(\ell_0,\rho_0)\in\mathsf{objs}(\rho'\bullet\rho_f)} \rho_0\right)\right] \\
&= \left[\ell' \mapsto \mathsf{erase}(\chi) \mid \ell' \mapsto \chi \in \rho_2 \bullet \ell \mapsto \mathsf{unq}(0) \bullet \rho_p \bullet \rho_f \bullet \left(\textstyle\bigodot_{(\ell_0,\rho_0)\in\mathsf{objs}(\rho'\bullet\rho_f)} \rho_0\right)\right] \\
&= \left[\ell' \mapsto \mathsf{erase}(\chi) \mid \ell' \mapsto \chi \in \rho_2 \bullet \rho_p \bullet \rho_f \bullet \left(\textstyle\bigodot_{(\ell_0,\rho_0)\in\mathsf{objs}(\rho'\bullet\rho_f)} \rho_0\right)\right] \uplus [\ell \mapsto 0]
\end{aligned}$$

We can move the $\ell \mapsto \mathsf{unq}(0)$ out of the composition, since we know the composition is defined from $\rho' \sharp \rho_f$; if anything else with ℓ in its domain were to be composed, the resulting composition would be undefined.

We now consider $\mu = \mathsf{erase}(\rho \bullet \rho_f)$ and manipulate it into a similar form. To do so, we apply H24, along with both H16 and H17 to pull out ℓ:

$$\begin{aligned}
\mathsf{erase}(\rho \bullet \rho_f) &= \left[\ell' \mapsto \mathsf{erase}(\chi) \mid \ell' \mapsto \chi \in \rho \bullet \rho_f \bullet \left(\textstyle\bigodot_{(\ell_0,\rho_0)\in\mathsf{objs}(\rho\bullet\rho_f)} \rho_0\right)\right] \\
&= \left[\ell' \mapsto \mathsf{erase}(\chi) \mid \ell' \mapsto \chi \in \rho_1 \bullet \rho_2 \bullet \rho_f \bullet \left(\textstyle\bigodot_{(\ell_0,\rho_0)\in(\ell,\rho_p)\cup\mathsf{objs}(\rho'\bullet\rho_f)} \rho_0\right)\right] \\
&= \left[\ell' \mapsto \mathsf{erase}(\chi) \mid \ell' \mapsto \chi \in \rho_2 \bullet \rho_p \bullet \rho_f \bullet \left(\textstyle\bigodot_{(\ell_0,\rho_0)\in\mathsf{objs}(\rho'\bullet\rho_f)} \rho_0\right)\right] \uplus [\ell \mapsto 1]
\end{aligned}$$

Therefore, when we take μ and augment it to obtain $\mu[\ell \mapsto 0]$, this changes $\mathsf{erase}(\rho \bullet \rho_f)$ to exactly $\mathsf{erase}(\rho' \bullet \rho_f)$, solving G3 and completing the proof.

□

Lemma F.87 (wp-share).

$$\textit{(wp-share)}\qquad \ell \mapsto 1 \star P \star (@_\ell P \mathrel{-\!\!\star} \mathit{wp}\ (\mathsf{e})\ \{\hat{Q}\}) \vDash \mathit{wp}\ (\mathsf{e})\ \{\hat{Q}\}$$

Proof. Unfolding $\vDash$, $\star$, and $\mapsto$, suppose we have $\omega, \rho, \rho_1, \rho_2, \rho_3$ such that

- $\checkmark\, \rho^{(H1)}$
- $\rho = \rho_1 \bullet \rho_2 \bullet \rho_3{}^{(H2)}$
- $\rho_1 = \ell \mapsto \mathsf{unq}(1)^{(H3)}$
- $P(\omega, \rho_2)^{(H4)}$
- $\left(@_\ell P \mathrel{-\!\!\star} \mathit{wp}\ (\mathsf{e})\ \{\hat{Q}\}\right)(\omega, \rho_3)^{(H5)}$

Unfolding $\mathit{wp}\ (-)\ \{-\}$, suppose

- $\omega^+ \sqsupseteq \omega^{(H6)}$

- $\rho_f \sharp \rho^{(H7)}$
- $\psi = \omega^+.\mathsf{sizes}^{(H8)}$
- $\mu = \mathsf{erase}(\rho \bullet \rho_f)^{(H9)}$
- $k < \omega^+.\mathsf{step}^{(H10)}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle^{(H11)}$
- $(\psi, \mu, \mathsf{e}) \longrightarrow^k (\psi', \mu', \mathsf{e}') \not\rightarrow^{(H12)}$

We must prove the existence of some ρ' such that

- $\rho_f \sharp \rho'^{(G1)}$
- $\psi' \supseteq \psi^{(G2)}$
- $\mu' = \mathsf{erase}(\rho' \bullet \rho_f)^{(G3)}$
- $\mathsf{e}' \in \mathtt{Word}^{(G4)}$
- $\hat{Q}(\mathsf{e}')(\omega', \rho')^{(G5)}$

Now, let $\rho_\ell = \ell \mapsto \mathsf{shr}(1, \rho_2)$. By unfolding $@_\ell$, note that $@_\ell\, P(\omega, \rho_\ell)$ holds using H4. We can use this and $\omega \sqsupseteq \omega$ to instantiate H5, giving us $wp\ (\mathsf{e})\ \{\hat{Q}\}(\omega, \rho_3 \bullet \rho_\ell)$.

Since $\rho_f \bullet \rho_3 \sharp \rho_1 \bullet \rho_2$ by unfolding $\sharp$ in H7, Unique Shared Convertibility gives us $\rho_f \bullet \rho_3 \sharp \rho_\ell$, or equivalently $\rho_f \sharp \rho_3 \bullet \rho_\ell$ by Res Composition Associative. This allows us to instantiate $wp\ (\mathsf{e})\ \{\hat{Q}\}(\omega, \rho_3 \bullet \rho_\ell)$ with

- $\omega^+ \sqsupseteq \omega$
- $\rho_f \sharp \rho_3 \bullet \rho_\ell$
- $\psi = \omega^+.\mathsf{sizes}$
- $\mathsf{erase}(\rho_3 \bullet \rho_\ell \bullet \rho_f)$
- $k < \omega^+.\mathsf{step}$
- $\omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi' \rangle$

It suffices to prove that $\mathsf{erase}(\rho_3 \bullet \rho_\ell \bullet \rho_f) = \mu^{(G6)}$. Once that is proved, providing H12 will guarantee the existence of some ρ' that solves all remaining goals above. To do so, first observe that $\mathsf{objs}(\rho_\ell) = (\ell, \rho_2) \cup \mathsf{objs}(\rho_2)$. Unfolding objs, clearly (ℓ, ρ_2) is in the objects of ρ_ℓ, by applying $\rightarrow\!\!\blacklozenge$-sub. However, any other object that is reachable must go through ρ_2 first, and thus must be an element of $\mathsf{objs}(\rho_2)$. We can use this observation alongside Object Composition to obtain $\mathsf{objs}(\rho_3 \bullet \rho_\ell \bullet \rho_f) = \mathsf{objs}(\rho_2 \bullet \rho_3 \bullet \rho_f) \cup (\ell, \rho_2)^{(H13)}$.

Next, since $\rho_2 \bullet \rho_3 \bullet \rho_f \sharp \rho_1$ by unfolding $\sharp$ in H7, applying Unique Erasure Separability yields

$$
\begin{aligned}
\mu &= \mathsf{erase}(\rho \bullet \rho_f) \\
&= \mathsf{erase}(\rho_2 \bullet \rho_3 \bullet \rho_f \bullet \rho_1) \\
&= \mathsf{erase}(\rho_2 \bullet \rho_3 \bullet \rho_f \bullet \ell \mapsto \mathsf{unq}(1)) \\
&= \mathsf{erase}(\rho_2 \bullet \rho_3 \bullet \rho_f) \uplus [\ell \mapsto 1]
\end{aligned}
$$

Also, by Unique Domain Exclusion, we have that ℓ is not in the domain of $\rho_2 \bullet \rho_3 \bullet \rho_f$, or in that of any of its objects. This, alongside H13 and the characterization of μ above, allow us to deduce that $\mathsf{erase}(\rho_3 \bullet \rho_\ell \bullet \rho_f) = \mu$ through the following series of equalities:

$$\begin{aligned}
&\left[\ell' \mapsto \mathsf{erase}(\chi) \mid \ell' \mapsto \chi \in \rho_3 \bullet \rho_\ell \bullet \rho_f \bullet \left(\bigodot_{(\ell_0,\rho_0)\in\mathsf{objs}(\rho_3\bullet\rho_\ell\bullet\rho_f)} \rho_0\right)\right] \\
=&\left[\ell' \mapsto \mathsf{erase}(\chi) \mid \ell' \mapsto \chi \in \rho_3 \bullet (\ell \mapsto \mathsf{shr}(1,\rho_2)) \bullet \rho_f \bullet \left(\bigodot_{(\ell_0,\rho_0)\in\mathsf{objs}(\rho_2\bullet\rho_3\bullet\rho_f)\cup(\ell,\rho_2)} \rho_0\right)\right] \\
=&\left[\ell' \mapsto \mathsf{erase}(\chi) \mid \ell' \mapsto \chi \in \rho_2 \bullet \rho_3 \bullet \rho_f \bullet \left(\bigodot_{(\ell_0,\rho_0)\in\mathsf{objs}(\rho_2\bullet\rho_3\bullet\rho_f)} \rho_0\right)\right] \uplus [\ell \mapsto \mathsf{erase}(\mathsf{shr}(1,\rho_2))] \\
=&\ \mathsf{erase}(\rho_2 \bullet \rho_3 \bullet \rho_f) \uplus [\ell \mapsto 1] \\
=&\ \mu
\end{aligned}$$

The fact that ℓ is not found in the domain of the rest of the composition allows us to pull out $[\ell \mapsto 1]$ using $\ell \mapsto \mathsf{shr}(1,\rho_2)$. We also pull out ρ_2 from the object composition for clarity before re-folding $\mathsf{erase}(-)$. This proves G6 and completes the proof. □

Lemma F.88 (ht-app).

$$\frac{}{P \star \{P\}\ \mathsf{e}\ \{\hat{Q}\} \vDash wp\ (\mathsf{e})\ \{\hat{Q}\}}\ \text{(HT-APP)}$$

Proof. Unfolding $\{-\}\ -\ \{-\}$, we must prove $P \star\ !\left(P \twoheadrightarrow\!\!\star\ wp\ (\mathsf{e})\ \{\hat{Q}\}\right) \vDash wp\ (\mathsf{e})\ \{\hat{Q}\}$. By !-L and $\star$-mono, it suffices to prove $P \star \left(P \mathrel{-\!\!\star} wp\ (\mathsf{e})\ \{\hat{Q}\}\right) \vDash wp\ (\mathsf{e})\ \{\hat{Q}\}$, which follows from $-\!\!\star$-L. □

Lemma F.89 (wp-adequacy). *If* $emp \vDash wp_{\mathsf{F}}\ (\mathsf{e})\ \{\mathtt{w}.\ \ulcorner \mathtt{w} \in \mathbb{Z} \urcorner\}$, *then* $\mathsf{ok}_{\mathsf{F}}(\mathsf{e})$.

Proof. Unfolding emp, $\vDash$, and ok (since $\checkmark\ \varnothing$), suppose we have k, ψ', μ', and e' such that

- $\forall\, \omega.\ wp_{\mathsf{F}}\ (\mathsf{e})\ \{\mathtt{w}.\ \ulcorner \mathtt{w} \in \mathbb{Z}\urcorner\}(\omega, \varnothing)^{(\mathrm{H1})}$
- $\mathsf{F} \vdash (\varnothing, \varnothing, \mathsf{e}) \longrightarrow^k (\psi', \mu', \mathsf{e}') \not\rightarrow^{(\mathrm{H2})}$

It remains to prove that $\mathsf{e}' \in \mathbb{Z}^{(\mathrm{G1})}$ and $\mu' = \varnothing^{(\mathrm{G2})}$.

Let $\hat{\omega} = \langle \mathsf{step} : k+1, \mathsf{sizes} : \varnothing\rangle$ and instantiate H1 with $\hat{\omega}$. Unfolding $wp\ (-)\ \{-\}$ tells us

$$\begin{aligned}
&\forall\, \omega^+ \sqsupseteq \hat{\omega}, \rho_f \mathrel{\sharp} \varnothing, k < \omega^+.\mathsf{step}, \psi', \mu', \mathsf{e}', \psi = \omega^+.\mathsf{sizes}, \omega' = \langle \mathsf{step} : \omega^+.\mathsf{step} - k, \mathsf{sizes} : \psi'\rangle\,. \\
&\quad \mathsf{F} \vdash (\psi, \mathsf{erase}(\varnothing \bullet \rho_f), \mathsf{e}) \longrightarrow^k (\psi', \mu', \mathsf{e}') \not\rightarrow \\
&\quad \Rightarrow \quad \exists\, \rho' \mathrel{\sharp} \rho_f.\psi' \supseteq \psi \land \mathsf{erase}(\rho' \bullet \rho_f) = \mu' \land \mathsf{e}' \in \mathtt{Word} \land \ulcorner \mathsf{e}' \in \mathbb{Z}\urcorner(\omega', \rho')
\end{aligned}$$

Instantiate this with $\hat{\omega} \sqsupseteq \hat{\omega}$, $\varnothing \mathrel{\sharp} \varnothing$, ψ', ρ', and e'. Supplying H2 tells us that there exists some ρ' where (among irrelevant things)

- $\mathsf{erase}(\rho' \bullet \varnothing) = \mu'^{(\mathrm{H3})}$
- $\ulcorner \mathsf{e}' \in \mathbb{Z}\urcorner(\omega', \rho')^{(\mathrm{H4})}$

By the definition of $\ulcorner - \urcorner$, G1 holds. Furthermore, $\rho' = \varnothing$ necessarily, so $\mathsf{erase}(\rho' \bullet \varnothing) = \varnothing = \mu'$, solving G2. □

F.3 Properties of the ABI

Lemma F.90 (lr-val).

$$\mathcal{V}[\![\mathsf{T}]\!](\mathtt{w}) \vDash \mathcal{E}[\![\mathsf{T}]\!](\mathtt{w})$$

Proof. By the definition of $\mathcal{E}[\![\mathsf{T}]\!]$, wp-val, and refl. □

Lemma F.91 (lr-bind).

$$\mathcal{E}[\![\mathsf{T}_1]\!](\mathsf{e}) \star \forall\, \mathtt{w}.\ \mathcal{V}[\![\mathsf{T}_1]\!](\mathtt{w}) \mathrel{-\!\!\star} \mathcal{E}[\![\mathsf{T}_2]\!](\mathsf{K}[\mathtt{w}]) \vDash \mathcal{E}[\![\mathsf{T}_2]\!](\mathsf{K}[\mathsf{e}])$$

Proof. By the definition of $\mathcal{E}[\![\mathsf{T}]\!]$ and WP-BIND, it suffices if

$$wp\ (\mathsf{e})\ \{\mathcal{V}[\![\mathsf{T}_1]\!]\} \star \forall\ \mathtt{w}.\ \mathcal{V}[\![\mathsf{T}_1]\!](\mathtt{w}) \mathrel{-\!\!\star} \mathcal{E}[\![\mathsf{T}_2]\!](\mathsf{K}[\mathtt{w}]) \vDash wp\ (\mathsf{e})\ \{\mathtt{w}.\ \mathcal{E}[\![\mathsf{T}_2]\!](\mathsf{K}[\mathtt{w}])\}$$

which follows by WP-RAMIFY. □

Lemma F.92 (LR-adequacy). *If* $emp \vDash \mathcal{E}[\![\mathbb{Z}]\!]^{\varsigma}_{\mathsf{F}}(\mathsf{e})$, *then* $\mathsf{ok}_{\mathsf{F}}(\mathsf{e})$.

Proof. By unfolding $\mathcal{E}[\![-]\!]$, $\mathcal{V}[\![-]\!]$, then $\mathcal{U}[\![-]\!]$ and applying WP-ADEQUACY. □

Definition F.93 (Canonical Semantic Signature). Let Σ be a fully rigid signature. Its *canonical semantic signature* is defined

$$(\!|\Sigma|\!)_{\mathsf{F}} \triangleq \left[\mathsf{X} \mapsto \left\langle \mathsf{kind} : \mathsf{k}, \mathsf{sel} : \left[\mathsf{s}_i \mapsto \left\langle \mathsf{off} : i, \mathsf{semty} : \triangleright\, \mathcal{V}[\![\mathsf{T}_i]\!]^{(\!|\Sigma|\!)}_{\mathsf{F}} \right\rangle \mid i < n\right]\right\rangle \mid \Sigma \ni \mathsf{rigid}\ \mathsf{k}\ \mathsf{X}\ \{\overline{\mathsf{s}_i : \mathsf{T}_i}^{i<n}\}\right]$$

Note the recursive use of $(\!|\Sigma|\!)$ is justified by the use of $\triangleright$. Because $\mathcal{V}[\![-]\!]$ is defined only in terms of operations that are non-expansive and contractive with respect to the step-index, recursive uses of $(\!|\Sigma|\!)$ inside of $\mathcal{V}[\![-]\!]$ are suitably guarded.

Lemma F.94 (Signature Substitution Unrestricted). $\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma)$ *is unrestricted:*

$$\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma) \vDash\ !\,\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma)$$

Proof. Immediate from the definition of $\mathcal{S}[\![-]\!]$ using !-IDEM. □

Lemma F.95 (C-weak).

$$\mathrm{dom}(\gamma') \supseteq \mathrm{dom}(\gamma) \Rightarrow C[\![\Gamma]\!](\gamma) \vDash C[\![\Gamma]\!](\gamma')$$

Proof. Suppose we have $\mathrm{dom}(\gamma') \supseteq \mathrm{dom}(\gamma)$. Unfolding $C[\![-]\!]$ and applying $\star$-MONO, it suffices to prove $\ulcorner \mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\Gamma)\urcorner \vDash \ulcorner \mathrm{dom}(\gamma') \supseteq \mathrm{dom}(\Gamma)\urcorner$. This follows by observing $\mathrm{dom}(\gamma') \supseteq \mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\Gamma)$. □

Lemma F.96 (C-split).

$$\mathcal{S}[\![\Sigma]\!](\varsigma) \star C[\![\Gamma_1, \Gamma_2]\!](\gamma) \dashv\vDash \mathcal{S}[\![\Sigma]\!](\varsigma) \star C[\![\Gamma_1]\!](\gamma) \star \mathcal{S}[\![\Sigma]\!](\varsigma) \star C[\![\Gamma_2]\!](\gamma)$$

Proof. By Signature Substitution Unrestricted, !-UNR and $\star$-MONO, $\mathcal{S}[\![\Sigma]\!](\varsigma)$ is handled. Unfolding $C[\![-]\!]$ and $\ulcorner - \urcorner$, it remains to prove both

- $\mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\Gamma_1, \Gamma_2) \Leftrightarrow \mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\Gamma_1) \wedge \mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\Gamma_2)^{(\mathrm{G1})}$
- $\bigstar_{\mathsf{x}:\mathsf{T}\in\Gamma_1,\Gamma_2} \mathcal{V}[\![\mathsf{T}]\!](\gamma(\mathsf{x})) \dashv\vDash \bigstar_{\mathsf{x}:\mathsf{T}\in\Gamma_1} \mathcal{V}[\![\mathsf{T}]\!](\gamma(\mathsf{x})) \star \bigstar_{\mathsf{x}:\mathsf{T}\in\Gamma_2} \mathcal{V}[\![\mathsf{T}]\!](\gamma(\mathsf{x}))^{(\mathrm{G2})}$

Note that each Γ is a multi-set (as evident from SRC-STAT-DUP), which does not change how Γ_1, Γ_2 is split into Γ_1 and Γ_2. G1 follows from $\mathrm{dom}(\Gamma_1, \Gamma_2) = \mathrm{dom}(\Gamma_1) \cup \mathrm{dom}(\Gamma_2)$ and properties of $\supseteq$. G2 follows from unfolding $\bigstar$, as each occurrence of any $\Gamma_1, \Gamma_2 \ni \mathsf{x} : \mathsf{T}$ appears in exactly one of Γ_1 or Γ_2 by the definition of Γ_1, Γ_2. □

Lemma F.97 (C-cons).

- *If* $\Gamma \ni \mathsf{x} : \mathsf{T}$, *then*

$$\mathcal{S}[\![\Sigma]\!](\varsigma) \star C[\![\Gamma]\!](\gamma) \vDash \mathcal{V}[\![\mathsf{T}]\!](\gamma(\mathtt{x})) \mathrel{-\!\!\star} (\mathcal{S}[\![\Sigma]\!](\varsigma) \star C[\![\Gamma, \mathsf{x} : \mathsf{T}]\!](\gamma))$$

- *If* $\mathsf{x} \notin \mathrm{dom}(\Gamma)$, *then*

$$\mathcal{S}[\![\Sigma]\!](\varsigma) \star C[\![\Gamma]\!](\gamma) \vDash \forall\ \mathtt{w}.\ \mathcal{V}[\![\mathsf{T}]\!](\mathtt{w}) \mathrel{-\!\!\star} (\mathcal{S}[\![\Sigma]\!](\varsigma) \star C[\![\Gamma, \mathsf{x} : \mathsf{T}]\!](\gamma[\mathtt{w}/\mathtt{x}]))$$

Proof. We prove each case separately, in similar ways. Note that if $\mathsf{x} \notin \mathrm{dom}(\Gamma)$, we can pick an arbitrary $\mathtt{w}$ for the new substitution to map $\mathtt{x}$ to.

