From Linearity to Borrowing (Technical Report)

July 29, 2025

Contents

1 Syntax

$$
\begin{array}{llll}
\textsc{Var} & \ni & x, y, \ldots & \\
\textsc{Loc} & \ni & \ell & \\
\textsc{Val} & \ni & v & ::= \; () \mid (v_1, v_2) \mid \mathsf{inj}_1\, v \mid \mathsf{inj}_2\, v \mid \lambda x.e \mid \Lambda.e \mid \ell \mid p \\
\textsc{Prim} & \ni & p & ::= \; \mathsf{alloc} \mid \mathsf{free} \mid \mathsf{load} \mid \mathsf{store} \mid \mathsf{store}\ v \\
\textsc{Expr} & \ni & e & ::= \; x \mid v \mid (e_1, e_2) \mid \mathsf{inj}_1\, e \mid \mathsf{inj}_2\, e \mid e_1;\, e_2 \mid \mathsf{let}\,(x, y) = e_1\ \mathsf{in}\ e_2 \\
 & & & \quad\ \mid \mathsf{case}\, e\, \{\mathsf{inj}_1\, x.e_1 \mid \mathsf{inj}_2\, y.e_2\} \mid e_2\ e_1 \\
\textsc{LifeVar} & \ni & 'a, 'b, \ldots & \\
\textsc{Life} & \ni & @a, @b \ldots & ::= \; ' \mid \top \mid @a \sqcup @b \mid @a \sqcap @b \\
\textsc{LifeCtx} & \ni & \Delta & : \; \textsc{LifeVar} \rightharpoonup \textsc{Life} \\
\textsc{Type} & \ni & T & ::= \; \mathbb{1} \mid T_1 \oplus T_2 \mid T_1 \otimes T_2 \mid T_1 \multimap T_2 \mid \mathsf{Ref}\ T \mid [@a]\, T \\
 & & & \quad\ \mid \mathsf{Imm}\ @a\ T \mid \mathsf{Mut}\ @a\ T \mid \forall\, 'a \sqsubset @b.\, T \mid \mathsf{Unk}
\end{array}
$$

2 Statics

$$\boxed{\Delta;\Gamma \vdash e : T}$$

ID
$$\frac{}{\Delta;\, x : T \vdash x : T}$$

$\mathbb{1}$I
$$\frac{}{\Delta;\, \bullet \vdash () : \mathbb{1}}$$

$\mathbb{1}$E
$$\frac{\Delta;\Gamma_1 \vdash e_1 : \mathbb{1} \quad \Delta;\Gamma_2 \vdash e_2 : T}{\Delta;\Gamma_1,\Gamma_2 \vdash e_1;\, e_2 : T}$$

$\otimes$I
$$\frac{\Delta;\Gamma_1 \vdash e_1 : T_1 \quad \Delta;\Gamma_2 \vdash e_2 : T_2}{\Delta;\Gamma_1,\Gamma_2 \vdash (e_1,e_2) : T_1 \otimes T_2}$$

$\otimes$E
$$\frac{\Delta;\Gamma_p \vdash e_p : T_1 \otimes T_2 \quad \Delta;\Gamma, x_1 : T_1, x_2 : T_2 \vdash e : T}{\Delta;\Gamma_p,\Gamma \vdash \mathsf{let}\,(x_1,x_2) = e_p;\;\; e : T}$$

$\oplus$I
$$\frac{\Delta;\Gamma \vdash e : T_i \quad i \in \{1,2\}}{\Delta;\Gamma \vdash i\, e : T_1 \oplus T_2}$$

$\oplus$E
$$\frac{\Delta;\Gamma_s \vdash e_s : T_1 \oplus T_2 \quad \Delta;\Gamma, x_b : T_b \vdash e_b : T \text{ for } b \in \{1,2\}}{\Delta;\Gamma_s,\Gamma \vdash \mathsf{match}\, e_s\, \{x_1 \Rightarrow e_1, x_2 \Rightarrow e_2\} : T}$$

$\multimap$I
$$\frac{\Delta;\Gamma, x : T_1 \vdash e : T_2}{\Delta;\Gamma \vdash \lambda x.e : T_1 \multimap T_2}$$

$\multimap$E
$$\frac{\Delta;\Gamma_1 \vdash e_1 : T_1 \quad \Delta;\Gamma_2 \vdash e_2 : T_1 \multimap T_2}{\Delta;\Gamma_1,\Gamma_2 \vdash e_1\;\, e_2 : T_2}$$

$\forall$ I
$$\frac{\Delta, ('a \sqsubset @b);\Gamma \vdash e : T}{\Delta;\Gamma \vdash \Lambda.e : \forall\, 'a \sqsubset @b.\, T}$$

$\forall$ E
$$\frac{\Delta;\Gamma \vdash e : \forall\, 'a \sqsubset @b.\, T \quad \Delta \vDash @a \sqsubset @b}{\Delta;\Gamma \vdash e[\,] : T[@a/'a]}$$

$[l]$ I
$$\frac{\Delta;\Gamma \vdash e : T \quad \Delta \vDash \Gamma \sqsupset @a}{\Delta;\Gamma \vdash \square e : [@a]\, T}$$

$[l]$ E
$$\frac{\Delta;\Gamma \vdash \square e : [@a]\, T}{\Delta;\Gamma \vdash \square e : T}$$

alloc
$$\frac{}{\Delta;\, \bullet \vdash \mathsf{alloc} : T \mathrel{-\!\star} \mathsf{Ref}\ T}$$

free
$$\frac{}{\Delta;\, \bullet \vdash \mathsf{free} : \mathsf{Ref}\ T \mathrel{-\!\star} T}$$

$\sqsubseteq$ Imm
$$\frac{\Delta;\Gamma \vdash e : \mathsf{Imm}\ @b\ T \quad \Delta \vDash @a \sqsubseteq @b}{\Delta;\Gamma \vdash e : \mathsf{Imm}\ @b\ T}$$

$\sqsubseteq$ Mut
$$\frac{\Delta;\Gamma \vdash e : \mathsf{Mut}\ @b\ T \quad \Delta \vDash @a \sqsubseteq @b}{\Delta;\Gamma \vdash e : \mathsf{Mut}\ @b\ T}$$

$\boxed{\Delta \vdash T}$ Presumes $\vDash \Delta$

$$\frac{}{\Delta \vdash \mathbb{1}} \qquad \frac{\Delta \vdash T_1 \quad \Delta \vdash T_2}{\Delta \vdash T_1 \otimes T_2} \qquad \frac{\Delta \vdash T_1 \quad \Delta \vdash T_2}{\Delta \vdash T_1 \oplus T_2} \qquad \frac{\Delta \vdash T_1 \quad \Delta \vdash T_2}{\Delta \vdash T_1 \mathrel{-\!\star} T_2} \qquad \frac{\Delta \vdash T}{\Delta \vdash \mathsf{Ref}\ T} \qquad \frac{\Delta, ('a \sqsubset @b) \vdash T \quad \Delta \vDash @b}{\Delta \vdash \forall\, ('a \sqsubset @b).T}$$

$$\frac{\Delta \vdash T \quad \Delta \vDash @a}{\Delta \vdash [@a]\, T} \qquad \frac{\Delta \vdash T \quad \Delta \vDash @a}{\Delta \vdash \mathsf{Imm}\ @a\ T} \qquad \frac{\Delta \vdash T \quad \Delta \vDash @a}{\Delta \vdash \mathsf{Mut}\ @a\ T}$$

$\boxed{\Delta \vdash T \sqsupset @a}$ Presumes $\vDash \Delta$ and $\Delta \vDash @a$

$$\frac{}{\Delta \vdash \mathbb{1} \sqsupset @a} \qquad \frac{\Delta \vdash T_1 \sqsupset @a \quad \Delta \vdash T_2 \sqsupset @a}{\Delta \vdash T_1 \otimes T_2 \sqsupset @a} \qquad \frac{\Delta \vdash T_1 \sqsupset @a \quad \Delta \vdash T_2 \sqsupset @a}{\Delta \vdash T_1 \oplus T_2 \sqsupset @a} \qquad \frac{\Delta \vdash T \sqsupset @a}{\Delta \vdash \mathsf{Ref}\ T \sqsupset @a}$$

$$\frac{\Delta \vDash @b \sqsupset @a}{\Delta \vdash [@b]\, T \sqsupset @a} \qquad \frac{\Delta \vDash @b \sqsupset @a}{\Delta \vdash \mathsf{Imm}\ @b\ T \sqsupset @a} \qquad \frac{\Delta \vDash @b \sqsupset @a}{\Delta \vdash \mathsf{Mut}\ @b\ T \sqsupset @a}$$

$$
\begin{array}{llcll}
\Delta \vdash & \mathsf{swap} & : & \mathsf{Ref}\ T_1 \mathrel{-\!\!\star} T_2 \mathrel{-\!\!\star} \mathsf{Ref}\ T_2 \otimes T_1 & \\
\Delta \vdash & \mathsf{copy} & : & \mathsf{Imm}\ @a\ T \mathrel{-\!\!\star} \mathsf{Imm}\ @a\ T \otimes \mathsf{Imm}\ @a\ T & \\
\Delta \vdash & \mathsf{forget} & : & \mathsf{Imm}\ @a\ T \mathrel{-\!\!\star} \mathbb{1} & \\
 & & & \mathsf{Mut}\ @a\ T \mathrel{-\!\!\star} \mathbb{1} & \\
 & & & \mathsf{Unk} \mathrel{-\!\!\star} \mathbb{1} & \\
\Delta \vdash & \mathsf{withbor} & : & \mathsf{Ref}\ T_1 \mathrel{-\!\!\star} (\forall\, 'a \sqsubset \textstyle\bigsqcap \Delta.\ \mathsf{Imm}\ 'a\ T_1 \mathrel{-\!\!\star} ['a]\, T_2) \mathrel{-\!\!\star} \mathsf{Ref}\ T_1 \otimes T_2 & \\
 & & & \mathsf{Ref}\ T_1 \mathrel{-\!\!\star} (\forall\, 'a \sqsubset \textstyle\bigsqcap \Delta.\ \mathsf{Mut}\ 'a\ T_1 \mathrel{-\!\!\star} ['a]\, T_2) \mathrel{-\!\!\star} \mathsf{Ref}\ T_1 \otimes T_2 & \Delta \vdash T_1 \sqsupset @b \\
 & & & \mathsf{Mut}\ @a\ T_1 \mathrel{-\!\!\star} (\forall\, 'b \sqsubset \textstyle\bigsqcap \Delta.\ \mathsf{Mut}\ 'b\ T_1 \mathrel{-\!\!\star} ['b]\, T_2) \mathrel{-\!\!\star} \mathsf{Mut}\ @a\ T_1 \otimes T_2 & \\
\Delta \vdash & \mathsf{withload} & : & \mathsf{Imm}\ @a\ T_1 \mathrel{-\!\!\star} (\forall\, 'b \sqsubset \textstyle\bigsqcap \Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \mathrel{-\!\!\star} ['b]\, T_2) \mathrel{-\!\!\star} T_2 & \\
\Delta \vdash & \mathsf{withswap} & : & \mathsf{Mut}\ @a\ T_1 \mathrel{-\!\!\star} (T_1 \mathrel{-\!\!\star} T_1 \otimes T_2) \mathrel{-\!\!\star} \mathsf{Mut}\ @a\ T_1 \otimes T_2 &
\end{array}
$$

$$
\underline{\mathsf{Imm}}\ 'b\ \mathbb{1} \triangleq \mathbb{1} \qquad \underline{\mathsf{Imm}}\ 'b\ (T_1 \oplus T_2) \triangleq \underline{\mathsf{Imm}}\ 'b\ T_1 \oplus \underline{\mathsf{Imm}}\ 'b\ T_2 \qquad \underline{\mathsf{Imm}}\ 'b\ (T_1 \otimes T_2) \triangleq \underline{\mathsf{Imm}}\ 'b\ T_1 \otimes \underline{\mathsf{Imm}}\ 'b\ T_2
$$

$$
\underline{\mathsf{Imm}}\ 'b\ (T_1 \mathrel{-\!\!\star} T_2) \triangleq \mathsf{Unk} \qquad \underline{\mathsf{Imm}}\ 'b\ (\mathsf{Ref}\ T) \triangleq \mathsf{Imm}\ 'b\ T \qquad \underline{\mathsf{Imm}}\ 'b\ (\mathsf{Imm}\ @a\ T) \triangleq \mathsf{Imm}\ @a\ T
$$

$$
\underline{\mathsf{Imm}}\ 'b\ ([@a]\,T) \triangleq \underline{\mathsf{Imm}}\ 'b\ T \qquad \underline{\mathsf{Imm}}\ 'b\ (\forall\, '.\, a \sqsubset @a.\ T) \triangleq \mathsf{Unk}
$$

$$
\textsc{LSub} \ni \delta : \textsc{LifeVar} \rightharpoonup \mathit{Life}
$$

$$
[\![\Delta]\!] \triangleq \{\delta \mid \mathrm{dom}(\Delta) \subseteq \mathrm{dom}(\delta) \wedge \forall\, 'a \in \mathrm{dom}(\Delta).\ \delta('a) \sqsubset \Delta('a)\delta\}
$$

$$
\vDash \Delta \triangleq [\![\Delta]\!] \neq \varnothing
$$

$$
@a\delta \triangleq \begin{cases} \delta('a) & , @a = 'a \\ \top & , @a = \top \\ @b_1\delta \sqcap @b_2\delta & , @a = @b_1 \sqcup @b_2 \\ @b_1\delta \sqcup @b_2\delta & , @a = @b_1 \sqcup @b_2 \end{cases}
$$

$$
\begin{aligned}
\Delta \vDash @a &\triangleq \forall\, \delta \in [\![\Delta]\!].\ @a\delta \text{ defined} \\
\Delta \vDash @a \sqsubset @b &\triangleq \forall\, \delta \in [\![\Delta]\!].\ @a\delta \sqsubset @b\delta
\end{aligned}
$$

3 Dynamics

$$
\begin{array}{lcll}
\textsc{Kont} & \ni & K & ::= \ [\,] \mid (K, e) \mid (v, K) \mid \mathsf{let}\,(x, y) = K\ \mathsf{in}\ e \mid \mathsf{case}\,K\,\{\mathsf{inj}_1\,x.e_1 \mid \mathsf{inj}_2\,y.e_2\} \mid e\ K \mid K\ v \\
\textsc{Mem} & \ni & \mu & : \ \ \textsc{Loc} \rightharpoonup \textsc{Val}
\end{array}
$$

$$\boxed{(\mu, e) \to (\mu', e')} \quad \boxed{(\mu, e) \mapsto (\mu', e')}$$

$$\to \quad \frac{(\mu, e) \mapsto (\mu', e')}{(\mu, K[e]) \to (\mu', K[e'])} \qquad \mathbb{1} \mapsto \quad \frac{}{(\mu, ();\ e) \mapsto (\mu, e)} \qquad \otimes \mapsto \quad \frac{}{(\mu, \mathsf{let}\,(x_1, x_2) = (v_1, v_2)\ \mathsf{in}\ e) \mapsto (\mu, e[v_1/x_1, v_2/x_2])}$$

$$\oplus \mapsto \quad \frac{}{(\mu, \mathsf{case}\,(\mathsf{inj}_i\ v)\,\{\mathsf{inj}_1\,x.e_1 \mid \mathsf{inj}_2\,y.e_2\}) \mapsto (\mu, e_i[v/x_i])} \qquad \multimap\!\!\mapsto \quad \frac{}{(\mu, (\lambda x.e)\ v) \mapsto (\mu, e[v/x])} \qquad \mathsf{alloc} \mapsto \quad \frac{}{(\mu, \mathsf{alloc}\ v) \mapsto (\mu \uplus \ell \mapsto v, \ell)}$$

$$\mathsf{free} \mapsto \quad \frac{}{(\mu \uplus \ell \mapsto v, \mathsf{free}\ \ell) \mapsto (\mu, v)} \qquad \mathsf{load} \mapsto \quad \frac{\mu(\ell) = v}{(\mu, \mathsf{load}\ \ell) \mapsto (\mu, v)} \qquad \mathsf{store} \mapsto \quad \frac{\ell \in \mathrm{dom}(\mu)}{(\mu, \mathsf{store}\ \ell\ v) \mapsto (\mu[\ell \mapsto v], ())}$$

$$\begin{array}{ll}
\mathsf{swap} & \triangleq \lambda x.\lambda y.\mathsf{let}\,z = \mathsf{load}\ x;\ \mathsf{store}\ x\ y;\ (x, y) \\
\mathsf{copy} & \triangleq \lambda x.(x, x) \\
\mathsf{forget} & \triangleq \lambda x.() \\
\mathsf{withbor} & \triangleq \lambda x.\lambda f.(x, f\ x) \\
\mathsf{withload} & \triangleq \lambda x.\lambda f.(x, f\ (\mathsf{load}\ x)) \\
\mathsf{withswap} & \triangleq \lambda x.\lambda f.\mathsf{let}\,(y, z) = f(\mathsf{load}\ x);\ \mathsf{store}\ x\ y;\ (x, z)
\end{array}$$

4 Logical Relation

$$\begin{array}{ll}
\mathcal{V}\llbracket \mathbb{1} \rrbracket_\delta(v) & \triangleq \ulcorner v = () \urcorner \\
\mathcal{V}\llbracket T_1 \otimes T_2 \rrbracket_\delta(v) & \triangleq \exists\, v_1, v_2.\ \ulcorner v = (v_1, v_2) \urcorner \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_1) \star \mathcal{V}\llbracket T_2 \rrbracket_\delta(v_2) \\
\mathcal{V}\llbracket T_1 \oplus T_2 \rrbracket_\delta(v) & \triangleq (\exists\, v_1.\ \ulcorner v = \mathsf{inj}_1\, v_1 \urcorner \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_1)) \vee (\exists\, v_2.\ \ulcorner v = \mathsf{inj}_2\, v_2 \urcorner \star \mathcal{V}\llbracket T_2 \rrbracket_\delta(v_2)) \\
\mathcal{V}\llbracket T_1 \multimap T_2 \rrbracket_\delta(v) & \triangleq \forall\, v'.\ \mathcal{V}\llbracket T_1 \rrbracket_\delta(v') \mathrel{-\!\!\star} \mathcal{E}\llbracket T_2 \rrbracket_\delta(v\ v') \\
\mathcal{V}\llbracket \forall\, 'a \sqsubset @b.\ T \rrbracket_\delta(v) & \triangleq \forall\, \alpha \sqsubset @b\delta.\ \mathcal{E}\llbracket T \rrbracket_\delta(v\ ()) \\
\mathcal{V}\llbracket [@a]\, T \rrbracket_\delta(v) & \triangleq [@a\delta]\, \mathcal{V}\llbracket T \rrbracket_\delta(v) \\
\mathcal{V}\llbracket \mathsf{Ref}\ T \rrbracket_\delta(v) & \triangleq \exists\, \ell, v'.\ \ulcorner v = \ell \urcorner \star \ell \mapsto v' \star \mathcal{V}\llbracket T \rrbracket_\delta(v') \\
\mathcal{V}\llbracket \mathsf{Imm}\ @a\ T \rrbracket_\delta(v) & \triangleq \exists\, \ell.\ \ulcorner v = \ell \urcorner \star \ell \mapsto \mathsf{Imm}\ @a\delta\ \mathcal{V}\llbracket T \rrbracket_\delta \\
\mathcal{V}\llbracket \mathsf{Mut}\ @a\ T \rrbracket_\delta(v) & \triangleq \exists\, \ell.\ \ulcorner v = \ell \urcorner \star \ell \mapsto \mathsf{Mut}\ @a\delta\ \mathcal{V}\llbracket T \rrbracket_\delta \\
\mathcal{V}\llbracket \mathsf{Unk} \rrbracket_\delta(v) & \triangleq \mathsf{emp} \\
\mathcal{E}\llbracket T \rrbracket_\delta(v) & \triangleq \mathsf{wp}\,(e)\,\{\mathcal{V}\llbracket T \rrbracket_\delta\} \\
\mathcal{D}\llbracket \Delta \rrbracket(\delta) & \triangleq \ulcorner \delta \in \llbracket \Delta \rrbracket \urcorner \\
\mathcal{G}\llbracket \Gamma \rrbracket(\gamma) & \triangleq \ulcorner \mathrm{dom}(\Gamma) \subseteq \mathrm{dom}(\delta) \urcorner \star \circledast_{x \in \mathrm{dom}(\Gamma)}\, \mathcal{V}\llbracket \Gamma(x) \rrbracket_\delta(\gamma(x)) \\
\Delta; \Gamma \vDash e : T & \triangleq !\, \forall\, \delta, \gamma.\ \mathcal{D}\llbracket \Delta \rrbracket(\delta) \mathrel{-\!\!\star} \mathcal{G}\llbracket \Gamma \rrbracket_\delta(\gamma) \mathrel{-\!\!\star} \mathcal{E}\llbracket T \rrbracket_\delta(\gamma(e))
\end{array}$$

5 Model

$$\begin{array}{lllll}
 & & \textsc{SProp}_\alpha & \triangleq & \textsc{Res}_\alpha \to \mathbb{P} \\
 & & \textsc{Res}_\alpha & \triangleq & \textsc{Loc} \rightharpoonup \textsc{Cell}_\alpha \\
 & & \textsc{Cell}_\alpha & \triangleq & \mathsf{own}(\textsc{Val}) + \mathsf{imm}(\textsc{Imm}_\alpha) + \mathsf{mut}(\textsc{Mut}_\alpha) \\
 & & \textsc{Imm}_\alpha & \triangleq & \{(\overline{\alpha} : \wp^+(\textsc{Life}), v : \textsc{Val}, \rho : \textsc{Res}_{\sqcup \overline{\alpha}}) \mid \sqcap \overline{\alpha} \sqsupset \alpha\} \\
 & & \textsc{Mut}_\alpha & \triangleq & \{(\beta \sqsupset \alpha, v : \textsc{Val}, \rho : \textsc{Res}_\beta, \hat{P} : \textsc{Val} \to \textsc{SProp}_\beta) \mid \hat{P}(v)(\rho)\} \\
P & \in & \textsc{SProp} & \triangleq & \textsc{Res} \to \mathbb{P} \\
\rho & \in & \textsc{Res} & \triangleq & \textsc{Loc} \rightharpoonup^{\mathsf{fin}} \textsc{Cell} \\
\psi & \in & \textsc{Cell} & \triangleq & \bigcup_\alpha \textsc{Cell}_\alpha \\
\alpha, \beta & \in & \textsc{Life} & \triangleq & (\mathbb{N}, \sqsubseteq \triangleq >, \sqcup \triangleq \min, \sqcap \triangleq \max, \top \triangleq 0)
\end{array}$$

$$@\psi \triangleq \begin{cases} \top, & \psi = \mathsf{own} \\ \alpha, & \psi = \mathsf{mut}(\alpha, \_, \_, \_) \\ \bigsqcap \overline{\alpha}, & \psi = \mathsf{imm}(\overline{\alpha}, \_, \_, \_) \end{cases}$$

$$\begin{array}{lcl}
@\rho & \triangleq & \bigsqcap_{\psi \in \mathrm{cod}(\rho)} @\psi \\
\downarrow\!\alpha & \triangleq & \alpha + 1 \\
\psi_1 \mathbin{\blacktriangleright\!\!\blacktriangleleft} \psi_2 & \triangleq & \exists\, \overline{\alpha_1}, \overline{\alpha_2}, v, \rho.\ \psi_1 = \mathsf{imm}(\overline{\alpha_1}, v, \rho) \land \psi_2 = \mathsf{imm}(\overline{\alpha_2}, v, \rho) \\
\psi_1 \bowtie \psi_2 & \triangleq & \psi_1 \mathbin{\blacktriangleright\!\!\blacktriangleleft} \psi_2 \lor \exists\, i, \overline{\alpha}, \beta, v, \rho, \hat{P}.\ \{\psi_1, \psi_2\} \in \{\mathsf{imm}(\overline{\alpha}, v, \rho), \mathsf{own}(v), \mathsf{mut}(\beta, v, \rho, \hat{P})\} \\
\psi_1 \bullet \psi_2 & \triangleq & \begin{cases} \mathsf{imm}(\overline{\alpha_1} \cup \overline{\alpha_2}, v, \rho), & \psi_1 = \mathsf{imm}(\overline{\alpha_1}, v, \rho) \land \psi_2 = \mathsf{imm}(\overline{\alpha_2}, v, \rho) \end{cases}
\end{array}$$