Case: $\Gamma \ni x : T$ By applying $-\!\!\star$-R, cancelling $\mathcal{S}[\![\Sigma]\!](\varsigma)$, and unfolding $\mathcal{C}[\![-]\!]$, it suffices if

$$\frac{\ulcorner \mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\Gamma)\urcorner \quad \overline{\mathcal{V}[\![T_i]\!](\gamma(x_i))}^{x_i:T_i\in\Gamma} \quad \mathcal{V}[\![T]\!](\gamma(x))}{\ulcorner \mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\Gamma, x : T)\urcorner \quad \overline{\mathcal{V}[\![T_j]\!](\gamma(x_j))}^{x_j:T_j\in\Gamma, x:T}}$$

Since $\mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\Gamma)$, it follows that $\mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\Gamma, x : T)$ as $\Gamma \ni x : T$ already. Unfolding $\bigstar$ thus completes the proof.

Case: $x \notin \mathrm{dom}(\Gamma)$ Applying $\forall$ -R, take an arbitrary w, then apply $-\!\!\star$-R, cancel $\mathcal{S}[\![\Sigma]\!](\varsigma)$, and unfold $\mathcal{C}[\![-]\!]$. It therefore suffices if

$$\frac{\ulcorner \mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\Gamma)\urcorner \quad \overline{\mathcal{V}[\![T_i]\!](\gamma(x_i))}^{x_i:T_i\in\Gamma} \quad \mathcal{V}[\![T]\!](w)}{\ulcorner \mathrm{dom}(\gamma[w/x]) \supseteq \mathrm{dom}(\Gamma, x : T)\urcorner \quad \overline{\mathcal{V}[\![T_j]\!](\gamma[w/x](x_j))}^{x_j:T_j\in\Gamma, x:T}}$$

Since $\mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\Gamma)$, it follows that $\mathrm{dom}(\gamma[w/x]) \supseteq \mathrm{dom}(\Gamma, x : T)$, as we add x to the domain of γ. Now, consider $\mathcal{V}[\![T_j]\!](\gamma[w/x](x_j))$. If $x_j : T_j$ is exactly $x : T$, which occurs once, then $\gamma[w/x](x_j) = \gamma[w/x](x) = w$ by the definition of substitution, even if $x \in \mathrm{dom}(\gamma)$. Otherwise, $x_j \neq x$ and $\gamma[w/x](x_j) = \gamma(x_j)$. With these observations, unfolding $\bigstar$ completes the proof, since the remaining $x_j : T_j \in \Gamma$ are exactly the $x_i : T_i \in \Gamma$.

□

Lemma F.98 ($\mathcal{C}$-uncons). *If* $\Gamma \ni x : T$, *then*

$$\mathcal{S}[\![\Sigma]\!](\varsigma) \star \mathcal{C}[\![\Gamma]\!](\gamma) \vDash \mathcal{V}[\![T]\!](\gamma(x)) \star (\mathcal{V}[\![T]\!](\gamma(x)) -\!\!\star (\mathcal{S}[\![\Sigma]\!](\varsigma) \star \mathcal{C}[\![\Gamma]\!](\gamma)))$$

Proof. Unfolding $\mathcal{C}[\![-]\!]$, we must prove

$$\frac{\mathcal{S}[\![\Sigma]\!](\varsigma) \quad \ulcorner \mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\Gamma)\urcorner \quad \overline{\mathcal{V}[\![T']\!](\gamma(x'))}^{x':T'\in\Gamma}}{\mathcal{V}[\![T]\!](\gamma(x)) \quad (\mathcal{V}[\![T]\!](\gamma(x)) -\!\!\star (\mathcal{S}[\![\Sigma]\!](\varsigma) \star \mathcal{C}[\![\Gamma]\!](\gamma)))}$$

Since $\Gamma \ni x : T$, we can apply $\star$-mono, cancelling $\mathcal{V}[\![T]\!](\gamma(x))$, followed by $-\!\!\star$-R to add it back. It therefore suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!](\varsigma) \quad \ulcorner \mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\Gamma)\urcorner \quad \overline{\mathcal{V}[\![T']\!](\gamma(x'))}^{x':T'\in\Gamma}}{\mathcal{S}[\![\Sigma]\!](\varsigma) \quad \mathcal{C}[\![\Gamma]\!](\gamma)}$$

which follows by cancelling $\mathcal{S}[\![\Sigma]\!](\varsigma)$ and refolding $\mathcal{C}[\![-]\!]$. □

F.4 Compiler Compliance

Theorem F.99 (Compiler Compliance).

$$\Sigma; \Gamma \vdash e : T \rightsquigarrow e \dashv F \Rightarrow \Sigma; \Gamma \vDash_F e : T$$

Proof. By induction on the compilation derivation, in each case appealing to the appropriate compatibility lemma in Compatibility Lemmas. □

Lemma F.100 (Cross-Compiler Linking). *For any two compliant compilers* $\rightsquigarrow_1$ *and* $\rightsquigarrow_2$, *if* $\Sigma; \Gamma_1 \vdash e_1 : T_1 \rightsquigarrow_1 e_1 \dashv F_1$ *and* $\Sigma; \Gamma_2, x : T_1 \vdash e_2 : T_2 \rightsquigarrow_2 e_2 \dashv F_2$ *(with* $x \notin \Gamma_2$*), then* $\Sigma; \Gamma_1, \Gamma_2 \vDash_{F_1,F_2}$ $\texttt{const}\ x = e_1;\ e_2 : T_2$.

Proof. Follows immediately from Safe Linking with the definition of compliant compilation.

□

Lemma F.101 (Safe Linking). *If* $\Sigma; \Gamma_1 \vDash_{F_1} e_1 : T_1$ *and* $\Sigma; \Gamma_2, x : T_1 \vDash_{F_2} e_2 : T_2$ *(with* $x \notin \Gamma_2$*), then* $\Sigma; \Gamma_1, \Gamma_2 \vDash_{F_1,F_2} \texttt{const}\ x = e_1;\ e_2 : T_2$.

Proof. Let $F = F_1, F_2$ and observe that $\Sigma; \Gamma_1 \vDash_{F_1} e_1 : T_1$ implies $\Sigma; \Gamma_1 \vDash_F e_1 : T_1$. This follows by unfolding $\vDash_{F_1}$ with the observation that $F \supseteq F_1$. Similarly, $\Sigma; \Gamma_2, x : T_1 \vDash_{F_2} e_2 : T_2$ implies $\Sigma; \Gamma_2, x : T_1 \vDash_F e_2 : T_2$. The result then follows from comp-let-compat. □

Theorem F.102 (Compiler Adequacy). *If* $\Sigma; \varnothing \vdash e : \mathbb{Z} \rightsquigarrow e \dashv F$ *and* $\Sigma \dashv F$*, then* $\mathsf{ok}_F(e)$.

Proof. In addition to $\Sigma \dashv F^{(H1)}$, applying Compiler Compliance gives us $\Sigma; \varnothing \vDash_F e : \mathbb{Z}^{(H2)}$. Unfolding $\vDash_F$, this is

$$\forall F' \supseteq F, \varsigma, \gamma.\ \mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \star \mathcal{C}[\![\varnothing]\!]^{\varsigma}_{F'}(\gamma) \vDash \mathcal{E}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(e[\gamma])$$

Since the context is $\varnothing$ and e's free variables are exactly those in the context (which is easily confirmed by induction on the compilation relation), e must be closed and thus $e[\gamma] = e$. Unfolding $\mathcal{C}[\![-]\!]$ reveals that $\mathcal{C}[\![\varnothing]\!]^{\varsigma}_{F'}(\gamma) \dashv\vDash \ulcorner \top \urcorner$. Thus, we can simplify as

$$\forall F' \supseteq F, \varsigma.\ \mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \vDash \mathcal{E}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(e)^{(H3)}$$

By Canonical Signature Satisfiable with H1, we have $emp \vDash \mathcal{S}[\![\Sigma]\!]_F(\!|\Sigma|\!)$. Instantiating H3 with $F \supseteq F$ and $(\!|\Sigma|\!)$, using trans as well, we have

$$emp \vDash \mathcal{E}[\![\mathbb{Z}]\!]^{(\!|\Sigma|\!)}_{F}(e)$$

$\mathsf{ok}_F(e)$ now follows from lr-adequacy. □

Lemma F.103 (Canonical Signature Satisfiable).

$$\Sigma \dashv F \Rightarrow F \subseteq F' \Rightarrow emp \vDash \mathcal{S}[\![\Sigma]\!]_{F'}(\!|\Sigma|\!)$$

Proof. Assume the premises $\Sigma \dashv F^{(H1)}$ and $F \subseteq F'^{(H2)}$. Applying $\triangleright$-ind, it suffices if

$$emp \wedge \triangleright \mathcal{S}[\![\Sigma]\!]_{F'}(\!|\Sigma|\!)_{F'} \vDash \mathcal{S}[\![\Sigma]\!]_{F'}(\!|\Sigma|\!)_{F'}$$

Inverting H1 with comp-Σ, we have that every definition in Σ is rigid$^{(H3)}$. Then $(\!|-|\!)$ is defined and ensures $\mathrm{dom}(\!|\Sigma|\!)_{F'} = \mathrm{dom}(\Sigma)^{(H4)}$. We now use $!$-emp and $!$-$\wedge_1$ to transform the proof obligation into

$$!\ (emp \wedge \triangleright \mathcal{S}[\![\Sigma]\!]_{F'}(\!|\Sigma|\!)_{F'}) \vDash \mathcal{S}[\![\Sigma]\!]_{F'}(\!|\Sigma|\!)_{F'}$$

Unfolding $\mathcal{S}$ and applying $!$-mono, we must show for arbitrary $m\ k\ X\ \{\overline{s_i : T_i}^{i<n}\} \in \Sigma$ that

$$\frac{emp \wedge \triangleright \mathcal{S}[\![\Sigma]\!]_{F'}(\!|\Sigma|\!)_{F'}}{\begin{array}{c} \ulcorner \mathrm{dom}((\!|\Sigma|\!)_{F'}) \supseteq \mathrm{dom}(\Sigma) \urcorner^{(G1)} \quad \ulcorner \delta.\mathsf{kind} = k \urcorner^{(G2)} \quad \ulcorner \mathrm{dom}(\delta.\mathsf{sel}) \supseteq \{s_i \mid i < n\} \urcorner^{(G3)} \\ \forall\, i < n.\ !\ wp_F\left(\left\langle \mathtt{sel}^{s_i}_X \right\rangle_{F'}\ ()\right) \{\mathtt{w}.\ \ulcorner \mathtt{w} = \delta.\mathsf{sel}(s_i).\mathsf{off} \urcorner\}^{(G4)} \\ \forall\, i < n, \mathtt{w}.\ \delta.\mathsf{sel}(s_i).\mathsf{semty}(\mathtt{w}) \equiv \triangleright \mathcal{V}[\![T_i]\!]^{(\!|\Sigma|\!)_{F'}}_{F}(\mathtt{w})^{(G5)} \\ \forall\, \ell.\ \{\ell \mapsto 0 \star \delta.\mathsf{obj}(\ell+1)\}\ \langle \mathtt{destr}_X \rangle_F\ (\ell)\ \{emp\}_{F'}{}^{(G6)} \\ \ulcorner m = \mathsf{rigid} \Rightarrow \mathrm{dom}(\delta.\mathsf{sel}) \subseteq \{s_i \mid i < n\} \wedge \forall i < n.\ \delta.\mathsf{sel}(s_i).\mathsf{off} = i \urcorner^{(G7)} \end{array}}$$

where

$$\delta = (\!|\Sigma|\!)_{F'}(X) = \left\langle \mathsf{kind} : k, \mathsf{sel} : \left[s_i \mapsto \left\langle \mathsf{off} : i, \mathsf{semty} : \triangleright \mathcal{V}[\![T_i]\!]^{(\!|\Sigma|\!)_{F'}}_{F'} \right\rangle \right] \right\rangle^{(H5)}$$

G1 holds by H4. G2 and G3 hold by H5. G7 holds by H3 and H5. G5 follows from H5 with $\equiv$-refl. Now, rewriting with Signature Substitution Unrestricted (implicitly using $\wedge$-mono and $\triangleright$-mono), we can apply $\triangleright$-$!$ to transform the premise into $!\triangleright\ (\mathcal{S}[\![\Sigma]\!]_{F'}(\!|\Sigma|\!)_{F'})$. Then by $!$-unr, it suffices to use this information in order to prove the following two goals:

- For G4, it suffices by $\forall$ -R and ! -MONO if for all $i < n$
$$\triangleright\, \mathcal{S}[\![\Sigma]\!]_{\mathsf{F}'}(\varsigma) \vDash wp_{\mathsf{F}} \left(\langle \mathtt{sel}^{\mathsf{s}_i}_{\mathsf{X}} \rangle_{\mathsf{F}'}\ ()\right) \{\mathtt{w}.\ \ulcorner \mathtt{w} = \delta.\mathsf{sel}(\mathsf{s}_i).\mathsf{off} \urcorner\}$$
Inverting H1 with COMP-Σ, we have $\mathsf{F} \ni \mathtt{sel}^{\mathsf{s}_i}_{\mathsf{X}}\ ()\ \{\underline{\mathtt{sel}}^{\ \mathsf{s}_i}_{\Sigma.\mathsf{X}}\}^{(\mathrm{H6})}$. Then by WP-APP with H6 and $\triangleright$ -MONO, it suffices if
$$\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}'}(\varsigma) \vDash wp_{\mathsf{F}} \left(\underline{\mathtt{sel}}^{\ \mathsf{s}_i}_{\Sigma.\mathsf{X}}\right) \{\mathtt{w}.\ \ulcorner \mathtt{w} = \delta.\mathsf{sel}(\mathsf{s}_i).\mathsf{off} \urcorner\}$$
which follows from SEL and H5.
- For G6, by $\forall$ -R, unfolding $\{-\}\ -\ \{-\}$, ! -MONO, and $-\!\!\star$-R, it suffices if for all ℓ,
$$\frac{\triangleright\, \mathcal{S}[\![\Sigma]\!]_{\mathsf{F}'}(\varsigma) \quad \ell \mapsto 0 \quad \delta.\mathsf{obj}(\ell+1)}{wp_{\mathsf{F}'}\ (\langle \mathtt{destr}_{\mathsf{X}} \rangle_{\mathsf{F}}\ (\ell))\ \{emp\}}$$
Inverting H1 with COMP-Σ, we have $\mathsf{F} \ni \mathtt{destr}_{\mathsf{X}}\ (\mathtt{r})\ \{\underline{\mathtt{destr}}^{\ \Sigma}_{\ \mathsf{X}}\ (\mathtt{r})\}^{(\mathrm{H7})}$. Then by WP-APP with H7, $\triangleright$ -R, and $\triangleright$ -MONO, it suffices if
$$\frac{\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}'}(\varsigma) \quad \ell \mapsto 0 \quad \delta.\mathsf{obj}(\ell+1)}{wp_{\mathsf{F}'}\ \left(\underline{\mathtt{destr}}^{\ \Sigma}_{\ \mathsf{X}}\ (\ell)\right)\ \{emp\}}$$
which follows from DROP then DESTROY with H5 and $\mathcal{O}[\![-]\!]$.

$\square$

LEMMA F.104 (SIGNATURE SATISFIABLE). *For any* Σ, *there exists a* F, ς *such that* $emp \vDash \mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma)$.

PROOF. Take Σ' to be the same as Σ but with every flex definition marked rigid. Then take F to satisfy $\Sigma' \dashv \mathsf{F}$ (which must exist, by COMP-Σ). Then apply CANONICAL SIGNATURE SATISFIABLE and use SIGNATURE PRESERVATION for each $\mathsf{X} \in \Sigma'$. $\square$

LEMMA F.105 (DUP).
$$\frac{P \vDash \Diamond\, \mathcal{V}[\![\mathsf{T}]\!](\mathtt{w})}{P \star \left(\forall\ n.\ P -\!\!\star \mathcal{V}[\![\mathsf{T}]\!](\mathtt{w}) -\!\!\star \hat{Q}(\mathtt{n})\right) \vDash wp\ \left(\underline{\mathtt{dup}}_{\ \mathsf{T}}\ (\mathtt{w})\right)\ \{\hat{Q}\}}$$

PROOF. By cases on T.

Case: $\mathsf{T} = \mathbb{Z}$. Unfolding $\mathcal{V}[\![-]\!]$, $\mathcal{U}[\![-]\!]$, and $\underline{\mathtt{dup}}_{\ \mathsf{T}}\ (-)$, it suffices if
$$\frac{P \quad \forall\ n.\ P -\!\!\star \ulcorner \mathtt{w} \in \mathbb{Z} \urcorner -\!\!\star \hat{Q}(\mathtt{n})}{wp\ (-1)\ \{\hat{Q}\}}$$
given the premise
$$P \vDash \Diamond\, \ulcorner \mathtt{w} \in \mathbb{Z} \urcorner^{(\mathrm{H1})}$$
By WP-VAL, $\forall$ -L, and $-\!\!\star$-L, it suffices if
$$P \vDash P \star \ulcorner \mathtt{w} \in \mathbb{Z} \urcorner$$
which follows from H1 with ! -$\ulcorner - \urcorner$, $\Diamond$ -!, and ! -UNR.

Case: $\mathsf{T} \neq \mathbb{Z}$ Unfolding $\mathcal{V}[\![-]\!]$, $\mathcal{R}[\![-]\!]$, and $\underline{\mathtt{dup}}_{\ \mathsf{T}}\ (-)$, it suffices if
$$\frac{P \quad \forall\ n.\ P -\!\!\star (\ulcorner \mathtt{w} \in \mathsf{Loc} \setminus \mathtt{null} \urcorner \star @_{\mathtt{w}}\, \mathcal{O}[\![\mathsf{T}]\!](\mathtt{w}+1)) -\!\!\star \hat{Q}(\mathtt{n})}{wp\ (\texttt{++w})\ \{\hat{Q}\}}$$
given
$$P \vDash \Diamond\ (\ulcorner \mathtt{w} \in \mathsf{Loc} \setminus \mathtt{null} \urcorner \star @_{\mathtt{w}}\, \mathcal{O}[\![\mathsf{T}]\!](\mathtt{w}+1))^{(\mathrm{H2})}$$

Applying $\diamond$-DROP and $\diamond$-! with H2, followed by $\ulcorner - \urcorner$-L, we learn $\mathtt{w} \in \mathsf{Loc} \setminus \mathtt{null}^{(H3)}$, so we rewrite for clarity

$$\frac{P \quad \forall\, n.\, P \twoheadrightarrow (\ulcorner \ell \in \mathsf{Loc} \setminus \mathtt{null} \urcorner \star @_\ell\, \mathcal{O}[\![\mathtt{T}]\!](\ell+1)) \twoheadrightarrow \hat{Q}(\mathtt{n})}{wp\ (\mathtt{++}\ell)\ \{\hat{Q}\}}$$

Applying WP-INCR-SHARE with H2 and $\diamond$-DROP, and then $\triangleright$-R, it suffices if

$$\frac{\forall\, n.\, P \twoheadrightarrow (\ulcorner \ell \in \mathsf{Loc} \setminus \mathtt{null} \urcorner \star @_\ell\, \mathcal{O}[\![\mathtt{T}]\!](\ell+1)) \twoheadrightarrow \hat{Q}(\mathtt{n})}{\forall\, n > 1.\, P \twoheadrightarrow @_\ell\, \mathcal{O}[\![\mathtt{T}]\!](\ell+1) \twoheadrightarrow \hat{Q}(\mathtt{n})}$$

which is straightforward with H3.

□

Lemma F.106 (drop).

$$\mathcal{S}[\![\Sigma]\!]_{\mathtt{F}}(\varsigma) \vDash \forall\, \mathtt{w},\ \mathtt{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathtt{T}]\!]^{\varsigma}_{\mathtt{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathtt{T}}(\mathtt{w})\ \{emp\}_{\mathtt{F}}$$

Proof. Applying $\triangleright$-IND, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{\mathtt{F}}(\varsigma) \wedge \triangleright \forall\, \mathtt{w},\ \mathtt{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathtt{T}]\!]^{\varsigma}_{\mathtt{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathtt{T}}(\mathtt{w})\ \{emp\}}{\forall\, \mathtt{w},\ \mathtt{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathtt{T}]\!]^{\varsigma}_{\mathtt{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathtt{T}}(\mathtt{w})\ \{emp\}_{\mathtt{F}}}$$

If $\Sigma = \varnothing$, then the goal is solved vacuously. Otherwise, we introduce arbitrary $\mathtt{w}$ and $\mathtt{T}$ at the meta-level with $\forall$-R and proceed by case analysis on $\mathtt{T} \dashv \Sigma^{(H1)}$.

Case: $\mathtt{T} = \mathbb{Z}$. After using Signature Substitution Unrestricted, $!$-$\wedge_1$, and $!$-IDEM, then unfolding $\{-\}\ -\ \{-\}$, we can apply $!$-MONO and $\twoheadrightarrow$-R. It therefore suffices if

$$\frac{!\left(\mathcal{S}[\![\Sigma]\!]_{\mathtt{F}}(\varsigma) \wedge \triangleright \forall\, \mathtt{w},\ \mathtt{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathtt{T}]\!]^{\varsigma}_{\mathtt{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathtt{T}}(\mathtt{w})\ \{emp\}\right) \quad \mathcal{V}[\![\mathbb{Z}]\!]^{\varsigma}_{\mathtt{F}}(\mathtt{w})}{wp_{\mathtt{F}}\left(\underline{\mathtt{drop}}^{\Sigma}_{\mathtt{T}}(\mathtt{w})\right)\{emp\}}$$

Unfolding the definitions of $\underline{\mathtt{drop}}_{\mathbb{Z}}(-)$, $\mathcal{V}[\![\mathbb{Z}]\!]$, and $\mathcal{U}[\![-]\!]$, we must prove

$$\frac{!\left(\mathcal{S}[\![\Sigma]\!]_{\mathtt{F}}(\varsigma) \wedge \triangleright \forall\, \mathtt{w},\ \mathtt{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathtt{T}]\!]^{\varsigma}_{\mathtt{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathtt{T}}(\mathtt{w})\ \{emp\}\right) \quad \ulcorner \mathtt{w} \in \mathbb{Z} \urcorner}{wp_{\mathtt{F}}\ (-1)\ \{emp\}}$$

which follows from WP-VAL, $!$-$\ulcorner - \urcorner$, and $!$-DROP.

Case: $\mathtt{T} \neq \mathbb{Z}$. Like above, we rewrite with Signature Substitution Unrestricted and $!$-$\wedge_1$, then unfold $\{-\}\ -\ \{-\}$. Applying $!$-MONO and $\twoheadrightarrow$-R, then unfolding $\underline{\mathtt{drop}}^{\Sigma}_{\mathtt{T}}(-)$, $\mathcal{V}[\![-]\!]$, and $\mathcal{R}[\![-]\!]$, it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{\mathtt{F}}(\varsigma) \wedge \triangleright \forall\, \mathtt{w},\ \mathtt{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathtt{T}]\!]^{\varsigma}_{\mathtt{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathtt{T}}(\mathtt{w})\ \{emp\} \\ \ulcorner \mathtt{w} \in \mathsf{Loc} \setminus \mathtt{null} \urcorner \quad @_{\mathtt{w}}\, \mathcal{O}[\![\mathtt{T}]\!]^{\varsigma}_{\mathtt{F}}(\mathtt{w}+1)\end{array}}{wp_{\mathtt{F}}\left(\mathtt{const\ y = --w;\ if\ (y)\ \{y\}\ else\ }\left\{\underline{\mathtt{destr}}^{\Sigma}_{\mathtt{T}}(\mathtt{w})\right\}\right)\{emp\}}$$

With $\ulcorner - \urcorner$-L, rename $\mathtt{w}$ to ℓ for clarity. Manipulating with $\triangleright$-R, $\triangleright$-$\wedge$, and $\triangleright$-$\star$, it suffices if

$$\frac{\triangleright\left(\mathcal{S}[\![\Sigma]\!]_{\mathtt{F}}(\varsigma) \wedge \forall\, \mathtt{w},\ \mathtt{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathtt{T}]\!]^{\varsigma}_{\mathtt{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathtt{T}}(\mathtt{w})\ \{emp\}\right) \quad @_\ell\, \mathcal{O}[\![\mathtt{T}]\!]^{\varsigma}_{\mathtt{F}}(\ell+1)}{wp_{\mathtt{F}}\left(\mathtt{const\ y = --w;\ if\ (y)\ \{y\}\ else\ }\left\{\underline{\mathtt{destr}}^{\Sigma}_{\mathtt{T}}(\mathtt{w})\right\}\right)\{emp\}}$$

We first use WP-BIND and WP-DECR-SHARE, cancelling $@_\ell\, \mathcal{O}[\![\mathtt{T}]\!]^{\varsigma}_{\mathtt{F}}(\ell+1)$ and applying $\triangleright$-MONO. Then, after applying WP-LET and $\triangleright$-R, it suffices to consider two cases:

- We must show
$$\frac{\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma) \wedge \forall\ \mathtt{w},\ \mathsf{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T}}\ (\mathtt{w})\ \{emp\} \quad \ulcorner n > 0 \urcorner}{wp_{\mathsf{F}}\ (\mathtt{if}\ (\mathtt{n})\ \{\mathtt{n}\}\ \mathtt{else}\ \{\underline{\mathtt{destr}}^{\Sigma}_{\mathsf{T}}\ (\ell)\})\ \{emp\}}$$
which is straightforward from WP-IF-T and $\triangleright$ -R, using SIGNATURE SUBSTITUTION UNRESTRICTED, ! -$\wedge_1$, ! -$\ulcorner - \urcorner$, and ! -DROP.
- We must show
$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma) \wedge \forall\ \mathtt{w},\ \mathsf{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T}}\ (\mathtt{w})\ \{emp\} \\ \mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma) \quad \ulcorner n = 0 \urcorner \quad \ell \mapsto 0 \quad \mathcal{O}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\ell+1)\end{array}}{wp_{\mathsf{F}}\ (\mathtt{if}\ (\mathtt{n})\ \{\mathtt{n}\}\ \mathtt{else}\ \{\underline{\mathtt{destr}}^{\Sigma}_{\mathsf{T}}\ (\ell)\})\ \{emp\}}$$
which follows by first applying WP-IF-F and $\triangleright$ -R, then DESTROY (with H1) after using SIGNATURE SUBSTITUTION UNRESTRICTED, ! -$\wedge_1$, ! -$\wedge$ /$\star$, and ! -L.

$\square$

LEMMA F.107 (DESTROY). *If* $\Sigma \vdash \mathsf{T}$, *then*
$$\frac{\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma) \quad \forall\ \mathtt{w},\ \mathsf{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T}}\ (\mathtt{w})\ \{emp\}_{\mathsf{F}}^{(H1)} \quad \ell \mapsto 0 \quad \mathcal{O}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\ell+1)}{wp_{\mathsf{F}}\ (\underline{\mathtt{destr}}^{\Sigma}_{\mathsf{T}}\ (\ell))\ \{emp\}}$$

PROOF. Assume $\Sigma \vdash \mathsf{T}^{(H2)}$ and proceed by cases on T.

Case: $\mathbb{Z}$**.** Trivial because $\mathcal{O}[\![\mathbb{Z}]\!](\ell) = \bot$.

Case: $\overline{\mathsf{T}_i}^i \to \mathsf{T}$**.** By $\mathcal{O}\left[\!\!\left[\overline{\mathsf{T}_i}^i \to \mathsf{T}\right]\!\!\right]$ and $\underline{\mathtt{destr}}_{\overline{\mathsf{T}_i}^i \to \mathsf{T}}\ (-)$, with ! -DROP, it suffices if
$$\ell \mapsto 0 \star Self \star \{\ell \mapsto 0 \star Self\}\ \langle \mathtt{destr}\rangle_{\mathsf{F}}\ (\ell)\ \{emp\}_{\mathsf{F}} \vDash wp_{\mathsf{F}}\ ({*}(\ell+2)\ (\ell))\ \{emp\}$$
where
$$Self = \ell + 1 \mapsto \langle \mathtt{call}\rangle_{\mathsf{F}} \star \ell + 2 \mapsto \langle \mathtt{destr}\rangle_{\mathsf{F}} \star Env$$
for some $\mathtt{call}$, $\mathtt{destr}$, and Env. This follows from WP-BOP, WP-LOAD, $\diamond$ -R, and HT-APP interspersed with WP-BIND and $\triangleright$ -R.

Case: X**.** By $\mathcal{O}[\![\mathsf{X}]\!]$, it suffices if
$$\frac{\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma) \quad \forall\ \mathtt{w},\ \mathsf{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T}}\ (\mathtt{w})\ \{emp\}_{\mathsf{F}} \quad \ell \mapsto 0 \quad \varsigma(\mathsf{X}).\mathsf{obj}(\ell+1)}{wp_{\mathsf{F}}\ (\underline{\mathtt{destr}}^{\Sigma}_{\mathsf{T}}\ (\ell))\ \{emp\}}$$
Note that by H2 and unfolding $\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma)$, there is some $\delta = \varsigma(\mathsf{X})^{(H3)}$. By H2, proceed by cases on the mode of X.

Case: $\Sigma \ni \mathsf{flex\ k\ X}\ \{-\}$**.** By $\underline{\mathtt{destr}}_{\mathsf{X}}\ (-)$ with ! -DROP, it suffices if
$$\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma) \star \ell \mapsto 0 \star \delta.\mathsf{obj}(\ell+1) \vDash wp_{\mathsf{F}}\ (\mathtt{destr}_{\mathsf{X}}\ (\ell))\ \{emp\}$$
which follows directly the definition of $\mathcal{S}[\![-]\!]$, ! -DROP, and HT-APP.

Case: $\Sigma \ni \mathsf{rigid\ k\ X}\ \{-\}$**.** By H3, $\mathcal{S}[\![-]\!]$, ! -$\star$, ! -DROP, and $\ulcorner - \urcorner$-L we have $\delta.\mathsf{kind} = \mathsf{k}^{(H4)}$, along with $n = |\mathsf{dom}(\delta.\mathsf{sel})|^{(H5)}$, $\forall\, i < n.\ \delta.\mathsf{sel}(\mathsf{s}_i).\mathsf{off} = i^{(H6)}$, and
$$\frac{\begin{array}{c}!\,\forall\ i < n, \mathtt{w}.\ \delta.\mathsf{sel}(\mathsf{s}_i).\mathsf{semty}(\mathtt{w}) \equiv \triangleright\, \mathcal{V}[\![\mathsf{T}_i]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}) \\ \forall\ \mathtt{w},\ \mathsf{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T}}\ (\mathtt{w})\ \{emp\}_{\mathsf{F}} \quad \ell \mapsto 0 \quad \varsigma(\mathsf{X}).\mathsf{obj}(\ell+1)\end{array}}{wp_{\mathsf{F}}\ (\underline{\mathtt{destr}}^{\Sigma}_{\mathsf{T}}\ (\ell))\ \{emp\}}$$
Now proceed by cases on the kind of X.

Case: $\mathsf{k} = \mathsf{struct}$ First, rewrite with H3, δ.obj using H4, H5, and $\underline{\mathtt{destr}}^{\Sigma}_{\mathsf{T}}(-)$. If $n = 0$, the proof is straightforward from $!$-DROP, WP-FREE, $\triangleright$-R, and WP-VAL. Otherwise, by simplifying with H6 and $\equiv$-L (using $!$-UNR $\max(0, n-1)$ times), it suffices if

$$\frac{\ell \mapsto 0 \quad size(\ell,\ 1 + |n|) \quad \overline{\ell + 1 + i \mapsto \mathtt{w}_{s_i}}^{i<n} \quad \overline{\triangleright\, \mathcal{V}[\![\mathsf{T}_i]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}_{s_i})}^{i<n} \quad \forall\ \mathtt{w},\ \mathsf{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T}}(\mathtt{w})\ \{emp\}_{\mathsf{F}}\ \text{(H1)}}{wp_{\mathsf{F}}\left(\overline{\mathtt{const}\ \mathtt{x_i} = \ell[\mathtt{i}+1];\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T_i}}(\mathtt{x_i});}^{i<n}\ \mathtt{free}(\ell);\ 0\right)\{emp\}}$$

for some $\overline{\mathtt{w}_{s_i}}$. By n applications of WP-BOP, WP-LOAD with $\diamond$-R, WP-LET, and the premise H1 (noting that it is unrestricted as both domains are inhabited) with H2 via WP-RAMIFY, all interspersed with WP-BIND, $\triangleright$-R, and $\triangleright$-MONO (to strip the $\triangleright$ s off the $\mathcal{V}[\![-]\!]$s), it suffices if

$$\frac{\ell \mapsto 0 \quad size(\ell,\ 1 + |n|) \quad \overline{\ell + 1 + i \mapsto \mathtt{w}_{s_i}}^{i<n}}{wp_{\mathsf{F}}\ (\mathtt{free}(\ell);\ 0)\ \{emp\}}$$

which follows from WP-FREE, $\triangleright$-R, and WP-VAL.

Case: $\mathsf{k} = \mathsf{enum}$ First, rewrite with H3, δ.obj using H4, H5, and $\underline{\mathtt{destr}}^{\Sigma}_{\mathsf{T}}(-)$. By simplifying with H6 and $\equiv$-L, it suffices if

$$\frac{\forall\ \mathtt{w},\ \mathsf{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T}}(\mathtt{w})\ \{emp\}_{\mathsf{F}} \qquad \ell \mapsto 0 \quad size(\ell,\ 3) \quad \ell + 1 \mapsto \mathtt{j} \quad \ell + 2 \mapsto \mathtt{w}_{s_j} \quad \triangleright\, \mathcal{V}[\![\mathsf{T}_j]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}_{s_j})}{wp_{\mathsf{F}}\left(\begin{array}{l}\overline{\mathtt{if}\ (\ell[1] = \mathtt{i})\ \{\mathtt{const}\ \mathtt{x_i} = \ell[2];\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T_i}}(\mathtt{x_i});\ \mathtt{free}(\ell);\ 0\}}^{i<n} \\ \mathtt{else}\ \{\mathtt{havoc}\}\end{array}\right)\{emp\}}$$

for some $\mathtt{j}$ and $\mathtt{w}_{s_j}$. Unfolding $-[-]$, by WP-BOP and WP-LOAD with $\diamond$-R, followed by WP-BIND, $\triangleright$-R, and $\triangleright$-MONO (to strip the $\triangleright$ off the $\mathcal{V}[\![-]\!]$), it suffices if

$$\frac{\forall\ \mathtt{w},\ \mathsf{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T}}(\mathtt{w})\ \{emp\}_{\mathsf{F}} \qquad \ell \mapsto 0 \quad size(\ell,\ 3) \quad \ell + 1 \mapsto \mathtt{j} \quad \ell + 2 \mapsto \mathtt{w}_{s_j} \quad \mathcal{V}[\![\mathsf{T}_j]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}_{s_j})}{wp_{\mathsf{F}}\left(\begin{array}{l}\overline{\mathtt{if}\ (\mathtt{j} = \mathtt{i})\ \{\mathtt{const}\ \mathtt{x_i} = \ell[2];\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T_i}}(\mathtt{x_i});\ \mathtt{free}(\ell);\ 0\}}^{i<n} \\ \mathtt{else}\ \{\mathtt{havoc}\}\end{array}\right)\{emp\}}$$

By $\max(j-1, 0)$ applications of WP-BOP and WP-IF-F interspersed with WP-BIND and $\triangleright$-R, it suffices if

$$\frac{\forall\ \mathtt{w},\ \mathsf{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T}}(\mathtt{w})\ \{emp\}_{\mathsf{F}}\ \text{(H1)} \qquad \ell \mapsto 0 \quad size(\ell,\ 3) \quad \ell + 1 \mapsto \mathtt{j} \quad \ell + 2 \mapsto \mathtt{w}_{s_j} \quad \mathcal{V}[\![\mathsf{T}_j]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}_{s_j})}{wp_{\mathsf{F}}\left(\begin{array}{l}\mathtt{if}\ (\mathtt{j} = \mathtt{j})\ \{\mathtt{const}\ \mathtt{x_i} = \ell[2];\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T_i}}(\mathtt{x_i});\ \mathtt{free}(\ell);\ 0\} \\ \overline{\mathtt{else\ if}\ (\mathtt{j} = \mathtt{i})\ \{\mathtt{const}\ \mathtt{x_i} = \ell[2];\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T_i}}(\mathtt{x_i});\ \mathtt{free}(\ell);\ 0\}}^{j<i<n} \\ \mathtt{else}\ \{\mathtt{havoc}\}\end{array}\right)\{emp\}}$$

By WP-BOP, WP-IF-T, then WP-LOAD with $\diamond$-R, all interspersed with WP-BIND and $\triangleright$-R, it suffices if

$$\dfrac{\forall\ \mathtt{w},\ \mathsf{T} \dashv \Sigma.\ \{\mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T}}\,(\mathtt{w})\ \{emp\}_{\mathsf{F}}^{(\mathrm{H1})} \quad \ell \mapsto 0 \quad size\,(\ell,\ 3) \quad \ell+1 \mapsto \mathtt{j} \quad \ell+2 \mapsto \mathtt{w}_{\mathtt{s_j}} \quad \mathcal{V}[\![\mathsf{T}_{\mathsf{j}}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}_{\mathtt{s_j}})}{wp_{\mathsf{F}}\left(\underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T_i}}\left(\mathtt{w}_{\mathtt{s_j}}\right);\ \mathtt{free}\,(\ell)\,;\ 0\right)\{emp\}}$$

By WP-SEQ and the premise H1 with H2 via HT-APP and WP-RAMIFY, using both WP-BIND and $\triangleright$ -R, it suffices if

$$\dfrac{\ell \mapsto 0 \quad size\,(\ell,\ 3) \quad \ell+1 \mapsto \mathtt{j} \quad \ell+2 \mapsto \mathtt{w}_{\mathtt{s_j}}}{wp_{\mathsf{F}}\,(\mathtt{free}\,(\ell)\,;\ 0)\,\{emp\}}$$

which follows from WP-FREE, $\triangleright$ -R, and WP-VAL.

□

Lemma F.108 (sel). *If* $\Sigma \ni \mathsf{m}\ \mathsf{k}\ \mathsf{X}\ \{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\}$, *then for all* $j < n$

$$\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma) \star \forall\ n.\ \ulcorner n = \varsigma(\mathsf{X}).\mathsf{sel}(\mathsf{s_j}).\mathsf{off}\urcorner \mathrel{-\!\!\star} \hat{Q}(\mathtt{n}) \vDash wp_{\mathsf{F}}\left(\underline{\mathtt{sel}}^{\mathsf{s_j}}_{\Sigma.\mathsf{X}}\right)\{\hat{Q}\}$$

Proof. Assume the premises $\Sigma \ni \mathsf{m}\ \mathsf{k}\ \mathsf{X}\ \{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\}^{(\mathrm{H1})}$ and $j < n^{(\mathrm{H2})}$. By cases on m.

Case: $\mathsf{m} = \mathsf{rigid}$. Unfolding $\underline{\mathtt{sel}}^{\mathsf{s_i}}_{\Sigma.\mathsf{X}}$, it suffices if

$$\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma) \star \forall\ n.\ \ulcorner n = \varsigma(\mathsf{X}).\mathsf{sel}(\mathsf{s_j}).\mathsf{off}\urcorner \mathrel{-\!\!\star} \hat{Q}(\mathtt{n}) \vDash wp_{\mathsf{F}}\,(\mathtt{j})\,\{\hat{Q}\}$$

By the definition of $\mathcal{S}$, $\ulcorner - \urcorner$-L, and Signature Substitution Unrestricted, it suffices if

$$\forall\ n.\ \ulcorner n = j\urcorner \mathrel{-\!\!\star} \hat{Q}(\mathtt{n}) \vDash wp_{\mathsf{F}}\,(\mathtt{j})\,\{\hat{Q}\}$$

which follows from WP-VAL.

Case: $\mathsf{m} = \mathsf{flex}$. Unfolding $\underline{\mathtt{sel}}^{\mathsf{s_i}}_{\Sigma.\mathsf{X}}$, it suffices if

$$\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}}(\varsigma) \star \forall\ n.\ \ulcorner n = \varsigma(\mathsf{X}).\mathsf{sel}(\mathsf{s_j}).\mathsf{off}\urcorner \mathrel{-\!\!\star} \hat{Q}(\mathtt{n}) \vDash wp_{\mathsf{F}}\left(\mathtt{sel}^{\mathsf{s_i}}_{\mathsf{X}}\ ()\right)\{\hat{Q}\}$$

By the definition of $\mathcal{S}$, Signature Substitution Unrestricted, and ! -L, it suffices if

$$\dfrac{wp_{\mathsf{F}}\left(\left\langle \mathtt{sel}^{\mathsf{s_i}}_{\mathsf{X}}\right\rangle_{\mathsf{F}}\ ()\right)\{\mathtt{w}.\ \ulcorner \mathtt{w} = \delta.\mathsf{sel}(\mathsf{s_i}).\mathsf{off}\urcorner\} \quad \forall\ n.\ \ulcorner n = \varsigma(\mathsf{X}).\mathsf{sel}(\mathsf{s_j}).\mathsf{off}\urcorner \mathrel{-\!\!\star} \hat{Q}(\mathtt{n})}{wp_{\mathsf{F}}\left(\mathtt{sel}^{\mathsf{s_i}}_{\mathsf{X}}\ ()\right)\{\hat{Q}\}}$$

which follows from WP-BIND, WP-FUNPTR, and WP-RAMIFY.

□

F.4.1 Compatibility Lemmas.