$$\psi_1 \circ \psi_2 \triangleq \begin{cases} \psi_1, & \psi_1 = \psi_2 \\ \psi_1 \bullet \psi_2, & \psi_1 \mathbin{\blacktriangleright\!\!\blacktriangleleft} \psi_2 \\ \mathsf{mut}(\alpha \sqcap \beta, v, \rho, \hat{P} \land \hat{Q}) & \exists\, \alpha, \beta, v, \rho, \hat{P}, \hat{Q}.\ \psi_1 = \mathsf{mut}(\alpha, v, \rho, \hat{P}) \land \psi_2 = \mathsf{mut}(\beta, v, \rho, \hat{Q}) \\ \psi_i & \exists\, \alpha, v, \rho, \hat{P}.\ \psi_i = \mathsf{mut}(\alpha, v, \rho, \hat{P}) \land \psi_{3-i} = \mathsf{own}(v) \\ \psi_i & \exists\, \overline{\alpha}, \beta, v, \rho, \hat{P}.\ \psi_i = \mathsf{imm}(\overline{\alpha}, v, \rho) \land \psi_{3-i} \in \{\mathsf{own}(v), \mathsf{mut}(\beta, v, \rho, \hat{P})\} \end{cases}$$

$$\begin{array}{lcl}
\rho_1 \mathbin{\blacktriangleright\!\!\triangleleft} \rho_2 & \triangleq & \forall\, \ell \in \mathrm{dom}(\rho_1) \cap \mathrm{dom}(\rho_2).\ \rho_1(\ell) \mathbin{\blacktriangleright\!\!\triangleleft} \rho_2(\ell) \\
\rho_1 \mathbin{\LEFTcircle} \rho_2 & \triangleq & \begin{cases} \rho_1/\mathrm{dom}(\rho_2) \uplus \rho_2/\mathrm{dom}(\rho_1) \uplus [\ell \mapsto \psi_1 \mathbin{\LEFTcircle} \psi_2 \mid \rho_1(\ell) = \psi_1 \land \rho_2(\ell) = \psi_2], & \rho_1 \mathbin{\blacktriangleright\!\!\triangleleft} \rho_2 \end{cases} \\
\rho|_\iota & \triangleq & \begin{cases} [\ell \mapsto \psi \mid \rho(\ell) = \psi = \iota(\ldots)], & \iota \in \{\mathsf{own}, \mathsf{mut}, \mathsf{imm}\} \end{cases} \\
\mathsf{ex}(\rho)_{\LEFTcircle} & \triangleq & \rho|_{\mathsf{own}} \mathbin{\LEFTcircle} \rho|_{\mathsf{mut}} \mathbin{\LEFTcircle} \LEFTCIRCLE\{\mathsf{ex}(\rho')_{\LEFTcircle} \mid \exists\, \ell.\ \rho(\ell) = \mathsf{mut}(\_, \_, \rho', \_)\} \\
\mathsf{ag}(\rho)_{\LEFTcircle} & \triangleq & \rho|_{\mathsf{imm}} \circ \bigcirc\{\mathsf{ag}(\rho') \mid \exists\, \ell.\ \rho(\ell) = \mathsf{mut}(\_, \_, \rho', \_)\} \circ \bigcirc\{\mathsf{ex}(\rho')_\circ \circ \mathsf{ag}(\rho') \mid \exists\, \ell.\ \rho(\ell) = \mathsf{imm}(\_, \_, \rho')\} \\
\llparenthesis \rho \rrparenthesis & \triangleq & \mathsf{ex}(\rho)_\bullet \bullet \mathsf{ag}(\rho) \\
\checkmark \rho & \triangleq & \llparenthesis \rho \rrparenthesis \text{ defined} \\
\llbracket \psi \rrbracket & \triangleq & \begin{cases} v, & \psi = \mathsf{own}(v) \lor \psi = \mathsf{mut}(\_, v, \_, \_) \lor \psi = \mathsf{imm}(\_, v, \_) \end{cases} \\
\llbracket \rho \rrbracket & \triangleq & \begin{cases} [\ell \mapsto v \mid \llbracket \llparenthesis \rho \rrparenthesis(\ell) \rrbracket = v] & \checkmark \rho \end{cases} \\
\rho_1 \mathrel{\#} \rho_2 & \triangleq & \rho_1 \mathbin{\blacktriangleright\!\!\blacktriangleleft} \rho_2 \land \checkmark (\rho_1 \bullet \rho_2)
\end{array}$$

$$\rho_1 \leftrightsquigarrow \rho_2 \triangleq \begin{cases} \forall\, \ell, \alpha, \overline{\beta}, v, \rho, \hat{P}. & \\ (\llparenthesis \rho_1 \rrparenthesis(\ell) = \mathsf{mut}(\alpha, \_, \_, \hat{P}) \Leftrightarrow \llparenthesis \rho_2 \rrparenthesis(\ell) = \mathsf{mut}(\alpha, \_, \_, \hat{P})) & \\ \land(\llparenthesis \rho_1 \rrparenthesis(\ell) = \mathsf{imm}(\overline{\beta}, v, \rho) \Leftrightarrow \llparenthesis \rho_2 \rrparenthesis(\ell) = \mathsf{mut}(\overline{\beta}, v, \rho)), & \checkmark \rho_1 \land \checkmark \rho_2 \end{cases}$$

$$\begin{array}{lcl}
\mathsf{reb}_\alpha(\rho) & \triangleq & \Big\{\rho' \mid @\rho \sqsupset \alpha \land \exists\, \pi : \mathrm{dom}(\rho') \to \textsc{Res}.\ \rho \geq \bullet_{\ell \in \mathrm{dom}(\pi)} \pi(\ell) \land \forall\, \ell \in \mathrm{dom}(\pi), v, \rho''.\ \ell \in \mathrm{dom}(\pi(\ell)) \\
& & \qquad \land\, \rho(\ell) = \mathsf{own}(v) \Rightarrow \rho'(\ell) = \mathsf{imm}(\{\alpha\}, v, \pi(\ell)/\ell) \\
& & \qquad \land\, \rho(\ell) = \mathsf{mut}(\_, v, \rho'', \_) \Rightarrow \rho'(\ell) = \mathsf{imm}(\{\alpha\}, v, \rho'') \land \mathrm{dom}(\pi(\ell)) = \{\ell\} \\
& & \qquad \land\, \rho(\ell) = \mathsf{imm}(\_, \_, \_) \Rightarrow \rho'(\ell) = \rho(\ell) \land \mathrm{dom}(\pi(\ell)) = \{\ell\}\Big\}
\end{array}$$

$$
\begin{array}{llcl}
\ell \mapsto v & (\rho) & \triangleq & \rho = \ell \mapsto \mathsf{own}(v) \\
\ell \mapsto \mathsf{Imm}\ \alpha\ \hat{P} & (\rho) & \triangleq & \exists\, \overline{\beta}, v, \rho'.\ \rho = \ell \mapsto \mathsf{imm}(\overline{\beta}, v, \rho') \land \hat{P}(v)(\rho') \land \alpha \sqsubseteq \bigsqcup \overline{\beta} \\
\ell \mapsto \mathsf{Mut}\ \alpha\ \hat{P} & (\rho) & \triangleq & \exists\, \beta \sqsupseteq \alpha, v, \rho'.\ \rho = \ell \mapsto \mathsf{mut}(\beta, v, \rho', \hat{P}) \\
[\alpha]\, P & (\rho) & \triangleq & P(\rho) \land @\rho \sqsupset \alpha \\
\mathsf{wp}\,(e)\,\{\hat{Q}\} & (\rho) & \triangleq & \forall\, \rho_f \,\#\, \rho.\ \exists\, \rho' \,\#\, \rho_f, \rho^{+} \,\#\, (\rho_f \bullet \rho'), v. \\
 & & & \quad (\llbracket \rho_f \bullet \rho \rrbracket, e) \to^{*} (\llbracket \rho_f \bullet \rho' \bullet \rho^{+} \rrbracket, v) \land \rho \leftrightsquigarrow \rho' \bullet \rho^{+} \land \rho^{+}|_{\mathsf{own}} = \varnothing \land \hat{Q}(v)(\rho') \\
\ulcorner P_{\textsc{Meta}} \urcorner & (\rho) & \triangleq & \rho = \varnothing \land P_{\textsc{Meta}} \\
P_1 \star P_2 & (\rho) & \triangleq & \exists\, \rho_1, \rho_2.\ \rho = \rho_1 \bullet \rho_2 \land P_1(\rho_1) \land P_2(\rho_2) \\
P_1 \mathrel{-\!\!\star} P_2 & (\rho) & \triangleq & \forall\, \rho_1, \rho_2.\ P_1(\rho_1) \Rightarrow \rho \bullet \rho_1 = \rho_2 \Rightarrow P_2(\rho_2) \\
\mathsf{emp} & & \triangleq & \ulcorner \top \urcorner \\
!P & & \triangleq & \mathsf{emp} \land P \\
\top & (\rho) & \triangleq & \top \\
\bot & (\rho) & \triangleq & \bot \\
P_1 \land P_2 & (\rho) & \triangleq & P_1(\rho) \land P_2(\rho) \\
P_1 \lor P_2 & (\rho) & \triangleq & P_1(\rho) \lor P_2(\rho) \\
P_1 \Rightarrow P_2 & (\rho) & \triangleq & P_1(\rho) \Rightarrow P_2(\rho) \\
\forall\, \hat{P} & (\rho) & \triangleq & \forall\, x. \hat{P}(x)(\rho) \\
\exists\, \hat{P} & (\rho) & \triangleq & \exists\, x. \hat{P}(x)(\rho) \\
\text{И}\, \hat{P} & & \triangleq & \exists\, \beta. \forall\, \alpha \sqsubset \beta. [\alpha]\, \hat{P}(\alpha) \\
\circlearrowleft_{\alpha} P & (\rho) & \triangleq & \exists\, \rho' \in \mathsf{reb}_{\alpha}(\rho).\ P(\rho')
\end{array}
$$

6 Theorems, Lemmas, Proofs

6.1 Standard Lemmas

There's no strict definition, but lemmas feel "standard" when their statement doesn't unfold resources or definitions, and don't include any particularly unusual/custom operations.

Lemma 6.1. $\rho_1 ⧑ \rho_2 = \rho_2 ⧑ \rho_1$

Proof. By definition, and the fact that $⧑$ is commutative on cells:

- In the case of $⧓$, commutativity is immediate
- In the case of $\bowtie$, the first case is just the previous, and the second case is immediate since sets are unordered.

□

Lemma 6.2. $\rho_1 ◐ \rho_2 = \rho_2 ◐ \rho_1$

Proof. The composability follows from lemma 6.1. The rest follows from the fact that composition on cells is commutative:

- in the case of $\bullet$, it's immediate because $\cup$ is commutative
- in the case of $\circ$, the first two cases are immediate, and the second two follow from noting ψ_i is invariant under changing the order of cells.

□

Lemma 6.3. $\rho_1 ◐ (\rho_2 ◐ \rho_3) = \rho_1 ◐ \rho_2 ◐ \rho_3$

Proof. Unfolding $◐$, the only interesting case is when $\ell \in \mathrm{dom}(\rho_1) \cap \mathrm{dom}(\rho_2) \cap \mathrm{dom}(\rho_3)$.

- In the $\bullet$ case, associativity follows from the associativity of $\cup$.

- In the $\circ$ case, split on $\rho_2 \circ \rho_3$. The first case is immediate.

  The second case follows from noting that imm always are preserved by $\circ$.

  In the third case, if $\rho_1(\ell)$ is owned, then the mut is the result, if it is mut then we use associativity of $\sqcap$ and $\wedge$, and if it is imm then the result is imm either way.

  In the fourth case, if $\rho_1(\ell)$ is owned, then the mut is the result, if it is mut then it's immediate, and if it is imm then the result is imm either way.

  And in the fifth case, if $\rho_1(\ell)$ is owned, then the imm is the result, if it is mut then it's the imm, and if it is imm then the imms are combined.

□

Lemma 6.4. $\rho \mathbin{◐} \varnothing = \rho$

Proof. By definition, $\mathrm{dom}(\rho) \cap \varnothing = \varnothing$, so $⧑$ holds immediately, and the result is trivially ρ. □

Lemma 6.5. If $\checkmark\, \rho$ then $\rho \# \varnothing$

Proof. Immediate by definition. □

Lemma 6.6. $\rho_1 \# \rho_2$ if and only if $\rho_2 \# \rho_1$

Proof. Follows from lemma 6.2 and by unfolding $\llparenthesis - \rrparenthesis$ with lemmas 6.20 and 6.18. □

Lemma 6.7. If $\rho_1 \# \rho_2$ then $[\![\rho_1 \bullet \rho_2]\!] = [\![\rho_1]\!] \cup [\![\rho_2]\!]$.

Proof. By lemmas 6.20 and 6.18, along with lemma 6.36, for every $\ell \in \mathrm{dom}([\![\rho_1 \bullet \rho_2]\!])$, $\ell \in \mathrm{dom}(\mathsf{ex}(\rho_1)_\bullet)$, $\ell \in \mathrm{dom}(\mathsf{ex}(\rho_2)_\bullet)$, or $\ell \in \mathrm{dom}(\mathsf{ag}(\rho_1) \circ \mathsf{ag}(\rho_2))$. In either of the first two cases, we're done. In the second case, we're done if $\ell \notin \mathrm{dom}(\mathsf{ag}(\rho_1)) \cap \mathrm{dom}(\mathsf{ag}(\rho_2))$. When $\ell \in \mathrm{dom}(\mathsf{ag}(\rho_1)) \cap \mathrm{dom}(\mathsf{ag}(\rho_2))$, then we get by the definition of $\circ$ that $[\![\mathsf{ag}(\rho_1)(\ell)]\!] = [\![\mathsf{ag}(\rho_2)(\ell)]\!]$, so we're done. □

Lemma 6.8. If $[\![\rho_2]\!] = [\![\rho_3]\!]$ and $\rho_1 \# \rho_2$ and $\rho_1 \# \rho_3$ then $[\![\rho_1 \bullet \rho_2]\!] = [\![\rho_1 \bullet \rho_3]\!]$

Proof. Immediate by lemma 6.7, and rewriting with $[\![\rho_2]\!] = [\![\rho_3]\!]$. □

Lemma 6.9. $\rho_1 ⧓ \rho_2$ iff $\rho_1 \bullet \rho_2$ is defined.

Proof. By definition. □

Lemma 6.10. If $\checkmark\, (\rho_1 \bullet \rho_2)$ then $\checkmark\, \rho_1$ and $\checkmark\, \rho_2$

Proof. By unfolding and applying theorems 6.18 and 6.20. □

Lemma 6.11. If $\rho_1 \bullet \rho_2 \# \rho_3$ then $\rho_1 \# \rho_3$ and $\rho_2 \# \rho_3$

Proof. Definedness of $\rho_1 \bullet \rho_3$ and $\rho_2 \bullet \rho_3$ follow from unfolding definitions; $\checkmark\, (\rho_1 \bullet \rho_3)$ and $\checkmark\, (\rho_2 \bullet \rho_3)$ follow from theorem 6.10 applied to $\checkmark\, (\rho_1 \bullet \rho_2 \bullet \rho_3)$. □

Lemma 6.12. If $\rho_1 \bullet \rho_2$ and $\rho_1 \bullet \rho_3$ and $\rho_2 \circ \rho_3$ are all defined, then so is $\rho_1 \bullet (\rho_2 \circ \rho_3)$.

Proof. The own-or-mut cells of ρ_1 are disjoint from the own-or-mut cells of ρ_2 and ρ_3, hence also disjoint from the own-or-mut cells of $\rho_2 \circ \rho_3$, because $\circ$ does not introduce new own-or-mut cells. For any location ℓ with $(\rho_2 \circ \rho_3)(\ell)$ an imm cell, it must be that either (1) $\rho_1(\ell) = \mathsf{imm}(\alpha_1, v, \rho)$ and $\rho_2(\ell) = \mathsf{imm}(\alpha_2, v, \rho)$ for some $\alpha_1, \alpha_2, v, \rho$, in which case $(\rho_2 \circ \rho_3)(\ell) = \mathsf{imm}(\alpha_1 \cup \alpha_2, v, \rho)$ and is hence composable with $\rho_1(\ell)$ by $\rho_1 ⧓ \rho_2$, or (2) one of $\rho_2(\ell)$ or $\rho_3(\ell)$ is an imm and the other is an own-or-mut—without loss of generality suppose it is ρ_2 that is own-or-mut—in which case $\ell \notin \mathrm{dom}(\rho_1)$ and hence ℓ is not in the overlap of ρ_1 and $\rho_2 \circ \rho_3$. It follows that the imm cells of ρ_1 agree on overlap with the imm cells of $\rho_2 \circ \rho_3$ up to lifetimes. □

Lemma 6.13. If $\rho_1 \bullet \rho_2$ and $\rho_1 \bullet \rho_3$ and $\rho_2 \bullet \rho_3$ are all defined, then so is $\rho_1 \bullet \rho_2 \bullet \rho_3$.

Proof. The own-or-mut cells of ρ_1, ρ_2, ρ_3 are all pairwise-disjoint, hence mutually disjoint, and the imm cells pairwise agree up to lifetimes, hence mutually agree up to lifetimes. □

Lemma 6.14. If $\rho_1 \circ \rho_2$ and $\rho_1 \circ \rho_3$ and $\rho_2 \circ \rho_3$ are all defined, then so is $\rho_1 \circ \rho_2 \circ \rho_3$.

Proof. Analogous to theorem 6.13. The only wrinkle is that $\circ$, unlike $\bullet$, merges imm cells with own and mut cells; however, it only does so when the given own-or-mut cell has the same value and subresource inside of it, so the resulting composites still agree on overlapping imm cells up to lifetimes. □

Lemma 6.15. If $\rho_1 \# \rho_2$ and $\rho_2 \# \rho_3$ and $\rho_1 \# \rho_3$ then $\rho_1 \# \rho_2 \bullet \rho_3$.

Proof. The composite $\rho_1 \bullet \rho_2 \bullet \rho_3$ is defined by theorem 6.13, so it only remains to show $\checkmark(\rho_1 \bullet \rho_2 \bullet \rho_3)$. By theorems 6.18 and 6.20, this amounts to showing definedness of $\mathsf{ex}(\rho_1)_\bullet \bullet \mathsf{ex}(\rho_2)_\bullet \bullet \mathsf{ex}(\rho_3)_\bullet \bullet (\mathsf{ag}(\rho_1) \circ \mathsf{ag}(\rho_2) \circ \mathsf{ag}(\rho_3))$ By assumption we have that

$$\begin{aligned}
\llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis &= \mathsf{ex}(\rho_1)_\bullet \bullet \mathsf{ex}(\rho_2)_\bullet \bullet (\mathsf{ag}(\rho_1) \circ \mathsf{ag}(\rho_2)) \\
\llparenthesis \rho_1 \bullet \rho_3 \rrparenthesis &= \mathsf{ex}(\rho_1)_\bullet \bullet \mathsf{ex}(\rho_3)_\bullet \bullet (\mathsf{ag}(\rho_1) \circ \mathsf{ag}(\rho_3)) \\
\llparenthesis \rho_2 \bullet \rho_3 \rrparenthesis &= \mathsf{ex}(\rho_2)_\bullet \bullet \mathsf{ex}(\rho_3)_\bullet \bullet (\mathsf{ag}(\rho_2) \circ \mathsf{ag}(\rho_3))
\end{aligned}$$

are all defined. Hence $\mathsf{ex}(\rho_1)_\bullet, \mathsf{ex}(\rho_2)_\bullet, \mathsf{ex}(\rho_3)_\bullet$ are pairwise-composable with respect to $\bullet$. Similarly, we also have that $\mathsf{ag}(\rho_1)_\bullet, \mathsf{ag}(\rho_2)_\bullet, \mathsf{ag}(\rho_3)_\bullet$ are pairwise-composable with respect to $\circ$. So, by theorems 6.13 and 6.14, this gives definedness of the triple composites $\mathsf{ex}(\rho_1)_\bullet \bullet \mathsf{ex}(\rho_2)_\bullet \bullet \mathsf{ex}(\rho_3)_\bullet$ and $\mathsf{ag}(\rho_1) \circ \mathsf{ag}(\rho_2) \circ \mathsf{ag}(\rho_3)$. It only remains to show that these triple composites are themselves composable. By two applications of theorem 6.12, this reduces to showing the following three composites are defined:

$$\begin{gathered}
\mathsf{ex}(\rho_1)_\bullet \bullet \mathsf{ex}(\rho_2)_\bullet \bullet \mathsf{ex}(\rho_3)_\bullet \bullet \mathsf{ag}(\rho_1) \\
\mathsf{ex}(\rho_1)_\bullet \bullet \mathsf{ex}(\rho_2)_\bullet \bullet \mathsf{ex}(\rho_3)_\bullet \bullet \mathsf{ag}(\rho_2) \\
\mathsf{ex}(\rho_1)_\bullet \bullet \mathsf{ex}(\rho_2)_\bullet \bullet \mathsf{ex}(\rho_3)_\bullet \bullet \mathsf{ag}(\rho_3)
\end{gathered}$$

The first composite $\mathsf{ex}(\rho_1)_\bullet \bullet \mathsf{ex}(\rho_2)_\bullet \bullet \mathsf{ex}(\rho_3)_\bullet \bullet \mathsf{ag}(\rho_1)$ is defined because $\mathsf{ex}(\rho_1)_\bullet$ and $\mathsf{ex}(\rho_2)_\bullet \bullet \mathsf{ex}(\rho_3)_\bullet$ and $\mathsf{ag}(\rho_1)$ are pairwise-composable by assumption, hence the triple composite is defined by theorem 6.13. The analogous arguments show that the second and third composites are defined as well. □

6.2 Non-standard Lemmas

Lemma 6.16. If $\rho \bullet \llparenthesis \rho' \rrparenthesis$ defined then $\rho \bullet \rho'$ defined.

Proof. The composite $\rho \bullet \llparenthesis \rho' \rrparenthesis$ is well-defined if and only if ρ and $\llparenthesis \rho' \rrparenthesis$ have disjoint own-or-mut cells and imm cells that agree up to lifetimes. Unravelling the definition of $\llparenthesis - \rrparenthesis$ reveals that the cells of ρ' are a subset of those of $\llparenthesis - \rrparenthesis$, so the same condition holds of ρ and ρ'. □

Lemma 6.17. If $\rho \# \ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P})$ then $\rho \bowtie \rho_v \bullet \ell \mapsto \mathsf{own}(v)$

Proof. Let $\rho_o = \ell \mapsto \mathsf{own}(v)$ and $\rho_m = \ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P})$. By theorem 6.9, it's enough to show $\rho \bullet \rho_v \bullet \rho_o$ is well defined. By assumption, it holds that $\checkmark \rho \bullet \rho_m$, so $\llparenthesis \rho \bullet \rho_m \rrparenthesis = \mathsf{ex}(\rho)_\bullet \bullet (\rho_m \bullet \mathsf{ex}(\rho_v)_\bullet) \bullet (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v))$ is well-defined. Hence, ignoring $\mathsf{ex}(\rho)_\bullet$ and $\mathsf{ag}(\rho)$ in this composite, we have that $\rho_m \bullet \mathsf{ex}(\rho_v)_\bullet \bullet \mathsf{ag}(\rho_v) = \rho_m \bullet \llparenthesis \rho_v \rrparenthesis$ is well-defined. This implies $\ell \notin \mathrm{dom} \llparenthesis \rho_v \rrparenthesis$, so $\rho_o \bullet \llparenthesis \rho_v \rrparenthesis$ well-defined, so $\rho_o \bullet \rho_v$ well-defined by theorem 6.16. Well-definedness of $\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v)$ implies ρ and ρ_v agree on imm cells up to lifetimes, hence the same of ρ and $\rho_o \bullet \rho_v$ (since ρ_o contains no imm cells). Well-definedness of $\mathsf{ex}(\rho)_\bullet \bullet (\rho_m \bullet \mathsf{ex}(\rho_v)_\bullet)$ implies ρ and $\rho_m \bullet \rho_v$ have disjoint own-or-mut cells, hence the same of ρ and $\rho_o \bullet \rho_v$ (since ρ_o and ρ_m have the same own-or-mut cells). Putting these together shows ρ and $\rho_o \bullet \rho_v$ are composable as needed. □

Lemma 6.18. If $\rho_1 \bowtie \rho_2$ then $\mathsf{ex}(\rho_1 \bullet \rho_2)_\bullet$ and $\mathsf{ex}(\rho_1)_\bullet \bullet \mathsf{ex}(\rho_2)_\bullet$ are Kleene-equal (the left-hand side is defined iff the right-hand side is, and in case both are defined they are equal).

Proof. Since $\rho_1 \bowtie \rho_2$, it must be that ρ_1 and ρ_2 have disjoint own-or-mut cells. Hence, writing ρ_{12} for the composite $\rho_1 \bullet \rho_2$, the following string of Kleene-equalities holds:

$$\begin{aligned}
\mathsf{ex}(\rho_{12})_\bullet &= \rho_{12}|_{\mathsf{own}} \bullet \rho_{12}|_{\mathsf{mut}} \bullet \mathop{\Large\bullet}_{\mathsf{mut}(\_,\_,\rho',\_)\in\rho_{12}} \mathsf{ex}(\rho')_\bullet \\
&= (\rho_1|_{\mathsf{own}} \bullet \rho_2|_{\mathsf{own}}) \bullet (\rho_1|_{\mathsf{mut}} \bullet \rho_2|_{\mathsf{mut}}) \bullet \left(\mathop{\Large\bullet}_{\mathsf{mut}(\_,\_,\rho',\_)\in\rho_1} \mathsf{ex}(\rho')_\bullet\right) \bullet \left(\mathop{\Large\bullet}_{\mathsf{mut}(\_,\_,\rho',\_)\in\rho_2} \mathsf{ex}(\rho')_\bullet\right) \\
&= \left(\rho_1|_{\mathsf{own}} \bullet \rho_1|_{\mathsf{mut}} \bullet \mathop{\Large\bullet}_{\mathsf{mut}(\_,\_,\rho',\_)\in\rho_1} \mathsf{ex}(\rho')_\bullet\right) \bullet \left(\rho_2|_{\mathsf{own}} \bullet \rho_2|_{\mathsf{mut}} \bullet \mathop{\Large\bullet}_{\mathsf{mut}(\_,\_,\rho',\_)\in\rho_2} \mathsf{ex}(\rho')_\bullet\right) \\
&= \mathsf{ex}(\rho_1)_\bullet \bullet \mathsf{ex}(\rho_2)_\bullet
\end{aligned}$$

□

Definition 6.1. Let $\llparenthesis \rho \rrparenthesis_\circ \coloneqq \mathsf{ag}(\rho) \circ \mathsf{ex}(\rho)_\circ$.

Lemma 6.19. If $\llparenthesis \rho \rrparenthesis_\circ$ defined then $\llparenthesis \rho \rrparenthesis_\circ$ and $\llparenthesis \rho \rrparenthesis_\circ \circ \llparenthesis \rho \rrparenthesis_\circ$ are Kleene-equal.

Proof. By induction on ρ, mutual with the statement that $\mathsf{ag}(\rho)$ and $\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho)$ are Kleene equal. □

Lemma 6.20. If $\rho_1 \bowtie \rho_2$ then $\mathsf{ag}(\rho_1 \bullet \rho_2)$ and $\mathsf{ag}(\rho_1) \circ \mathsf{ag}(\rho_2)$ are Kleene-equal.

Proof. Since $\rho_1 \bowtie \rho_2$, it holds that the mut cells of ρ_1 and ρ_2 are disjoint and the imm cells of ρ_1 and ρ_2 agree up to lifetimes. Hence, writing ρ_{12} for the composite $\rho_1 \bullet \rho_2$,

$$\begin{aligned}
\mathsf{ag}(\rho_1 \bullet \rho_2) &= \rho_{12}|_{\mathsf{imm}} \circ \bigcirc_{\mathsf{mut}(\_,\_,\rho',\_)\in\rho_{12}} \mathsf{ag}(\rho') \circ \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_{12}} \llparenthesis \rho' \rrparenthesis_\circ \\
&= (\rho_1|_{\mathsf{imm}} \circ \rho_2|_{\mathsf{imm}}) \circ \left(\bigcirc_{\mathsf{mut}(\_,\_,\rho',\_)\in\rho_1} \mathsf{ag}(\rho') \circ \bigcirc_{\mathsf{mut}(\_,\_,\rho',\_)\in\rho_2} \mathsf{ag}(\rho')\right) \circ \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_{12}} \llparenthesis \rho' \rrparenthesis_\circ .
\end{aligned}$$

Now consider the final term in this equation, the big composite $\rho_{\mathsf{ag}} \coloneqq \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_{12}} \llparenthesis \rho' \rrparenthesis_\circ$. It has one component for each imm cell $(\_,\_,\rho')$ in ρ_{12}. The composition $\circ$ operates cellwise, and the imm cells of ρ_{12} are the union (up to lifetimes) of the imm cells of ρ_1 and the imm cells of ρ_2, so by inclusion-exclusion ρ_{ag} is equal to

$$\bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_1\setminus\rho_2} \llparenthesis \rho' \rrparenthesis_\circ \circ \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_2\setminus\rho_1} \llparenthesis \rho' \rrparenthesis_\circ \circ \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_1\cap\rho_2} \llparenthesis \rho' \rrparenthesis_\circ .$$

By theorem 6.19, we have that

$$\bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_1\cap\rho_2} \llparenthesis \rho' \rrparenthesis_\circ = \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_1\cap\rho_2} \left(\llparenthesis \rho' \rrparenthesis_\circ \circ \llparenthesis \rho' \rrparenthesis_\circ\right) = \left(\bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_1\cap\rho_2} \llparenthesis \rho' \rrparenthesis_\circ\right) \circ \left(\bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_1\cap\rho_2} \llparenthesis \rho' \rrparenthesis_\circ\right).$$

Hence,

$$\begin{aligned}
\rho_{\mathsf{ag}} &= \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_1\setminus\rho_2} \llparenthesis \rho' \rrparenthesis_\circ \circ \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_2\setminus\rho_1} \llparenthesis \rho' \rrparenthesis_\circ \circ \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_1\cap\rho_2} \llparenthesis \rho' \rrparenthesis_\circ \\
&= \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_1\setminus\rho_2} \llparenthesis \rho' \rrparenthesis_\circ \circ \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_2\setminus\rho_1} \llparenthesis \rho' \rrparenthesis_\circ \circ \left(\bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_1\cap\rho_2} \llparenthesis \rho' \rrparenthesis_\circ\right) \circ \left(\bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_1\cap\rho_2} \llparenthesis \rho' \rrparenthesis_\circ\right) \\
&= \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_1} \llparenthesis \rho' \rrparenthesis_\circ \circ \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_2} \llparenthesis \rho' \rrparenthesis_\circ .
\end{aligned}$$

Putting this all together,

$$\begin{aligned}
&\mathsf{ag}(\rho_1 \bullet \rho_2) \\
&= (\rho_1|_{\mathsf{imm}} \circ \rho_2|_{\mathsf{imm}}) \circ \left(\bigcirc_{\mathsf{mut}(\_,\_,\rho',\_)\in\rho_1} \mathsf{ag}(\rho') \circ \bigcirc_{\mathsf{mut}(\_,\_,\rho',\_)\in\rho_2} \mathsf{ag}(\rho')\right) \circ \rho_{\mathsf{ag}} \\
&= (\rho_1|_{\mathsf{imm}} \circ \rho_2|_{\mathsf{imm}}) \circ \left(\bigcirc_{\mathsf{mut}(\_,\_,\rho',\_)\in\rho_1} \mathsf{ag}(\rho') \circ \bigcirc_{\mathsf{mut}(\_,\_,\rho',\_)\in\rho_2} \mathsf{ag}(\rho')\right) \circ \left(\bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_1} \llparenthesis \rho' \rrparenthesis_\circ \circ \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_2} \llparenthesis \rho' \rrparenthesis_\circ\right) \\
&= \left(\rho_1|_{\mathsf{imm}} \circ \bigcirc_{\mathsf{mut}(\_,\_,\rho',\_)\in\rho_1} \mathsf{ag}(\rho') \circ \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_1} \llparenthesis \rho' \rrparenthesis_\circ\right) \circ \left(\rho_2|_{\mathsf{imm}} \circ \bigcirc_{\mathsf{mut}(\_,\_,\rho',\_)\in\rho_2} \mathsf{ag}(\rho') \circ \bigcirc_{\mathsf{imm}(\_,\_,\rho')\in\rho_2} \llparenthesis \rho' \rrparenthesis_\circ\right) \\
&= \mathsf{ag}(\rho_1) \circ \mathsf{ag}(\rho_2)
\end{aligned}$$

as needed. □

Lemma 6.21. If $\rho \mathrel{\#} \rho_v \bullet \ell \mapsto \mathsf{own}(v)$ then $\rho \bowtie \ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P})$

Proof. The hypothesis implies the composite $\rho \bullet \rho_v \bullet (\ell \mapsto \mathsf{own}(v))$ is well-defined, which implies $\ell \notin \mathrm{dom}(\rho)$, which implies $\rho \bowtie \ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P})$ as needed. □

Lemma 6.22. If $\rho \mathrel{\#} \ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P})$ then $\rho \mathrel{\#} \rho_v \bullet \ell \mapsto \mathsf{own}(v)$

Proof. Let $\rho_o = \ell \mapsto \mathsf{own}(v)$ and $\rho_m = \ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P})$, so we have $\rho \mathrel{\#} \rho_m$ with aim to show $\rho \mathrel{\#} \rho_v \bullet \rho_o$. Our hypothesis implies $\checkmark(\rho \bullet \ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P}))$, which amounts to well-definedness of the following composite:

$$\rho_{\mathsf{hyp}} \coloneqq \mathsf{ex}(\rho)_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet \bullet \rho_m \bullet (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v)).$$

We have that $\rho \bowtie \rho_v \bullet \rho_o$ by theorem 6.17, so it only remains to show $\checkmark(\rho \bullet \rho_v \bullet \rho_o)$, which amounts to showing well-definedness of the following composite:

$$\rho_{\mathsf{goal}} \coloneqq \mathsf{ex}(\rho \bullet \rho_v)_\bullet \bullet \rho_o \bullet \mathsf{ag}(\rho \bullet \rho_v).$$

By theorem 6.17, it holds that $\rho \bullet \rho_v \bullet \rho_o$ is well-defined, hence also that $\rho \bullet \rho_v$ is well-defined. This implies, by theorems 6.18 and 6.20, that well-definedness of ρ_{goal} is equivalent to well-definedness of

$$(\mathsf{ex}(\rho)_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet) \bullet \rho_o \bullet (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v)).$$

Since ρ_o contains a single own cell, this composite is well-defined if and only if the same composite is defined when ρ_o is replaced by ρ_m; this is precisely well-definedness of ρ_{hyp}. □

Lemma 6.23. If $\rho \mathrel{\#} \rho_v \bullet \ell \mapsto \mathsf{own}(v)$ then $\rho \mathrel{\#} \ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P})$

Proof. Analogous to theorem 6.22. Let $\rho_o = \ell \mapsto \mathsf{own}(v)$ and $\rho_m = \ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P})$, so we have $\rho \mathrel{\#} \rho_v \bullet \rho_o$ with aim to show $\rho \mathrel{\#} \rho_m$. We have $\rho \bowtie \rho_m$ by theorem 6.21, so it only remains to show $\checkmark(\rho \bullet \rho_m)$, which amounts to showing well-definedness of

$$\rho_{\mathsf{goal}} \coloneqq \mathsf{ex}(\rho)_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet \bullet \rho_m \bullet (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v))$$

given well-definedness of

$$\rho_{\mathsf{hyp}} \coloneqq \mathsf{ex}(\rho \bullet \rho_v)_\bullet \bullet \rho_o \bullet \mathsf{ag}(\rho \bullet \rho_v).$$

We have by the assumption $\rho \mathrel{\#} \rho_v \bullet \rho_o$ that $\rho \bullet \rho_v$ defined, so by theorems 6.18 and 6.20 the well-definedness of ρ_{hyp} is equivalent to well-definedness of

$$\mathsf{ex}(\rho \bullet \rho_v)_\bullet \bullet \rho_o \bullet \mathsf{ag}(\rho \bullet \rho_v).$$

Since ρ_o contains a single own cell, this composite is well-defined if and only if the same composite is defined when ρ_o is replaced by ρ_m; this is precisely well-definedness of ρ_{goal}, which is what we wanted to show. □

Lemma 6.24. $\rho \mathrel{\#} \ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P})$ iff $\rho \mathrel{\#} \rho_v \bullet \ell \mapsto \mathsf{own}(v)$

Proof. Combine theorems 6.22 and 6.23. □

Lemma 6.25. Assuming all resources and composition are defined, $\left[\!\!\left[\ell \mapsto \mathsf{mut}(n, v, \rho_v, \hat{P})\right]\!\!\right] = [\![\rho_v \bullet \ell \mapsto \mathsf{own}(v)]\!]$

Proof. By unfolding. □

Lemma 6.26. Assuming all resources and composition are defined, $[\![\ell \mapsto \mathsf{imm}(\alpha, v, \rho_v)]\!] = [\![\rho_v \bullet \ell \mapsto \mathsf{own}(v)]\!]$

Proof. By unfolding. □

Lemma 6.27. If $@\rho \sqsupset \alpha$ and $\rho \bullet \ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P}) \leftrightsquigarrow \rho'$ then $\rho' = \rho'/\ell \bullet \ell \mapsto \mathsf{mut}(\alpha, v', \rho'_v, \hat{P})$

Proof. Let $\rho_m = \ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P})$. By assumption, $(\!|\rho \bullet \rho_m|\!)$ and $(\!|\rho'|\!)$ have the same borrows. This implies there must be a mut cell in $(\!|\rho'|\!)$ matching $\ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P})$, which amounts to a v', ρ'_v such that $(\ell \mapsto \mathsf{mut}(\alpha, v', \rho'_v, \hat{P})) \in (\!|\rho'|\!)$. Furthermore, since $@\rho \sqsupset \alpha$, all borrows in $(\!|\rho'|\!)$ other than $(\ell \mapsto \mathsf{mut}(\alpha, v', \rho'_v, \hat{P}))$ must be disjoint from α, which by well-formedness of the resource ρ' implies that the cell $(\ell \mapsto \mathsf{mut}(\alpha, v', \rho'_v, \hat{P}))$ cannot be in any ρ'' for any $\mathsf{mut}(\_, \_, \rho'', \_)$ or $\mathsf{imm}(\_, \_, \rho'')$ in ρ'. Hence it must be that $\rho'(\ell) = \mathsf{mut}(\alpha, v', \rho'_v, \hat{P})$, so $\rho' = \rho'/\ell \bullet \ell \mapsto \mathsf{mut}(\alpha, v', \rho'_v, \hat{P})$ as needed. □

Lemma 6.28. Assuming all compositions are defined and valid, $\rho \bullet \ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P}) \leftrightsquigarrow \rho' \bullet \ell \mapsto \mathsf{mut}(\alpha, v', \rho_v', \hat{P})$ iff $\rho \bullet \ell \mapsto \mathsf{own}(v) \bullet \rho_v \leftrightsquigarrow \rho' \bullet \ell \mapsto \mathsf{own}(v') \bullet \rho_v'$

Proof. We have the following string of iffs: $\rho \bullet \ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P}) \leftrightsquigarrow \rho' \bullet \ell \mapsto \mathsf{mut}(\alpha, v', \rho_v', \hat{P})$ if and only if

$$\mathsf{ex}(\rho)_\bullet \bullet (\ell \mapsto \mathsf{mut}(\alpha, v, \rho_v, \hat{P})) \bullet \mathsf{ex}(\rho_v)_\bullet \bullet (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v))$$

and

$$\mathsf{ex}(\rho')_\bullet \bullet (\ell \mapsto \mathsf{mut}(\alpha, v', \rho_v', \hat{P})) \bullet \mathsf{ex}(\rho_v')_\bullet \bullet (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho_v'))$$

have the same borrows (by unravelling definitions), if and only if

$$\mathsf{ex}(\rho)_\bullet \bullet (\ell \mapsto \mathsf{own}(v)) \bullet \mathsf{ex}(\rho_v)_\bullet \bullet (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v))$$

and

$$\mathsf{ex}(\rho')_\bullet \bullet (\ell \mapsto \mathsf{own}(v')) \bullet \mathsf{ex}(\rho_v')_\bullet \bullet (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho_v'))$$

have the same borrows (by exclusivity of ℓ), if and only if $\rho \bullet \ell \mapsto \mathsf{own}(v) \bullet \rho_v \leftrightsquigarrow \rho' \bullet \ell \mapsto \mathsf{own}(v') \bullet \rho_v'$. □

Lemma 6.29. If $@\rho \sqsupset \alpha$ and $\rho \# \rho_v \bullet \ell \mapsto \mathsf{own}(v)$ and $\rho \bullet \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v) \leftrightsquigarrow \rho'$ then $\rho' = \rho'/\ell \bullet \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v)$.

Proof. Let $\rho_i = \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v)$. By assumption, $\llparenthesis \rho \bullet \rho_i \rrparenthesis$ and $\llparenthesis \rho' \rrparenthesis$ have the same borrows. And by assumption, $\rho \# \rho_v \bullet \ell \mapsto \mathsf{own}(v)$, so $\ell \notin \mathrm{dom}(\llparenthesis \rho \rrparenthesis)$. This implies there must be an imm cell in $\llparenthesis \rho' \rrparenthesis$ matching ρ_i exactly, ie $\llparenthesis \rho' \rrparenthesis(\ell) = \mathsf{imm}(\{\alpha\}, v, \rho_v)$. Furthermore, since $@\rho \sqsupset \alpha$, all borrows in $\llparenthesis \rho' \rrparenthesis$ other than ρ_i must be disjoint from α, which by well-formedness of the resource ρ' implies that the cell $(\mathsf{imm}(\{\alpha\}, v, \rho_v, \hat{P}))$ cannot be in any ρ'' for any $\mathsf{mut}(\_, \_, \rho'', \_)$ or $\mathsf{imm}(\_, \_, \rho'')$ in ρ'. Hence it must be that $\rho'(\ell) = \mathsf{imm}(\{\alpha\}, v, \rho_v,)$, so $\rho' = \rho'/\ell \bullet \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v)$ as needed. □

Lemma 6.30. If $\rho \bowtie (\rho_1 \circ \rho_2)$ and $\rho|_{\mathsf{imm}} = \varnothing$ then $\rho \bowtie \rho_1$ and $\rho \bowtie \rho_2$

Proof. Since $\rho|_{\mathsf{imm}} = \varnothing$, the fact that $\rho \bowtie (\rho_1 \circ \rho_2)$ implies $\mathrm{dom}(\rho) \cap \mathrm{dom}(\rho_1 \circ \rho_2) = \varnothing$.
Unfolding $\circ$, $\mathrm{dom}(\rho_1 \circ \rho_2) = \mathrm{dom}(\rho_1) \cup \mathrm{dom}(\rho_2)$. Therefore, $\mathrm{dom}(\rho) \cap (\mathrm{dom}(\rho_1) \cup \mathrm{dom}(\rho_2)) = \varnothing$, and therefore $\mathrm{dom}(\rho) \cap \mathrm{dom}(\rho_1) = \varnothing$ and $\mathrm{dom}(\rho) \cap \mathrm{dom}(\rho_2) = \varnothing$. Therefore by definition, $\rho \bowtie \rho_1$ and $\rho \bowtie \rho_2$. □

Lemma 6.31. If $\rho \bowtie \rho'$ then $\rho \circ \rho' = \rho \bullet \rho'$.

Proof. It suffices to show for any cells ψ and ψ', if $\psi \bowtie \psi'$ then $\psi \circ \psi' = \psi \bullet \psi'$. Unfolding $\psi \circ \psi'$, we have that either

- $\psi = \psi'$ and $\psi \circ \psi' = \psi$
- $\psi \neq \psi'$, and $\psi \bowtie \psi'$ so $\psi \circ \psi' = \psi \bullet \psi'$
- The last case is unreachable.

$\psi \circ \psi'$ only disagrees with $\bullet$ when $\psi = \psi' = \mathsf{own}(\_)$ or $\mathsf{mut}(\_, \_, \_, \_)$. But this is impossible since $\psi \bowtie \psi'$. □

Lemma 6.32. If $\mathsf{ex}(\rho)_\bullet$ defined, then $\mathsf{ex}(\rho)_\bullet = \mathsf{ex}(\rho)_\circ$.

Proof. By induction on ρ, unfolding ex, and repeatedly applying lemma 6.31. □

Lemma 6.33. If $\llparenthesis \rho \rrparenthesis$ defined, then $\llparenthesis \rho \rrparenthesis = \llparenthesis \rho \rrparenthesis_\circ$.

Proof. By unfolding $\llparenthesis - \rrparenthesis$ and $\llparenthesis - \rrparenthesis_\circ$, and applying lemmas 6.31 and 6.32. □

Lemma 6.34. If $\rho \# \rho_v \bullet \ell \mapsto \mathsf{own}(v)$ and $@\rho_v \sqsupset \alpha$ then $\rho \# \ell \mapsto \mathsf{imm}(\alpha, v, \rho_v)$

Proof. By lemma 6.11, we have $\rho \mathbin{\#} \rho_v$ and $\rho \mathbin{\#} \ell \mapsto \mathsf{own}(v)$. Unfolding these, we have $\ell \notin \mathrm{dom}(\llparenthesis \rho \bullet \rho_v \rrparenthesis)$, and by lemmas 6.20, 6.18, 6.31, and 6.32 the following are all defined and equal

$$\begin{aligned}\llparenthesis \rho \bullet \rho_v \rrparenthesis &= \mathsf{ex}(\rho \bullet \rho_v)_\bullet \bullet \mathsf{ag}(\rho \bullet \rho_v)\\ &= \mathsf{ex}(\rho)_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet \bullet (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v))\\ &= \mathsf{ex}(\rho)_\bullet \bullet (\mathsf{ex}(\rho_v)_\bullet \circ \mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v))\\ &= \mathsf{ex}(\rho)_\bullet \bullet (\mathsf{ex}(\rho_v)_\circ \circ \mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v))\\ &= \mathsf{ex}(\rho)_\bullet \bullet (\llparenthesis \rho_v \rrparenthesis_\circ \circ \mathsf{ag}(\rho))\end{aligned}$$

The last equality, with the fact that ℓ is not in the domain, is sufficient to complete the proof. □

Lemma 6.35. If $\llparenthesis \rho \bullet \rho' \rrparenthesis$ is defined then $\llparenthesis \rho \rrparenthesis$ and $\llparenthesis \rho' \rrparenthesis$ are defined.

Proof. Unfolding $\llparenthesis - \rrparenthesis$ in the hypothesis and applying lemmas 6.20 and 6.18, we get the following are all defined and equal:

$$\begin{aligned}\llparenthesis \rho \bullet \rho' \rrparenthesis &= \mathsf{ex}(\rho \bullet \rho')_\bullet \bullet \mathsf{ag}(\rho \bullet \rho')\\ &= \mathsf{ex}(\rho)_\bullet \bullet \mathsf{ex}(\rho')_\bullet \bullet (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho'))\end{aligned}$$

We can finish the proof by noting the following composability constraints:

- $\mathsf{ex}(\rho)_\bullet \bullet \mathsf{ex}(\rho')_\bullet \mathrel{\blacktriangleright\!\!\blacktriangleleft} \mathsf{ag}(\rho)$ by lemmas 6.30 and 6.36
- $\mathsf{ex}(\rho)_\bullet \mathrel{\blacktriangleright\!\!\blacktriangleleft} \mathsf{ag}(\rho)$ by the previous constraint, which implies $\llparenthesis \rho \rrparenthesis$ is defined
- $\mathsf{ex}(\rho)_\bullet \bullet \mathsf{ex}(\rho')_\bullet \mathrel{\blacktriangleright\!\!\blacktriangleleft} \mathsf{ag}(\rho')$ by lemmas 6.30 and 6.36
- $\mathsf{ex}(\rho')_\bullet \mathrel{\blacktriangleright\!\!\blacktriangleleft} \mathsf{ag}(\rho')$ by the previous constraint, which implies $\llparenthesis \rho' \rrparenthesis$ is defined

□

Lemma 6.36. If $\mathsf{ex}(\rho)_{\LEFTcircle}$ is defined then $\mathsf{ex}(\rho)_{\LEFTcircle}|_{\mathsf{imm}} = \varnothing$.

Proof. By induction on ρ and unfolding ex, noting at each level only mut and own are kept. □

Lemma 6.37. If $\rho \mathrel{\blacktriangleright\!\!\blacktriangleleft} \rho_1$ and $\rho \mathrel{\blacktriangleright\!\!\blacktriangleleft} \rho_2$ and $\rho_1 \bowtie \rho_2$ then $\rho \mathrel{\blacktriangleright\!\!\blacktriangleleft} \rho_1 \circ \rho_2$.