Lemma F.109 (comp-let-compat).

$$\dfrac{\Sigma; \Gamma_1 \vDash_{\mathsf{F}} \mathsf{e}_1 : \mathsf{T}_1 \quad \Sigma; \Gamma_2, \mathsf{x} : \mathsf{T}_1 \vDash_{\mathsf{F}} \mathsf{e}_2 : \mathsf{T}_2 \quad \mathsf{x} \notin \mathrm{dom}(\Gamma_2)}{\Sigma; \Gamma_1, \Gamma_2 \vDash_{\mathsf{F}} \mathtt{const}\ \mathtt{x} = \mathtt{e}_1;\ \mathtt{e}_2 : \mathsf{T}_2}\ (\textit{COMP-LET-COMPAT})$$

Proof. Unfold $\vDash$ and consider arbitrary $\mathsf{F}' \supseteq \mathsf{F}, \varsigma, \gamma^{(\mathrm{H1})}$. Assume the premises $\Sigma; \Gamma_1 \vDash_{\mathsf{F}} \mathsf{e}_1 : \mathsf{T}_1^{(\mathrm{H2})}$, $\Sigma; \Gamma_2, \mathsf{x} : \mathsf{T}_1 \vDash_{\mathsf{F}} \mathsf{e}_2 : \mathsf{T}_2^{(\mathrm{H3})}$, and $\mathsf{x} \notin \Gamma_2^{(\mathrm{H4})}$. We must show

$$\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}'}(\varsigma) \star \mathcal{C}[\![\Gamma_1, \Gamma_2]\!]^{\varsigma}_{\mathsf{F}'}(\gamma) \vDash \mathcal{E}[\![\mathsf{T}_2]\!]^{\varsigma}_{\mathsf{F}'}(\mathtt{const}\ \mathtt{x} = \mathtt{e}_1;\ \mathtt{e}_2[\gamma])$$

By $\mathcal{C}$-SPLIT and simplifying substitutions, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \mathcal{C}[\![\Gamma_1]\!]^{\varsigma}_{F'}(\gamma) \quad \mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \mathcal{C}[\![\Gamma_2]\!]^{\varsigma}_{F'}(\gamma)}{\mathcal{E}[\![T_2]\!]^{\varsigma}_{F'}(\mathtt{const}\ x = e_1[\gamma];\ e_2[\gamma \setminus x])}$$

Then by $\mathcal{C}$-CONS with H4, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \mathcal{C}[\![\Gamma_1]\!]^{\varsigma}_{F'}(\gamma) \quad \forall\, w.\ \mathcal{V}[\![T_1]\!]^{\varsigma}_{F'}(w) \mathrel{-\!\!\star} \left(\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \star \mathcal{C}[\![\Gamma_2, x : T_1]\!]^{\varsigma}_{F'}(\gamma[w/x])\right)}{\mathcal{E}[\![T_2]\!]^{\varsigma}_{F'}(\mathtt{const}\ x = e_1[\gamma];\ e_2[\gamma \setminus x])}$$

Observe that $\mathcal{C}[\![\Gamma_2, x : T_1]\!]^{\varsigma}_{F'}(\gamma[w/x]) \vDash \mathcal{C}[\![\Gamma_2, x : T_1]\!]^{\varsigma}_{F'}((\gamma \setminus x)[w/x])$, since the substitutions are equivalent (noting $[w/x]$ takes precedence). Applying this fact, H2, and H3, using H1 and $\mathrel{-\!\!\star}$-MONO, it suffices if

$$\frac{\mathcal{E}[\![T_1]\!]^{\varsigma}_{F'}(e_1[\gamma]) \quad \forall\, w.\ \mathcal{V}[\![T_1]\!]_{F'}(w) \mathrel{-\!\!\star} \mathcal{E}[\![T_2]\!](e_2[\gamma \setminus x][w/x])}{\mathcal{E}[\![T_2]\!]_{F'}(\mathtt{const}\ x = e_1[\gamma];\ e_2[\gamma \setminus x])}$$

By LR-BIND, it suffices if

$$\frac{\mathcal{V}[\![T_1]\!]^{\varsigma}_{F'}(w) \quad \forall\, w.\ \mathcal{V}[\![T_1]\!]_{F'}(w) \mathrel{-\!\!\star} \mathcal{E}[\![T_2]\!](e_2[\gamma \setminus x][w/x])}{\mathcal{E}[\![T_2]\!]_{F'}(\mathtt{const}\ x = w;\ e_2[\gamma \setminus x])}$$

which follows by $\mathrel{-\!\!\star}$-L, WP-LET, and $\triangleright$ -R. ◻

LEMMA F.110 (COMP-VAR-COMPAT).

$$\text{(COMP-VAR-COMPAT)}\quad \Sigma; x : T \vDash_F x : T$$

PROOF. Unfold $\vDash$ and consider arbitrary $F' \supseteq F, \varsigma, \gamma$, By SIGNATURE SUBSTITUTION UNRESTRICTED, ! -DROP, and LR-VAL, it suffices if

$$\mathcal{C}[\![x : T]\!]^{\varsigma}_{F'}(\gamma) \vDash \mathcal{V}[\![T]\!]^{\varsigma}_{F'}(x[\gamma])$$

By $\mathcal{C}[\![-]\!]$ and $\ulcorner - \urcorner$-L, it suffices if

$$\mathcal{V}[\![T]\!]^{\varsigma}_{F'}(\gamma(x)) \vDash \mathcal{V}[\![T]\!]^{\varsigma}_{F'}(x[\gamma])$$

where $x \in \mathrm{dom}(\gamma)$, which follows by substitution. ◻

LEMMA F.111 (COMP-DUP-COMPAT).

$$\text{(COMP-DUP-COMPAT)}\quad \frac{\Gamma \ni x : T_1 \quad \Sigma; \Gamma, x : T_1 \vDash_F e : T_2}{\Sigma; \Gamma \vDash_F \underline{\mathtt{dup}}_{T_1}\ (x)\,; e : T_2}$$

PROOF. Unfold $\vDash$ and consider arbitrary $F' \supseteq F, \varsigma, \gamma^{(H1)}$. Also assume the premises $\Gamma \ni x : T_1{}^{(H2)}$ and $\Sigma; \Gamma, x : T_1 \vDash_{F'} e : T_2{}^{(H3)}$. We must show

$$\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \star \mathcal{C}[\![\Gamma]\!]^{\varsigma}_{F'}(\gamma) \vDash \mathcal{E}[\![T_2]\!]^{\varsigma}_{F'}(\underline{\mathtt{dup}}_{T_1}\ (\gamma(x))\,; e[\gamma])$$

By $\mathcal{C}$-UNCONS with H2, it suffices if

$$\frac{\mathcal{V}[\![T_1]\!]^{\varsigma}_{F'}(\gamma(x)) \quad \mathcal{V}[\![T_1]\!]^{\varsigma}_{F'}(\gamma(x)) \mathrel{-\!\!\star} \left(\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \star \mathcal{C}[\![\Gamma]\!]^{\varsigma}_{F'}(\gamma)\right)}{\mathcal{E}[\![T_2]\!]^{\varsigma}_{F'}(\underline{\mathtt{dup}}_{T_1}\ (\gamma(x))\,; e[\gamma])}$$

By $\mathcal{C}$-CONS with H2 and $\mathrel{-\!\!\star}$-MONO, it suffices if

$$\frac{\mathcal{V}[\![T_1]\!]^{\varsigma}_{F'}(\gamma(x)) \quad \mathcal{V}[\![T_1]\!]^{\varsigma}_{F'}(\gamma(x)) \mathrel{-\!\!\star} \left(\mathcal{V}[\![T_1]\!]^{\varsigma}_{F'}(\gamma(x)) \mathrel{-\!\!\star} \left(\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \star \mathcal{C}[\![\Gamma, x : T_1]\!]^{\varsigma}_{F'}(\gamma)\right)\right)}{\mathcal{E}[\![T_2]\!]^{\varsigma}_{F'}(\underline{\mathtt{dup}}_{T_1}\ (\gamma(x))\,; e[\gamma])}$$

Then by H3 using H1 and $-\!\!\star$-MONO, followed by $-\!\!\star$-CURRY, it suffices if

$$\frac{\mathcal{V}[\![\mathrm{T}_1]\!]^{\varsigma}_{\mathrm{F}'}(\gamma(\mathrm{x})) \quad (\mathcal{V}[\![\mathrm{T}_1]\!]^{\varsigma}_{\mathrm{F}'}(\gamma(\mathrm{x})) \star \mathcal{V}[\![\mathrm{T}_1]\!]^{\varsigma}_{\mathrm{F}'}(\gamma(\mathrm{x}))) -\!\!\star \mathcal{E}[\![\mathrm{T}_2]\!]^{\varsigma}_{\mathrm{F}'}(\mathrm{e}[\gamma])}{\mathcal{E}[\![\mathrm{T}_2]\!]^{\varsigma}_{\mathrm{F}'}(\underline{\mathrm{dup}}_{\mathrm{T}_1}\ (\gamma(\mathrm{x}))\,;\mathrm{e}[\gamma])}$$

By $\mathcal{E}[\![-]\!]$ and WP-SEQ, it suffices if

$$\frac{\mathcal{V}[\![\mathrm{T}_1]\!](\gamma(\mathrm{x})) \quad (\mathcal{V}[\![\mathrm{T}_1]\!](\gamma(\mathrm{x})) \star \mathcal{V}[\![\mathrm{T}_1]\!](\gamma(\mathrm{x}))) -\!\!\star \mathcal{E}[\![\mathrm{T}_2]\!](\mathrm{e}[\gamma])}{wp\left(\underline{\mathrm{dup}}_{\mathrm{T}_1}\ (\gamma(\mathrm{x}))\right)\{\triangleright\, \mathcal{E}[\![\mathrm{T}_2]\!](\mathrm{e}[\gamma])\}}$$

By WP-RAMIFY and $\triangleright$ -R, it suffices if

$$\mathcal{V}[\![\mathrm{T}_1]\!](\gamma(\mathrm{x})) \vDash wp\left(\underline{\mathrm{dup}}_{\mathrm{T}_1}\ (\gamma(\mathrm{x}))\right)\{\mathcal{V}[\![\mathrm{T}_1]\!](\gamma(\mathrm{x})) \star \mathcal{V}[\![\mathrm{T}_1]\!]\}$$

which is exactly DUP. □

LEMMA F.112 (COMP-DROP-COMPAT).

$$\text{(COMP-DROP-COMPAT)}\quad \frac{\Sigma;\Gamma \vDash_{\mathrm{F}} \mathrm{e} : \mathrm{T}_2}{\Sigma;\Gamma,\mathrm{x} : \mathrm{T}_1 \vDash_{\mathrm{F}} \underline{\mathrm{drop}}^{\Sigma}_{\mathrm{T}_1}\ (\mathrm{x})\,;\mathrm{e} : \mathrm{T}_2}$$

PROOF. Unfold $\vDash$ and consider arbitrary $\mathrm{F}' \supseteq \mathrm{F}, \varsigma, \gamma^{(\mathrm{H1})}$. Also assume the premise $\Sigma;\Gamma \vDash_{\mathrm{F}'} \mathrm{e} : \mathrm{T}_2{}^{(\mathrm{H2})}$. We must show

$$\mathcal{S}[\![\Sigma]\!]_{\mathrm{F}'}(\varsigma) \star \mathcal{C}[\![\Gamma,\mathrm{x} : \mathrm{T}_1]\!]^{\varsigma}_{\mathrm{F}'}(\gamma) \vDash \mathcal{E}[\![\mathrm{T}_2]\!]^{\varsigma}_{\mathrm{F}'}(\underline{\mathrm{drop}}^{\Sigma}_{\mathrm{T}_1}\ (\gamma(\mathrm{x}))\,;\mathrm{e}[\gamma])$$

By $\mathcal{C}$-SPLIT, $\mathcal{C}[\![-]\!]$, ! -DROP, and substitution, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{\mathrm{F}'}(\varsigma) \quad \mathcal{V}[\![\mathrm{T}_1]\!]^{\varsigma}_{\mathrm{F}'}(\gamma(\mathrm{x})) \quad \mathcal{S}[\![\Sigma]\!]_{\mathrm{F}'}(\varsigma) \quad \mathcal{C}[\![\Gamma]\!]^{\varsigma}_{\mathrm{F}'}(\gamma)}{\mathcal{E}[\![\mathrm{T}_2]\!]^{\varsigma}_{\mathrm{F}'}(\underline{\mathrm{drop}}^{\Sigma}_{\mathrm{T}_1}\ (\gamma(\mathrm{x}))\,;\mathrm{e}[\gamma])}$$

By H2 with H1, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{\mathrm{F}'}(\varsigma) \quad \mathcal{V}[\![\mathrm{T}_1]\!]^{\varsigma}_{\mathrm{F}'}(\gamma(\mathrm{x})) \quad \mathcal{E}[\![\mathrm{T}_2]\!]^{\varsigma}_{\mathrm{F}'}(\mathrm{e}[\gamma])}{\mathcal{E}[\![\mathrm{T}_2]\!]^{\varsigma}_{\mathrm{F}'}(\underline{\mathrm{drop}}^{\Sigma}_{\mathrm{T}_1}\ (\gamma(\mathrm{x}))\,;\mathrm{e}[\gamma])}$$

By $\mathcal{E}[\![-]\!]$ and WP-SEQ, it suffices if

$$\mathcal{S}[\![\Sigma]\!]_{\mathrm{F}'}(\varsigma) \star \mathcal{V}[\![\mathrm{T}_1]\!]^{\varsigma}_{\mathrm{F}}(\mathrm{w}) \star \mathcal{E}[\![\mathrm{T}_2]\!]^{\varsigma}_{\mathrm{F}}(\mathrm{e}[\gamma]) \vDash wp_{\mathrm{F}}\left(\underline{\mathrm{drop}}^{\Sigma}_{\mathrm{T}_1}\ (\gamma(\mathrm{x}))\right)\{\triangleright\, \mathcal{E}[\![\mathrm{T}_2]\!]^{\varsigma}_{\mathrm{F}}(\mathrm{e}[\gamma])\}$$

By WP-MONO, $\triangleright$ -R, and $-\!\!\star$-*emp* we can rewrite as

$$\mathcal{S}[\![\Sigma]\!]_{\mathrm{F}'}(\varsigma) \star \mathcal{V}[\![\mathrm{T}_1]\!]^{\varsigma}_{\mathrm{F}}(\mathrm{w}) \star (emp -\!\!\star \mathcal{E}[\![\mathrm{T}_2]\!]^{\varsigma}_{\mathrm{F}}(\mathrm{e}[\gamma])) \vDash wp_{\mathrm{F}}\left(\underline{\mathrm{drop}}^{\Sigma}_{\mathrm{T}_1}\ (\gamma(\mathrm{x}))\right)\{\mathcal{E}[\![\mathrm{T}_2]\!]^{\varsigma}_{\mathrm{F}}(\mathrm{e}[\gamma])\}$$

Applying WP-RAMIFY, it suffices if

$$\mathcal{S}[\![\Sigma]\!]_{\mathrm{F}'}(\varsigma) \star \mathcal{V}[\![\mathrm{T}_1]\!]^{\varsigma}_{\mathrm{F}}(\mathrm{w}) \vDash wp_{\mathrm{F}}\left(\underline{\mathrm{drop}}^{\Sigma}_{\mathrm{T}_1}\ (\gamma(\mathrm{x}))\right)\{emp\}$$

which follows from DROP. □

LEMMA F.113 (COMP-I-$\mathbb{Z}$-COMPAT).

$$\text{(COMP-I-}\mathbb{Z}\text{-COMPAT)}\quad \Sigma;\varnothing \vDash_{\mathrm{F}} \mathrm{n} : \mathbb{Z}$$

Proof. Unfold $\vDash$ and consider arbitrary $F' \supseteq F, \varsigma, \gamma^{(H1)}$. By Signature Substitution Unrestricted, ! -drop, and lr-val, it suffices if

$$\mathcal{C}[\![\varnothing]\!]^{\varsigma}_{F'}(\gamma) \vDash \mathcal{V}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(\mathtt{n}[\gamma])$$

Unfolding $\mathcal{C}[\![-]\!]$, $\mathcal{V}[\![-]\!]$, $\mathcal{U}[\![-]\!]$, and simplifying the substitution, it suffices if

$$\ulcorner \mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\varnothing) \urcorner \vDash \ulcorner \mathtt{n} \in \mathbb{Z} \urcorner$$

which follows since $\mathrm{dom}(\gamma) \supseteq \mathrm{dom}(\varnothing)$ and $\mathtt{n} \in \mathbb{Z}$. □

Lemma F.114 (comp-$\oplus$-$\mathbb{Z}$-compat).

$$\frac{\Sigma; \Gamma_1 \vDash_F \mathtt{e}_1 : \mathbb{Z} \qquad \Sigma; \Gamma_2 \vDash_F \mathtt{e}_2 : \mathbb{Z}}{\Sigma; \Gamma_1, \Gamma_2 \vDash_F \mathtt{e}_1 \oplus \mathtt{e}_2 : \mathbb{Z}}\ (\textsc{comp-}\oplus\textsc{-}\mathbb{Z}\textsc{-compat})$$

Proof. Unfold $\vDash$ and consider arbitrary $F' \supseteq F, \varsigma, \gamma^{(H1)}$. Assume the premises $\Sigma; \Gamma_1 \vDash_F \mathtt{e}_1 : \mathbb{Z}^{(H2)}$ and $\Sigma; \Gamma_2 \vDash_F \mathtt{e}_2 : \mathbb{Z}^{(H3)}$. We must show

$$\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \star \mathcal{C}[\![\Gamma_1, \Gamma_2]\!]^{\varsigma}_{F'}(\gamma) \vDash \mathcal{E}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}((\mathtt{e}_1 \oplus \mathtt{e}_2)[\gamma])$$

By $\mathcal{C}$-split and simplifying substitutions, it suffices if

$$\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \star \mathcal{C}[\![\Gamma_1]\!]^{\varsigma}_{F'}(\gamma) \star \mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \star \mathcal{C}[\![\Gamma_2]\!]^{\varsigma}_{F'}(\gamma) \vDash \mathcal{E}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(\mathtt{e}_1[\gamma] \oplus \mathtt{e}_2[\gamma])$$

Then by H2 and H3 with H1, it suffices if

$$\mathcal{E}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(\mathtt{e}_1[\gamma]) \star \mathcal{E}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(\mathtt{e}_2[\gamma]) \vDash \mathcal{E}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(\mathtt{e}_1[\gamma] \oplus \mathtt{e}_2[\gamma])$$

By lr-bind, $\forall$ -R, and $-\!\!\star$-R, it suffices if

$$\mathcal{V}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(\mathtt{w}_1) \star \mathcal{E}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(\mathtt{e}_2[\gamma]) \vDash \mathcal{E}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(\mathtt{w}_1 \oplus \mathtt{e}_2[\gamma])$$

Again, by lr-bind, $\forall$ -R, and $-\!\!\star$-R, it suffices if

$$\mathcal{V}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(\mathtt{w}_1) \star \mathcal{V}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(\mathtt{w}_2) \vDash \mathcal{E}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(\mathtt{w}_1 \oplus \mathtt{w}_2)$$

By $\mathcal{E}[\![-]\!]$, wp-bop, and $\triangleright$ -R, it suffices if

$$\mathcal{V}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(\mathtt{w}_1) \star \mathcal{V}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}(\mathtt{w}_2) \vDash \mathcal{V}[\![\mathbb{Z}]\!]^{\varsigma}_{F'}([\![\oplus]\!](\mathtt{w}_1, \mathtt{w}_2))$$

which follows after unfolding $\mathcal{V}[\![-]\!]$, $\mathcal{U}[\![-]\!]$, and $[\![\oplus]\!]$. □

Lemma F.115 (comp-I$\longrightarrow$-compat).

$$\frac{\Gamma = \overline{\mathtt{y_j} : \mathsf{T_j}}^{j<m} \qquad \Sigma; \Gamma, \mathtt{z_f} : \overline{\mathsf{T_i}}^{i<n} \longrightarrow \mathsf{T}, \overline{\mathtt{x_i} : \mathsf{T_i}}^{i<n} \vDash_F \mathtt{e} : \mathsf{T} \qquad \Gamma \not\ni \mathtt{z_f}, \overline{\mathtt{x}}^{i<n} \text{ distinct}}{\Sigma; \Gamma \vDash_F \mathtt{e_f} : \overline{\mathsf{T_i}}^{i<n} \longrightarrow \mathsf{T}}\ (\textsc{comp-I}\longrightarrow\textsc{-compat})$$

where

$$F \supseteq \left\{ \begin{array}{l} \mathtt{call_k}\left(\mathtt{z_f}, \overline{\mathtt{x_i}}^{i<n}\right) \left\{ \overline{\mathtt{const\ y_j} = *(\mathtt{z_f} + 3 + \mathtt{j});\ \underline{\mathtt{dup}}_{\mathsf{T_j}}\left(\mathtt{y_j}\right)}^{j<m} ; \mathtt{e} \right\}, \\ \mathtt{destr_k}\left(\mathtt{z_f}\right) \left\{ \overline{\mathtt{const\ y_j} = *(\mathtt{z_f} + 3 + \mathtt{j});\ \underline{\mathtt{drop}}^{\Sigma}_{\mathsf{T_j}}\left(\mathtt{y_j}\right)}^{j<m} ; \mathtt{free}\left(\mathtt{z_f}\right);\ 0 \right\} \end{array} \right\}$$

and

$$\mathtt{e}_{\mathtt{f}} \triangleq \left\{ \begin{array}{l} \mathtt{const\ z_f = malloc\,(3+m);} \\ \mathtt{*z_f = 1;} \\ \mathtt{*(z_f + 1) = call_k;} \\ \mathtt{*(z_f + 2) = destr_k;} \\ \overline{\mathtt{*(z_f + 3 + j) = y_j;}}^{j<m} \\ \mathtt{z_f} \end{array} \right\}$$

Proof. Unfold $\vDash$ and consider arbitrary $\mathtt{F}' \supseteq \mathtt{F}^{(\mathrm{H1})}$, along with ς, γ. Also assume the premises $\Gamma = \overline{\mathtt{y_j} : \mathtt{T_j}}^{j<m\,(\mathrm{H2})}$ and $\Sigma; \Gamma, \mathtt{z_f} : \overline{\mathtt{T_i}}^{i<n} \to \mathtt{T}, \overline{\mathtt{x_i} : \mathtt{T_i}}^{i<n} \vDash_{\mathtt{F}} \mathtt{e} : \mathtt{T}^{(\mathrm{H3})}$. Simplifying substitutions via $C[\![-]\!]$ and H2, it suffices if

$$\mathcal{S}[\![\Sigma]\!]_{\mathtt{F}'}(\varsigma) \star C[\![\Gamma]\!]^{\varsigma}_{\mathtt{F}'}(\gamma) \vDash wp \left(\begin{array}{l} \mathtt{const\ z_f = malloc\,(3+m);} \\ \mathtt{*z_f = 1;} \\ \mathtt{*(z_f + 1) = call_k;} \\ \mathtt{*(z_f + 2) = destr_k;} \\ \overline{\mathtt{*(z_f + 3 + j) =} (\gamma \setminus \mathtt{z_f})(\mathtt{y_j});}^{j<m} \\ \mathtt{z_f} \end{array} \right) \{\mathcal{V}\left[\!\!\left[\overline{\mathtt{T_i}}^{i<n} \to \mathtt{T}\right]\!\!\right]^{\varsigma}_{\mathtt{F}'}\}$$