Proof. Unfolding the definition of $\mathrel{\blacktriangleright\!\!\blacktriangleleft}$, we have for any $\ell \in \mathrm{dom}(\rho) \cap \mathrm{dom}(\rho_1)$, $\rho(\ell) = \mathsf{imm}(\_, \rho, v)$ and $\rho_1(\ell) = \mathsf{imm}(\_, \rho, v)$, and similarly for ρ_2. By the definition of $\circ$, if $\ell' \in \mathrm{dom}(\rho) \cap \mathrm{dom}(\rho_1) \cap \mathrm{dom}(\rho_2)$, then $(\rho_1 \circ \rho_2)(\ell) = \mathsf{imm}(\_, \rho, v)$, which is sufficient to complete the proof. □

Lemma 6.38. If

- $\rho \mathbin{\#} \rho_v \bullet \ell \mapsto \mathsf{own}(v)^{(\mathrm{H1})}$
- $\rho' \mathbin{\#} \rho^{+(\mathrm{H2})}$
- $@\rho \sqsupset \alpha^{(\mathrm{H3})}$
- $@\rho' \sqsupset \alpha^{(\mathrm{H4})}$
- $\rho^{+}|_{\mathsf{own}} = \varnothing^{(\mathrm{H5})}$
- $\rho \bullet \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v) \leftrightsquigarrow \rho' \bullet \rho^{+(\mathrm{H6})}$

then $\rho' \bullet \rho^{+}/\ell \mathbin{\#} \rho_v \bullet \ell \mapsto \mathsf{own}(v)^{(\mathrm{G1})}$

Proof. By lemma 6.29 with H3 and H1 and H6, $\rho' \bullet \rho^+ = (\rho' \bullet \rho^+)/\ell \bullet \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v)^{(\mathrm{H7})}$.
By H4 and H7, $\rho' \bullet \rho^+ = \rho' \bullet \rho^+/\ell \bullet \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v)$.
Then in order to show G1, it suffices to show $\llparenthesis \rho' \bullet \rho^+/\ell \bullet \rho_v \bullet \ell \mapsto \mathsf{own}(v) \rrparenthesis$ is defined. By unfolding $\llparenthesis - \rrparenthesis$ and applying lemmas 6.18 and 6.20, the following are Kleene-equal, so it suffices to show any are defined to get all are defined:

$$\begin{aligned}\llparenthesis \rho' \bullet \rho^+/\ell \bullet \rho_v \bullet \ell \mapsto \mathsf{own}(v) \rrparenthesis &= \mathsf{ex}(\rho' \bullet \rho^+/\ell \bullet \rho_v \bullet \ell \mapsto \mathsf{own}(v))_\bullet \bullet \mathsf{ag}(\rho' \bullet \rho^+/\ell \bullet \rho_v \bullet \ell \mapsto \mathsf{own}(v)) \\ &= \mathsf{ex}(\rho')_\bullet \bullet \mathsf{ex}(\rho^+/\ell)_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet \bullet \ell \mapsto \mathsf{own}(v) \bullet (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho^+/\ell) \circ \mathsf{ag}(\rho_v))\end{aligned}$$

Applying similar reasoning to $\rho' \bullet \rho^+/\ell \bullet \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v)$ with H2, we get the following are all defined and equal:

$$\begin{aligned}\llparenthesis \rho' \bullet \rho^+/\ell \bullet \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v) \rrparenthesis &= \mathsf{ex}(\rho' \bullet \rho^+/\ell \bullet \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v))_\bullet \bullet \mathsf{ag}(\rho' \bullet \rho^+/\ell \bullet \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v)) \\ &= \mathsf{ex}(\rho')_\bullet \bullet \mathsf{ex}(\rho^+/\ell)_\bullet \bullet (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho^+/\ell) \circ \mathsf{ag}(\ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v))) \\ &= \mathsf{ex}(\rho')_\bullet \bullet \mathsf{ex}(\rho^+/\ell)_\bullet \bullet (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho^+/\ell) \circ \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v) \circ \llparenthesis \rho_v \rrparenthesis_\circ)\end{aligned}$$

By lemma 6.35 with H1, we have $\llparenthesis \rho_v \rrparenthesis$ is defined. Then by lemma 6.33, $\llparenthesis \rho_v \rrparenthesis = \llparenthesis \rho_v \rrparenthesis_\circ$. Therefore, we have the following are defined and equal:

$$\begin{aligned}\llparenthesis \rho' \bullet \rho^+/\ell \bullet \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v) \rrparenthesis &= \dots \\ &= \mathsf{ex}(\rho')_\bullet \bullet \mathsf{ex}(\rho^+/\ell)_\bullet \bullet (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho^+/\ell) \circ \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v) \circ \llparenthesis \rho_v \rrparenthesis) \\ &= \mathsf{ex}(\rho')_\bullet \bullet \mathsf{ex}(\rho^+/\ell)_\bullet \bullet (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho^+/\ell) \circ \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v) \circ (\mathsf{ex}(\rho_v)_\bullet \bullet \mathsf{ag}(\rho_v)))\end{aligned}$$

By lemma 6.31, we get the following are defined and equal:

$$\begin{aligned}\llparenthesis \rho' \bullet \rho^+/\ell \bullet \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v) \rrparenthesis &= \dots \\ &= \mathsf{ex}(\rho')_\bullet \bullet \mathsf{ex}(\rho^+/\ell)_\bullet \bullet (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho^+/\ell) \circ \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v) \circ \mathsf{ex}(\rho_v)_\bullet \circ \mathsf{ag}(\rho_v))\end{aligned}$$

Applying lemmas 6.30 and 6.36 multiple times, we get:

- $\mathsf{ex}(\rho')_\bullet \bullet \mathsf{ex}(\rho^+/\ell)_\bullet \bowtie (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho^+/\ell) \circ \mathsf{ag}(\rho_v))$
- $\mathsf{ex}(\rho')_\bullet \bullet \mathsf{ex}(\rho^+/\ell)_\bullet \bowtie \mathsf{ex}(\rho_v)_\bullet$
- $\mathsf{ex}(\rho')_\bullet \bullet \mathsf{ex}(\rho^+/\ell)_\bullet \bowtie \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_v)$, which implies $\mathsf{ex}(\rho')_\bullet \bullet \mathsf{ex}(\rho^+/\ell)_\bullet \bowtie \ell \mapsto \mathsf{own}(v)$.

With these facts, it suffices to show $\mathsf{ex}(\rho_v)_\bullet \bullet \ell \mapsto \mathsf{own}(v) \bowtie (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho^+/\ell) \circ \mathsf{ag}(\rho_v))$. And by lemma 6.37 with $\llparenthesis \rho_v \bullet \ell \mapsto \mathsf{own}(v) \rrparenthesis$ defined from lemma 6.35 with H1, it suffices to show $\mathsf{ex}(\rho_v)_\bullet \bullet \ell \mapsto \mathsf{own}(v) \bowtie (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho^+/\ell))$. By lemma 6.36, $(\mathsf{ex}(\rho_v)_\bullet \bullet \ell \mapsto \mathsf{own}(v))|_{\mathsf{imm}} = \varnothing$, so it suffices to show

$$\mathrm{dom}(\mathsf{ex}(\rho_v)_\bullet \bullet \ell \mapsto \mathsf{own}(v)) \cap \mathrm{dom}(\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho^+/\ell)) = \varnothing$$

Assume for sake of contradiction that $\ell' \in \mathrm{dom}(\mathsf{ex}(\rho_v)_\bullet \bullet \ell \mapsto \mathsf{own}(v))$ and $\ell' \in \mathrm{dom}(\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho^+/\ell))$. By the definition of ag, $\ell' \in \mathrm{dom}(\rho'|_{\mathsf{imm}})$, $\ell' \in \mathrm{dom}(\rho^+/\ell|_{\mathsf{imm}})$, or there are some ℓ'', ρ''_v such that $(\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho^+/\ell))(\ell'') = \mathsf{imm}(\_, \_, \rho''_v)$ and $\ell' \in \mathrm{dom}(\llparenthesis \rho''_v \rrparenthesis_\circ)$. In either of the first two cases, by H6, $\ell' \in \llparenthesis \rho \rrparenthesis|_{\mathsf{imm}}$, which is a contradiction with the fact that $\rho \mathbin{\#} \rho_v \bullet \ell \mapsto \mathsf{own}(v)$ from H1. And in the third, by the same reasoning about update, $\ell'' \in \mathrm{dom}(\llparenthesis \rho \rrparenthesis|_{\mathsf{imm}})$, and therefore $\ell' \in \mathrm{dom}(\mathsf{ag}(\rho))$, which again is a contradiction for the same reason. □

Definition 6.2. Let $\psi \sim \psi' := (\psi = \mathsf{mut}(\alpha, \_, \_, \hat{P}) \wedge \psi' = \mathsf{mut}(\alpha, \_, \_, \hat{P})) \vee (\psi = \psi' = \mathsf{imm}(\overline{\alpha}, v, \rho))$.

Lemma 6.39. If

- $\rho \mathbin{\#} \ell \mapsto \mathsf{own}(v) \bullet \rho_v{}^{(\mathrm{H1})}$
- $\rho' \mathbin{\#} \ell \mapsto \mathsf{own}(v) \bullet \rho_v{}^{(\mathrm{H2})}$

- $\rho \bullet \ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \leftrightsquigarrow \rho' \bullet \ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v)^{(\mathrm{H3})}$

then $\rho \bullet \ell \mapsto \mathsf{own}(v) \bullet \rho_v \leftrightsquigarrow \rho' \bullet \ell \mapsto \mathsf{own}(v) \bullet \rho_v$

Proof. By H1 and H2, we have $\rho_{of} = \llparenthesis \rho \bullet \ell \mapsto \mathsf{own}(v) \bullet \rho_v \rrparenthesis$ and $\rho'_{of} = \llparenthesis \rho' \bullet \ell \mapsto \mathsf{own}(v) \bullet \rho_v \rrparenthesis$ are defined. We want to show $\mathrm{dom}(\rho_{of}|_{\mathsf{imm},\mathsf{mut}}) = \mathrm{dom}(\rho'_{of}|_{\mathsf{imm},\mathsf{mut}})^{(\mathrm{G1})}$ and $\forall\, \ell \in \mathrm{dom}(\rho_{of}|_{\mathsf{imm},\mathsf{mut}}).\ \rho_{of}(\ell) \sim \rho'_{of}(\ell)^{(\mathrm{G2})}$. By lemmas 6.18 and 6.20, we have all of the following are defined and equal:

$$\begin{aligned}
\rho_{of} &= \llparenthesis \rho \bullet \ell \mapsto \mathsf{own}(v) \bullet \rho_v \rrparenthesis \\
&= \mathsf{ex}(\rho \bullet \ell \mapsto \mathsf{own}(v) \bullet \rho_v)_\bullet \bullet \mathsf{ag}(\rho \bullet \ell \mapsto \mathsf{own}(v) \bullet \rho_v) \\
&= \mathsf{ex}(\rho)_\bullet \bullet \mathsf{ex}(\ell \mapsto \mathsf{own}(v))_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet \bullet (\mathsf{ag}(\rho) \circ \mathsf{ag}(\ell \mapsto \mathsf{own}(v)) \circ \mathsf{ag}(\rho_v)) \\
&= \ell \mapsto \mathsf{own}(v) \bullet \mathsf{ex}(\rho)_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet \bullet (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v))
\end{aligned}$$

$$\begin{aligned}
\rho'_{of} &= \dots \\
&= \ell \mapsto \mathsf{own}(v) \bullet \mathsf{ex}(\rho')_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet \bullet (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho_v))
\end{aligned}$$

By H3, we also have $\rho_{if} = \llparenthesis \rho \bullet \ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \rrparenthesis$ and $\rho'_{if} = \llparenthesis \rho' \bullet \ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \rrparenthesis$ are defined, and $\mathrm{dom}(\rho_{if}|_{\mathsf{imm},\mathsf{mut}}) = \mathrm{dom}(\rho'_{if}|_{\mathsf{imm},\mathsf{mut}})^{(\mathrm{H4})}$. Applying similar reasoning to above:

$$\begin{aligned}
\rho_{if} &= \llparenthesis \rho \bullet \ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \rrparenthesis \\
&= \mathsf{ex}(\rho \bullet \ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v))_\bullet \bullet \mathsf{ag}(\rho \bullet \ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v)) \\
&= \mathsf{ex}(\rho)_\bullet \bullet \mathsf{ex}(\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v))_\bullet \bullet (\mathsf{ag}(\rho) \circ \mathsf{ag}(\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v))) \\
&= \mathsf{ex}(\rho)_\bullet \bullet (\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \circ \mathsf{ag}(\rho) \circ \llparenthesis \rho_v \rrparenthesis_\circ)
\end{aligned}$$

$$\begin{aligned}
\rho'_{if} &= \dots \\
&= \mathsf{ex}(\rho')_\bullet \bullet (\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \circ \mathsf{ag}(\rho') \circ \llparenthesis \rho_v \rrparenthesis_\circ)
\end{aligned}$$

By lemma 6.10 with H1, $\checkmark \rho_v$. Then by lemma 6.35, $\llparenthesis \rho_v \rrparenthesis = \llparenthesis \rho_v \rrparenthesis_\circ$. Rewriting, unfolding $\llparenthesis - \rrparenthesis$, and using lemma 6.31 in the previous equalities:

$$\begin{aligned}
\rho_{if} &= \dots \\
&= \mathsf{ex}(\rho)_\bullet \bullet (\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \circ \mathsf{ag}(\rho) \circ \llparenthesis \rho_v \rrparenthesis) \\
&= \mathsf{ex}(\rho)_\bullet \bullet (\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \circ \mathsf{ag}(\rho) \circ (\mathsf{ex}(\rho_v)_\bullet \bullet \mathsf{ag}(\rho_v))) \\
&= \mathsf{ex}(\rho)_\bullet \bullet (\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \circ \mathsf{ag}(\rho) \circ \mathsf{ex}(\rho_v)_\bullet \circ \mathsf{ag}(\rho_v)) \\
&= \mathsf{ex}(\rho)_\bullet \bullet (\mathsf{ex}(\rho_v)_\bullet \circ (\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \circ (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v))))
\end{aligned}$$

$$\begin{aligned}
\rho'_{if} &= \dots \\
&= \mathsf{ex}(\rho')_\bullet \bullet (\mathsf{ex}(\rho_v)_\bullet \circ (\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \circ (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho_v))))
\end{aligned}$$

Note we have the following composability statements:

- $\mathsf{ex}(\rho_v)_\bullet \bowtie \mathsf{ag}(\rho_v)$, from $\checkmark \rho_v$
- $\mathsf{ex}(\rho_v)_\bullet \bowtie \mathsf{ag}(\rho)$, from the rewritten form of ρ_{of} with lemmas 6.30 and 6.36.
- $\mathsf{ex}(\rho_v)_\bullet \bowtie \mathsf{ag}(\rho')$, similarly from the rewritten form of ρ'_{of} with lemmas 6.30 and 6.36.
- $\mathsf{ex}(\rho_v)_\bullet \bowtie \ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v)$, since $\mathsf{ex}(\rho_v)_\bullet \bowtie \ell \mapsto \mathsf{own}(v)$ and $\mathsf{ex}(\rho_v)_\bullet|_{\mathsf{imm}} = \varnothing$ by lemma 6.36.

With these statements and lemmas 6.37 and 6.31, we get:

$$\begin{aligned}\rho_{if} &= \ldots \\ &= \mathsf{ex}(\rho)_\bullet \bullet (\mathsf{ex}(\rho_v)_\bullet \circ (\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \circ (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v)))) \\ &= \mathsf{ex}(\rho)_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet \bullet (\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \circ (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v)))\end{aligned}$$

$$\begin{aligned}\rho'_{if} &= \ldots \\ &= \mathsf{ex}(\rho')_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet \bullet (\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \circ (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho_v)))\end{aligned}$$

By the rewritings of ρ_{of} and ρ'_{of}, we have:

$$\begin{aligned}&\ell \mapsto \mathsf{own}(v) \bowtie \mathsf{ex}(\rho)_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet \bullet (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v)) \\ &\ell \mapsto \mathsf{own}(v) \bowtie \mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v) \\ &\ell \mapsto \mathsf{own}(v) \bowtie \mathsf{ex}(\rho')_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet \bullet (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho_v)) \\ &\ell \mapsto \mathsf{own}(v) \bowtie \mathsf{ag}(\rho') \circ \mathsf{ag}(\rho_v)\end{aligned}$$

Therefore, $\ell \notin \mathrm{dom}(\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v))$ and similarly for ρ', so:

$$\begin{aligned}&\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \bowtie \mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v) \\ &\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \bowtie \mathsf{ag}(\rho') \circ \mathsf{ag}(\rho_v)\end{aligned}$$

With these and lemma 6.31, we get:

$$\begin{aligned}\rho_{if} &= \ldots \\ &= \mathsf{ex}(\rho)_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet \bullet (\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \circ (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v))) \\ &= \ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \bullet \mathsf{ex}(\rho)_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet \bullet (\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v))\end{aligned}$$

$$\begin{aligned}\rho'_{if} &= \ldots \\ &= \ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v) \bullet \mathsf{ex}(\rho')_\bullet \bullet \mathsf{ex}(\rho_v)_\bullet \bullet (\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho_v))\end{aligned}$$

Now the only difference between ρ_{of} and ρ_{if}, as well as ρ'_{of} and ρ'_{if}, is $\ell \mapsto \mathsf{own}(v)$ vs $\ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho_v)$, and we additionally know $\ell \notin \mathrm{dom}(\mathsf{ag}(\rho) \circ \mathsf{ag}(\rho_v))$, and $\ell \notin \mathrm{dom}(\mathsf{ag}(\rho') \circ \mathsf{ag}(\rho_v))$. Therefore we have G1 and G2:

$$\begin{aligned}\mathrm{dom}(\rho_{of})|_{\mathsf{imm},\mathsf{mut}} = \mathrm{dom}(\rho'_{of})|_{\mathsf{imm},\mathsf{mut}} &= \mathrm{dom}(\rho_{if}|_{\mathsf{imm},\mathsf{mut}})/\ell = \mathrm{dom}(\rho'_{if}|_{\mathsf{imm},\mathsf{mut}})/\ell \\ \rho_{of}|_{\mathsf{imm},\mathsf{mut}} &= \rho_{if}|_{\mathsf{imm},\mathsf{mut}}/\ell \\ \rho'_{of}|_{\mathsf{imm},\mathsf{mut}} &= \rho'_{if}|_{\mathsf{imm},\mathsf{mut}}/\ell\end{aligned}$$

□

Lemma 6.40. $\ell \mapsto \mathsf{own}(v_1) \# \rho$ if any only if $\ell \mapsto \mathsf{own}(v_2) \# \rho$

Proof. By the definition of #, $\ell \notin (\!|\rho|\!)$, so the condition follows immediately. □

Lemma 6.41. If $\ell \mapsto \mathsf{own}(-) \bowtie \rho$, then $\ell \notin \rho$.

Proof. By definition. □

Lemma 6.42. If $\ell \mapsto \mathsf{mut}(-,-,-,-) \bowtie \rho$, then $\ell \notin \rho$.

Proof. By definition. □

Lemma 6.43. $\ell \mapsto \mathsf{imm}(\overline{\alpha} \cup \overline{\beta}, v, \rho') = \ell \mapsto \mathsf{imm}(\overline{\alpha}, v, \rho') \bullet \ell \mapsto \mathsf{imm}(\overline{\beta}, v, \rho')$

Proof. By definition. □

Lemma 6.44. If $\ell \mapsto \mathsf{imm}(\overline{\alpha}, v_1, \rho_1') \bowtie \ell \mapsto \mathsf{imm}(\overline{\beta}, v_2, \rho_2')$, then $v_1 = v_2$ and $\rho_1' = \rho_2'$.

Proof. By definition. □

Lemma 6.45. $@(\rho_1 \bullet \rho_2) \sqsupset \alpha$ if and only if $@\rho_1 \sqsupset \alpha$ and $\rho_2 \sqsupset \alpha$.

Proof. In either direction, this follows from noting that if $\ell \in \mathrm{dom}(\rho_1) \cap \mathrm{dom}(\rho_2)$, then $\rho_1(\ell) = \mathsf{imm}(\overline{\alpha}, v, \rho)$ and $\rho_2(\ell) = \mathsf{imm}(\overline{\beta}, v, \rho)$, And $\overline{\alpha} \cup \overline{\beta} \sqsupset \alpha$ iff $\overline{\alpha} \sqsupset \alpha$ and $\overline{\beta} \sqsupset \alpha$. □

Lemma 6.46. $\rho_1 \# \rho_2 \bullet \rho_3$ if and only if $\rho_1 \bullet \rho_2 \# \rho_3$.

Proof. By unfolding # and lemma 6.3. □

Lemma 6.47. $\rho \leftrightsquigarrow \rho$

Proof. By definition. □

Lemma 6.48. If $\rho_1 \# \rho_2$ and $\rho_1 \# \rho_3$ and $\rho_2 \leftrightsquigarrow \rho_3$, then $\rho_1 \bullet \rho_2 \leftrightsquigarrow \rho_1 \bullet \rho_3$.

Proof. By the compatibility hypotheses, we have $\checkmark(\rho_1 \bullet \rho_2)$ and $\checkmark(\rho_1 \bullet \rho_3)$. It suffices to show that $\mathrm{dom}(\llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis|_{\mathsf{mut,imm}}) = \mathrm{dom}(\llparenthesis \rho_1 \bullet \rho_3 \rrparenthesis|_{\mathsf{mut,imm}})$ and for every $\ell \in \mathrm{dom}(\llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis|_{\mathsf{mut,imm}})$, $\llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis(\ell) \sim \llparenthesis \rho_1 \bullet \rho_3 \rrparenthesis(\ell)$.

By unfolding $\checkmark$, $\llparenthesis - \rrparenthesis$, and by lemmas 6.20 and 6.18, the following equalities hold, with all resources defined:

$$\begin{aligned}\llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis &= \mathsf{ex}(\rho_1 \bullet \rho_2)_\bullet \bullet \mathsf{ag}(\rho_1 \bullet \rho_2) \\ &= \mathsf{ex}(\rho_1)_\bullet \bullet \mathsf{ex}(\rho_2)_\bullet \bullet (\mathsf{ag}(\rho_1) \circ \mathsf{ag}(\rho_2))\end{aligned}$$

$$\begin{aligned}\llparenthesis \rho_1 \bullet \rho_3 \rrparenthesis &= \mathsf{ex}(\rho_1 \bullet \rho_3)_\bullet \bullet \mathsf{ag}(\rho_1 \bullet \rho_3) \\ &= \mathsf{ex}(\rho_1)_\bullet \bullet \mathsf{ex}(\rho_3)_\bullet \bullet (\mathsf{ag}(\rho_1) \circ \mathsf{ag}(\rho_3))\end{aligned}$$

From unfolding $\rho_2 \leftrightsquigarrow \rho_3$, we get that $\mathrm{dom}(\llparenthesis \rho_2 \rrparenthesis|_{\mathsf{mut,imm}}) = \mathrm{dom}(\llparenthesis \rho_3 \rrparenthesis|_{\mathsf{mut,imm}})$. Therefore the domain constraint follows immediately from the equalities above.

Let $\ell \in \mathrm{dom}(\llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis|_{\mathsf{mut,imm}})$. We want to show $\llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis(\ell) \sim \llparenthesis \rho_1 \bullet \rho_3 \rrparenthesis(\ell)$. By lemma 6.36, all of the domains of ex resources contain no imms, and therefore we get that the domains of $\mathsf{ex}(\rho_1)$, $\mathsf{ex}(\rho_2)$, and $\mathsf{ag}(\rho_1) \circ \mathsf{ag}(\rho_2)$ are all disjoint, and similarly for ρ_3. Then there are 3 cases:

- $\ell \in \mathrm{dom}(\mathsf{ex}(\rho_1))$. Then $\mathsf{ex}(\rho_1)(\ell) = \llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis(\ell) = \llparenthesis \rho_1 \bullet \rho_3 \rrparenthesis(\ell)$
- $\ell \in \mathrm{dom}(\mathsf{ex}(\rho_2))$. Then from our update hypothesis, we have $\llparenthesis \rho_2 \rrparenthesis(\ell) \sim \llparenthesis \rho_3 \rrparenthesis(\ell)$, which is sufficient since $\llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis(\ell) = \llparenthesis \rho_2 \rrparenthesis(\ell)$ and $\llparenthesis \rho_1 \bullet \rho_3 \rrparenthesis(\ell) = \llparenthesis \rho_3 \rrparenthesis(\ell)$.
- $\ell \in \mathrm{dom}(\mathsf{ag}(\rho_1) \circ \mathsf{ag}(\rho_2))$. If $\ell \notin \mathrm{dom}(\mathsf{ag}(\rho_1)) \cap \mathrm{dom}(\mathsf{ag}(\rho_2))$, then we are done by similar reasoning to the previous cases. Otherwise, by the definition of ag, either $\ell \in \mathrm{dom}(\rho_1|_{\mathsf{imm}})$ or there are some ℓ', ρ' such that $\mathsf{ag}(\rho_1)(\ell') = \mathsf{imm}(\_, \_, \rho')$ and $\ell \in \mathrm{dom}(\llparenthesis \rho' \rrparenthesis_\circ)$, and similarly for ρ_2. Otherwise, unfolding $\circ$, there are 4 cases:
  - $\mathsf{ag}(\rho_1)(\ell) = \mathsf{ag}(\rho_2)(\ell)$. Then $\llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis(\ell) = \llparenthesis \rho_1 \bullet \rho_3 \rrparenthesis(\ell)$.
  - $\mathsf{ag}(\rho_1)(\ell) \bowtie \mathsf{ag}(\rho_2)(\ell)$. Then there are $\overline{\alpha}, \overline{\beta}, v, \rho$ such that $\mathsf{ag}(\rho_1)(\ell) = \mathsf{imm}(\overline{\alpha}, v, \rho)$ and $\mathsf{ag}(\rho_2)(\ell) = \mathsf{imm}(\overline{\beta}, v, \rho)$. From the update hypothesis, we get $\mathsf{ag}(\rho_2)(\ell) = \mathsf{ag}(\rho_3)(\ell)$, which is sufficient with the above to show $\llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis(\ell) \sim \llparenthesis \rho_1 \bullet \rho_3 \rrparenthesis(\ell)$.
  - $\exists\, \alpha, \beta, v, \rho_i, \hat{P}, \hat{Q}$ such that $\mathsf{ag}(\rho_1)(\ell) = \mathsf{mut}(\alpha, v, \rho_i, \hat{P})$ and $\mathsf{ag}(\rho_2)(\ell) = \mathsf{mut}(\beta, v, \rho_i, \hat{Q})$. By the update hypothesis, we have $\mathsf{ag}(\rho_3)(\ell) = \mathsf{mut}(\beta, \_, \_, \hat{Q})$. And furthermore, by the definition of ag, there must exist ℓ', ρ' such that $\mathsf{ag}(\rho_2)(\ell') = \mathsf{imm}(\_, \_, \rho')$ and $\mathsf{ag}(\rho_2)(\ell) = \llparenthesis \rho' \rrparenthesis_\circ(\ell)$. By the update hypothesis, we also have $\mathsf{ag}(\rho_3)(\ell') = \mathsf{ag}(\rho_2)(\ell')$, which implies $\mathsf{ag}(\rho_3)(\ell) = \mathsf{mut}(\beta, v, \rho_i, \hat{Q})$. Therefore, $\mathsf{ag}(\rho_1)(\ell) \circ \mathsf{ag}(\rho_2)(\ell) = \mathsf{ag}(\rho_1)(\ell) \circ \mathsf{ag}(\rho_3)(\ell) = \mathsf{mut}(\alpha \sqcap \beta, v, \rho_i, \hat{P} \wedge \hat{Q})$.

- $\exists\, \alpha, v, \rho_i, \hat{P}$ such that $\mathsf{ag}(\rho_i)(\ell) = \mathsf{mut}(\alpha, v, \rho_i, \hat{P})$ and $\mathsf{ag}(\rho_{3-i})(\ell) = \mathsf{own}(v)$. If $i = 1$ then we're done, because $\llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis(\ell) = \llparenthesis \rho_1 \bullet \rho_3 \rrparenthesis(\ell) = \llparenthesis \rho_1 \rrparenthesis(\ell)$. Otherwise, by the update hypothesis, $\llparenthesis \rho_3 \rrparenthesis(\ell) = \mathsf{mut}(\alpha, \_, \_, \hat{P})$. By the definition of $\mathsf{ag}(\rho_2)$, there are ℓ', ρ' such that $\llparenthesis \rho_2 \rrparenthesis(\ell') = \mathsf{imm}(\_, \_, \rho')$ and $\ell \in \mathrm{dom}(\llparenthesis \rho' \rrparenthesis_\circ)$. Then by the update relation, $\llparenthesis \rho_3 \rrparenthesis(\ell') = \mathsf{imm}(\_, \_, \rho')$, and therefore $\mathsf{ag}(\rho_3)(\ell) = \mathsf{mut}(\alpha, v, \rho_i, \hat{P})$. And finally, $\mathsf{ag}(\rho_2)(\ell) = \mathsf{ag}(\rho_3)(\ell)$, so $\llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis(\ell) = \llparenthesis \rho_1 \bullet \rho_3 \rrparenthesis(\ell)$.
- $\exists\, \overline{\alpha}, \beta, v, \rho_i, \hat{P}$ such that $\mathsf{ag}(\rho_i)(\ell) = \mathsf{imm}(\overline{\alpha}, v, \rho_i)$ and $\mathsf{ag}(\rho_{3-i})(\ell) \in \{\mathsf{own}(v), \mathsf{mut}(\beta, v, \rho', \hat{P})\}$. If $i = 1$, then we're done because $\mathsf{ag}(\rho_1)(\ell) = \llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis(\ell) = \llparenthesis \rho_1 \bullet \rho_3 \rrparenthesis(\ell)$. Otherwise, by the update hypothesis, $\mathsf{ag}(\rho_2)(\ell) = \mathsf{ag}(\rho_3)(\ell) = \llparenthesis \rho_1 \bullet \rho_2 \rrparenthesis(\ell) = \llparenthesis \rho_1 \bullet \rho_3 \rrparenthesis(\ell)$.

□

Lemma 6.49. If $\rho_1 \leftrightsquigarrow \rho_2$ and $\rho_2 \leftrightsquigarrow \rho_3$, then $\rho_1 \leftrightsquigarrow \rho_3$.

Proof. Follows from noting that $\sim$ is transitive, since imms are required to be equal and muts are required to have the same lifetime and predicates □

Lemma 6.50. If $@\rho \sqsupset \alpha$ and $\rho \leftrightsquigarrow \rho'$, then $@\rho' \sqsupset \alpha$.

Proof. Follows from unfolding the update relation and noting that all borrows must have the same lifetime before and after updating. □

Lemma 6.51. If $\llparenthesis \rho \rrparenthesis(\ell) = \mathsf{imm}(\overline{\alpha}, \rho_i, v)$ and $\llparenthesis \rho' \rrparenthesis(\ell) = \mathsf{imm}(\overline{\beta}, \rho_i, v)$ and $\rho \# \rho'$ then $\llparenthesis \rho \bullet \rho' \rrparenthesis(\ell) = \mathsf{imm}(\overline{\alpha} \cup \overline{\beta}, \rho_i, v)$

Proof. Follows by lemma 6.20, noting that by the definition of $\circ$ and $\bullet$, $\mathsf{imm}(\overline{\alpha}, \rho_i, v) \circ \mathsf{imm}(\overline{\beta}, \rho_i, v) = \mathsf{imm}(\overline{\alpha}, \rho_i, v) \bullet \mathsf{imm}(\overline{\beta}, \rho_i, v) = \mathsf{imm}(\overline{\alpha} \bullet \overline{\beta}, \rho_i, v)$. □

Definition 6.3. $\rho \boxminus \rho' \triangleq \rho|_{\mathsf{own},\mathsf{mut}} \bullet \rho''$ where

- $\rho'|_{\mathsf{own},\mathsf{mut}} = \varnothing$
- $\rho'' \leq \rho|_{\mathsf{imm}}$
- if $\ell \in \mathrm{dom}(\rho|_{\mathsf{imm}}) \setminus \mathrm{dom}(\rho')$ then $\ell \in \mathrm{dom}(\rho'')$
- if $\ell \in \mathrm{dom}(\rho|_{\mathsf{imm}}) \cap \mathrm{dom}(\rho')$ and $\rho(\ell) = \mathsf{imm}(\overline{\alpha}, \rho_i, v)$ and $\rho'(\ell) = \mathsf{imm}(\overline{\beta}, \rho_i, v)$ then
  - if $\overline{\alpha} \setminus \overline{\beta} = \varnothing$, then $\ell \notin \rho''$,
  - if $\overline{\alpha} \setminus \overline{\beta} \neq \varnothing$, then $\rho'(\ell) = \mathsf{imm}(\overline{\alpha} \setminus \overline{\beta}, \rho_i, v)$

Intuitively, $\rho \boxminus \rho'$ is ρ without the immutable borrows in ρ'. But since immutable borrows can alias at the same location, "without" means removing the lifetimes of borrows from ρ', but keeping the lifetimes only in ρ. One could define $\boxminus$ so that ρ' can contain own/mut as well, but it doesn't seem useful to do so.

This subtraction operation is used below, particularly in the following lemma, which is the foundation for the reborrow wp rule. When we run with the reborrowed resource, in order to simulate the run with the borrowed resource, we need to "perform surgery" on the resource to remove traces of the reborrow. In the frame rules this surgery is "easy" (haha...), because we originally have an owned resource. Here, every location is immutably borrowed and may be freely aliased, so the best we can do is remove the fresh parts of the reborrow. By subtracting the reborrowed resource, we get exactly the "leftovers" we need to keep with the immutable borrow to complete the proof.

Lemma 6.52. Let $\rho_{\mathsf{reb}} = \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}})}$. If $\rho \in \mathsf{reb}_\alpha(\rho'_i)$ and $\rho \bullet \rho_e \leftrightsquigarrow \rho' \bullet \rho^+$ and $@\rho_e \sqsupset \alpha$ and $@\rho' \sqsupset \alpha$ then $\rho^+ = (\rho^+ \boxminus \rho_{\mathsf{reb}}) \bullet \rho_{\mathsf{reb}}$ and $@(\rho^+ \boxminus \rho_{\mathsf{reb}}) \sqsupset \alpha$

Proof. Unfolding reb in $\rho \in \mathsf{reb}_\alpha(\rho'_i)$, we get $\rho|_{\mathsf{own},\mathsf{mut}} = \varnothing$, $\rho'_i \sqsupset \alpha$, and for every $\ell \in \mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}})$, if $\ell \in \mathrm{dom}(\rho)$, then there are ρ_ℓ, v_ℓ such that $\rho(\ell) = \mathsf{imm}(\{\alpha\}, \rho_\ell, v_\ell)$.

Let $\ell \in \mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}}) \cap \mathrm{dom}(\rho)$. By the update hypothesis, there is a $\overline{\beta_\ell}$ such that $\llparenthesis \rho \bullet \rho_e \rrparenthesis(\ell) = \llparenthesis \rho' \bullet \rho^+ \rrparenthesis(\ell) = \mathsf{imm}(\overline{\beta_\ell}, \rho_\ell, v_\ell)$ and $\alpha \in \overline{\beta_\ell}$. Since $\rho' \sqsupset \alpha$, it must be the case that there is a $\overline{\beta^+_\ell} \subseteq \overline{\beta_\ell}$ such that $\llparenthesis \rho^+ \rrparenthesis(\ell) = \mathsf{imm}(\overline{\beta^+_\ell}, \rho_\ell, v_\ell)$, with $\alpha \in \overline{\beta^+_\ell}$. And since $\rho'_i, \rho_e \sqsupset \alpha$, there are no borrows, mutable or immutable, at any lifetime shorter than α, so

there cannot be any borrow that contains $\rho(\ell) = \ell \mapsto \mathsf{imm}(\{\alpha\}, \rho_\ell, v_\ell)$.
Therefore, $\rho^+ = (\rho^+ \boxminus \ell \mapsto \mathsf{imm}(\{\alpha\}, \rho_\ell, v_\ell)) \bullet \ell \mapsto \mathsf{imm}(\{\alpha\}, \rho_\ell, v_\ell)^{(\mathrm{H1})}$.

Note that

$$\rho_{\mathsf{reb}} = \mathop{\Large\bullet}_{\ell \in \mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}}) \cap \mathrm{dom}(\rho)} \rho(\ell)$$

Rewriting with H1 for every $\ell \in \mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}}) \cap \mathrm{dom}(\rho)$, gives us the equality $\rho^+ = (\rho^+ \boxminus \rho_{\mathsf{reb}}) \bullet \rho_{\mathsf{reb}}$.

The outlives constraint $@(\rho^+ \boxminus \rho_{\mathsf{reb}}) \sqsupset \alpha$ follows from noting that all parts of the resource outlive α except for the locations in ρ that are mut or own in ρ'_i. □

Lemma 6.53. If $\rho \in \mathsf{reb}_\beta(\rho')$ and $\rho_f \mathrel{\#} \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v)$ then $\rho_f \mathrel{\blacktriangleright\!\!\blacktriangleleft} \rho$.

Proof. Note $\mathrm{dom}(\rho) \subseteq \mathrm{dom}(\rho')$, and $\rho|_{\mathsf{own},\mathsf{mut}} = \varnothing$. For any $\ell \in \mathrm{dom}(\rho_f) \cap \mathrm{dom}(\rho)$, the only way for $\rho_f(\ell)$ to not be composable with $\rho(\ell)$ is for $\rho_f(\ell)$ to be own or mut. But since $\rho_f \mathrel{\#} \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v)$, we know after unfolding and applying lemmas 6.18 and 6.20 and 6.30, that $\mathsf{ex}(\rho_f)_\bullet \mathrel{\blacktriangleright\!\!\blacktriangleleft} \llparenthesis \rho' \rrparenthesis_\circ$, which means overlapping with an own or mut can never happen. □

Lemma 6.54. If $\rho \in \mathsf{reb}_\beta(\rho')$ and $\checkmark\, \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v)$ then $\mathrm{dom}(\mathsf{ag}(\rho)) \subseteq \mathrm{dom}(\llparenthesis \rho' \rrparenthesis_\circ)$

Proof. By unfolding $\rho \in \mathsf{reb}_\beta(\rho')$, we get that

- $\mathrm{dom}(\rho) \subseteq \mathrm{dom}(\rho')$
- $\rho|_{\mathrm{dom}(\rho'|_{\mathsf{imm}})} = \rho'|_{\mathsf{imm}}|_{\mathrm{dom}(\rho)}$
- for every $\ell \in \mathrm{dom}(\rho) \cap \mathrm{dom}(\rho'|_{\mathsf{own},\mathsf{mut}})$, there is a ρ'' such that $\rho(\ell) = \mathsf{imm}(\_, \rho'', \_)$ and either $\rho'' \leq \rho'$, or $\rho'(\ell) = \mathsf{mut}(\_, \rho'', \_, \_)$, and therefore $\mathrm{dom}(\llparenthesis \rho'' \rrparenthesis_\circ) \subseteq \mathrm{dom}(\llparenthesis \rho' \rrparenthesis_\circ)$.

Collecting all of these, we get that every immutable borrow in ρ is in $\llparenthesis \rho' \rrparenthesis_\circ$, and every witness is also in $\llparenthesis \rho \rrparenthesis_\circ$. □

Lemma 6.55. If $\rho \in \mathsf{reb}_\beta(\rho')$ and $\rho_f \mathrel{\#} \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v)$ then $\rho_f \mathrel{\#} \rho$.
As a corollary, $\rho \mathrel{\#} \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v)$, which follows from setting $\rho_f = \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v)$.

Proof. Let $\rho_i = \mathsf{imm}(\overline{\alpha}, \rho', v)$. By lemma 6.53, $\rho_f \mathrel{\blacktriangleright\!\!\blacktriangleleft} \rho$. It suffices to show that $\llparenthesis \rho_f \bullet \rho \rrparenthesis$ is defined. Unfolding the hypothesis $\rho_f \mathrel{\#} \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v)$ applying lemmas 6.20 and 6.18, and unfolding the definitions of ex and ag, we get the following are all defined and equal:

$$\begin{aligned}
\llparenthesis \rho_f \bullet \rho_i \rrparenthesis &= \mathsf{ex}(\rho_f \bullet \rho_i)_\bullet \bullet \mathsf{ag}(\rho_f \bullet \rho_i) \\
&= \mathsf{ex}(\rho_f)_\bullet \bullet \mathsf{ex}(\rho_i)_\bullet \bullet (\mathsf{ag}(\rho_f) \circ \mathsf{ag}(\rho_i)) \\
&= \mathsf{ex}(\rho_f)_\bullet \bullet (\mathsf{ag}(\rho_f) \circ \rho_i \circ \llparenthesis \rho' \rrparenthesis_\circ)
\end{aligned}$$

By lemma 6.30 applied to the last equation, with lemma 6.36, we get $\mathsf{ex}(\rho_f)_\bullet \mathrel{\blacktriangleright\!\!\blacktriangleleft} \rho_i \circ \llparenthesis \rho' \rrparenthesis_\circ$, $\mathsf{ex}(\rho_f)_\bullet \mathrel{\blacktriangleright\!\!\blacktriangleleft} \rho_i$, and $\mathsf{ex}(\rho_f)_\bullet \mathrel{\blacktriangleright\!\!\blacktriangleleft} \llparenthesis \rho' \rrparenthesis_\circ$.

By unfolding our goal, applying lemmas 6.20 and 6.18, unfolding the definitions of ex and ag, and noting that $\mathrm{dom}(\rho|_{\mathsf{own},\mathsf{mut}}) = \varnothing$, we get that if one of the following are defined, then all are defined and equal.

$$\begin{aligned}
\llparenthesis \rho_f \bullet \rho \rrparenthesis &= \mathsf{ex}(\rho_f \bullet \rho)_\bullet \bullet \mathsf{ag}(\rho_f \bullet \rho) \\
&= \mathsf{ex}(\rho_f)_\bullet \bullet \mathsf{ex}(\rho)_\bullet \bullet (\mathsf{ag}(\rho_f) \circ \mathsf{ag}(\rho)) \\
&= \mathsf{ex}(\rho_f)_\bullet \bullet (\mathsf{ag}(\rho_f) \circ \mathsf{ag}(\rho))
\end{aligned}$$

By lemma 6.37 applied to the last equation, it suffices to show $\mathsf{ag}(\rho_f) \bowtie \mathsf{ag}(\rho)$ and $\mathsf{ex}(\rho_f)_\bullet \mathrel{\blacktriangleright\!\!\blacktriangleleft} \mathsf{ag}(\rho)$. By lemma 6.54, $\mathrm{dom}(\mathsf{ag}(\rho)) \subseteq \mathrm{dom}(\llparenthesis \rho' \rrparenthesis_\circ)$. Now we can complete the proof:

- $\mathsf{ag}(\rho_f) \bowtie \mathsf{ag}(\rho)$: For any location $\ell \in \mathrm{dom}(\mathsf{ag}(\rho_f)) \cap \mathrm{dom}(\mathsf{ag}(\rho))$, it suffices to show $\mathsf{ag}(\rho_f)(\ell) \bowtie \mathsf{ag}(\rho)(\ell)$. We have $\mathsf{ag}(\rho_f) \bowtie \llparenthesis \rho' \rrparenthesis_\circ$. This follows by unfolding reb, and noting ρ and ρ' differ only by potentially changing from own or mut to imm, but witnesses and values always stay the same.

- $\mathsf{ex}(\rho_f)_\bullet \bowtie \mathsf{ag}(\rho)$: Since $\mathsf{ex}(\rho_f)_\bullet \bowtie \llparenthesis \rho' \rrparenthesis_\circ$, and $\mathsf{ex}(\rho_f)_\bullet|_{\mathsf{imm}} = \varnothing$, we have that $\mathrm{dom}(\mathsf{ex}(\rho_f)_\bullet) \cap \mathrm{dom}(\llparenthesis \rho' \rrparenthesis_\circ) = \varnothing$. By unfolding the definition of $\bowtie$, it suffices to show $\mathrm{dom}(\mathsf{ex}(\rho_f)_\bullet) \cap \mathrm{dom}(\mathsf{ag}(\rho)) = \varnothing$, which is implied by $\mathrm{dom}(\mathsf{ag}(\rho)) \subseteq \mathrm{dom}(\llparenthesis \rho' \rrparenthesis_\circ)$.

□

Lemma 6.56. If $\rho \in \mathsf{reb}_\beta(\rho')$ and $\checkmark(\ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v))$ then $\left\llbracket \rho|_{\mathrm{dom}(\rho'|_{\mathsf{mut,own}})} \bullet \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v) \right\rrbracket = \llbracket \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v) \rrbracket$

Proof. By lemma 6.55, $\rho \# \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v)$. Then by lemma 6.11, $\rho|_{\mathrm{dom}(\rho'|_{\mathsf{mut,own}})} \# \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v)$. For any ℓ, it suffices to show $\left\llbracket \rho|_{\mathrm{dom}(\rho'|_{\mathsf{mut,own}})} \bullet \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v) \right\rrbracket(\ell) = \llbracket \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v) \rrbracket(\ell)$. By unfolding $\llbracket - \rrbracket$, $\llparenthesis - \rrparenthesis$, ex and ag, and by lemma 6.20, the following are all defined and equal:

$$\begin{aligned}
\llparenthesis \rho|_{\mathrm{dom}(\rho'|_{\mathsf{mut,own}})} \bullet \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v) \rrparenthesis &= \mathsf{ag}(\rho|_{\mathrm{dom}(\rho'|_{\mathsf{mut,own}})} \bullet \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v)) \\
&= \mathsf{ag}(\rho|_{\mathrm{dom}(\rho'|_{\mathsf{mut,own}})}) \circ \mathsf{ag}(\ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v)) \\
&= \mathsf{ag}(\rho|_{\mathrm{dom}(\rho'|_{\mathsf{mut,own}})}) \circ \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v) \circ \llparenthesis \rho' \rrparenthesis_\circ
\end{aligned}$$

By lemma 6.54, $\mathrm{dom}(\llparenthesis \rho|_{\mathrm{dom}(\rho'|_{\mathsf{mut,own}})} \rrparenthesis) \subseteq \mathrm{dom}(\llparenthesis \rho' \rrparenthesis)$. Since values and witnesses must agree because of the fact that $\rho|_{\mathrm{dom}(\rho'|_{\mathsf{mut,own}})} \# \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho', v)$, we have that the erasures must agree. □

Lemma 6.57. Let $\rho_i = \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho'_i, v)$. If $\rho \in \mathsf{reb}_\beta(\rho'_i)$, then $\llparenthesis \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i \rrparenthesis = \llparenthesis \rho_i \rrparenthesis$

Proof. By unfolding reb, we have that $\rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \leq \rho'_i|_{\mathsf{imm}}$, and $\rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})}|_{\mathsf{mut,own}} = \varnothing$. Therefore, unfolding $\llparenthesis - \rrparenthesis$, ex, ag, and applying lemma 6.20, we have the following are equal:

$$\begin{aligned}
\llparenthesis \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i \rrparenthesis &= \mathsf{ex}(\rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i)_\bullet \bullet \mathsf{ag}(\rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i) \\
&= \mathsf{ag}(\rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i) \\
&= \mathsf{ag}(\rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})}) \circ \mathsf{ag}(\rho_i) \\
&= \mathsf{ag}(\rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})}) \circ \rho_i \circ \llparenthesis \rho'_i \rrparenthesis_\circ \\
&= \mathsf{ag}(\rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})}) \circ \llparenthesis \rho'_i|_{\mathsf{imm}} \rrparenthesis_\circ \circ \rho_i \circ \llparenthesis \rho'_i|_{\mathsf{mut,own}} \rrparenthesis_\circ \\
&= \llparenthesis \rho'_i|_{\mathsf{imm}} \rrparenthesis_\circ \circ \rho_i \circ \llparenthesis \rho'_i|_{\mathsf{mut,own}} \rrparenthesis_\circ \\
&= \rho_i \circ \llparenthesis \rho'_i \rrparenthesis_\circ \\
&= \mathsf{ag}(\rho_i) \\
&= \llparenthesis \rho_i \rrparenthesis
\end{aligned}$$

□

Lemma 6.58. Let $\rho_i = \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho'_i, v)$. If

- $\rho \in \mathsf{reb}_\beta(\rho'_i)$
- $\rho \bullet \rho_b \leftrightsquigarrow \rho' \bullet \rho^+$
- $@\rho_b \sqsupset \beta$
- $@\rho' \sqsupset \beta$
- $\rho_b \# \rho_i$
- $\rho' \bullet \rho^+ \# \rho_i$

then $\llbracket \rho \bullet \rho_b \bullet \rho_i \rrbracket = \llbracket \rho_b \bullet \rho_i \rrbracket$ and $\llbracket \rho' \bullet \rho^+ \bullet \rho_i \rrbracket = \left\llbracket \rho' \bullet (\rho^+ \boxminus \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{mut,own}})}) \bullet \rho_i \right\rrbracket$

Proof. By lemma 6.56, $\left\llbracket \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}})} \bullet \rho_i \right\rrbracket = \llbracket \rho_i \rrbracket^{(\mathrm{H1})}$. Note $\mathrm{dom}(\rho) \subseteq \mathrm{dom}(\rho'_i)$ by unfolding reb. By lemma 6.8 and rewriting with H1, we have:

$$\begin{aligned}\llbracket \rho \bullet \rho_i \rrbracket &= \left\llbracket \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}})} \bullet \rho_i \right\rrbracket \\ &= \left\llbracket \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i \right\rrbracket\end{aligned}$$

By lemma 6.57 $\llparenthesis \rho_i \rrparenthesis = \llparenthesis \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i \rrparenthesis$, which implies $\llbracket \rho_i \rrbracket = \left\llbracket \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i \right\rrbracket$, which combined with the equation above $\llbracket \rho \bullet \rho_i \rrbracket = \left\llbracket \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i \right\rrbracket$, means $\llbracket \rho \bullet \rho_i \rrbracket = \llbracket \rho_i \rrbracket^{(\mathrm{H2})}$.

To show $\llbracket \rho \bullet \rho_b \bullet \rho_i \rrbracket = \llbracket \rho_b \bullet \rho_i \rrbracket$, by lemma 6.8, it suffices to show $\llbracket \rho \bullet \rho_i \rrbracket = \llbracket \rho_i \rrbracket$, which we have by H2.