Using $\mathtt{z_f} \notin \overline{\mathtt{y_j} : \mathtt{T_j}}^{j<m}$, we conclude that $(\gamma \setminus \mathtt{z_f})(\mathtt{y_j}) = \gamma(\mathtt{y_j})$ and simplify accordingly. By wp-bop, wp-malloc, and wp-let interspersed with appropriate uses of wp-bind, $\triangleright$ -R, and $-\!\!\star$-R, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{\mathtt{F}'}(\varsigma) \quad C[\![\Gamma]\!]^{\varsigma}_{\mathtt{F}'}(\gamma) \quad \overline{\ell + j \mapsto ☣}^{j<3+m} \quad size\,(\ell,\ 3+m)}{wp\left(\mathtt{*}\ell \mathtt{\ = 1;\ *(}\ell\mathtt{\ + 1) = call_k;\ *(}\ell\mathtt{\ + 2) = destr_k;}\ \overline{\mathtt{*(}\ell\mathtt{\ + 3 + j) =}\ \gamma(\mathtt{y_j});}^{j<m}\ \ell\right) \{\mathcal{V}\left[\!\!\left[\overline{\mathtt{T_i}}^{i<n} \to \mathtt{T}\right]\!\!\right]^{\varsigma}_{\mathtt{F}'}\}}$$

where $\ell \neq \mathtt{null}^{(\mathrm{H4})}$ by wp-malloc. By applying wp-store three times, alongside wp-bop and wp-funptr twice each (with appropriate uses of wp-bind, $\triangleright$ -R and $-\!\!\star$-R in between) it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{\mathtt{F}'}(\varsigma) \quad C[\![\Gamma]\!]^{\varsigma}_{\mathtt{F}'}(\gamma) \\ \ell \mapsto 1 \quad \ell + 1 \mapsto \langle \mathtt{call_k} \rangle_{\mathtt{F}'} \quad \ell + 2 \mapsto \langle \mathtt{destr_k} \rangle_{\mathtt{F}'} \quad \overline{\ell + 3 + j \mapsto ☣}^{j<m} \quad size\,(\ell,\ 3+m)\end{array}}{wp\left(\overline{\mathtt{*(}\ell\mathtt{\ + 3 + j) =}\ \gamma(\mathtt{y_j});}^{j<m}\ \ell\right) \{\mathcal{V}\left[\!\!\left[\overline{\mathtt{T_i}}^{i<n} \to \mathtt{T}\right]\!\!\right]^{\varsigma}_{\mathtt{F}'}\}}$$

By unfolding $C[\![-]\!]$, along with m more applications of wp-bop and wp-store, again interspersed with wp-bind, $\triangleright$ -R and $-\!\!\star$-R as fit, it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{\mathtt{F}'}(\varsigma) \quad \overline{\ell + 3 + j \mapsto \gamma(\mathtt{y_j}) \star \mathcal{V}[\![\mathtt{T_j}]\!](\gamma(\mathtt{y_j}))}^{j<m} \\ \ell \mapsto 1 \quad \ell + 1 \mapsto \langle \mathtt{call_k} \rangle_{\mathtt{F}'} \quad \ell + 2 \mapsto \langle \mathtt{destr_k} \rangle_{\mathtt{F}'} \quad size\,(\ell,\ 3+m)\end{array}}{wp\ (\ell)\ \{\mathcal{V}\left[\!\!\left[\overline{\mathtt{T_i}}^{i<n} \to \mathtt{T}\right]\!\!\right]^{\varsigma}_{\mathtt{F}'}\}}$$

Make the following abbreviations

$$\begin{array}{lcl} Env & \triangleq & \bigstar_{j<m} \ell + 3 + j \mapsto \gamma(\mathtt{y_j}) \star \mathcal{V}[\![\mathtt{T_j}]\!](\gamma(\mathtt{y_j})) \star size\,(\ell,\ 3+m) \\ Self & \triangleq & \ell + 1 \mapsto \langle \mathtt{call_k} \rangle_{\mathtt{F}'} \star \ell + 2 \mapsto \langle \mathtt{destr_k} \rangle_{\mathtt{F}'} \star Env \end{array}$$

Then by wp-share, $-\!\!\star$-R, and wp-val, it suffices if

$$\mathcal{S}[\![\Sigma]\!]_{\mathtt{F}'}(\varsigma) \star @_{\ell}\, Self \vDash \mathcal{V}\left[\!\!\left[\overline{\mathtt{T_i}}^{i<n} \to \mathtt{T}\right]\!\!\right]^{\varsigma}_{\mathtt{F}'}(\ell)$$

Applying $\mathrel{-\!\!\star}$-L and cancelling, we proceed by $\triangleright$ -IND. It suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \land \triangleright \left(@_\ell\, \mathit{Self} \mathrel{-\!\!\star} \mathcal{V}\left[\!\!\left[\overline{T_i}^{i<n} \to T\right]\!\!\right]^{\varsigma}_{F'}(\ell)\right)}{@_\ell\, \mathit{Self} \mathrel{-\!\!\star} \mathcal{V}\left[\!\!\left[\overline{T_i}^{i<n} \to T\right]\!\!\right]^{\varsigma}_{F'}(\ell)}$$

By $\mathrel{-\!\!\star}$-R, $\mathcal{V}[\![-]\!]$ with H4, $\mathcal{O}[\![-]\!]$, @ -! with ! -$\{-\}$ $-$ $\{-\}$, and $\exists$ -R, it suffices if

$$\frac{@_\ell\, \mathit{Self} \quad \mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \land \triangleright \left(@_\ell\, \mathit{Self} \mathrel{-\!\!\star} \mathcal{V}\left[\!\!\left[\overline{T_i}^{i<n} \to T\right]\!\!\right]^{\varsigma}_{F'}(\ell)\right)}{\begin{array}{c} @_\ell\, \mathit{Self} \quad \{\ell \mapsto 0 \star \mathit{Self}\}\ \langle \mathtt{destr_k}\rangle_{F'}\ (\ell)\ \{\mathit{emp}\} \\ \forall\ \overline{\mathtt{w_i}}^{i<n}.\ \{@_\ell\, \mathit{Self} \star \bigstar_{i<n} \mathcal{V}[\![T_i]\!]^{\varsigma}_{F'}(\mathtt{w_i})\}\ \langle \mathtt{call_k}\rangle_{F'}\ (\ell, \overline{\mathtt{w_i}}^{i<n})\ \{\mathcal{V}[\![T]\!]^{\varsigma}_{F'}\} \end{array}}$$

Cancelling $@_\ell$ *Self* and applying Signature Substitution Unrestricted, ! -$\land_1$, and ! -unr we break the remaining proof obligation down into two goals:

- Simplifying with ! -L and $\land$-L, we must show

  $$\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \vDash \{\ell \mapsto 0 \star \mathit{Self}\}\ \langle \mathtt{destr_k}\rangle_{F'}\ (\ell)\ \{\mathit{emp}\}$$

  Unfolding $\{-\}$ $-$ $\{-\}$, and applying Signature Substitution Unrestricted, ! -mono, and $\mathrel{-\!\!\star}$-R, it suffices if

  $$\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \star \ell \mapsto 0 \star \mathit{Self} \vDash \mathit{wp}_{F'}\ (\langle \mathtt{destr_k}\rangle_{F'}\ (\ell))\ \{\mathit{emp}\}$$

  By wp-app with $\mathtt{destr_k}$ and H1, and $\triangleright$ -R, it suffices if

  $$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \ell \mapsto 0 \quad \mathit{Self}}{\mathit{wp}\ \left(\overline{\mathtt{const\ y_j = *(\ell + 3 + j);\ \underline{drop}^{\Sigma}_{T_j}\ (y_j)}}^{j<m}\mathtt{;free\ (\ell)\ ;\ 0}\right)\ \{\mathit{emp}\}}$$

  By m applications of wp-bop, wp-load, wp-let, wp-seq, and drop, all interspersed with applications of wp-bind, $\triangleright$ -R, $\mathrel{-\!\!\star}$-R, $\diamond$ -R, $\diamond$ -drop, and ! -unr, along with appeals to the definitions of *Self* and *Env*, it suffices if

  $$\frac{\begin{array}{c} \ell \mapsto 0 \\ \ell + 1 \mapsto \langle \mathtt{call_k}\rangle_{F'} \quad \ell + 2 \mapsto \langle \mathtt{destr_k}\rangle_{F'} \quad \overline{\ell + 3 + j \mapsto \gamma(\mathtt{y_j})}^{j<m} \quad \mathit{size}\,(\ell,\ 3 + m) \end{array}}{\mathit{wp}\ (\mathtt{free\ (\ell)\ ;\ 0})\ \{\mathit{emp}\}}$$

  which holds by wp-free, $\triangleright$ -R, and wp-val.

- We must also show

  $$\frac{!\ \left(\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \land \triangleright \left(@_\ell\, \mathit{Self} \mathrel{-\!\!\star} \mathcal{V}\left[\!\!\left[\overline{T_i}^{i<n} \to T\right]\!\!\right]^{\varsigma}_{F'}(\ell)\right)\right)}{\forall\ \overline{\mathtt{w_i}}^{i<n}.\ \{@_\ell\, \mathit{Self} \star \bigstar_{i<n} \mathcal{V}[\![T_i]\!]^{\varsigma}_{F'}(\mathtt{w_i})\}\ \langle \mathtt{call_k}\rangle_{F'}\ (\ell, \overline{\mathtt{w_i}}^{i<n})\ \{\mathcal{V}[\![T]\!]^{\varsigma}_{F'}\}}$$

  Noting that $\mathtt{Word}$ is inhabited, applying ! -$\{-\}$ $-$ $\{-\}$, ! -$\forall$, ! -mono, $\forall$ -R, and $\mathrel{-\!\!\star}$-R it suffices to show for all $\overline{\mathtt{w_i}}^{i<n}$ that

  $$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \land \triangleright \left(@_\ell\, \mathit{Self} \mathrel{-\!\!\star} \mathcal{V}\left[\!\!\left[\overline{T_i}^{i<n} \to T\right]\!\!\right]^{\varsigma}_{F'}(\ell)\right) \quad @_\ell\, \mathit{Self} \quad \overline{\mathcal{V}[\![T_i]\!]^{\varsigma}_{F'}(\mathtt{w_i})}^{i<n}}{\mathit{wp}\ (\langle \mathtt{call_k}\rangle_{F'}\ (\ell, \overline{\mathtt{w_i}}^{i<n}))\ \{\mathcal{V}[\![T]\!]_{F'\varsigma}\}}$$

  By wp-app with $\mathtt{call_k}$ and H1, it suffices if

  $$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \land \triangleright \left(@_\ell\, \mathit{Self} \mathrel{-\!\!\star} \mathcal{V}\left[\!\!\left[\overline{T_i}^{i<n} \to T\right]\!\!\right]^{\varsigma}_{F'}(\ell)\right) \quad @_\ell\, \mathit{Self} \quad \overline{\mathcal{V}[\![T_i]\!]^{\varsigma}_{F'}(\mathtt{w_i})}^{i<n}}{\triangleright\ \mathit{wp}\ \left(\overline{\mathtt{const\ y_j = *(\ell + 3 + j);\ \underline{dup}_{T_j}\ (y_j)}}^{j<m}\mathtt{;e}[\ell/\mathtt{z_f}, \overline{\mathtt{w_i}/\mathtt{x_i}}^{i<n}]\right)\ \{\mathcal{V}[\![T]\!]^{\varsigma}_{F'}\}}$$

Crucially, after $\triangleright$ -R (using $\wedge$-MONO) and $\triangleright$ -$\wedge$, we can apply $\triangleright$ -MONO. It therefore suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \wedge \left(@_\ell\, Self \mathrel{-\!\!\star} \mathcal{V}\left[\!\!\left[\overline{T_i}^{i<n} \to T\right]\!\!\right]^{\varsigma}_{F'}(\ell)\right) \quad @_\ell\, Self \quad \overline{\mathcal{V}[\![T_i]\!]^{\varsigma}_{F'}(w_i)}^{i<n}}{wp\left(\overline{\texttt{const}\ y_j = *(\ell + 3 + j);\ \underline{\texttt{dup}}_{T_j}(y_j)}^{j<m};\ e[\ell/z_f, \overline{w_i/x_i}^{i<n}]\right)\{\mathcal{V}[\![T]\!]^{\varsigma}_{F'}\}}$$

By m applications of WP-BOP, WP-LOAD, WP-LET, WP-SEQ, and DUP, all interspersed with applications of WP-BIND, $\triangleright$ -R, $\mathrel{-\!\!\star}$-R, $\diamond$ -@ , and $\diamond$ -DROP, along with appeals to the definitions of *Self* and *Env*, it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \wedge \left(@_\ell\, Self \mathrel{-\!\!\star} \mathcal{V}\left[\!\!\left[\overline{T_i}^{i<n} \to T\right]\!\!\right]^{\varsigma}_{F'}(\ell)\right) \\ @_\ell\, Self \quad \overline{\mathcal{V}[\![T_i]\!]^{\varsigma}_{F'}(w_i)}^{i<n} \quad \overline{\mathcal{V}[\![T_j]\!]^{\varsigma}_{F'}(\gamma(y_j))}^{j<m}\end{array}}{wp\left(e[\ell/z_f, \overline{w_i/x_i}^{i<n}, \overline{\gamma(y_j)/y_j}^{j<m}]\right)\{\mathcal{V}[\![T]\!]^{\varsigma}_{F'}\}}$$

By SIGNATURE SUBSTITUTION UNRESTRICTED, ! -$\wedge_1$, ! -UNR, ! -L, $\wedge$-L, and $\mathrel{-\!\!\star}$-L, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \mathcal{V}\left[\!\!\left[\overline{T_i}^{i<n} \to T\right]\!\!\right](\ell) \quad \overline{\mathcal{V}[\![T_i]\!]^{\varsigma}_{F'}(w_i)}^{i<n} \quad \overline{\mathcal{V}[\![T_j]\!]^{\varsigma}_{F'}(\gamma(y_j))}^{j<m}}{wp\left(e[\ell/z_f, \overline{w_i/x_i}^{i<n}, \overline{\gamma(y_j)/y_j}^{j<m}]\right)\{\mathcal{V}[\![T]\!]^{\varsigma}_{F'}\}}$$

which follows from H3 with H1 and the definitions of $\mathcal{C}[\![-]\!]$ and $\mathcal{E}[\![-]\!]$.

$\square$

LEMMA F.116 (COMP-E$\longrightarrow$-COMPAT).

$$\text{(COMP-E}\longrightarrow\text{-COMPAT)}\quad \frac{\overline{\Sigma; \Gamma_i \vDash_F e_i : T_i}^{i<n} \quad \Sigma; \Gamma_f \vDash_F e_f : \overline{T_i}^{i<n} \to T}{\Sigma; \overline{\Gamma_i}^{i<n}, \Gamma_f \vDash_F \texttt{const}\ x_f = e_f;\ (*(x_f + 1))\ (x_f, \overline{e_i}^{i<n}) : T}$$

PROOF. Unfold $\vDash$ and consider arbitrary $F' \supseteq F, \varsigma, \gamma^{(H1)}$. Assume that $\overline{\Sigma; \Gamma_i \vDash_F e_i : T_i}^{i<n\,(H2)}$ and $\Sigma; \Gamma_f \vDash_F e_f : \overline{T_i}^{i<n} \to T^{(H3)}$. We must show

$$\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \star \mathcal{C}\left[\!\!\left[\overline{\Gamma_i}^{i}, \Gamma_f\right]\!\!\right]^{\varsigma}_{F'}(\gamma) \vDash \mathcal{E}[\![T]\!]^{\varsigma}_{F'}(\texttt{const}\ x_f = e_f;\ (*(x_f + 1))\ (x_f, \overline{e_i}^{i})\ [\gamma])$$

By $\mathcal{C}$-SPLIT and simplifying substitutions, it suffices if

$$\frac{\overline{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma)}^{i<n} \quad \overline{\mathcal{C}[\![\Gamma_i]\!]^{\varsigma}_{F'}(\gamma)}^{i<n} \quad \mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \mathcal{C}[\![\Gamma_f]\!]^{\varsigma}_{F'}(\gamma)}{\mathcal{E}[\![T]\!]^{\varsigma}_{F'}(\texttt{const}\ x_f = e_f[\gamma];\ (*(x_f + 1))\ \left(x_f, \overline{e_i[\gamma]}^{i<n}\right))}$$

By H2 and H3 with H1, it suffices if

$$\frac{\overline{\mathcal{E}[\![T_i]\!]_{F'}(e_i[\gamma])}^{i<n} \quad \mathcal{E}\left[\!\!\left[\overline{T_i}^{i<n} \to T\right]\!\!\right]^{\varsigma}_{F'}(e_f[\gamma])}{\mathcal{E}[\![T]\!]^{\varsigma}_{F'}(\texttt{const}\ x_f = e_f[\gamma];\ (*(x_f + 1))\ \left(x_f, \overline{e_i[\gamma]}^{i<n}\right))}$$

By LR-BIND and WP-LET with $\mathcal{V}[\![-]\!]$, $\mathcal{R}[\![-]\!]$, and $\mathcal{O}[\![-]\!]$, it suffices if for any $\ell \in \mathsf{Loc}_{\mathbb{N}^+}$

$$\frac{\overline{\mathcal{E}[\![T_i]\!]_{F'}(e_i[\gamma])}^{i<n} \quad @_\ell\, \mathcal{O}\left[\!\!\left[\overline{T_i}^{i<n} \to T\right]\!\!\right]^{\varsigma}_{F'}(\ell + 1)}{\mathcal{E}[\![T]\!]^{\varsigma}_{F'}((*(\ell + 1))\ \left(\ell, \overline{e_i[\gamma]}^{i<n}\right))}$$

Unfolding $\mathcal{O}[\![-]\!]$, this is

$$\dfrac{\overline{\mathcal{E}[\![\mathsf{T}_i]\!]_{\mathsf{F}'}(\mathsf{e}_i[\gamma])}^{i<n} \qquad @_\ell \begin{pmatrix} \exists\, \mathtt{call}, \mathtt{destr}, \mathit{Env}.\ \text{let } \mathit{Self} = \ell+1 \mapsto \langle \mathtt{call}\rangle_{\mathsf{F}'} \star \ell+2 \mapsto \langle \mathtt{destr}\rangle_{\mathsf{F}'} \star \mathit{Env} \text{ in} \\ \quad \mathit{Self} \\ \star \quad \forall\, \overline{\mathtt{w}_i}^{i<n}.\{\bigstar_{i<n}\mathcal{V}[\![\mathsf{T}_i]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}_i) \star @_\ell\, \mathit{Self}\}\ \langle \mathtt{call}\rangle_{\mathsf{F}'}\ (\ell, \overline{\mathtt{w}_i}^{i<n})\ \{\mathtt{w}.\ \mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}_{\mathsf{F}} \\ \star \quad \{\ell \mapsto 0 \star \mathit{Self}\}\ \langle \mathtt{destr}\rangle_{\mathsf{F}'}\ (\ell)\ \{\mathit{emp}\}_{\mathsf{F}} \end{pmatrix}}{\mathcal{E}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}'}\left((*(\ell+1))\left(\ell, \overline{\mathsf{e}_i[\gamma]}^{i<n}\right)\right)}$$

Applying $@$-$\exists$ and $\exists$-R, there exist $\mathtt{call}$, $\mathtt{destr}$, and Env. Abbreviate $\mathit{Self} = \ell+1 \mapsto \langle \mathtt{call}\rangle_{\mathsf{F}'} \star \ell+2 \mapsto \langle \mathtt{destr}\rangle_{\mathsf{F}'} \star \mathit{Env}$, then observe that

$$!\begin{pmatrix} \forall\, \overline{\mathtt{w}_i}^{i<n}.\{\bigstar_{i<n}\mathcal{V}[\![\mathsf{T}_i]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}_i) \star @_\ell\, \mathit{Self}\}\ \mathtt{call}(\ell, \overline{\mathtt{w}_i}^{i<n})\ \{\mathtt{w}.\ \mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}_{\mathsf{F}} \\ \star \quad \{\ell \mapsto 0 \star \mathit{Self}\}\ \mathtt{destr}(\ell)\ \{\mathit{emp}\}_{\mathsf{F}} \end{pmatrix}$$

by applying $!$-$\forall$ (noting that the domain $\mathtt{Word}$ is inhabited), $!$-$\{-\}-\{-\}$, and $!$-$\star$. By $@$-$!$, $!$-L, and $!$-DROP it suffices if

$$\dfrac{\overline{\mathcal{E}[\![\mathsf{T}_i]\!]_{\mathsf{F}'}(\mathsf{e}_i[\gamma])}^{i<n} \qquad @_\ell\, \mathit{Self} \qquad \forall\, \overline{\mathtt{w}_i}^{i<n}.\{\bigstar_{i<n}\mathcal{V}[\![\mathsf{T}_i]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}_i) \star @_\ell\, \mathit{Self}\}\ \langle \mathtt{call}\rangle_{\mathsf{F}'}\ (\ell, \overline{\mathtt{w}_i}^{i<n})\ \{\mathtt{w}.\ \mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}_{\mathsf{F}}}{\mathcal{E}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}'}\left((*(\ell+1))\left(\ell, \overline{\mathsf{e}_i[\gamma]}^{i<n}\right)\right)}$$

By WP-BIND and WP-LOAD with $\diamond$-$@$, $\diamond$-DROP, and $\triangleright$-R, appealing to the definition of Self, it suffices if

$$\dfrac{\overline{\mathcal{E}[\![\mathsf{T}_i]\!]_{\mathsf{F}'}(\mathsf{e}_i[\gamma])}^{i<n} \qquad @_\ell\, \mathit{Self} \qquad \forall\, \overline{\mathtt{w}_i}^{i<n}.\{\bigstar_{i<n}\mathcal{V}[\![\mathsf{T}_i]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}_i) \star @_\ell\, \mathit{Self}\}\ \langle \mathtt{call}\rangle_{\mathsf{F}'}\ (\ell, \overline{\mathtt{w}_i}^{i<n})\ \{\mathtt{w}.\ \mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}_{\mathsf{F}}}{\mathcal{E}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}'}\left(\langle \mathtt{call}\rangle_{\mathsf{F}'}\left(\ell, \overline{\mathsf{e}_i[\gamma]}^{i<n}\right)\right)}$$

By n applications of LR-BIND, it suffices if

$$\dfrac{\overline{\mathcal{V}[\![\mathsf{T}_i]\!]_{\mathsf{F}'}(\mathtt{w}_i)}^{i<n} \qquad @_\ell\, \mathit{Self} \qquad \forall\, \overline{\mathtt{w}_i}^{i<n}.\{\bigstar_{i<n}\mathcal{V}[\![\mathsf{T}_i]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}_i) \star @_\ell\, \mathit{Self}\}\ \langle \mathtt{call}\rangle_{\mathsf{F}'}\ (\ell, \overline{\mathtt{w}_i}^{i<n})\ \{\mathtt{w}.\ \mathcal{V}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w})\}_{\mathsf{F}}}{\mathcal{E}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F}'}\left(\langle \mathtt{call}\rangle_{\mathsf{F}'}\left(\ell, \overline{\mathtt{w}_i}^{i<n}\right)\right)}$$

which follows from $\mathcal{E}[\![-]\!]$ and HT-APP.