By lemma 6.52, $\rho^+ = (\rho^+ \boxminus \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}})}) \bullet \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}})}$. Rewriting with this equation, we have the following are equal:

$$\llbracket \rho' \bullet \rho^+ \bullet \rho_i \rrbracket = \left\llbracket \rho' \bullet (\rho^+ \boxminus \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}})}) \bullet \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}})} \bullet \rho_i \right\rrbracket$$

To show $\llbracket \rho' \bullet \rho^+ \bullet \rho_i \rrbracket = \left\llbracket \rho' \bullet (\rho^+ \boxminus \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}})}) \bullet \rho_i \right\rrbracket$, by the previous equation and lemma 6.8, it suffices to show $\left\llbracket \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}})} \bullet \rho_i \right\rrbracket = \llbracket \rho_i \rrbracket$, which we have by H1. □

Lemma 6.59. Let $\rho_i = \ell \mapsto \mathsf{imm}(\overline{\alpha}, \rho'_i, v)$. If

- $\rho \in \mathsf{reb}_\beta(\rho'_i)$
- $\rho \bullet \rho_b \leftrightsquigarrow \rho' \bullet \rho^+$
- $@\rho_b \sqsupset \beta$
- $@\rho' \sqsupset \beta$
- $\rho_b \# \rho_i$
- $\rho' \bullet \rho^+ \# \rho_i$

then $\rho_i \bullet \rho_b \leftrightsquigarrow \rho' \bullet (\rho^+ \boxminus \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}})}) \bullet \rho_i$

Proof. Let $\rho_{\mathsf{reb}} = \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{mut},\mathsf{own}})}$. By lemma 6.52, $\rho^+ = (\rho^+ \boxminus \rho_{\mathsf{reb}}) \bullet \rho_{\mathsf{reb}}$, and $@(\rho^+ \boxminus \rho_{\mathsf{reb}}) \sqsupset \beta$. And note by unfolding reb, $\rho = \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_{\mathsf{reb}}$. Rewriting with these two equations in the update hypothesis, we get $\rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_{\mathsf{reb}} \bullet \rho_b \leftrightsquigarrow \rho' \bullet (\rho^+ \boxminus \rho_{\mathsf{reb}}) \bullet \rho_{\mathsf{reb}}$.

By lemma 6.57, $\llparenthesis \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i \rrparenthesis = \llparenthesis \rho_i \rrparenthesis$. Unfolding, this additionally implies $\mathsf{ag}(\rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i) = \mathsf{ag}(\rho_i)$. Note that $\llparenthesis \rho_b \bullet \rho_i \rrparenthesis$ is defined by the hypothesis. Unfolding $\llparenthesis - \rrparenthesis$, ex, and applying lemmas 6.18 and 6.20, we get

$$\begin{aligned}\llparenthesis \rho_i \bullet \rho_b \rrparenthesis &= \mathsf{ex}(\rho_i \bullet \rho_b)_\bullet \bullet \mathsf{ag}(\rho_i \bullet \rho_b) \\ &= \mathsf{ex}(\rho_i)_\bullet \bullet \mathsf{ex}(\rho_b)_\bullet \bullet \mathsf{ag}(\rho_i) \circ \mathsf{ag}(\rho_b) \\ &= \mathsf{ex}(\rho_b)_\bullet \bullet \mathsf{ag}(\rho_i) \circ \mathsf{ag}(\rho_b) \\ &= \mathsf{ex}(\rho_b)_\bullet \bullet \mathsf{ag}(\rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i) \circ \mathsf{ag}(\rho_b) \\ &= \mathsf{ex}(\rho_b)_\bullet \bullet \mathsf{ag}(\rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i \bullet \rho_b) \\ &= \llparenthesis \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i \bullet \rho_b \rrparenthesis\end{aligned}$$

Rewriting with this equation, it suffices to show $\rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i \bullet \rho_b \leftrightsquigarrow \rho' \bullet (\rho^+ \boxminus \rho_{\mathsf{reb}}) \bullet \rho_i$. Unfolding, it suffices to show $\mathrm{dom}(\llparenthesis \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i \bullet \rho_b \rrparenthesis|_{\mathsf{imm},\mathsf{mut}}) = \mathrm{dom}(\llparenthesis \rho' \bullet (\rho^+ \boxminus \rho_{\mathsf{reb}}) \bullet \rho_i \rrparenthesis|_{\mathsf{imm},\mathsf{mut}})$ and for every $\ell \in \mathrm{dom}(\llparenthesis \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i \bullet \rho_b \rrparenthesis|_{\mathsf{imm},\mathsf{mut}})$, $\llparenthesis \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_i \bullet \rho_b \rrparenthesis(\ell) \sim \llparenthesis \rho' \bullet (\rho^+ \boxminus \rho_{\mathsf{reb}}) \bullet \rho_i \rrparenthesis(\ell)$. By the rewritten update hypothesis above, we have $\llparenthesis \rho|_{\mathrm{dom}(\rho'_i|_{\mathsf{imm}})} \bullet \rho_{\mathsf{reb}} \bullet \rho_b \rrparenthesis(\ell) \sim \llparenthesis \rho' \bullet (\rho^+ \boxminus \rho_{\mathsf{reb}}) \bullet \rho_{\mathsf{reb}} \rrparenthesis(\ell)$. If $\ell \notin \mathrm{dom}(\rho_{\mathsf{reb}})$, then this is immediate, by the hypothesis and unfolding reb. If $\ell \in \mathrm{dom}(\rho_{\mathsf{reb}})$, then since all components of the composition besides for ρ_{reb} outlive β, neither have the immutable borrow at β from ρ_{reb}, and both get the borrow from ρ_i. □

Lemma 6.60. If $\Delta \vdash T \sqsupset @a$ and $\delta \in [\![\Delta]\!]$, and $\rho \in \mathcal{V}[\![T]\!]_\delta$ then $@\rho \sqsupset @a\delta$

Proof. Proceed by induction on the derivation $\Delta \vdash T \sqsupset @a$:

- $$\frac{}{\Delta \vdash \mathbb{1} \sqsupset @a}$$

  $T = \mathbb{1}$. Then $\rho = \varnothing$, so we're done.

- $$\frac{\Delta \vdash T_1 \sqsupset @a \quad \Delta \vdash T_2 \sqsupset @a}{\Delta \vdash T_1 \otimes T_2 \sqsupset @a}$$

  $T = T_1 \otimes T_2$. Then there are ρ_1, ρ_2 such that $\rho = \rho_1 \bullet \rho_2$, $\rho_1 \in \mathcal{V}[\![T_1]\!]_\delta$, and $\rho_2 \in \mathcal{V}[\![T_2]\!]_\delta$. By the IH, $@\rho_1 \sqsupset @a\delta$, and $@\rho_2 \sqsupset @a\delta$, which by $[\,]*$ completes the case.

- $$\frac{\Delta \vdash T_1 \sqsupset @a \quad \Delta \vdash T_2 \sqsupset @a}{\Delta \vdash T_1 \oplus T_2 \sqsupset @a}$$

  $T = T_1 \oplus T_2$. Then either $\rho \in \mathcal{V}[\![T_1]\!]_\delta$, or $\rho \in \mathcal{V}[\![T_2]\!]_\delta$. In either case, by the IH, $@\rho \sqsupset @a\delta$.

- $$\frac{\Delta \vdash T \sqsupset @a}{\Delta \vdash \mathsf{Ref}\ T \sqsupset @a}$$

  $T = \mathsf{Ref}\ T$. Then there is a v, ℓ, ρ_T such that $\rho = \ell \mapsto \mathsf{own}(v) \bullet \rho_T$ and $\rho_T \in \mathcal{V}[\![T]\!]_\delta(v)$. By the IH, $@\rho_T \sqsupset @a\delta$, and $@(\ell \mapsto \mathsf{own}(v)) \sqsupset @a\delta$, which by $[\,]*$ completes the case.

- $$\frac{\Delta \vDash @b \sqsupset @a}{\Delta \vdash [@b]\, T \sqsupset @a}$$

  $T = [@b]\, T$. Then $\rho \in [@b\delta]\, \mathcal{V}[\![T]\!]_\delta$. Unfolding, we have $@\rho \sqsupset @b\delta$. And by the hypothesis, $@b\delta \sqsupset @a\delta$. Therefore $@\rho \sqsupset @a\delta$.

- $$\frac{\Delta \vDash @b \sqsupset @a}{\Delta \vdash \mathsf{Imm}\ @b\ T \sqsupset @a}$$

  $T = \mathsf{Imm}\ @b\ T$. Then there is an ℓ such that $\rho \in \ell \mapsto \mathsf{Imm}\ @b\delta\ \mathcal{V}[\![T]\!]_\delta$. Unfolding, we have that there are $\overline{\beta}, v, \rho'$ such that $\rho = \ell \mapsto \mathsf{imm}(\overline{\beta}, v, \rho')$ and $\mathcal{V}[\![T]\!]_\delta(v)$ and $@b\delta \sqsubseteq \bigsqcup \overline{\beta}$. And by the hypothesis, $@b\delta \sqsupset @a\delta$. Therefore $@\rho \sqsupset @a\delta$.

- $$\frac{\Delta \vDash @b \sqsupset @a}{\Delta \vdash \mathsf{Mut}\ @b\ T \sqsupset @a}$$

  $T = \mathsf{Mut}\ @b\ T$. Then there is an ℓ such that $\rho \in \ell \mapsto \mathsf{Mut}\ @b\delta\ \mathcal{V}[\![T]\!]_\delta$. Unfolding, we have that there are $\beta \sqsupseteq @b\delta, v, \rho'$ such that $\rho = \ell \mapsto \mathsf{mut}(\beta, v, \rho', \mathcal{V}[\![T]\!]_\delta)$. And by the hypothesis, $@b\delta \sqsupset @a\delta$. Therefore $@\rho \sqsupset @a\delta$.

□

Lemma 6.61. If $\rho_1' \in \mathsf{reb}_\alpha(\rho_1)$, $\rho_2' \in \mathsf{reb}_\alpha(\rho_2)$, and $\rho_1 \bowtie \rho_2$, then $\rho_1' \bullet \rho_2' \in \mathsf{reb}_\alpha(\rho_1 \bullet \rho_2)$.

Proof. Unfolding the definition of reb, the only interesting cases are locations ℓ that are in both ρ_1' and ρ_2'. By the definition of reb, $\rho_1'|_{\mathsf{mut,own}} = \rho_2'|_{\mathsf{mut,own}} = \varnothing$. And by the definition of $\bullet$, $\rho_1|_{\mathsf{mut,own}}$ is disjoint from $\rho_2|_{\mathsf{mut,own}}$. Therefore, any overlapping locations of ρ_1' and ρ_2' are in $(\rho_1 \bullet \rho_2)|_{\mathsf{imm}}$, which means $(\rho_1' \bullet \rho_2')(\ell) = (\rho_1 \bullet \rho_2)(\ell)$, which is sufficient to complete the proof. □

Lemma 6.62. If $\Delta \vdash \Gamma \sqsupset @a$ and $\delta \in [\![\Delta]\!]$, then $\mathcal{G}[\![\Gamma]\!]_\delta(\gamma) \vDash [@a\delta]\,\mathcal{G}[\![\Gamma]\!]_\delta(\gamma)$.

Proof. Let $\rho \in \mathcal{G}[\![\Gamma]\!]_\delta(\gamma)^{(\mathrm{H1})}$. We want to show $[@a\delta]\,\mathcal{G}[\![\Gamma]\!]_\delta(\gamma)^{(\mathrm{G1})}$. Unfolding $[@a\delta]$, we want to show $@\rho \sqsupset @a\delta^{(\mathrm{G2})}$. Unfolding $\mathcal{G}$ in H1, we get $\rho \in \ulcorner \mathrm{dom}(\Gamma) \subseteq \mathrm{dom}(\delta) \urcorner \star \circledast_{x \in \mathrm{dom}(\Gamma)} \mathcal{V}[\![\Gamma(x)]\!]_\delta(\gamma(x))^{(\mathrm{H2})}$. Unfolding further, there exists $\overline{\rho_x}$ such that $\rho = \bullet\, \overline{\rho_x}^{(\mathrm{H3})}$ and $\forall\, x \in \mathrm{dom}(\Gamma).\ \rho_x \in \mathcal{V}[\![\Gamma(x)]\!]_\delta(\gamma(x))^{(\mathrm{H4})}$.

By $[]\star$, it suffices to show $\forall\, x \in \mathrm{dom}(\Gamma).\ @\rho_x \sqsupset @a\delta$. Let $x \in \mathrm{dom}(\Gamma)$. By lemma 6.60, it suffices to show $\Delta \vDash \Gamma(x) \sqsupset @a$. and $\delta \in [\![\Delta]\!]$, both of which follow from the hypotheses. □

Lemma 6.63. $\alpha \sqsupset {\downarrow}\alpha$

Proof. Unfolding the definition of $\downarrow$, ${\downarrow}\alpha = \alpha + 1$, and $\alpha < \alpha + 1$, so $\alpha \sqsupset \alpha + 1$. □

6.3 Frame and Anti-Frame

Theorem 6.64 (Imm Frame)**.** $\ell \mapsto v \star \hat{P}(v) \star (\text{И}\alpha.\,\mathsf{Imm}\ \alpha\ \hat{P} \mathrel{-\!\!\star} \mathsf{wp}\,(e)\,\{[\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})\}) \vDash \mathsf{wp}\,(e)\,\{\hat{Q}\}$

Proof. Let $\rho \in \ell \mapsto v \star \hat{P}(v) \star (\text{И}\alpha.\,\mathsf{Imm}\ \alpha\ \hat{P} \mathrel{-\!\!\star} \mathsf{wp}\,(e)\,\{[\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})\})^{(\mathrm{H1})}$.
By Lemma 6.112, $\text{И}\alpha.\,\rho \in \ell \mapsto v \star \hat{P}(v) \star (\mathsf{Imm}\ \alpha\ \hat{P} \mathrel{-\!\!\star} \mathsf{wp}\,(e)\,\{[\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})\})^{(\mathrm{H2})}$.
We want to show $\rho \in \mathsf{wp}\,(e)\,\{\hat{Q}\}^{(\mathrm{G1})}$. Unfolding wp, let $\rho_f \# \rho^{(\mathrm{H3})}$. We want to show $\exists\,\rho' \# \rho_f{}^{(\mathrm{G2})}, \rho^+ \# \rho' \bullet \rho_f{}^{(\mathrm{G3})}, v$.

- $([\![\rho_f \bullet \rho]\!], e) \Downarrow ([\![\rho_f \bullet \rho' \bullet \rho^+]\!], v)^{(\mathrm{G4})}$
- $\rho \leftrightsquigarrow \rho' \bullet \rho^{+(\mathrm{G5})}$
- $\rho^+|_{\mathsf{own}} = \varnothing^{(\mathrm{G6})}$
- $\rho' \in \hat{Q}(v)^{(\mathrm{G7})}$

Unfolding И in H2, $\exists\,\beta.\ \forall\,\alpha \sqsubset \beta.\ \rho \in [\alpha]\,(\ell \mapsto v \star \hat{P}(v) \star (\mathsf{Imm}\ \alpha\ \hat{P} \mathrel{-\!\!\star} \mathsf{wp}\,(e)\,\{[\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})\}))$.
Let α be some lifetime where $\alpha \sqsubset \beta^{(\mathrm{H4})}$. Such an α always exists because for any lifetime, the set of lifetimes shorter than it is infinite. Then specializing to α, we have
$\rho \in [\alpha]\,(\ell \mapsto v \star \hat{P}(v) \star (\mathsf{Imm}\ \alpha\ \hat{P} \mathrel{-\!\!\star} \mathsf{wp}\,(e)\,\{[\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})\}))^{(\mathrm{H5})}$.
Applying Lemma 6.104, we have $\rho \in [\alpha]\,\ell \mapsto v \star [\alpha]\,\hat{P}(v) \star [\alpha]\,(\mathsf{Imm}\ \alpha\ \hat{P} \mathrel{-\!\!\star} \mathsf{wp}\,(e)\,\{[\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})\})^{(\mathrm{H6})}$.
Unfolding $\star$ and $[\alpha]$ in H6, $\exists\,\rho_\ell, \rho_{\hat{P}(v)}, \rho_b$. such that

- $\rho = \rho_\ell \bullet \rho_{\hat{P}(v)} \bullet \rho_b$
- $\rho_\ell \in \ell \mapsto v^{(\mathrm{H7})}$
- $\rho_{\hat{P}(v)} \in \hat{P}(v)^{(\mathrm{H8})}$
- $\rho_b \in \mathsf{Imm}\ \alpha\ \hat{P} \mathrel{-\!\!\star} \mathsf{wp}\,(e)\,\{[\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})\}^{(\mathrm{H9})}$
- $@\rho_{\hat{P}(v)} \sqsupset \alpha^{(\mathrm{H10})}$
- $@\rho_b \sqsupset \alpha^{(\mathrm{H11})}$

Suppose we have $\rho_i = \ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_{\hat{P}(v)})$. This resource is well formed by H10.
We establish a bunch of compatibility conditions with our starting resources and the "fictional" ρ_i:

- $\rho_b \mathbin{\#} \rho_\ell \bullet \rho_{\hat{P}(v)}{}^{(\mathrm{H12})}$: by definition of ρ, $\rho_b \bowtie \rho_\ell \bullet \rho_{\hat{P}(v)}$, so we just need $\checkmark\,\rho$, which follows by lemma 6.10 with $\checkmark\,\rho \bullet \rho_f$ from H3.
- $\rho_b \mathbin{\#} \rho_i{}^{(\mathrm{H13})}$: by lemma 6.34 with H12 and H10.
- $\rho_f \mathbin{\#} \rho_\ell \bullet \rho_{\hat{P}(v)}{}^{(\mathrm{H14})}$: by lemma 6.11 with H3.
- $\rho_f \mathbin{\#} \rho_i{}^{(\mathrm{H15})}$: by lemma 6.34 with H14 and H10.
- $\rho_f \mathbin{\#} \rho_b{}^{(\mathrm{H16})}$: by lemma 6.11 with H3.
- $\rho_f \mathbin{\#} \rho_b \bullet \rho_i{}^{(\mathrm{H17})}$: by lemma 6.15 with H15 and H16 and H13.

By the definition of $\mathrel{-\!\!\star}$ and H9 and H13, $\rho_b \bullet \rho_i \in \mathsf{wp}\,(e)\,\big\{[\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})\big\}$.
Unfolding wp, and setting $\rho_f = \rho_f$ and $\rho = \rho_b \bullet \rho_i$ with H13 and H17 for the compatibility requirements, $\exists\, \rho' \mathbin{\#} \rho_f{}^{(\mathrm{H18})}$, $\rho^+ \mathbin{\#} \rho' \bullet \rho_f{}^{(\mathrm{H19})}$, v'.

- $([\![\rho_f \bullet \rho_b \bullet \rho_i]\!], e) \Downarrow ([\![\rho_f \bullet \rho' \bullet \rho^+]\!], v')^{(\mathrm{H20})}$
- $\rho_b \bullet \rho_i \leftrightsquigarrow \rho' \bullet \rho^{+\,(\mathrm{H21})}$
- $\rho^+|_{\mathsf{own}} = \varnothing^{(\mathrm{H22})}$
- $\rho' \in [\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})(v')^{(\mathrm{H23})}$

Unfolding $[\alpha]$ in H23, we have $@\rho' \sqsupset \alpha^{(\mathrm{H24})}$ and $\rho' \in \ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q}(v')^{(\mathrm{H25})}$.
By lemma 6.29 with H11 and H12 and H21, $\rho' \bullet \rho^+ = (\rho' \bullet \rho^+)/\ell \bullet \rho_i$.
By H24, $\ell \notin \mathrm{dom}(\rho')$, so $\rho' \bullet \rho^+ = \rho' \bullet \rho^+/\ell \bullet \rho_i{}^{(\mathrm{H26})}$.
Now we establish a bunch more compatibility results, this time for the "owned" resource after running e:

- $\rho' \mathbin{\#} \rho^{+\,(\mathrm{H27})}$ by lemma 6.11 with H19.
- $\rho' \bullet \rho^+/\ell \mathbin{\#} \rho_\ell \bullet \rho_{\hat{P}(v)}{}^{(\mathrm{H28})}$, by lemma 6.38 with H12 and H27 and H11 and H24 and H22 and H21.
- $\rho' \bullet \rho^+/\ell \mathbin{\#} \rho_f{}^{(\mathrm{H29})}$ by lemma 6.11 with H19.
- $\rho' \bullet \rho^+/\ell \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \mathbin{\#} \rho_f{}^{(\mathrm{H30})}$, by lemma 6.15 with H28 and H29 and H14.
- $\rho' \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \mathbin{\#} \rho_f{}^{(\mathrm{H31})}$, by lemma 6.11 with H30.
- $\rho^+/\ell \mathbin{\#} \rho' \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \bullet \rho_f{}^{(\mathrm{H32})}$, by H30.
- $\rho' \mathbin{\#} \rho_\ell \bullet \rho_{\hat{P}(v)}{}^{(\mathrm{H33})}$, by lemma 6.11 with H28.

By lemmas 6.26 and 6.8 with H12 and H28 and H20, $([\![\rho_f \bullet \rho]\!], e) \Downarrow \big(\big[\!\!\big[\rho_f \bullet \rho' \bullet \rho^+/\ell \bullet \rho_\ell \bullet \rho_{\hat{P}(v)}\big]\!\!\big], v'\big)^{(\mathrm{H34})}$.
By lemma 6.39 with H12 and H28 and H21, $\rho \leftrightsquigarrow \rho' \bullet \rho^+/\ell \bullet \rho_\ell \bullet \rho_{\hat{P}(v)}{}^{(\mathrm{H35})}$.
By the definition of $\mathrel{-\!\!\star}$, $\rho' \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \in \hat{Q}(v')^{(\mathrm{H36})}$.
Now we can prove our goals, setting $\rho' = \rho' \bullet \rho_\ell \bullet \rho_{\hat{P}(v)}$, and $\rho^+ = \rho^+/\ell$,

- G2: $\rho' \bullet \rho_\ell \bullet \rho_{\hat{P}(V)} \mathbin{\#} \rho_f$ by H31
- G3: $\rho^+/\ell \mathbin{\#} \rho' \bullet \rho_\ell \bullet \rho_{\hat{P}(V)} \bullet \rho_f$ by H32.

- G4: $([\![\rho_f \bullet \rho]\!], e) \Downarrow (\left[\!\!\left[\rho_f \bullet \rho' \bullet \rho^+/\ell \bullet \rho_\ell \bullet \rho_{\hat{P}(v)}\right]\!\!\right], v')$ by H34
- G5: $\rho \leftrightsquigarrow \rho' \bullet \rho^+/\ell \bullet \rho_\ell \bullet \rho_{\hat{P}(v)}$ by H35
- G6: $\rho^+|_{\mathsf{own}} = \varnothing$ by H22
- G7: $\rho' \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \in \hat{Q}(v')$ by H36

□

Theorem 6.65 (Mut Frame)**.** If $\hat{P} \vDash [\beta]\,\hat{P}$, then
$\ell \mapsto v \star \hat{P}(v) \star (\text{И}\alpha.\,\mathsf{Mut}\ \alpha\ \hat{P} \mathrel{-\!\!\star} \mathsf{wp}\,(e)\left\{[\alpha]\,\forall\, v'.\ \ell \mapsto v' \mathrel{-\!\!\star} \hat{P}(v') \mathrel{-\!\!\star} \hat{Q}\right\}) \vDash \mathsf{wp}\,(e)\left\{\hat{Q}\right\}$

Proof. Let $\rho \in \ell \mapsto v \star \hat{P}(v) \star (\text{И}\alpha.\,\mathsf{Mut}\ \alpha\ \hat{P} \mathrel{-\!\!\star} \mathsf{wp}\,(e)\left\{[\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})\right\})^{(\text{H1})}$.
By Lemma 6.112, $\text{И}\alpha.\,\rho \in \ell \mapsto v \star \hat{P}(v) \star (\mathsf{Mut}\ \alpha\ \hat{P} \mathrel{-\!\!\star} \mathsf{wp}\,(e)\left\{[\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})\right\})^{(\text{H2})}$.
We want to show $\rho \in \mathsf{wp}\,(e)\left\{\hat{Q}\right\}^{(\text{G1})}$. Unfolding wp, let $\rho_f \# \rho^{(\text{H3})}$. We want to show $\exists\,\rho' \# {\rho_f}^{(\text{G2})}, \rho^+ \# \rho' \bullet {\rho_f}^{(\text{G3})}, v$.