□

Lemma F.117 (COMP-I-struct-COMPAT).

(COMP-I-struct-COMPAT)

$$\dfrac{\Sigma \ni \mathsf{rigid\ struct}\ \mathsf{X}\ \{\overline{\mathsf{s}_i : \mathsf{T}}^{i<n}\} \qquad \overline{\Sigma; \Gamma_i \vDash_{\mathsf{F}} \mathsf{e}_i : \mathsf{T}_i}^{i<n}}{\Sigma; \overline{\Gamma_i}^{i<n} \vDash_{\mathsf{F}} \mathtt{const\ x = malloc\ (n+1);\ *x = 1;}\ \overline{\mathtt{*(x+1+i) = e_i;}}^{i<n}\ \mathtt{x} : \mathsf{X}}$$

Proof. Unfold $\vDash$ and consider $\mathsf{F}' \supseteq \mathsf{F}, \varsigma, \gamma^{(\mathrm{H1})}$. Assume that $\Sigma \ni \mathsf{rigid\ struct}\ \mathsf{X}\ \{\overline{\mathsf{s}_i : \mathsf{T}}^{i<n}\}^{(\mathrm{H2})}$ and $\overline{\Sigma; \Gamma_i \vDash \mathsf{e}_i : \mathsf{T}_i}^{i<n\,(\mathrm{H3})}$. We must show

$$\dfrac{\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}'}(\varsigma) \qquad \mathcal{C}\left[\!\!\left[\overline{\Gamma_i}^{i<n}\right]\!\!\right]^{\varsigma}_{\mathsf{F}'}(\gamma)}{\mathcal{E}[\![\mathsf{X}]\!]^{\varsigma}_{\mathsf{F}'}\left(\mathtt{const\ x = malloc\ (n+1);\ *x = 1;}\ \overline{\mathtt{*(x+1+i) = e_i[\gamma];}}^{i<n}\ \mathtt{x}\right)}$$

By C-SPLIT, it suffices if

$$\frac{\overline{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma)}^{i<n} \quad \overline{\mathcal{C}[\![\Gamma_i]\!]^{\varsigma}_{F'}(\gamma)}^{i<n}}{\mathcal{E}[\![X]\!]^{\varsigma}_{F'}(\mathtt{const\ x = malloc\ (n+1);\ *x = 1;\ }\overline{\mathtt{*(x+1+i) = e_i}[\gamma];}^{i<n}\ \mathtt{x})}$$

By SIGNATURE SUBSTITUTION UNRESTRICTED and ! -UNR, then H3 with H1 and $\vDash$, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \overline{\mathcal{E}[\![T_i]\!]^{\varsigma}_{F'}(\mathtt{e_i}[\gamma])}^{i<n}}{\mathcal{E}[\![X]\!]^{\varsigma}_{F'}(\mathtt{const\ x = malloc\ (n+1);\ *x = 1;\ }\overline{\mathtt{*(x+1+i) = e_i}[\gamma];}^{i<n}\ \mathtt{x})}$$

By WP-BOP, WP-MALLOC, and WP-LET interspersed with WP-BIND and $\triangleright$ -R, it suffices if for any $\ell \in \mathsf{Loc}_{\mathbb{N}^+}$ (H4)

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \overline{\mathcal{E}[\![T_i]\!]^{\varsigma}_{F'}(\mathtt{e_i}[\gamma])}^{i<n} \quad \overline{\ell + i \mapsto ☣}^{i<n+1} \quad \mathit{size}\,(\ell,\ n+1)}{\mathcal{E}[\![X]\!]^{\varsigma}_{F'}(\mathtt{*}\ell\mathtt{\ = 1;\ }\overline{\mathtt{*(}\ell\mathtt{+1+i) = e_i}[\gamma];}^{i<n}\ \ell)}$$

By WP-STORE and $\triangleright$ -R, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \overline{\mathcal{E}[\![T_i]\!]^{\varsigma}_{F}(\mathtt{e_i}[\gamma])}^{i<n} \quad \ell \mapsto \mathtt{1} \quad \overline{\ell + 1 + i \mapsto ☣}^{i<n} \quad \mathit{size}\,(\ell,\ n+1)}{\mathcal{E}[\![X]\!]^{\varsigma}_{F}(\overline{\mathtt{*(}\ell\mathtt{+1+i) = e_i}[\gamma];}^{i<n}\ \ell)}$$

By n applications of LR-BIND, WP-BOP, and WP-STORE, interspersed with WP-BIND and $\triangleright$ -R, it suffices if for any $\overline{\mathtt{w_i}}^{i<n}$

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \overline{\mathcal{V}[\![T_i]\!]^{\varsigma}_{F}(\mathtt{w_i})}^{i<n} \quad \ell \mapsto \mathtt{1} \quad \overline{\ell + 1 + i \mapsto \mathtt{w_i}}^{i<n} \quad \mathit{size}\,(\ell,\ n+1)}{\mathcal{E}[\![X]\!]^{\varsigma}_{F}(\ell)}$$

By WP-SHARE, LR-VAL, $\mathcal{V}[\![-]\!]$ with H4, $\mathcal{R}[\![-]\!]$, @ -!, and @ -MONO, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \overline{\mathcal{V}[\![T_i]\!]^{\varsigma}_{F}(\mathtt{w_i})}^{i<n} \quad \overline{\ell + 1 + i \mapsto \mathtt{w_i}}^{i<n} \quad \mathit{size}\,(\ell,\ n+1)}{\varsigma(X).\mathsf{obj}(\ell+1)}$$

Note that by H2 and unfolding $\mathcal{S}[\![-]\!]$, there is some $\delta = \varsigma(X)$ (H5). Since the mode of X is rigid, by by H5, we have we have $\delta.\mathsf{kind} = \mathsf{struct}$ (H6), $n = |\mathsf{dom}(\delta.\mathsf{sel})|$ (H7), $\forall\, i < n.\ \delta.\mathsf{sel}(\mathsf{s_i}).\mathsf{off} = i$ (H8), and it suffices if

$$\frac{!\,\forall\, i < n, \mathtt{w}.\ \delta.\mathsf{sel}(\mathsf{s_i}).\mathsf{semty}(\mathtt{w}) \equiv \triangleright\, \mathcal{V}[\![T_i]\!]^{\varsigma}_{F}(\mathtt{w}) \\ \overline{\mathcal{V}[\![T_i]\!]^{\varsigma}_{F}(\mathtt{w_i})}^{i<n} \quad \overline{\ell + 1 + i \mapsto \mathtt{w_i}}^{i<n} \quad \mathit{size}\,(\ell,\ n+1)}{\varsigma(X).\mathsf{obj}(\ell+1)}$$

If $n = 0$, we are done with ! -DROP. Otherwise, unfolding $\delta.\mathsf{obj}$ with H6 and H5, it suffices if

$$\frac{!\,\forall\, i < n, \mathtt{w}.\ \delta.\mathsf{sel}(\mathsf{s_i}).\mathsf{semty}(\mathtt{w}) \equiv \triangleright\, \mathcal{V}[\![T_i]\!]^{\varsigma}_{F}(\mathtt{w}) \\ \overline{\mathcal{V}[\![T_i]\!]^{\varsigma}_{F}(\mathtt{w_i})}^{i<n} \quad \overline{\ell + 1 + i \mapsto \mathtt{w_i}}^{i<n} \quad \mathit{size}\,(\ell,\ n+1)}{\mathit{size}\,(\ell,\ 1 + |\mathsf{dom}(\delta.\mathsf{sel})|) \quad \overline{\exists\, \mathtt{w_s}.\ \ell + 1 + \delta.\mathsf{sel}(s).\mathsf{off} \mapsto \mathtt{w_s} \star \delta.\mathsf{sel}(s).\mathsf{semty}(\mathtt{w_s})}^{s \in \mathsf{dom}(\delta.\mathsf{sel})}}$$

which follows from H7, H8, ! -UNR, $\triangleright$ -R, and $\equiv$-L. ◻

LEMMA F.118 (COMP-E-struct-COMPAT).

(*COMP-E-struct-COMPAT*)

$$\frac{\Sigma \ni \mathsf{m\ struct\ X}\,\{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\} \qquad \Sigma; \Gamma \vDash_{F} \mathtt{e} : X}{\Sigma; \Gamma \vDash_{F} \mathtt{const\ x = e;\ const\ x_j = *\Big(x + \underline{sel}^{\,s_j}_{\,\Sigma.X} + 1\Big);\ \underline{dup}_{\,T_j}\,(x_j)\,;\underline{drop}^{\,\Sigma}_{\,X}\,(x)\,;x_j} : T_j}$$

Proof. Unfold $\vDash$ and consider $F' \supseteq F, \varsigma, \gamma^{(H1)}$. Assume the premises $\Sigma \ni \mathtt{m\ struct}\ X\ \{\overline{s_i : T}^{i<n}\}^{(H2)}$, and $\Sigma; \Gamma \vDash_F e : X^{(H3)}$ We must show

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \mathcal{C}[\![\Gamma]\!]^{\varsigma}_{F'}(\gamma)}{\mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}\left(\mathtt{const}\ x = e[\gamma];\ \mathtt{const}\ x_j = *\left(x + \underline{\mathtt{sel}}\,{}^{s_j}_{\Sigma.X} + 1\right);\ \underline{\mathtt{dup}}_{T_j}\ (x_j)\,;\underline{\mathtt{drop}}\,{}^{\Sigma}_{X}\ (x)\,; x_j\right)}$$

By Signature Substitution Unrestricted and $!$-unr, then H3 with H1, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \mathcal{E}[\![X]\!]^{\varsigma}_{F'}(e[\gamma])}{\mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}\left(\mathtt{const}\ x = e[\gamma];\ \mathtt{const}\ x_j = *\left(x + \underline{\mathtt{sel}}\,{}^{s_j}_{\Sigma.X} + 1\right);\ \underline{\mathtt{dup}}_{T_j}\ (x_j)\,;\underline{\mathtt{drop}}\,{}^{\Sigma}_{X}\ (x)\,; x_j\right)}$$

By lr-bind, $\mathcal{V}[\![-]\!]$, $\mathcal{R}[\![-]\!]$, and $\mathcal{O}[\![-]\!]$, it suffices if for any $\ell \in \mathsf{Loc}_{\mathbb{N}^+}{}^{(H4)}$

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad @_\ell\, \varsigma(X).\mathsf{obj}(\ell + 1)}{\mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}\left(\mathtt{const}\ x = \ell;\ \mathtt{const}\ x_j = *\left(x + \underline{\mathtt{sel}}\,{}^{s_j}_{\Sigma.X} + 1\right);\ \underline{\mathtt{dup}}_{T_j}\ (x_j)\,;\underline{\mathtt{drop}}\,{}^{\Sigma}_{X}\ (x)\,; x_j\right)}$$

By wp-let and $\triangleright$-R, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad @_\ell\, \varsigma(X).\mathsf{obj}(\ell + 1)}{\mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}\left(\mathtt{const}\ x_j = *\left(\ell + \underline{\mathtt{sel}}\,{}^{s_j}_{\Sigma.X} + 1\right);\ \underline{\mathtt{dup}}_{T_j}\ (x_j)\,;\underline{\mathtt{drop}}\,{}^{\Sigma}_{X}\ (\ell)\,; x_j\right)}$$

Note that by H2, $!$-unr and unfolding $\mathcal{S}[\![-]\!]$, there is some $\delta = \varsigma(X)^{(H5)}$. Since the mode of X is indeterminate, by H5, we have we have $\delta.\mathsf{kind} = \mathsf{struct}^{(H6)}$ and it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad !\,\forall\ i < n, w.\ \delta.\mathsf{sel}(s_i).\mathsf{semty}(w) \equiv \triangleright \mathcal{V}[\![T_i]\!]^{\varsigma}_{F}(w) \quad @_\ell\, \delta.\mathsf{obj}(\ell + 1)}{\mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}\left(\mathtt{const}\ x_j = *\left(\ell + \underline{\mathtt{sel}}\,{}^{s_j}_{\Sigma.X} + 1\right);\ \underline{\mathtt{dup}}_{T_j}\ (x_j)\,;\underline{\mathtt{drop}}\,{}^{\Sigma}_{X}\ (\ell)\,; x_j\right)}$$

Then by $\delta.\mathsf{obj}$ with H6 and H5, and also $\star$-$\exists$ and $@$-$\exists$, it suffices if for any $\overline{w_s}^{s \in \mathrm{dom}(\delta.\mathsf{sel})}$

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad !\,\forall\ i < n, w.\ \delta.\mathsf{sel}(s_i).\mathsf{semty}(w) \equiv \triangleright \mathcal{V}[\![T_i]\!]^{\varsigma}_{F}(w) \\ @_\ell\left(\mathit{size}\,(\ell,\ 1 + |\mathrm{dom}(\delta.\mathsf{sel})|) \star \bigstar_{s \in \mathrm{dom}(\delta.\mathsf{sel})}\ \ell + 1 + \delta.\mathsf{sel}(s).\mathsf{off} \mapsto w_s \star \delta.\mathsf{sel}(s).\mathsf{semty}(w_s)\right)\end{array}}{\mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}\left(\mathtt{const}\ x_j = *\left(\ell + \underline{\mathtt{sel}}\,{}^{s_j}_{\Sigma.X} + 1\right);\ \underline{\mathtt{dup}}_{T_j}\ (x_j)\,;\underline{\mathtt{drop}}\,{}^{\Sigma}_{X}\ (\ell)\,; x_j\right)}$$

By $!$-L and $\forall$-L, it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \delta.\mathsf{sel}(s_j).\mathsf{semty}(w) \equiv \triangleright \mathcal{V}[\![T_j]\!]^{\varsigma}_{F}(w_{s_j}) \\ @_\ell\left(\mathit{size}\,(\ell,\ 1 + |\mathrm{dom}(\delta.\mathsf{sel})|) \star \bigstar_{s \in \mathrm{dom}(\delta.\mathsf{sel})}\ \ell + 1 + \delta.\mathsf{sel}(s).\mathsf{off} \mapsto w_s \star \delta.\mathsf{sel}(s).\mathsf{semty}(w_s)\right)\end{array}}{\mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}\left(\mathtt{const}\ x_j = *\left(\ell + \underline{\mathtt{sel}}\,{}^{s_j}_{\Sigma.X} + 1\right);\ \underline{\mathtt{dup}}_{T_j}\ (x_j)\,;\underline{\mathtt{drop}}\,{}^{\Sigma}_{X}\ (\ell)\,; x_j\right)}$$

By $!$-$\equiv$, $!$-unr, $@$-$!$, and $\equiv$-l to use $\equiv$ to rewrite under the $@_\ell$, then $\triangleright$-R, $\triangleright$-$\star$, and $@$-$\triangleright$, it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \delta.\mathsf{sel}(s_j).\mathsf{semty}(w) \equiv \triangleright \mathcal{V}[\![T_j]\!]^{\varsigma}_{F}(w_{s_j}) \\ \triangleright @_\ell\left(\begin{array}{ll} & \mathit{size}\,(\ell,\ 1 + |\mathrm{dom}(\delta.\mathsf{sel})|) \\ \star & \mathcal{V}[\![T_j]\!]^{\varsigma}_{F'}(w_{s_j}) \\ \star & \ell + 1 + \delta.\mathsf{sel}(s_j).\mathsf{off} \mapsto w_{s_j} \\ \star & \bigstar_{s \in \mathrm{dom}(\delta.\mathsf{sel}) \setminus s_j}\ \ell + 1 + \delta.\mathsf{sel}(s).\mathsf{off} \mapsto w_s \star \delta.\mathsf{sel}(s).\mathsf{semty}(w_s)\end{array}\right)\end{array}}{\mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}\left(\mathtt{const}\ x_j = *\left(\ell + \underline{\mathtt{sel}}\,{}^{s_j}_{\Sigma.X} + 1\right);\ \underline{\mathtt{dup}}_{T_j}\ (x_j)\,;\underline{\mathtt{drop}}\,{}^{\Sigma}_{X}\ (\ell)\,; x_j\right)}$$

By two uses of WP-BOP and also SEL with $!$-UNR, all interspersed with WP-BIND, $\triangleright$-R, and $\triangleright$-MONO (to strip the $\triangleright$), it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \delta.\mathrm{sel}(s_j).\mathrm{semty}(w) \equiv \triangleright \mathcal{V}[\![T_j]\!]^{\varsigma}_{F}(w_{s_j}) \\ @_\ell \left(\begin{array}{ll} & \mathit{size}(\ell,\ 1+|\mathrm{dom}(\delta.\mathrm{sel})|) \\ \star & \mathcal{V}[\![T_j]\!]^{\varsigma}_{F'}(w_{s_j}) \\ \star & \ell+1+\delta.\mathrm{sel}(s_j).\mathrm{off} \mapsto w_{s_j} \\ \star & \bigstar_{s\in\mathrm{dom}(\delta.\mathrm{sel})\setminus s_j} \ell+1+\delta.\mathrm{sel}(s).\mathrm{off}\mapsto w_s \star \delta.\mathrm{sel}(s).\mathrm{semty}(w_s)\end{array}\right)\end{array}}{\mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}\left(\mathtt{const}\ x_j\ = *(\ell+\delta.\mathrm{sel}(s_j).\mathrm{off}+1);\ \underline{\mathtt{dup}}_{T_j}(x_j);\underline{\mathtt{drop}}^{\Sigma}_{X}(\ell);x_j\right)}$$

By WP-LET and WP-LOAD with $\diamond$-@ and $\diamond$-DROP, interspersed with WP-BIND and $\triangleright$-R, it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \delta.\mathrm{sel}(s_j).\mathrm{semty}(w) \equiv \triangleright \mathcal{V}[\![T_j]\!]^{\varsigma}_{F}(w_{s_j}) \\ @_\ell \left(\begin{array}{ll} & \mathit{size}(\ell,\ 1+|\mathrm{dom}(\delta.\mathrm{sel})|) \\ \star & \mathcal{V}[\![T_j]\!]^{\varsigma}_{F'}(w_{s_j}) \\ \star & \ell+1+\delta.\mathrm{sel}(s_j).\mathrm{off} \mapsto w_{s_j} \\ \star & \bigstar_{s\in\mathrm{dom}(\delta.\mathrm{sel})\setminus s_j} \ell+1+\delta.\mathrm{sel}(s).\mathrm{off}\mapsto w_s \star \delta.\mathrm{sel}(s).\mathrm{semty}(w_s)\end{array}\right)\end{array}}{\mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}\left(\underline{\mathtt{dup}}_{T_j}\left(w_{s_j}\right);\underline{\mathtt{drop}}^{\Sigma}_{X}(\ell);w_{s_j}\right)}$$

By WP-SEQ and DUP with $\diamond$-@ and $\diamond$-DROP, followed by WP-RAMIFY and $\triangleright$-R, it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \delta.\mathrm{sel}(s_j).\mathrm{semty}(w) \equiv \triangleright \mathcal{V}[\![T_j]\!]^{\varsigma}_{F}(w_{s_j}) \\ \mathcal{V}[\![T_j]\!]^{\varsigma}_{F'}(w_{s_j}) \quad @_\ell \left(\begin{array}{ll} & \mathit{size}(\ell,\ 1+|\mathrm{dom}(\delta.\mathrm{sel})|) \\ \star & \mathcal{V}[\![T_j]\!]^{\varsigma}_{F'}(w_{s_j}) \\ \star & \ell+1+\delta.\mathrm{sel}(s_j).\mathrm{off} \mapsto w_{s_j} \\ \star & \bigstar_{s\in\mathrm{dom}(\delta.\mathrm{sel})\setminus s_j} \ell+1+\delta.\mathrm{sel}(s).\mathrm{off}\mapsto w_s \star \delta.\mathrm{sel}(s).\mathrm{semty}(w_s)\end{array}\right)\end{array}}{\mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}\left(\underline{\mathtt{drop}}^{\Sigma}_{X}(\ell);w_{s_j}\right)}$$

By $!$-$\equiv$, @-$!$, and $\equiv$-L, along with @-MONO and $\triangleright$-R, we can once again use $\equiv$ to rewrite under the $@_\ell$. It therefore suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \mathcal{V}[\![T_j]\!]^{\varsigma}_{F'}(w_{s_j}) \\ @_\ell \left(\mathit{size}(\ell,\ 1+|\mathrm{dom}(\delta.\mathrm{sel})|) \star \bigstar_{s\in\mathrm{dom}(\delta.\mathrm{sel})} \ell+1+\delta.\mathrm{sel}(s).\mathrm{off}\mapsto w_s \star \delta.\mathrm{sel}(s).\mathrm{semty}(w_s)\right)\end{array}}{\mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}\left(\underline{\mathtt{drop}}^{\Sigma}_{X}(\ell);w_{s_j}\right)}$$

By @-$\exists$ and $\star$-$\exists$, and folding $\mathcal{V}[\![-]\!]$ (using H4), $\mathcal{R}[\![-]\!]$, $\mathcal{O}[\![-]\!]$, and $\delta.\mathrm{obj}$ with H5 and H6, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \mathcal{V}[\![T_j]\!]^{\varsigma}_{F'}(w_{s_j}) \quad \mathcal{V}[\![X]\!]^{\varsigma}_{F'}(\ell)}{\mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}\left(\underline{\mathtt{drop}}^{\Sigma}_{X}(\ell);w_{s_j}\right)}$$

By WP-SEQ and DROP, followed by WP-RAMIFY and $\triangleright$-R, it suffices if

$$\frac{\mathcal{V}[\![T_j]\!]^{\varsigma}_{F'}(w_{s_j})}{\mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}\left(w_{s_j}\right)}$$

which follows by LR-VAL. $\square$

Lemma F.119 (comp-I-enum-compat).

(comp-I-enum-compat)

$$\frac{\Sigma \ni \mathsf{m}\ \mathsf{enum}\ \mathsf{X}\ \{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\} \qquad \Sigma; \Gamma \vDash_{\mathsf{F}} \mathsf{e_j} : \mathsf{T_j}}{\Sigma; \Gamma \vDash_{\mathsf{F}} \mathtt{const}\ \mathtt{x} = \mathtt{malloc}\,(3);\ *\mathtt{x} = 1;\ *(\mathtt{x}+1) = \underline{\mathtt{sel}}\,{}^{\mathsf{s_j}}_{\Sigma.\mathsf{X}};\ *(\mathtt{x}+2) = \mathsf{e_j};\ \mathtt{x} : \mathsf{X}}$$

Proof. Unfold $\vDash$ and consider $\mathsf{F}' \supseteq \mathsf{F}, \varsigma, \gamma^{(H1)}$. Assume the premises $\Sigma \ni \mathsf{m}\ \mathsf{struct}\ \mathsf{X}\ \{\overline{\mathsf{s_i} : \mathsf{T}}^{i<n}\}^{(H2)}$ and $\Sigma; \Gamma \vDash_{\mathsf{F}} \mathsf{e_j} : \mathsf{T_j}^{(H3)}$. We must show

$$\frac{\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}'}(\varsigma) \qquad \mathcal{C}[\![\Gamma]\!]^{\varsigma}_{\mathsf{F}'}(\gamma)}{\mathcal{E}[\![\mathsf{X}]\!]^{\varsigma}_{\mathsf{F}'}\left(\mathtt{const}\ \mathtt{x} = \mathtt{malloc}\,(3);\ *\mathtt{x} = 1;\ *(\mathtt{x}+1) = \underline{\mathtt{sel}}\,{}^{\mathsf{s_j}}_{\Sigma.\mathsf{X}};\ *(\mathtt{x}+2) = \mathsf{e_j}[\gamma];\ \mathtt{x}\right)}$$

By Signature Substitution Unrestricted and ! -unr, then H3 with H1, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}'}(\varsigma) \qquad \mathcal{E}[\![\mathsf{T_j}]\!]^{\varsigma}_{\mathsf{F}'}(\mathsf{e_j}[\gamma])}{\mathcal{E}[\![\mathsf{X}]\!]^{\varsigma}_{\mathsf{F}'}\left(\mathtt{const}\ \mathtt{x} = \mathtt{malloc}\,(3);\ *\mathtt{x} = 1;\ *(\mathtt{x}+1) = \underline{\mathtt{sel}}\,{}^{\mathsf{s_j}}_{\Sigma.\mathsf{X}};\ *(\mathtt{x}+2) = \mathsf{e_j}[\gamma];\ \mathtt{x}\right)}$$

By wp-malloc, wp-store, and wp-bop, all interspersed with wp-bind and $\triangleright$ -R, it suffices if for any $\ell \in \mathsf{Loc}_{\mathbb{N}^+}{}^{(H4)}$

$$\frac{\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}'}(\varsigma) \quad \mathcal{E}[\![\mathsf{T_j}]\!]^{\varsigma}_{\mathsf{F}'}(\mathsf{e_j}[\gamma]) \quad \mathit{size}\,(\ell,\ 3) \quad \ell \mapsto 1 \quad \ell+1 \mapsto ☣ \quad \ell+2 \mapsto ☣}{\mathcal{E}[\![\mathsf{X}]\!]^{\varsigma}_{\mathsf{F}'}\left(*(\ell+1) = \underline{\mathtt{sel}}\,{}^{\mathsf{s_j}}_{\Sigma.\mathsf{X}};\ *(\ell+2) = \mathsf{e_j}[\gamma];\ \ell\right)}$$

Note that by H2, ! -unr and unfolding $\mathcal{S}[\![-]\!]$, there is some $\delta = \varsigma(\mathsf{X})^{(H5)}$. Since the mode of X is indeterminate, by H5, we have we have $\delta.\mathsf{kind} = \mathsf{enum}^{(H6)}$ and it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{\mathsf{F}'}(\varsigma) \quad !\,\forall\ i < n, \mathtt{w}.\ \delta.\mathsf{sel}(\mathsf{s_i}).\mathsf{semty}(\mathtt{w}) \equiv \triangleright\,\mathcal{V}[\![\mathsf{T_i}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}) \\ \mathcal{E}[\![\mathsf{T_j}]\!]^{\varsigma}_{\mathsf{F}'}(\mathsf{e_j}[\gamma]) \quad \mathit{size}\,(\ell,\ 3) \quad \ell \mapsto 1 \quad \ell+1 \mapsto ☣ \quad \ell+2 \mapsto ☣\end{array}}{\mathcal{E}[\![\mathsf{X}]\!]^{\varsigma}_{\mathsf{F}'}\left(*(\ell+1) = \underline{\mathtt{sel}}\,{}^{\mathsf{s_j}}_{\Sigma.\mathsf{X}};\ *(\ell+2) = \mathsf{e_j}[\gamma];\ \ell\right)}$$

Then by wp-bind and sel with H5, it suffices if

$$\frac{\begin{array}{c}!\,\forall\ i < n, \mathtt{w}.\ \delta.\mathsf{sel}(\mathsf{s_i}).\mathsf{semty}(\mathtt{w}) \equiv \triangleright\,\mathcal{V}[\![\mathsf{T_i}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}) \\ \mathcal{E}[\![\mathsf{T_j}]\!]^{\varsigma}_{\mathsf{F}'}(\mathsf{e_j}[\gamma]) \quad \mathit{size}\,(\ell,\ 3) \quad \ell \mapsto 1 \quad \ell+1 \mapsto ☣ \quad \ell+2 \mapsto ☣\end{array}}{\mathcal{E}[\![\mathsf{X}]\!]^{\varsigma}_{\mathsf{F}'}\left(*(\ell+1) = \delta.\mathsf{sel}(\mathsf{s_j}).\mathsf{off};\ *(\ell+2) = \mathsf{e_j}[\gamma];\ \ell\right)}$$

By wp-store and wp-bop interspersed with wp-bind and $\triangleright$ -R, it suffices if

$$\frac{\begin{array}{c}!\,\forall\ i < n, \mathtt{w}.\ \delta.\mathsf{sel}(\mathsf{s_i}).\mathsf{semty}(\mathtt{w}) \equiv \triangleright\,\mathcal{V}[\![\mathsf{T_i}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w}) \\ \mathcal{E}[\![\mathsf{T_j}]\!]^{\varsigma}_{\mathsf{F}'}(\mathsf{e_j}[\gamma]) \quad \mathit{size}\,(\ell,\ 3) \quad \ell \mapsto 1 \quad \ell+1 \mapsto \delta.\mathsf{sel}(\mathsf{s_j}).\mathsf{off} \quad \ell+2 \mapsto ☣\end{array}}{\mathcal{E}[\![\mathsf{X}]\!]^{\varsigma}_{\mathsf{F}'}\left(*(\ell+2) = \mathsf{e_j}[\gamma];\ \ell\right)}$$

By lr-bind, then ! -L and $\forall$ -L, it suffices if for any $\mathtt{w_j}$

$$\frac{\begin{array}{c}\delta.\mathsf{sel}(\mathsf{s_j}).\mathsf{semty}(\mathtt{w}) \equiv \triangleright\,\mathcal{V}[\![\mathsf{T_j}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w_j}) \\ \mathcal{V}[\![\mathsf{T_j}]\!]^{\varsigma}_{\mathsf{F}'}(\mathtt{w_j}) \quad \mathit{size}\,(\ell,\ 3) \quad \ell \mapsto 1 \quad \ell+1 \mapsto \delta.\mathsf{sel}(\mathsf{s_j}).\mathsf{off} \quad \ell+2 \mapsto ☣\end{array}}{\mathcal{E}[\![\mathsf{X}]\!]^{\varsigma}_{\mathsf{F}'}\left(*(\ell+2) = \mathtt{w_j};\ \ell\right)}$$

By wp-store, $\triangleright$ -R, and lr-val, it suffices if

$$\frac{\begin{array}{c}\delta.\mathsf{sel}(\mathsf{s_j}).\mathsf{semty}(\mathtt{w}) \equiv \triangleright\,\mathcal{V}[\![\mathsf{T_j}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w_j}) \\ \mathcal{V}[\![\mathsf{T_j}]\!]^{\varsigma}_{\mathsf{F}'}(\mathtt{w_j}) \quad \mathit{size}\,(\ell,\ 3) \quad \ell \mapsto 1 \quad \ell+1 \mapsto \delta.\mathsf{sel}(\mathsf{s_j}).\mathsf{off} \quad \ell+2 \mapsto \mathtt{w_j}\end{array}}{\mathcal{V}[\![\mathsf{X}]\!]^{\varsigma}_{\mathsf{F}'}(\ell)}$$

By WP-SHARE, $\mathcal{V}[\![-]\!]$ with H4, $\mathcal{R}[\![-]\!]$, $\mathcal{O}[\![-]\!]$, and H5, it suffices if

$$\frac{\delta.\mathsf{sel}(\mathsf{s_j}).\mathsf{semty}(\mathtt{w}) \equiv \triangleright \mathcal{V}[\![\mathsf{T_j}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w_j}) \quad @_\ell\ (\mathcal{V}[\![\mathsf{T_j}]\!]^{\varsigma}_{\mathsf{F'}}(\mathtt{w_j}) \star \mathit{size}\,(\ell,\ 3) \star \ell+1 \mapsto \delta.\mathsf{sel}(\mathsf{s_j}).\mathsf{off} \star \ell+2 \mapsto \mathtt{w_j})}{@_\ell\ \varsigma(\mathsf{X}).\mathsf{obj}(\ell+1)}$$

By !-≡, @-!, and @-MONO with $\delta.\mathsf{obj}$ and H6, it suffices if

$$\frac{\delta.\mathsf{sel}(\mathsf{s_j}).\mathsf{semty}(\mathtt{w}) \equiv \triangleright \mathcal{V}[\![\mathsf{T_j}]\!]^{\varsigma}_{\mathsf{F}}(\mathtt{w_j}) \quad \mathcal{V}[\![\mathsf{T_j}]\!]^{\varsigma}_{\mathsf{F'}}(\mathtt{w_j}) \quad \mathit{size}\,(\ell,\ 3) \quad \ell+1 \mapsto \delta.\mathsf{sel}(\mathsf{s_j}).\mathsf{off} \quad \ell+2 \mapsto \mathtt{w_j}}{\mathit{size}\,(\ell,\ 3) \quad \bigvee_{\mathsf{s}\in\mathrm{dom}(\delta.\mathsf{sel})} \ell+1 \mapsto \delta.\mathsf{sel}(\mathsf{s}).\mathsf{off} \star \exists\, \mathtt{w_s}.\ \ell+2 \mapsto \mathtt{w_s} \star \delta.\mathsf{sel}(\mathsf{s}).\mathsf{semty}(\mathtt{w_s})}$$

which holds by selecting $\mathsf{s_j}$ and applying ≡-L with ▷-R. □

LEMMA F.120 (COMP-E-enum-COMPAT).

(*COMP-E-enum-COMPAT*)

$$\frac{\Sigma \ni \mathsf{rigid\ enum\ X}\,\{\overline{\mathsf{s_i} : \mathsf{T}}^{i<n}\} \quad \Sigma;\Gamma_1 \vDash_{\mathsf{F}} \mathsf{e} : \mathsf{X} \quad \overline{\Sigma;\Gamma_2,\mathsf{x_i} : \mathsf{T_i} \vDash_{\mathsf{F}} \mathsf{e_i} : \mathsf{T_i}}^{i<n} \quad \Gamma_2 \not\ni \overline{\mathsf{x_i}}^{i<n}}{\Sigma;\Gamma_1,\Gamma_2 \vDash_{\mathsf{F}} \left\{\begin{array}{l}\mathtt{const\ x = e;}\\ \mathtt{const\ y = *(x+1);}\\ \overline{\mathtt{if\ (y = i)}\ \left\{\mathtt{const\ x_i = *(x+2);}\ \underline{\mathtt{dup}}_{\mathsf{T_i}}(\mathtt{x_i});\underline{\mathtt{drop}}^{\Sigma}_{\mathsf{X}}(\mathtt{x});\mathtt{e_i}\right\}}^{i}\\ \mathtt{else\ \{havoc\}}\end{array}\right\} : \mathsf{T}}$$

PROOF. Unfold ⊨ and consider $\mathsf{F'} \supseteq \mathsf{F}, \varsigma, \gamma^{(H1)}$. Also, assume that $\Sigma \ni \mathsf{rigid\ enum\ X}\,\{\overline{\mathsf{s_i} : \mathsf{T_i}}^{i<n}\}^{(H2)}$, $\Sigma;\Gamma_1 \vDash_{\mathsf{F}} \mathsf{e} : \mathsf{X}^{(H3)}$ $\overline{\Sigma;\Gamma_2,\mathsf{x_i} : \mathsf{T_i} \vDash_{\mathsf{F}} \mathsf{e_i} : \mathsf{T}}^{i<n\,(H4)}$. We must show

$$\frac{\mathcal{S}[\![\Sigma]\!]_{\mathsf{F'}}(\varsigma) \quad \mathcal{C}[\![\Gamma_1,\Gamma_2]\!]^{\varsigma}_{\mathsf{F'}}(\gamma)}{\mathcal{E}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F'}}\left(\begin{array}{l}\mathtt{const\ x = e}[\gamma]\mathtt{;}\\ \mathtt{const\ y = *(x+1);}\\ \overline{\mathtt{if\ (y = i)}\ \left\{\mathtt{const\ x_i = *(x+2);}\ \underline{\mathtt{dup}}_{\mathsf{T_i}}(\mathtt{x_i});\underline{\mathtt{drop}}^{\Sigma}_{\mathsf{X}}(\mathtt{x});\mathtt{e_i}[\gamma \setminus \mathtt{x_i}]\right\}}^{i}\\ \mathtt{else\ \{havoc\}}\end{array}\right)}$$

By $\mathcal{C}$-SPLIT and n applications of ∧-R with $\mathcal{C}$-CONS (with !-UNR as needed), it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{\mathsf{F'}}(\varsigma) \quad \mathcal{C}[\![\Gamma_1]\!]^{\varsigma}_{\mathsf{F'}}(\gamma) \quad \bigwedge_{i<n} \forall\, \mathtt{w_i}.\ \mathcal{V}[\![\mathsf{T_i}]\!]^{\varsigma}_{\mathsf{F'}}(\mathtt{w_i}) \mathrel{-\!\!\star} (\mathcal{S}[\![\Sigma]\!]_{\mathsf{F'}}(\varsigma) \star \mathcal{C}[\![\Gamma_2,\mathsf{x_i} : \mathsf{T_i}]\!]^{\varsigma}_{\mathsf{F'}}(\gamma[\mathtt{w_i}/\mathtt{x_i}]))}{\mathcal{E}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F'}}\left(\begin{array}{l}\mathtt{const\ x = e}[\gamma]\mathtt{;}\\ \mathtt{const\ y = *(x+1);}\\ \overline{\mathtt{if\ (y = i)}\ \left\{\mathtt{const\ x_i = *(x+2);}\ \underline{\mathtt{dup}}_{\mathsf{T_i}}(\mathtt{x_i});\underline{\mathtt{drop}}^{\Sigma}_{\mathsf{X}}(\mathtt{x});\mathtt{e_i}[\gamma \setminus \mathtt{x_i}]\right\}}^{i}\\ \mathtt{else\ \{havoc\}}\end{array}\right)}$$

Simplify with the observation that $(\gamma\setminus\mathtt{x_i})[\mathtt{w_i}/\mathtt{x_i}] = \gamma[\mathtt{w_i}/\mathtt{x_i}]$, since $\mathtt{w_i}$ will take priority as the value for $\mathtt{x_i}$ in the parallel substitution, regardless of whether $\mathtt{x_i}$ is in γ. By SIGNATURE SUBSTITUTION UNRESTRICTED and !-UNR, then H3 with H1 and ⊨, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{\mathsf{F'}}(\varsigma) \quad \mathcal{E}[\![\mathsf{X}]\!]^{\varsigma}_{\mathsf{F'}}(\mathtt{e}[\gamma]) \quad \bigwedge_{i<n} \forall\, \mathtt{w_i}.\ \mathcal{V}[\![\mathsf{T_i}]\!]^{\varsigma}_{\mathsf{F'}}(\mathtt{w_i}) \mathrel{-\!\!\star} \mathcal{E}[\![\mathsf{T_i}]\!]^{\varsigma}_{\mathsf{F'}}(\mathtt{e_i}[\gamma \setminus \mathtt{x_i}][\mathtt{w_i}/\mathtt{x_i}])}{\mathcal{E}[\![\mathsf{T}]\!]^{\varsigma}_{\mathsf{F'}}\left(\begin{array}{l}\mathtt{const\ x = e}[\gamma]\mathtt{;}\\ \mathtt{const\ y = *(x+1);}\\ \overline{\mathtt{if\ (y = i)}\ \left\{\mathtt{const\ x_i = *(x+2);}\ \underline{\mathtt{dup}}_{\mathsf{T_i}}(\mathtt{x_i});\underline{\mathtt{drop}}^{\Sigma}_{\mathsf{X}}(\mathtt{x});\mathtt{e_i}[\gamma \setminus \mathtt{x_i}]\right\}}^{i}\\ \mathtt{else\ \{havoc\}}\end{array}\right)}$$

By LR-BIND, $\mathcal{V}[\![-]\!]$, $\mathcal{R}[\![-]\!]$, and $\mathcal{O}[\![-]\!]$, it suffices if for any $\ell \in \mathsf{Loc}_{\mathbb{N}^+}{}^{(\mathrm{H5})}$

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad @_\ell\, \varsigma(X).\mathsf{obj}(\ell+1) \quad \bigwedge_{i<n} \forall\, w_i.\ \mathcal{V}[\![T_i]\!]^{\varsigma}_{F'}(w_i) \mathrel{-\!\!\star} \mathcal{E}[\![T_i]\!]^{\varsigma}_{F'}(e_i[\gamma \setminus x_i][w_i/x_i])}{\mathcal{E}[\![X]\!]^{\varsigma}_{F'}\left(\begin{array}{l}\texttt{const x = }\ell;\\ \texttt{const y = *(x + 1);}\\ \overline{\texttt{if (y = i) }\left\{\texttt{const x}_i\texttt{ = *(x + 2); }\underline{\texttt{dup}}_{T_i}(x_i);\underline{\texttt{drop}}^{\Sigma}_{X}(x);e_i[\gamma\setminus x_i]\right\}}^{i<n}\\ \texttt{else \{havoc\}}\end{array}\right)}$$

By WP-LET and WP-BOP interspersed with WP-BIND and $\triangleright$ -R, it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad @_\ell\, \varsigma(X).\mathsf{obj}(\ell+1) \quad \bigwedge_{i<n} \forall\, w_i.\ \mathcal{V}[\![T_i]\!]^{\varsigma}_{F'}(w_i) \mathrel{-\!\!\star} \mathcal{E}[\![T_i]\!]^{\varsigma}_{F'}(e_i[\gamma \setminus x_i][w_i/x_i])}{\mathcal{E}[\![X]\!]^{\varsigma}_{F'}\left(\begin{array}{l}\texttt{const y = *(}\ell\texttt{ + 1);}\\ \overline{\texttt{if (y = i) }\left\{\texttt{const x}_i\texttt{ = *(}\ell\texttt{ + 2); }\underline{\texttt{dup}}_{T_i}(x_i);\underline{\texttt{drop}}^{\Sigma}_{X}(\ell);e_i[\gamma\setminus x_i]\right\}}^{i<n}\\ \texttt{else \{havoc\}}\end{array}\right)}$$

Note that by H2, ! -UNR and unfolding $\mathcal{S}[\![-]\!]$, there is some $\delta = \varsigma(X)^{(\mathrm{H6})}$. Since the mode of X is rigid, by H6, we have we have $\delta.\mathsf{kind} = \mathsf{enum}^{(\mathrm{H7})}$, $n = |\mathsf{dom}(\delta.\mathsf{sel})|^{(\mathrm{H8})}$, $\forall\, i < n.\ \delta.\mathsf{sel}(s_i).\mathsf{off} = i^{(\mathrm{H9})}$, and it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad !\,\forall\, i < n, w.\ \delta.\mathsf{sel}(s_i).\mathsf{semty}(w) \equiv \triangleright\, \mathcal{V}[\![T_i]\!]^{\varsigma}_{F}(w)\\ \mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad @_\ell\, \varsigma(X).\mathsf{obj}(\ell+1) \quad \bigwedge_{i<n} \forall\, w_i.\ \mathcal{V}[\![T_i]\!]^{\varsigma}_{F'}(w_i) \mathrel{-\!\!\star} \mathcal{E}[\![T_i]\!]^{\varsigma}_{F'}(e_i[\gamma \setminus x_i][w_i/x_i])\end{array}}{\mathcal{E}[\![X]\!]^{\varsigma}_{F'}\left(\begin{array}{l}\texttt{const y = *(}\ell\texttt{ + 1);}\\ \overline{\texttt{if (y = i) }\left\{\texttt{const x}_i\texttt{ = *(}\ell\texttt{ + 2); }\underline{\texttt{dup}}_{T_i}(x_i);\underline{\texttt{drop}}^{\Sigma}_{X}(\ell);e_i[\gamma\setminus x_i]\right\}}^{i<n}\\ \texttt{else \{havoc\}}\end{array}\right)}$$