- $([\![\rho_f \bullet \rho]\!], e) \Downarrow ([\![\rho_f \bullet \rho' \bullet \rho^+]\!], v)^{(\text{G4})}$
- $\rho \leftrightsquigarrow \rho' \bullet \rho^{+(\text{G5})}$
- $\rho^+|_{\mathsf{own}} = \varnothing^{(\text{G6})}$
- $\rho' \in \hat{Q}(v)^{(\text{G7})}$

Unfolding И in H2, $\exists\,\gamma.\ \forall\,\alpha \sqsubset \gamma.\ \rho \in [\alpha]\,(\ell \mapsto v \star \hat{P}(v) \star (\mathsf{Mut}\ \alpha\ \hat{P} \mathrel{-\!\!\star} \mathsf{wp}\,(e)\left\{[\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})\right\}))$.
Let α be some lifetime where $\alpha \sqsubset \gamma \sqcap \beta^{(\text{H4})}$. Such an α always exists because for any lifetime, the set of lifetimes shorter than it is infinite. Then specializing to α, we have
$\rho \in [\alpha]\,(\ell \mapsto v \star \hat{P}(v) \star (\mathsf{Mut}\ \alpha\ \hat{P} \mathrel{-\!\!\star} \mathsf{wp}\,(e)\left\{[\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})\right\}))^{(\text{H5})}$.
Applying Lemma 6.104, we have $\rho \in [\alpha]\,\ell \mapsto v \star [\alpha]\,\hat{P}(v) \star [\alpha]\,(\mathsf{Mut}\ \alpha\ \hat{P} \mathrel{-\!\!\star} \mathsf{wp}\,(e)\left\{[\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})\right\})^{(\text{H6})}$.
Unfolding $\star$ and $[\alpha]$ in H6, $\exists\,\rho_\ell, \rho_{\hat{P}(v)}, \rho_b$. such that

- $\rho = \rho_\ell \bullet \rho_{\hat{P}(v)} \bullet \rho_b$
- $\rho_\ell \in \ell \mapsto v^{(\text{H7})}$
- $\rho_{\hat{P}(v)} \in \hat{P}(v)^{(\text{H8})}$
- $\rho_b \in \mathsf{Mut}\ \alpha\ \hat{P} \mathrel{-\!\!\star} \mathsf{wp}\,(e)\left\{[\alpha]\,(\ell \mapsto v \mathrel{-\!\!\star} \hat{P}(v) \mathrel{-\!\!\star} \hat{Q})\right\}^{(\text{H9})}$
- $@\rho_{\hat{P}(v)} \sqsupset \alpha^{(\text{H10})}$
- $@\rho_b \sqsupset \alpha^{(\text{H11})}$

Suppose we have $\rho_m = \ell \mapsto \mathsf{mut}(\alpha, v, \rho_{\hat{P}(v)}, \hat{P})$. This resource is well formed by H4.
We establish a bunch of compatibility conditions with our starting resources and the “fictional” ρ_m:

- $\rho_b \# \rho_\ell \bullet {\rho_{\hat{P}(v)}}^{(\text{H12})}$: by definition of ρ, $\rho_b \bowtie \rho_\ell \bullet \rho_{\hat{P}(v)}$, so we just need $\checkmark\rho$, which follows by lemma 6.10 with $\checkmark\rho \bullet \rho_f$ from H3.
- $\rho_b \# {\rho_m}^{(\text{H13})}$: by lemma 6.24 with H12 and H10.
- $\rho_f \# \rho_\ell \bullet {\rho_{\hat{P}(v)}}^{(\text{H14})}$: by lemma 6.11 with H3.
- $\rho_f \# {\rho_m}^{(\text{H15})}$: by lemma 6.24 with H14 and H10.

- $\rho_f \mathbin{\#} \rho_b{}^{\text{(H16)}}$: by lemma 6.11 with H3.
- $\rho_f \mathbin{\#} \rho_b \bullet \rho_m{}^{\text{(H17)}}$: by lemma 6.15 with H15 and H16 and H13.

By the definition of $-\!\!*$ and H9 and H13, $\rho_b \bullet \rho_m \in \mathsf{wp}\,(e)\,\big\{[\alpha]\,(\ell \mapsto v -\!\!* \hat{P}(v) -\!\!* \hat{Q})\big\}$.
Unfolding wp, and setting $\rho_f = \rho_f$ and $\rho = \rho_b \bullet \rho_m$ with H13 and H17 for the compatibility requirements, $\exists\, \rho' \mathbin{\#} \rho_f{}^{\text{(H18)}}, \rho^+ \mathbin{\#} \rho' \bullet \rho_f{}^{\text{(H19)}}, v'$.

- $(\llbracket \rho_f \bullet \rho_b \bullet \rho_m \rrbracket, e) \Downarrow (\llbracket \rho_f \bullet \rho' \bullet \rho^+ \rrbracket, v')^{\text{(H20)}}$
- $\rho_b \bullet \rho_m \leftrightsquigarrow \rho' \bullet \rho^{+\,\text{(H21)}}$
- $\rho^+|_{\mathsf{own}} = \varnothing^{\text{(H22)}}$
- $\rho' \in [\alpha]\,(\ell \mapsto v -\!\!* \hat{P}(v) -\!\!* \hat{Q})(v')^{\text{(H23)}}$

Unfolding $[\alpha]$ in H23, we have $@\rho' \sqsupset \alpha^{\text{(H24)}}$ and $\rho' \in \ell \mapsto v -\!\!* \hat{P}(v) -\!\!* \hat{Q}(v')^{\text{(H25)}}$.
By lemma 6.27 with H11 and H21, $\rho' \bullet \rho^+ = (\rho' \bullet \rho^+)/\ell \bullet \rho_m$.
By H24, $\ell \notin \mathrm{dom}(\rho')$, so $\rho' \bullet \rho^+ = \rho' \bullet \rho^+/\ell \bullet \rho_m{}^{\text{(H26)}}$.
Now we establish a bunch more compatibility results, this time for the "owned" resource after running e:

- $\rho' \bullet \rho^+/\ell \mathbin{\#} \rho_\ell \bullet \rho_{\hat{P}(v)}{}^{\text{(H27)}}$, by lemma 6.24 with $\checkmark\, \rho' \bullet \rho^+$ from H19 and H26.
- $\rho' \bullet \rho^+/\ell \mathbin{\#} \rho_f{}^{\text{(H28)}}$ by lemma 6.11 with H19.
- $\rho' \bullet \rho^+/\ell \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \mathbin{\#} \rho_f{}^{\text{(H29)}}$, by lemma 6.15 with H27 and H28 and H14.
- $\rho' \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \mathbin{\#} \rho_f{}^{\text{(H30)}}$, by lemma 6.11 with H29.
- $\rho^+/\ell \mathbin{\#} \rho' \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \bullet \rho_f{}^{\text{(H31)}}$, by H29.
- $\rho' \mathbin{\#} \rho_\ell \bullet \rho_{\hat{P}(v)}{}^{\text{(H32)}}$, by lemma 6.11 with H27.

By lemmas 6.25 and 6.8 with H12 and H27 and H20, $(\llbracket \rho_f \bullet \rho \rrbracket, e) \Downarrow \big(\big\llbracket \rho_f \bullet \rho' \bullet \rho^+/\ell \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \big\rrbracket, v'\big)^{\text{(H33)}}$.
By lemma 6.28 with H12 and H27 and H21, $\rho \leftrightsquigarrow \rho' \bullet \rho^+/\ell \bullet \rho_\ell \bullet \rho_{\hat{P}(v)}{}^{\text{(H34)}}$.
By the definition of $-\!\!*$, $\rho' \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \in \hat{Q}(v')^{\text{(H35)}}$.
Now we can prove our goals, setting $\rho' = \rho' \bullet \rho_\ell \bullet \rho_{\hat{P}(v)}$, and $\rho^+ = \rho^+/\ell$,

- G2: $\rho' \bullet \rho_\ell \bullet \rho_{\hat{P}(V)} \mathbin{\#} \rho_f$ by H30
- G3: $\rho^+/\ell \mathbin{\#} \rho' \bullet \rho_\ell \bullet \rho_{\hat{P}(V)} \bullet \rho_f$ by H31.
- G4: $(\llbracket \rho_f \bullet \rho \rrbracket, e) \Downarrow \big(\big\llbracket \rho_f \bullet \rho' \bullet \rho^+/\ell \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \big\rrbracket, v'\big)$ by H33
- G5: $\rho \leftrightsquigarrow \rho' \bullet \rho^+/\ell \bullet \rho_\ell \bullet \rho_{\hat{P}(v)}$ by H34
- G6: $\rho^+|_{\mathsf{own}} = \varnothing$ by H22
- G7: $\rho' \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \in \hat{Q}(v')$ by H35

□

Theorem 6.66 (Anti Frame)**.**
$\ell \mapsto \mathsf{Mut}\ \alpha\ \hat{P} \star (\forall\, v.\ \ell \mapsto v -\!\!* \hat{P}(v) -\!\!* \mathsf{wp}\,(e)\,\big\{\exists\, v.\ \ell \mapsto v \star \hat{P}(v) \star (\ell \mapsto \mathsf{Mut}\ \alpha\ \hat{P} -\!\!* \hat{Q})\big\}) \vDash \mathsf{wp}\,(e)\,\big\{\hat{Q}\big\}$

Proof. Let $\rho \in \ell \mapsto \mathsf{Mut}\ \alpha\ \hat{P} \star (\forall v.\ \ell \mapsto v \mathrel{-\!\!*} \hat{P}(v) \mathrel{-\!\!*} \mathsf{wp}\,(e)\,\big\{\exists v.\ \ell \mapsto v \star \hat{P}(v) \star (\ell \mapsto \mathsf{Mut}\ \alpha\ \hat{P} \mathrel{-\!\!*} \hat{Q})\big\})^{(\mathrm{H1})}$.
We want to show $\rho \in \mathsf{wp}\,(e)\,\big\{\hat{Q}\big\}^{(\mathrm{G1})}$. Unfolding wp, let $\rho_f \mathrel{\#} \rho^{(\mathrm{H2})}$. We want to show $\exists\, \rho' \mathrel{\#} \rho_f{}^{(\mathrm{G2})}, \rho^+ \mathrel{\#} \rho' \bullet \rho_f{}^{(\mathrm{G3})}, v$.

- $(\llbracket \rho_f \bullet \rho \rrbracket, e) \Downarrow (\llbracket \rho_f \bullet \rho' \bullet \rho^+ \rrbracket, v)^{(\mathrm{G4})}$
- $\rho \leftrightsquigarrow \rho' \bullet \rho^{+(\mathrm{G5})}$
- $\rho^+|_{\mathsf{own}} = \varnothing^{(\mathrm{G6})}$
- $\rho' \in \hat{Q}(v)^{(\mathrm{G7})}$

Unfolding $\star$ in H1, $\exists\, \rho_m, \rho_a$.

- $\rho = \rho_m \bullet \rho_a$
- $\rho_m \in \ell \mapsto \mathsf{Mut}\ \alpha\ \hat{P}^{(\mathrm{H3})}$
- $\rho_a \in \forall v.\ \ell \mapsto v \mathrel{-\!\!*} \hat{P}(v) \mathrel{-\!\!*} \mathsf{wp}\,(e)\,\big\{\exists v.\ \ell \mapsto v \star \hat{P}(v) \star (\ell \mapsto \mathsf{Mut}\ \alpha\ \hat{P} \mathrel{-\!\!*} \hat{Q})\big\}^{(\mathrm{H4})}$

Unfolding $\ell \mapsto \mathsf{Mut}$ in H3, $\exists\, \beta \sqsupseteq \alpha, v, \rho_{\hat{P}(v)} \in \hat{P}(v)$. $\rho_m = \ell \mapsto \mathsf{mut}(\beta, v, \rho_{\hat{P}(v)}, \hat{P})^{(\mathrm{H5})}$.
Specializing H4 to v, $\rho_a \in \ell \mapsto v \mathrel{-\!\!*} \hat{P}(v) \mathrel{-\!\!*} \mathsf{wp}\,(e)\,\big\{\exists v.\ \ell \mapsto v \star \hat{P}(v) \star (\ell \mapsto \mathsf{Mut}\ \alpha\ \hat{P} \mathrel{-\!\!*} \hat{Q})\big\}^{(\mathrm{H6})}$.
By lemma 6.11 with H2, $\rho_m \mathrel{\#} \rho_a$. Let $\rho_\ell = \ell \mapsto \mathsf{own}(v)$. Then by lemma 6.24, $\rho_a \mathrel{\#} \rho_\ell \bullet \rho_{\hat{P}(v)}{}^{(\mathrm{H7})}$.
By lemma 6.11 with H2, $\rho_m \mathrel{\#} \rho_f$. Then by lemma 6.24, $\rho_f \mathrel{\#} \rho_\ell \bullet \rho_{\hat{P}(v)}{}^{(\mathrm{H8})}$.
By the definition of $\mathrel{-\!\!*}$ with H7, $\rho_a \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \in \mathsf{wp}\,(e)\,\big\{\exists v.\ \ell \mapsto v \star \hat{P}(v) \star (\ell \mapsto \mathsf{Mut}\ \alpha\ \hat{P} \mathrel{-\!\!*} \hat{Q})\big\}^{(\mathrm{H9})}$.
Unfolding wp, and setting $\rho_f = \rho_f$ and $\rho = \rho_a \bullet \rho_\ell \bullet \rho_{\hat{P}(v)}$ with H8 for the compatibility requirement, $\exists\, \rho' \mathrel{\#} \rho_f{}^{(\mathrm{H10})}$, $\rho^+ \mathrel{\#} \rho' \bullet \rho_f{}^{(\mathrm{H11})}$, v'.

- $\left(\left\llbracket \rho_f \bullet \rho_a \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \right\rrbracket, e\right) \Downarrow (\llbracket \rho_f \bullet \rho' \bullet \rho^+ \rrbracket, v')^{(\mathrm{H12})}$
- $\rho_a \bullet \rho_\ell \bullet \rho_{\hat{P}(v)} \leftrightsquigarrow \rho' \bullet \rho^{+(\mathrm{H13})}$
- $\rho^+|_{\mathsf{own}} = \varnothing^{(\mathrm{H14})}$
- $\rho' \in \exists v.\ \ell \mapsto v \star \hat{P}(v) \star (\ell \mapsto \mathsf{Mut}\ \alpha\ \hat{P} \mathrel{-\!\!*} \hat{Q}(v'))^{(\mathrm{H15})}$

Unfolding $\exists$ and $\star$ in H15, $\exists\, v'', \rho''_\ell, \rho_{\hat{P}(v'')}, \rho_b$.

- $\rho' = \rho''_\ell \bullet \rho_{\hat{P}(v'')} \bullet \rho_b{}^{(\mathrm{H16})}$
- $\rho''_\ell \in \ell \mapsto v''^{(\mathrm{H17})}$
- $\rho_{\hat{P}(v'')} \in \hat{P}(v'')^{(\mathrm{H18})}$
- $\rho_b \in (\ell \mapsto \mathsf{Mut}\ \alpha\ \hat{P} \mathrel{-\!\!*} \hat{Q}(v'))^{(\mathrm{H19})}$

Let $\rho''_m = \ell \mapsto \mathsf{mut}(\beta, v'', \rho_{\hat{P}(v'')}, \hat{P})$. Note since ρ_m is well formed, ρ''_m is as well.
Now we establish a bunch more compatibility results for the "mutably borrowed" resource after running e:

- $\rho_b \bullet \rho^+ \mathrel{\#} \rho''_m{}^{(\mathrm{H20})}$: by lemma 6.11 with H11, $\rho' \mathrel{\#} \rho^+$, and then by lemma 6.24.
- $\rho_f \mathrel{\#} \rho_b \bullet \rho^+ \bullet \rho''_m{}^{(\mathrm{H21})}$: by H11, $\rho' \bullet \rho^+ \mathrel{\#} \rho_f$, and therefore by lemma 6.24.
- $\rho_b \mathrel{\#} \rho''_m{}^{(\mathrm{H22})}$: by lemma 6.11 with H21.

- $\rho_b \bullet \rho''_m \mathrel{\#} \rho_f{}^{(\text{H23})}$: by lemma 6.11 with H21.

By lemmas 6.25 and 6.8 with H21 and H12, $(\llbracket \rho_f \bullet \rho \rrbracket, e) \Downarrow (\llbracket \rho_f \bullet \rho_b \bullet \rho^+ \bullet \rho''_m \rrbracket, v')^{(\text{H24})}$.
By lemma 6.28 with H20 and H13, $\rho \leftrightsquigarrow \rho_b \bullet \rho^+ \bullet \rho''_m{}^{(\text{H25})}$.
By the definition of $-\!\!*$ with H22, $\rho_b \bullet \rho''_m \in \hat{Q}(v')^{(\text{H26})}$.
Now we can prove our goals, setting $\rho' = \rho_b \bullet \rho''_m$, and $\rho^+ = \rho^+$,

- G2: $\rho_b \bullet \rho''_m \mathrel{\#} \rho_f$ by H23
- G3: $\rho^+ \mathrel{\#} \rho_b \bullet \rho''_m \bullet \rho_f$ by H21.
- G4: $(\llbracket \rho_f \bullet \rho \rrbracket, e) \Downarrow (\llbracket \rho_f \bullet \rho_b \bullet \rho''_m \bullet \rho^+ \rrbracket, v')$ by H24
- G5: $\rho \leftrightsquigarrow \rho_b \bullet \rho''_m \bullet \rho^+$ by H25
- G6: $\rho^+|_{\mathsf{own}} = \varnothing$ by H14
- G7: $\rho_b \bullet \rho''_m \in \hat{Q}(v')$ by H26

□

6.4 Standard Entailments

Lemma 6.67 (REFL)**.** $P \vDash P$

Proof. By inspection. □

Lemma 6.68 (TRANS)**.** $\dfrac{P \vDash Q \quad Q \vDash R}{P \vDash R}$

Proof. Suppose $P \vDash Q$ and $Q \vDash R$. Let ρ be arbitrary such that $P(\rho)$. By $P \vDash Q$, $Q(\rho)$. By $Q \vDash R$, $R(\rho)$. □

Lemma 6.69 ($\top$R)**.** $P \vDash \top$

Proof. By inspection. □

Lemma 6.70 ($\bot$L)**.** $\bot \vDash P$

Proof. By inspection. □

Lemma 6.71 ($\wedge$R)**.** $\dfrac{P \vDash Q_1 \quad P \vDash Q_2}{P \vDash Q_1 \wedge Q_2}$

Proof. Suppose $P \vDash Q_1$ and $P \vDash Q_2$. Let ρ be arbitrary such that $P(\rho)$. By $P \vDash Q_1$, $Q_1(\rho)$. By $P \vDash Q_2$, $Q_2(\rho)$. □

Lemma 6.72 ($\wedge$L)**.** $P_1 \wedge P_2 \vDash P_i$

Proof. By inspection. □

Lemma 6.73 ($\vee$R)**.** $P_i \vDash P_1 \vee P_2$

Proof. Let ρ be arbitrary such that $P_i(\rho)$. Since $i \in \{1, 2\}$, $P_1(\rho) \vee P_2(\rho)$. □

Lemma 6.74 ($\vee$L)**.** $\dfrac{P_1 \vDash Q \quad P_2 \vDash Q}{P_1 \vee P_2 \vDash Q}$

Proof. Suppose $P_1 \vDash Q$ and $P_2 \vDash Q$. Let ρ be arbitrary such that $P_1(\rho) \vee P_2(\rho)$. By cases on $P_1(\rho) \vee P_2(\rho)$. □

Lemma 6.75 ($\Rightarrow$R)**.** $\dfrac{P \wedge Q \vDash R}{P \vDash Q \Rightarrow R}$

Proof. Suppose $P \wedge Q \vDash R$. Let ρ be arbitrary such that $P(\rho)$. Suppose $Q(\rho)$. Immediate. □

Lemma 6.76 ($\Rightarrow$L)**.** $P \land (P \Rightarrow Q) \vDash Q$

Proof. By inspection. □

Lemma 6.77 ($\forall$ R)**.** $\dfrac{\forall\, x.\ (P \vDash Q(x))}{P \vDash \forall\, x.\ Q(x)}$

Proof. Suppose $\forall\, x.\ P \vDash \hat{Q}(x)$. Let ρ be arbitrary such that $P(\rho)$. Let x be arbitrary. Immediate. □

Lemma 6.78 ($\forall$ L)**.** $\dfrac{P(x) \vDash Q}{(\forall\, x.\ P(x)) \vDash Q}$

Proof. Suppose $\hat{P}(x) \vDash Q$. Let ρ, x be arbitrary such that $\hat{P}(x)(\rho)$. Immediate. □

Lemma 6.79 ($\exists$ R)**.** $\dfrac{P \vDash Q(x)}{P \vDash \exists\, x.\ Q(x)}$

Proof. Suppose $P \vDash \hat{Q}(x)$. Let ρ be arbitrary such that $P(\rho)$. Choose x. Immediate. □

Lemma 6.80 ($\exists$ L)**.** $\dfrac{\forall\, x.\ (P(x) \vDash Q)}{(\exists\, x.\ P(x)) \vDash Q}$

Proof. Suppose $\hat{P}(x) \vDash Q$. Let x, ρ be arbitrary such that $\hat{P}(x)(\rho)$. Immediate. □

Lemma 6.81 ($\ulcorner\urcorner$R)**.** $\dfrac{Q_{\text{meta}}}{P \vDash P \star \ulcorner Q_{\text{meta}} \urcorner}$

Proof. Suppose Q_{meta}. Let ρ be arbitrary such that $P(\rho)$. Choose $\exists\, \rho_1, \rho_2$ to be $\rho, \varnothing$. Then by theorem 6.4 and inspection. □

Lemma 6.82 ($\ulcorner\urcorner$L)**.** $\dfrac{P_{\text{meta}} \Rightarrow (Q \vDash R)}{\ulcorner P_{\text{meta}} \urcorner \star Q \vDash R}$

Proof. Suppose $P_{\text{meta}} \Rightarrow (Q \vDash R)$. Let ρ be arbitrary such that $\rho = \varnothing \bullet \rho_2$, P_{meta}, and $Q(\rho_2)$ for some ρ_2. By theorem 6.2 and theorem 6.4, $\rho = \rho_2$. Immediate. □

Lemma 6.83 ($!$ MONO)**.** $\dfrac{P \vDash Q}{!\,P \vDash !\,Q}$

Proof. Suppose $P \vDash Q$. Let ρ be arbitrary such that $(!\,P)(\rho)$. By unfolding, $\rho = \varnothing$ and $P(\varnothing)$. Immediate. □

Lemma 6.84 ($!$L)**.** $!\,P \vDash Q$

Proof. By inspection. □

Lemma 6.85 ($!$ UNR)**.** $!\,P \Dashv\vDash !\,P \star !\,P$

Proof. **Case $\vDash$.** Let ρ be arbitrary such that $\rho = \varnothing$ and $P(\varnothing)$. Then by choosing $\exists\, \rho_1, \rho_2$ to be $\varnothing, \varnothing$.

Case $\Dashv$. Let ρ be arbitrary such that $\rho = \varnothing \bullet \varnothing$, $P(\varnothing)$, and $P(\varnothing)$. Immediate. □

Lemma 6.86 ($!\land$)**.** $(!\,P) \land Q \vDash (!\,P) \star Q$

Proof. Let ρ be arbitrary such that $\rho = \varnothing$, $P(\varnothing)$, and $Q(\varnothing)$. Choosing $\exists\, \rho_1, \rho_2$ to be $\varnothing, \varnothing$. Immediate. □

Lemma 6.87 ($!$4)**.** $!\,P \vDash !\,!\,P$

Proof. By inspection. □

Lemma 6.88 ($!\,\forall$)**.** $\forall\, x.\ !\,P(x) \vDash !\,\forall\, x.\ P(x)$

Proof. Suppose $X \neq \varnothing$. Let ρ be arbitrary such that $\forall\, x \in X.\ \rho = \varnothing \wedge \hat{P}(x)(\rho)$. From $X \neq \varnothing$, it follows that $\rho = \varnothing$ and $\forall\, x.\ \hat{P}(x)(\rho)$. Immediate. □

Lemma 6.89 ($!\,\exists$)**.** $\exists\, x.\ !\,P(x) \vDash !\,\exists\, x.\ P(x)$

Proof. Let ρ be arbitrary such that $\rho = \varnothing$ and $\hat{P}(x)(\varnothing)$ for some x. Choose $\exists\, x$ to be x. Immediate. □

Lemma 6.90 ($\star$COM)**.** $P \star Q \vDash Q \star P$

Proof. By inspection, using theorem 6.2. □

Lemma 6.91 ($\star$ASC)**.** $(P \star Q) \star R \vDash P \star (Q \star R)$

Proof. By inspection, using theorem 6.3. □

Lemma 6.92 ($\star$MONO)**.** $\dfrac{P_1 \vDash Q_1 \quad P_2 \vDash Q_2}{P_1 \star P_2 \vDash Q_1 \star Q_2}$

Proof. Suppose $P_1 \vDash Q_1$ and $P_2 \vDash Q_2$. Let ρ be arbitrary such that $\rho = \rho_1 \bullet \rho_2$, $P_1(\rho_1)$, and $P_2(\rho)$ for some ρ_1, ρ_2. It follows that $Q_1(\rho)$ and $Q_2(\rho)$. Choose $\exists\, \rho_1, \rho_2$ to be ρ_1, ρ_2. Immediate. □

Lemma 6.93 ($-\!\!\star$R)**.** $\dfrac{P \star Q \vDash R}{P \vDash Q -\!\!\star R}$

Proof. Suppose $P \star Q \vDash R$. Let ρ be arbitrary such that $P(\rho)$. Let ρ_1, ρ_2 be arbitrary such that $Q(\rho_1)$ and $\rho \bullet \rho_1 = \rho_2$. By $P \star Q \vDash R$ with $\rho \bullet \rho_1$, $R(\rho \bullet \rho_1)$. □

Lemma 6.94 ($-\!\!\star$L)**.** $P \star (P -\!\!\star Q) \vDash Q$

Proof. Let ρ be arbitrary such that $\rho = \rho_1 \bullet \rho_2$, $P(\rho_1)$, $(P -\!\!\star Q)(\rho_2)$. By $(P -\!\!\star Q)(\rho_2)$ with ρ_1, $Q(\rho_2 \bullet \rho_1)$. By theorem 6.2, $Q(\rho_1 \bullet \rho_2)$. □

Lemma 6.95 ($\mapsto$EX)**.** $\ell \mapsto v_1 \star \ell \mapsto \_ \vDash \bot$

Proof. By contradiction, using theorem 6.41. □

6.5 Non-standard Entailments

Lemma 6.96 ($[\,]$-MONO)**.** $\dfrac{P \vDash Q}{[\alpha]\, P \vDash [\alpha]\, Q}$

Proof. Suppose $P \vDash Q$. Let ρ be arbitrary such that $P(\rho)$ and $@\rho \sqsupset \alpha$. By $P \vDash Q$ and $P(\rho)$, $Q(\rho)$. □

Lemma 6.97 ($[\,]$L)**.** $[\alpha]\, P \vDash P$

Proof. By inspection. □

Lemma 6.98 ($[\,]$R)**.** $\dfrac{[\alpha]\, P \vDash Q}{[\alpha]\, P \vDash [\alpha]\, Q}$

Proof. By inspection. □

Lemma 6.99 ($[\,]$4)**.** $[\alpha]\,[\beta]\, P \vDash [\alpha \sqcup \beta]\, P$

Proof. **Case $\vDash$.** Let ρ be arbitrary such that $P(\rho)$, $@\rho \sqsupset \alpha$, and $@\rho \sqsupset \beta$. By lattice laws, it follows that $@p \sqsupset \alpha \sqcup \beta$.