Then by δ.obj with H7 and H6, and simplifying with ! -*size* $(-, -)$ and @ -! , it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad !\,\forall\, i < n, w.\ \delta.\mathsf{sel}(s_i).\mathsf{semty}(w) \equiv \triangleright\, \mathcal{V}[\![T_i]\!]^{\varsigma}_{F}(w)\\ @_\ell\left(\bigvee_{s\in\mathsf{dom}(\delta.\mathsf{sel})} \ell+1 \mapsto \delta.\mathsf{sel}(s).\mathsf{off} \star \exists\, w_s.\ \ell+2 \mapsto w_s \star \delta.\mathsf{sel}(s).\mathsf{semty}(w_s)\right)\\ \mathit{size}\,(\ell,\ 3) \quad \bigwedge_{i<n} \forall\, w_i.\ \mathcal{V}[\![T_i]\!]^{\varsigma}_{F'}(w_i) \mathrel{-\!\!\star} \mathcal{E}[\![T_i]\!]^{\varsigma}_{F'}(e_i[\gamma \setminus x_i][w_i/x_i])\end{array}}{\mathcal{E}[\![X]\!]^{\varsigma}_{F'}\left(\begin{array}{l}\texttt{const y = *(}\ell\texttt{ + 1);}\\ \overline{\texttt{if (y = i) }\left\{\texttt{const x}_i\texttt{ = *(}\ell\texttt{ + 2); }\underline{\texttt{dup}}_{T_i}(x_i);\underline{\texttt{drop}}^{\Sigma}_{X}(\ell);e_i[\gamma\setminus x_i]\right\}}^{i<n}\\ \texttt{else \{havoc\}}\end{array}\right)}$$

By @ -$\vee$, $\vee$-L, and H8, we have $n > 0^{(\mathrm{H10})}$ cases; if $n = 0$, then the disjunct under the jump is false, and we apply @ -$\bot$ (which is the expected nullary generalization of @ -$\vee$). Simplifying with ! -UNR ! -L, $\forall$ -L, ! -$\equiv$, @ -! , and $\equiv$-L to use $\equiv$ to rewrite under the $@_\ell$, then applying @ -$\exists$, it suffices if for any $j < n$ and w_j

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma)\\ !\,\forall\, i < n, w.\ \delta.\mathsf{sel}(s_i).\mathsf{semty}(w) \equiv \triangleright\, \mathcal{V}[\![T_i]\!]^{\varsigma}_{F}(w) \quad @_\ell\left(\ell+1 \mapsto j \star \ell+2 \mapsto w_j \star \triangleright\, \mathcal{V}[\![T_j]\!]^{\varsigma}_{F'}(w_j)\right)\\ \mathit{size}\,(\ell,\ 3) \quad \mathcal{V}[\![T_j]\!]^{\varsigma}_{F'}(w_j) \mathrel{-\!\!\star} \mathcal{E}[\![T_j]\!]^{\varsigma}_{F'}(e_j[\gamma \setminus x_j][w_j/x_j])\end{array}}{\mathcal{E}[\![X]\!]^{\varsigma}_{F'}\left(\begin{array}{l}\texttt{const y = *(}\ell\texttt{ + 1);}\\ \overline{\texttt{if (y = i) }\left\{\texttt{const x}_i\texttt{ = *(}\ell\texttt{ + 2); }\underline{\texttt{dup}}_{T_i}(x_i);\underline{\texttt{drop}}^{\Sigma}_{X}(\ell);e_i[\gamma\setminus x_i]\right\}}^{i<n}\\ \texttt{else \{havoc\}}\end{array}\right)}$$

By WP-LOAD—with $\diamond$-@ and $\diamond$-DROP—and WP-LET, interspersed with WP-BIND, it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \\ !\,\forall\, i < n, \mathtt{w}.\ \delta.\mathsf{sel}(\mathtt{s}_i).\mathsf{semty}(\mathtt{w}) \equiv \triangleright\, \mathcal{V}[\![\mathtt{T}_i]\!]^{\varsigma}_{F}(\mathtt{w}) \quad @_\ell\ (\ell+1 \mapsto \mathtt{j} \star \ell+2 \mapsto \mathtt{w}_j \star \triangleright\, \mathcal{V}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{w}_j)) \\ \mathit{size}\,(\ell,\ 3) \quad \mathcal{V}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{w}_j) \mathrel{-\!\!\star} \mathcal{E}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{e}_j[\gamma \setminus \mathtt{x}_j][\mathtt{w}_j/\mathtt{x}_j])\end{array}}{\mathcal{E}[\![\mathtt{X}]\!]^{\varsigma}_{F'}\left(\overline{\mathtt{if}\ (\mathtt{j} = \mathtt{i})\ \left\{\mathtt{const}\ \mathtt{x}_i = *(\ell+2);\ \underline{\mathtt{dup}}_{\mathtt{T}_i}(\mathtt{x}_i)\,;\underline{\mathtt{drop}}^{\Sigma}_{\mathtt{X}}(\ell)\,;\mathtt{e}_i[\gamma \setminus \mathtt{x}_i]\right\}}^{i<n}\ \mathtt{else}\ \{\mathtt{havoc}\}\right)}$$

By @-MONO, $\triangleright$-R, $\triangleright$-$\star$, and @-$\triangleright$, it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \\ !\,\forall\, i < n, \mathtt{w}.\ \delta.\mathsf{sel}(\mathtt{s}_i).\mathsf{semty}(\mathtt{w}) \equiv \triangleright\, \mathcal{V}[\![\mathtt{T}_i]\!]^{\varsigma}_{F}(\mathtt{w}) \quad \triangleright\, @_\ell\ (\ell+1 \mapsto \mathtt{j} \star \ell+2 \mapsto \mathtt{w}_j \star \mathcal{V}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{w}_j)) \\ \mathit{size}\,(\ell,\ 3) \quad \mathcal{V}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{w}_j) \mathrel{-\!\!\star} \mathcal{E}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{e}_j[\gamma \setminus \mathtt{x}_j][\mathtt{w}_j/\mathtt{x}_j])\end{array}}{\mathcal{E}[\![\mathtt{X}]\!]^{\varsigma}_{F'}\left(\overline{\mathtt{if}\ (\mathtt{j} = \mathtt{i})\ \left\{\mathtt{const}\ \mathtt{x}_i = *(\ell+2);\ \underline{\mathtt{dup}}_{\mathtt{T}_i}(\mathtt{x}_i)\,;\underline{\mathtt{drop}}^{\Sigma}_{\mathtt{X}}(\ell)\,;\mathtt{e}_i[\gamma \setminus \mathtt{x}_i]\right\}}^{i<n}\ \mathtt{else}\ \{\mathtt{havoc}\}\right)}$$

By $\max(j-1, 0)$ applications of WP-BOP and WP-IF-F, and then one more application of WP-BOP, interspersed with WP-BIND, $\triangleright$-R, and $\triangleright$-MONO (to strip the $\triangleright$, recalling H10), it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \\ !\,\forall\, i < n, \mathtt{w}.\ \delta.\mathsf{sel}(\mathtt{s}_i).\mathsf{semty}(\mathtt{w}) \equiv \triangleright\, \mathcal{V}[\![\mathtt{T}_i]\!]^{\varsigma}_{F}(\mathtt{w}) \quad @_\ell\ (\ell+1 \mapsto \mathtt{j} \star \ell+2 \mapsto \mathtt{w}_j \star \mathcal{V}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{w}_j)) \\ \mathit{size}\,(\ell,\ 3) \quad \mathcal{V}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{w}_j) \mathrel{-\!\!\star} \mathcal{E}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{e}_j[\gamma \setminus \mathtt{x}_j][\mathtt{w}_j/\mathtt{x}_j])\end{array}}{\mathcal{E}[\![\mathtt{X}]\!]^{\varsigma}_{F'}\left(\mathtt{if}\ (1)\ \left\{\mathtt{const}\ \mathtt{x}_j = *(\ell+2);\ \underline{\mathtt{dup}}_{\mathtt{T}_j}(\mathtt{x}_j)\,;\underline{\mathtt{drop}}^{\Sigma}_{\mathtt{X}}(\ell)\,;\mathtt{e}_j[\gamma \setminus \mathtt{x}_j]\right\}\ \overline{\mathtt{else}\ \{\cdots\}}^{n-j}\ \mathtt{else}\ \{\mathtt{havoc}\}\right)}$$

By WP-IF-T, and WP-BOP, all interspersed with WP-BIND, and $\triangleright$-R, it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \\ !\,\forall\, i < n, \mathtt{w}.\ \delta.\mathsf{sel}(\mathtt{s}_i).\mathsf{semty}(\mathtt{w}) \equiv \triangleright\, \mathcal{V}[\![\mathtt{T}_i]\!]^{\varsigma}_{F}(\mathtt{w}) \quad @_\ell\ (\ell+1 \mapsto \mathtt{j} \star \ell+2 \mapsto \mathtt{w}_j \star \mathcal{V}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{w}_j)) \\ \mathit{size}\,(\ell,\ 3) \quad \mathcal{V}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{w}_j) \mathrel{-\!\!\star} \mathcal{E}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{e}_j[\gamma \setminus \mathtt{x}_j][\mathtt{w}_j/\mathtt{x}_j])\end{array}}{\mathcal{E}[\![\mathtt{X}]\!]^{\varsigma}_{F'}\left(\mathtt{const}\ \mathtt{x}_j = *(\ell+2);\ \underline{\mathtt{dup}}_{\mathtt{T}_j}(\mathtt{x}_j)\,;\underline{\mathtt{drop}}^{\Sigma}_{\mathtt{X}}(\ell)\,;\mathtt{e}_j[\gamma \setminus \mathtt{x}_j]\right)}$$

By WP-LOAD—with $\diamond$-@ and $\diamond$-DROP—and WP-LET, interspersed with WP-BIND, $\triangleright$-R, and $\mathrel{-\!\!\star}$-R, it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \\ !\,\forall\, i < n, \mathtt{w}.\ \delta.\mathsf{sel}(\mathtt{s}_i).\mathsf{semty}(\mathtt{w}) \equiv \triangleright\, \mathcal{V}[\![\mathtt{T}_i]\!]^{\varsigma}_{F}(\mathtt{w}) \quad @_\ell\ (\ell+1 \mapsto \mathtt{j} \star \ell+2 \mapsto \mathtt{w}_j \star \mathcal{V}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{w}_j)) \\ \mathit{size}\,(\ell,\ 3) \quad \mathcal{V}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{w}_j) \mathrel{-\!\!\star} \mathcal{E}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{e}_j[\gamma \setminus \mathtt{x}_j][\mathtt{w}_j/\mathtt{x}_j])\end{array}}{\mathcal{E}[\![\mathtt{X}]\!]^{\varsigma}_{F'}\left(\underline{\mathtt{dup}}_{\mathtt{T}_j}(\mathtt{w}_j)\,;\underline{\mathtt{drop}}^{\Sigma}_{\mathtt{X}}(\ell)\,;\mathtt{e}_j\gamma[\mathtt{w}_j/\mathtt{x}_j]\right)}$$

By WP-SEQ, DUP with $\diamond$-R, WP-RAMIFY, and $\triangleright$-R, it suffices if

$$\frac{\begin{array}{c}\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \\ !\,\forall\, i < n, \mathtt{w}.\ \delta.\mathsf{sel}(\mathtt{s}_i).\mathsf{semty}(\mathtt{w}) \equiv \triangleright\, \mathcal{V}[\![\mathtt{T}_i]\!]^{\varsigma}_{F}(\mathtt{w}) \quad @_\ell\ (\ell+1 \mapsto \mathtt{j} \star \ell+2 \mapsto \mathtt{w}_j \star \mathcal{V}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{w}_j)) \\ \mathit{size}\,(\ell,\ 3) \quad \mathcal{V}[\![\mathtt{T}_j]\!]^{\varsigma}_{F}(\mathtt{w}_j) \quad \mathcal{V}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{w}_j) \mathrel{-\!\!\star} \mathcal{E}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{e}_j[\gamma \setminus \mathtt{x}_j][\mathtt{w}_j/\mathtt{x}_j])\end{array}}{\mathcal{E}[\![\mathtt{X}]\!]^{\varsigma}_{F'}\left(\underline{\mathtt{drop}}^{\Sigma}_{\mathtt{X}}(\ell)\,;\mathtt{e}_j[\gamma \setminus \mathtt{x}_j][\mathtt{w}_j/\mathtt{x}_j]\right)}$$

Refolding with $\mathcal{V}[\![-]\!]$ (using H5), $\mathcal{R}[\![-]\!]$, δ.obj, H6, and H7 (using $\equiv$-L like above as appropriate), it suffices if

$$\frac{\mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \quad \mathcal{V}[\![\mathtt{X}]\!]^{\varsigma}_{F'}(\ell) \quad \mathcal{E}[\![\mathtt{T}_j]\!]^{\varsigma}_{F'}(\mathtt{e}_j[\gamma \setminus \mathtt{x}_j][\mathtt{w}_j/\mathtt{x}_j])}{\mathcal{E}[\![\mathtt{X}]\!]^{\varsigma}_{F'}\left(\underline{\mathtt{drop}}^{\Sigma}_{\mathtt{X}}(\ell)\,;\mathtt{e}_j[\gamma \setminus \mathtt{x}_j][\mathtt{w}_j/\mathtt{x}_j]\right)}$$

which follows by WP-SEQ, DROP, WP-RAMIFY, and $\triangleright$-R. $\square$

F.5 Library Evolution

Definition F.121 (Supported Evolution). Σ *supports evolution* to Σ' if for all Γ, e, F, T,

$$\Sigma; \Gamma \vDash_F e : T \Rightarrow \Sigma'; \Gamma \vDash_F e : T$$

LEMMA F.122 (PRESERVED SIGNATURE EVOLUTION). *Σ supports evolution to Σ' if for all F, ς,*

$$\mathcal{S}[\![\Sigma']\!]_F(\varsigma) \vDash \mathcal{S}[\![\Sigma]\!]_F(\varsigma)$$

PROOF. Assume the premise, that $\mathcal{S}[\![\Sigma']\!]_F(\varsigma) \vDash \mathcal{S}[\![\Sigma]\!]_F(\varsigma)^{(H1)}$. Unfolding Supported Evolution and $\vDash$, it suffices if for all Γ, e, F, T,

$$\begin{aligned} & \forall F' \supseteq F, \varsigma, \gamma.\ \mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \star \mathcal{C}[\![\Gamma]\!]^{\varsigma}_{F'}(\gamma) \vDash \mathcal{E}[\![T]\!]^{\varsigma}_{F'}(e[\gamma]) \\ \Rightarrow\ & \forall F' \supseteq F, \varsigma, \gamma.\ \mathcal{S}[\![\Sigma']\!]_{F'}(\varsigma) \star \mathcal{C}[\![\Gamma]\!]^{\varsigma}_{F'}(\gamma) \vDash \mathcal{E}[\![T]\!]^{\varsigma}_{F'}(e[\gamma]) \end{aligned}$$

Then assume

- $\forall F' \supseteq F, \varsigma, \gamma.\ \mathcal{S}[\![\Sigma]\!]_{F'}(\varsigma) \star \mathcal{C}[\![\Gamma]\!]^{\varsigma}_{F'}(\gamma) \vDash \mathcal{E}[\![T]\!]^{\varsigma}_{F'}(e[\gamma])^{(H2)}$

and take arbitrary $F' \supseteq F^{(H3)}$, $\varsigma^{(H4)}$, and $\gamma^{(H5)}$. It suffices if

$$\mathcal{S}[\![\Sigma']\!]_{F'}(\varsigma) \star \mathcal{C}[\![\Gamma]\!]^{\varsigma}_{F'}(\gamma) \vDash \mathcal{E}[\![T]\!]^{\varsigma}_{F'}(e[\gamma]))$$

which, after applying H1, follows from instantiating H2 with H3, H4, and H5. □

LEMMA F.123 (SIGNATURE PRESERVATION). *If $\{s_j : T_j \mid j < m\} \supseteq \{s_i : T_i \mid i < n\}$, then*

$$\mathcal{S}\left[\!\!\left[\Sigma, \mathsf{m}\ \mathsf{k}\ X\ \{\overline{s_j : T_j}^{j<m}\}\right]\!\!\right]_F(\varsigma) \vDash \mathcal{S}\left[\!\!\left[\Sigma, \mathsf{flex}\ \mathsf{k}\ X\ \{\overline{s_i : T_i}^{i<n}\}\right]\!\!\right]_F(\varsigma)$$

PROOF. Assume the premise $\{s_j : T_j \mid j < m\} \supseteq \{s_i : T_i \mid i < n\}^{(H1)}$. If there are no $j < m$ then there must not be any $i < n$ and the proof is trivial. Otherwise, unfolding $\mathcal{S}$ and simplifying and letting $\delta = \varsigma(X)$, it suffices to show

$$\frac{\begin{array}{c} \ulcorner \mathrm{dom}(\varsigma) \supseteq \mathrm{dom}(\Sigma, \mathsf{m}\ \mathsf{k}\ X\ \{\overline{s_j : T_j}^{j<m}\})\urcorner^{(H8)} \quad \forall\ \mathsf{m'}\ \mathsf{k}\ Y\ \{\cdots\} \in \Sigma.\ \ldots^{(H7)} \quad \ulcorner \delta.\mathrm{kind} = \mathsf{k}\urcorner^{(H6)} \\ \ulcorner \mathrm{dom}(\delta.\mathrm{sel}) \supseteq \{s_j \mid j < m\}\urcorner^{(H5)} \quad \forall\ j < m.\ !\ \mathit{wp}_F\left(\langle \mathtt{sel}^{s_j}_X\rangle_F\ ()\right)\{\mathtt{w}.\ \ulcorner \mathtt{w} = \delta.\mathrm{sel}(s_j).\mathrm{off}\urcorner\}^{(H4)} \\ \forall\ j < m, \mathtt{w}.\ \delta.\mathrm{sel}(s_j).\mathrm{semty}(\mathtt{w}) \equiv \triangleright \mathcal{V}[\![T_j]\!]^{\varsigma}_F(\mathtt{w})^{(H3)} \\ \forall\ \ell.\ \{\ell \mapsto 0 \star \delta.\mathrm{obj}(\ell+1)\}\ \langle \mathtt{destr}_X\rangle_F\ (\ell)\ \{\mathit{emp}\}_F^{(H2)} \end{array}}{\begin{array}{c} \ulcorner \mathrm{dom}(\varsigma) \supseteq \mathrm{dom}(\Sigma, \mathsf{flex}\ \mathsf{k}\ X\ \{\overline{s_i : T_i}^{i<n}\})\urcorner^{(G1)} \quad \forall\ \mathsf{m'}\ \mathsf{k}\ Y\ \{\cdots\} \in \Sigma.\ \ldots^{(G2)} \quad \ulcorner \delta.\mathrm{kind} = \mathsf{k}\urcorner^{(G3)} \\ \ulcorner \mathrm{dom}(\delta.\mathrm{sel}) \supseteq \{s_i \mid i < n\}\urcorner^{(G4)} \quad \forall\ i < n.\ !\ \mathit{wp}_F\left(\langle \mathtt{sel}^{s_i}_X\rangle_F\ ()\right)\{\mathtt{w}.\ \ulcorner \mathtt{w} = \delta.\mathrm{sel}(s_i).\mathrm{off}\urcorner\}^{(G5)} \\ \forall\ i < n, \mathtt{w}.\ \delta.\mathrm{sel}(s_i).\mathrm{semty}(\mathtt{w}) \equiv \triangleright \mathcal{V}[\![T_i]\!]^{\varsigma}_F(\mathtt{w})^{(G6)} \\ \forall\ \ell.\ \{\ell \mapsto 0 \star \delta.\mathrm{obj}(\ell+1)\}\ \langle \mathtt{destr}_X\rangle_F\ (\ell)\ \{\mathit{emp}\}_F^{(G7)} \end{array}}$$

We can discharge each proof obligation separately, using $\star$-MONO. G1 follows from H8, which also ensures that δ is well defined. G2 follows from H7. G3 follows from H6. G4 follows from H5 and H1. G5 follows from H4 and H1. G6 follows from H3 and H1. G7 follows from H2. □

LEMMA F.124 (CROSS-VERSION LINKING). *If Σ supports evolution to Σ', and both $\Sigma'; \Gamma_1 \vDash_{F_1} e_1 : T_1$, and $\Sigma; \Gamma_2, x : T_1 \vDash_{F_2} e_2 : T_2$, (with $x \notin \Gamma_2$), then $\Sigma'; \Gamma_1, \Gamma_2 \vDash_{F_1, F_2} \mathtt{const}\ x = e_1;\ e_2 : T_2$.*

PROOF. By Supported Evolution, $\Sigma; \Gamma_2, x : T_1 \vDash_{F_2} e_2 : T_2$ implies $\Sigma'; \Gamma_2, x : T_1 \vDash_{F_2} e_2 : T_2$. Using this, the result follows from COMP-LET-COMPAT. □

LEMMA F.125 (EVOLUTION ADEQUACY). *If Σ supports evolution to Σ' and $\Sigma' \dashv F$, then $\Sigma; \varnothing \vdash e : \mathbb{Z} \rightsquigarrow e \dashv F$ implies $\mathrm{ok}_F(e)$.*

Proof. Suppose we have $\Sigma' \dashv \mathtt{F}^{(\mathrm{H1})}$ and, applying Compiler Compliance, $\Sigma; \varnothing \vDash_{\mathtt{F}} \mathtt{e} : \mathbb{Z}$. By the definition of Supported Evolution, we also have $\Sigma'; \varnothing \vDash_{\mathtt{F}} \mathtt{e} : \mathbb{Z}$. Unfolding $\vDash_{\mathtt{F}}$ and $C[\![-]\!]$ as in the proof of Compiler Adequacy, we have

$$\forall\, \mathtt{F}' \supseteq \mathtt{F}, \varsigma.\ \mathcal{S}[\![\Sigma']\!]_{\mathtt{F}'}(\varsigma) \vDash \mathcal{E}[\![\mathbb{Z}]\!]^{\varsigma}_{\mathtt{F}'}(\mathtt{e})$$

By Canonical Signature Satisfiable with H1, we have $emp \vDash \mathcal{S}[\![\Sigma']\!]_{\mathtt{F}}(\!|\, \Sigma' \,|\!)$. $\mathsf{ok}_{\mathtt{F}}(\mathtt{e})$ follows after instantiating this with $\mathtt{F} \supseteq \mathtt{F}$ and $(\!|\, \Sigma' \,|\!)$, then applying lr-adequacy. □