Case $\Dashv$. Let ρ be arbitrary such that $P(\rho)$, $@\rho \sqsupset \alpha \sqcup \beta$. By lattice laws, $@\rho \sqsupset \alpha$ and $@\rho \sqsupset \beta$. □

Lemma 6.100 ($[\,]\ \sqsupseteq$)**.** $\dfrac{\alpha \sqsupseteq \beta}{[\alpha]\, P \vDash [\beta]\, P}$

Proof. Suppose $\alpha \sqsupseteq \beta$. Let ρ be arbitrary such that $P(\rho)$ and $@\rho \sqsupset \alpha$. By transitivity, $@\rho \sqsupset \alpha \sqsupseteq \beta$. Thus, $@\rho \sqsupset \beta$. □

Lemma 6.101 ($[]\,\exists\,\textsc{r}$)**.** $P \vDash \exists\,\alpha.[\alpha]\,P$

Proof. Let ρ be arbitrary such that $P(\rho)$. Choose $\exists\,\alpha$ to be $\downarrow@\rho$. By theorem 6.63, $@\rho \sqsupset \downarrow@\rho$. □

Lemma 6.102 ($[]\,\forall$)**.** $\forall\,x.\ [\alpha]\,P(x) \dashv\vDash [\alpha]\,\forall\,x.\ P(x)$

Proof. **Case:** $\vDash$**.** Suppose $X \neq \varnothing$. Let ρ be arbitrary such that $\forall\,x \in X.\ \hat{P}(x)(\rho) \wedge @\rho \sqsupset \alpha$. Since $X \neq \varnothing$, it follows that $@\rho \sqsupset \alpha$ and $\forall\,x \in X.\ \hat{P}(x)(\rho)$.

Case: $\dashv$**.** Similar to the previous case, but without the domain restriction on x. □

Lemma 6.103 ($[]\,\exists$)**.** $\exists\,x.\ [\alpha]\,P(x) \dashv\vDash [\alpha]\,\exists\,x.\ P(x)$

Proof. **Case:** $\vDash$**.** Let ρ be arbitrary such that $\hat{P}(x)(\rho)$ for some x and $@p \sqsupset \alpha$. Choose $\exists\,x$ to be x. Immediate.

Case: $\dashv$**.** Similar to previous case. □

Lemma 6.104 ($[]\,\star$)**.** $[\alpha]\,(P \star Q) \dashv\vDash [\alpha]\,P \star [\alpha]\,Q \quad [\alpha]\,(P \star Q) \dashv\vDash [\alpha]\,P \star [\alpha]\,Q$

Proof. **Case** $\vDash$**.** Let ρ be arbitrary such that $\rho = \rho_1 \bullet \rho_2$, $P(\rho_q)$, $Q(\rho_2)$, and $@(\rho_1 \bullet \rho_2) \sqsupset \alpha$. Choose $\exists\,\rho_1, \rho_2$ to be ρ_1, ρ_2. It suffices to show that $@\rho_1 \sqsupset \alpha$ and $@\rho_2 \sqsupset \alpha$, which follows by theorem 6.45.

Case $\dashv$**.** Similar to previous case. □

Lemma 6.105 ($[]\,\vee$)**.** $[\alpha]\,(P \vee Q) \dashv\vDash [\alpha]\,P \vee [\alpha]\,Q$

Proof. **Case** $\vDash$**.** Let ρ be arbitrary such that $(P(\rho) \vee Q(\rho)) \wedge @\rho \sqsupset \alpha$. It suffices if $(P(\rho) \wedge @\rho \sqsupset \alpha) \vee (Q(\rho) \wedge @\rho \sqsupset \alpha)$, which follows by De Morgan's laws.

Case $\dashv$**.** Similar to previous case. □

Lemma 6.106 ($[]\,!$)**.** $[\alpha]\,!\,P \dashv\vDash\ !\,[\alpha]\,P$

Proof. By inspection. □

Lemma 6.107 ($[]\ \mapsto$)**.** $\ell \mapsto v \vDash [\alpha]\,\ell \mapsto v$

Proof. By inspection. □

Lemma 6.108 (И-mono)**.** $\dfrac{\forall\,\alpha \sqsubset \beta'.\ ([\alpha]\,P(\alpha) \vDash [\alpha]\,Q(\alpha))}{\text{И}\alpha.\,P(\alpha) \vDash \text{И}\alpha.\,Q(\alpha)}$

Proof.

Proof step	Current goal
Unfold И.	$\exists\,\beta.\forall\,\alpha \sqsubset \beta.[\alpha]\,P(\alpha) \vDash \exists\,\beta.\forall\,\alpha \sqsubset \beta.[\alpha]\,Q(\alpha)$
Apply $\exists\,$L. Choose $\beta := \beta \sqcap \beta'$ on right. Fix $\alpha \sqsubset \beta \sqcap \beta'$.	$(\forall\,\alpha \sqsubset \beta.[\alpha]\,P(\alpha)) \vDash [\alpha]\,Q(\alpha)$
Choose $\alpha := \alpha$ on left.	$[\alpha]\,P(\alpha) \vDash [\alpha]\,Q(\alpha)$
Follows by assumption because $\alpha \sqsubset \beta'$.	□

Lemma 6.109 (ИL)**.** $\dfrac{\forall\,\alpha \sqsubset \beta'.\ ([\alpha]\,P(\alpha) \vDash Q)}{\text{И}\alpha.\,P(\alpha) \vDash Q}$

Proof.

Proof step	Current goal
Unfold И.	$\exists\,\beta.\forall\,\alpha \sqsubset \beta.[\alpha]\,P(\alpha) \vDash Q$
Fix β arbitrary.	$\forall\,\alpha \sqsubset \beta.[\alpha]\,P(\alpha) \vDash Q$
Choose arbitrary $\alpha \sqsubset \beta \sqcap \beta'$, always possible $\sqsubset$ is infinitely decreasing.	$[\alpha]\,P(\alpha) \vDash Q$
Follows by assumption because $\alpha \sqsubset \beta'$.	□

Lemma 6.110 (ИR)**.** $P \vDash \text{И}\alpha.\,P$

Proof.

Proof step	Current goal
Unfold И.	$P \vDash \exists\, \beta.\ \forall\, \alpha \sqsubset \beta.\ [\alpha]\, P$
Apply $[\,]\,\exists\,\mathrm{R}$ on left.	$\exists\, \beta.[\beta]\, P \vDash \exists\, \beta.\ \forall\, \alpha \sqsubset \beta.\ [\alpha]\, P$
Fix β arbitrary.	$[\beta]\, P \vDash \exists\, \beta.\ \forall\, \alpha \sqsubset \beta.\ [\alpha]\, P$
Choose $\beta := \beta$.	$[\beta]\, P \vDash \forall\, \alpha \sqsubset \beta.\ [\alpha]\, P$
Fix $\alpha \sqsubset \beta$ arbitrary.	$[\beta]\, P \vDash [\alpha]\, P$
Apply $[\,]\ \sqsupseteq$.	□

Lemma 6.111 ($\text{И}\star$)**.** $\text{И}\alpha.\, P(\alpha) \star \text{И}\alpha.\, Q(\alpha) \vDash \text{И}\alpha.\, (P(\alpha) \star Q(\alpha))$

Proof.

Proof step	Current goal
Unfold И.	$(\exists\, \beta_P.\ \forall\, \alpha_P \sqsubset \beta_P.\ P(\alpha_P)) \star (\exists\, \beta_Q.\ \forall\, \alpha_Q \sqsubset \beta_Q.\ Q(\alpha_Q)) \vDash \exists\, \beta.\ \forall\, \alpha \sqsubset \beta.\ (P(\alpha) \star Q(\alpha))$
Fix arbitrary β_P, β_Q.	$(\forall\, \alpha_P \sqsubset \beta_P.\ P(\alpha_P)) \star (\forall\, \alpha_Q \sqsubset \beta_Q.\ Q(\alpha_Q)) \vDash \exists\, \beta.\ \forall\, \alpha \sqsubset \beta.\ (P(\alpha) \star Q(\alpha))$
Choose $\beta := \beta_P \sqcap \beta_Q$.	$(\forall\, \alpha_P \sqsubset \beta_P.\ P(\alpha_P)) \star (\forall\, \alpha_Q \sqsubset \beta_Q.\ Q(\alpha_Q)) \vDash \forall\, \alpha \sqsubset \beta_P \sqcap \beta_Q.\ (P(\alpha) \star Q(\alpha))$
Fix $\alpha \sqsubset \beta_P \sqcap \beta_Q$.	$(\forall\, \alpha_P \sqsubset \beta_P.\ P(\alpha_P)) \star (\forall\, \alpha_Q \sqsubset \beta_Q.\ Q(\alpha_Q)) \vDash P(\alpha) \star Q(\alpha)$
Choose $\alpha_P := \alpha, \alpha_Q := \alpha$.	$P(\alpha) \star Q(\alpha) \vDash P(\alpha) \star Q(\alpha)$

□

Lemma 6.112 ($\text{И}\mathrm{F}$)**.** $P \star \text{И}\alpha.\, Q(\alpha) \vDash \text{И}\alpha.\, ([\alpha]\, P \star Q(\alpha))$

Proof.

$$\begin{aligned}
P \star \text{И}\alpha.\, Q(\alpha) &\vDash \exists\, \beta.\ [\beta]\, P \star \text{И}\alpha.\, Q(\alpha) && \text{by } [\,]\,\exists\,\mathrm{R}\\
&\vDash \exists\, \beta.\ [\beta]\,[\beta]\, P \star \text{И}\alpha.\, Q(\alpha) && \text{by } [\,]\,4\\
&\vDash (\exists\, \beta.\ \forall\, \alpha \sqsubset \beta.\ [\alpha]\,[\alpha]\, P) \star \text{И}\alpha.\, Q(\alpha) && \text{by } [\,]\text{-}\sqsupseteq \text{ and monotonicity}\\
&\vDash \text{И}\alpha.\, [\alpha]\, P \star \text{И}\alpha.\, Q(\alpha) && \text{definition of } \text{И}\\
&\vDash \text{И}\alpha.\, ([\alpha]\, P \star Q(\alpha)) && \text{by } \text{И}\star
\end{aligned}$$

□

Lemma 6.113 (I-MONO)**.** $\dfrac{\forall\, v.\ \hat{P}(v) \vDash \hat{Q}(v)}{\ell \mapsto\!\mathrm{I}_\alpha\, \hat{P} \vDash \ell \mapsto\!\mathrm{I}_\alpha\, \hat{Q}}$

Proof. Suppose $\forall\, v.\ \hat{P}(v) \vDash \hat{Q}(v)$. Let ρ be arbitrary such that $\rho = \ell \mapsto \mathsf{imm}(\tilde{\beta}, v, \rho')$, $\hat{P}(v)(\rho')$, and $\alpha \sqsubseteq \bigsqcup\tilde{\beta}$ for some v, ρ', $\tilde{\beta}$. Choose $\exists\, \tilde{\beta}, v, \rho'$ to be $\tilde{\beta}, v, \rho'$. It suffices if $\hat{Q}(v)(\rho')$, which follows by $\forall\, v.\ \hat{P}(v) \vDash \hat{Q}(v)$ and $\hat{P}(v)(\rho')$. □

Lemma 6.114 (I $\sqsupseteq$)**.** $\dfrac{\alpha \sqsupseteq \beta}{\ell \mapsto\!\mathrm{I}_\alpha\, \hat{P} \vDash \ell \mapsto\!\mathrm{I}_\beta\, \hat{P}}$

Proof. Suppose $\alpha \sqsupseteq \beta$. Let ρ be arbitrary such that $\rho = \ell \mapsto \mathsf{imm}(\tilde{\beta}, v, \rho')$, $\hat{P}(v)(\rho')$, and $\alpha \sqsubseteq \bigsqcup\tilde{\beta}$ for some v, ρ', $\tilde{\beta}$. Choose $\exists\, \tilde{\beta}, v, \rho'$ to be $\tilde{\beta}, v, \rho'$. It suffices if $\beta \sqsubseteq \bigsqcup\tilde{\beta}$. By transitivity, it follows that $\beta \sqsubseteq \alpha \sqsubseteq \bigsqcup\tilde{\beta}$. □

Lemma 6.115 (I-AG)**.** $\ell \mapsto\!\mathrm{I}_\alpha\, \hat{P} \star \ell \mapsto\!\mathrm{I}_\beta\, \hat{Q} \vDash \ell \mapsto\!\mathrm{I}_{\alpha \sqcup \beta}\, (\hat{P} \wedge \hat{Q})$

Proof. Let ρ be arbitrary such that $\rho = \rho_1 \bullet \rho_2$, $\rho_1 = \ell \mapsto \mathsf{imm}(\tilde{\beta}_1, v_1, \rho_1')$, $\hat{P}(v_1)(\rho_1')$, $\alpha \sqsubseteq \bigsqcup\tilde{\beta}_1$, $\rho_2 = \ell \mapsto \mathsf{imm}(\tilde{\beta}_2, v_2, \rho_2')$, $\hat{Q}(v_2)(\rho_2')$, and $\beta \sqsubseteq \bigsqcup\tilde{\beta}_2$ for some ρ_1, ρ_2, $\tilde{\beta}_1$, $\tilde{\beta}_2$, v_1, v_2, ρ_1', and ρ_2'. We must show $\exists\, \tilde{\beta}, v, \rho'$. $\rho = \ell \mapsto \mathsf{imm}(\tilde{\beta}, v, \rho') \wedge \hat{P}(v)(\rho') \wedge \hat{Q}(v)(\rho') \wedge \alpha \sqcup \beta \sqsubseteq \bigsqcup\tilde{\beta}$.

By definition, $\rho = \rho_1 \bullet \rho_2 = \ell \mapsto \mathsf{imm}(\tilde{\beta}_1, v_1, \rho_1') \bullet \ell \mapsto \mathsf{imm}(\tilde{\beta}_2, v_2, \rho_2') = \ell \mapsto \mathsf{imm}(\tilde{\beta}_1 \cup \tilde{\beta}_2, v_1, \rho_1')$, $v_1 = v_2$, and $\rho_1' = \rho_2'$. Choose $\exists\, \tilde{\beta}, v, \rho'$ to be $\tilde{\beta}_1 \cup \tilde{\beta}_2, v_1, \rho_1'$. All proof obligations are immediate except $\alpha \sqcup \beta \sqsubseteq \bigsqcup(\tilde{\beta}_1 \cup \tilde{\beta}_2)$. This follows from the lattice laws given $\alpha \sqsubseteq \tilde{\beta}_1$ and $\beta \sqsubseteq \tilde{\beta}_2$. □

Lemma 6.116 (I-DUP)**.** $\ell \mapsto\!\mathrm{I}_\alpha\, \hat{P} \vDash \ell \mapsto\!\mathrm{I}_\alpha\, \hat{P} \star \ell \mapsto\!\mathrm{I}_\alpha\, \hat{P}$

Proof. Let ρ be arbitrary such that $\rho = \ell \mapsto \mathsf{imm}(\tilde{\beta}, v, \rho')$, $\hat{P}(v)(\rho')$, and $\alpha \sqsubseteq \bigsqcup\tilde{\beta}$ for some $\tilde{\beta}$, v, ρ'. Choose $\exists\, \rho_1, \rho_2$ to be ρ, ρ. It suffices if $\rho = \rho \bullet \rho$, which follows from theorem 6.43. □

Lemma 6.117 (M-INV)**.** $\dfrac{\forall\, v.\ \hat{P}(v) \dashv\vDash \hat{Q}(v)}{\ell \mapsto\!\mathrm{M}_\alpha\, \hat{P} \dashv\vDash \ell \mapsto\!\mathrm{M}_\alpha\, \hat{Q}}$

Proof. By inspection, using functional extensionality. □

Lemma 6.118 (M $\sqsupseteq$)**.** $\dfrac{\alpha \sqsupseteq \beta}{\ell \mapsto\!\mathrm{M}_\alpha\, \hat{P} \vDash \ell \mapsto\!\mathrm{M}_\beta\, \hat{P}}$

Proof. Suppose $\alpha \sqsupseteq \beta$. Let ρ be arbitrary such that $\rho = \ell \mapsto \mathsf{mut}(\beta_0, v, \rho', \hat{P})$ for some $\beta_0 \sqsupseteq \alpha$, v, ρ'. Choose $\exists\, \beta, v, \rho'$ to be β_0, v, ρ'. It suffices if $\beta_0 \sqsupseteq \beta$. By transitivity, $\beta_0 \sqsupseteq \alpha \sqsupseteq \beta$. □

Lemma 6.119 (M-EX)**.** $\ell \mapsto\!\mathrm{M}_\alpha\, \hat{P} \star \ell \mapsto \_ \vDash \bot$

Proof. By inspection, using theorem 6.42. □

6.6 Reborrowing Entailments

Lemma 6.120 ($\circlearrowleft$-MONO)**.** $\dfrac{P \vDash Q}{\circlearrowleft_\alpha P \vDash \circlearrowleft_\alpha Q}$

Proof. Suppose $P \vDash Q$. Let ρ be arbitrary such that $P(\rho')$ for some $\rho' \in \mathsf{reb}_\alpha(\rho)$. Choose ρ'. By $P \vDash Q$ with ρ' and $P(\rho')$, we obtain $Q(\rho')$. □

Lemma 6.121 ($\circlearrowleft$ $\mapsto$)**.** $\ell \mapsto v \star [\alpha]\, \hat{P}(v) \vDash \circlearrowleft_\alpha \ell \mapsto\!\mathrm{I}_\alpha\, \hat{P}$

Proof. Let ρ be arbitrary such that $\rho = \rho_1 \bullet \rho_2$, $\rho_1 = \ell \mapsto \mathsf{own}(v)$, $\hat{P}(v)(\rho_2)$, and $@\rho_2 \sqsupset \alpha$ for some ρ_1 and ρ_2. Choose $\exists\, \rho' \in \mathsf{reb}_\alpha(\rho)$ to be $\ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_2)$. Choose $\exists\, \tilde{\beta}, v, \rho'$ to be $\{\alpha\}, v, \rho_2$. Most proof obligations are immediate, but it remains to show $\ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_2) \in \mathsf{reb}_\alpha(\rho)$. Choose $\exists\, \pi$ to be $\ell \mapsto \rho$. It suffices if:

- $@\rho \sqsupset \alpha$: Since $\rho = \ell \mapsto \mathsf{own}(v) \bullet \rho_2$, it suffices if $@(\ell \mapsto \mathsf{own}(v)) \sqsupset \alpha$, which holds by definition, and $@\rho_2 \sqsupset \alpha$, which is immediate.
- $\rho \geq \bigbullet_{\ell \in \mathrm{dom}(\pi)} \pi(\ell)$: Since $\mathrm{dom}(\pi) = \{\ell\}$ and $\pi(\ell) = \rho$, this is simply equivalent to $\rho \geq \rho$.
- $\forall\, \ell \in \mathrm{dom}(\pi), v, \rho''.\ \ldots$: Since $\mathrm{dom}(\pi) = \{\ell\}$ and $\rho(\ell) = \mathsf{own}(v)$, this simplifies to $(\ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho_2))(\ell) = \mathsf{imm}(\{\alpha\}, v, \pi(\ell) \smallsetminus \ell)$, which holds by inspection.

□

Lemma 6.122 ($\circlearrowleft$M)**.** $[\alpha]\, (\ell \mapsto\!\mathrm{M}_\beta\, \hat{P}) \vDash \circlearrowleft_\alpha (\ell \mapsto\!\mathrm{I}_\alpha\, \hat{P})$

Proof. Let ρ be arbitrary such that $\rho = \ell \mapsto \mathsf{mut}(\beta, v, \rho', \hat{P})$ (which implies $\hat{P}(v)$) and $@\rho \sqsupset \alpha$ for some $\beta \sqsupseteq \alpha$, v, and ρ'. Choose $\exists\, \rho' \in \mathsf{reb}_\alpha(\rho)$ to be $\ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho')$. Choose $\exists\, \tilde{\beta}, v, \rho'$ to be $\{\alpha\}, v, \rho'$. Most proof obligations are immediate, but it remains to show $\ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho') \in \mathsf{reb}_\alpha(\rho)$. Choose $\exists\, \pi$ to be $\ell \mapsto \rho$. It suffices if:

- $@\rho \sqsupset \alpha$: Immediate.
- $\rho \geq \bigbullet_{\ell \in \mathrm{dom}(\pi)} \pi(\ell)$: Since $\mathrm{dom}(\pi) = \{\ell\}$ and $\pi(\ell) = \rho$, this is simply equivalent to $\rho \geq \rho$.
- $\forall\, \ell \in \mathrm{dom}(\pi), v, \rho''.\ \ldots$: Since $\mathrm{dom}(\pi) = \{\ell\}$ and $\rho(\ell) = \mathsf{mut}(\beta, v, \rho', \hat{P})$, this can be simplified to $(\ell \mapsto \mathsf{imm}(\{\alpha\}, v, \rho'))(\ell) = \mathsf{imm}(\{\alpha\}, v, \rho') \wedge \mathrm{dom}(\pi(\ell)) = \{\ell\}$, which holds by inspection.

□

Lemma 6.123 ($\circlearrowleft$I)**.** $[\alpha]\, (\ell \mapsto\!\mathrm{I}_\beta\, \hat{P}) \vDash \circlearrowleft_\alpha (\ell \mapsto\!\mathrm{I}_\beta\, \hat{P})$

Proof. Let ρ be arbitrary such that $\rho = \ell \mapsto \mathsf{imm}(\tilde{\beta}, v, \rho')$, $\hat{P}(v)(\rho')$, $\beta \sqsupseteq \bigsqcup \tilde{\beta}$, and $@\rho \sqsupset \alpha$ for some $\tilde{\beta}$, v, and ρ'. Choose $\exists\, \rho' \in \mathsf{reb}_\alpha(\rho)$ to be $\ell \mapsto \mathsf{imm}(\tilde{\beta}, v, \rho')$. Choose $\exists\, \tilde{\beta}, v, \rho'$ to be $\tilde{\beta}, v, \rho'$. Most proof obligations are immediate, but it remains to show $\ell \mapsto \mathsf{imm}(\tilde{\beta}, v, \rho') \in \mathsf{reb}_\alpha(\rho)$. Choose $\exists\, \pi$ to be $\ell \mapsto \rho$. It suffices if:

- $@\rho \sqsupset \alpha$: Immediate.

- $\rho \geq \bullet_{\ell \in \mathrm{dom}(\pi)} \pi(\ell)$: Since $\mathrm{dom}(\pi) = \{\ell\}$ and $\pi(\ell) = \rho$, this is simply equivalent to $\rho \geq \rho$.

- $\forall\, \ell \in \mathrm{dom}(\pi), v, \rho''.\ \ldots$: Since $\mathrm{dom}(\pi) = \{\ell\}$ and $\rho(\ell) = \mathsf{imm}(\tilde{\beta}, v, \rho')$, this simplifies to $(\ell \mapsto \mathsf{imm}(\tilde{\beta}, v, \rho'))(\ell) = \rho(\ell) \wedge \mathrm{dom}(\pi(\ell)) = \{\ell\}$, which holds by inspection.

□

Lemma 6.124 ($\circlearrowright \ulcorner\urcorner$). $\ulcorner P \urcorner \vDash \circlearrowright_{\alpha} \ulcorner P \urcorner$

Proof. Let ρ be arbitrary such that $\rho = \varnothing$ and P. Choose $\exists\, \rho' \in \mathsf{reb}_{\alpha}(\rho)$ to be $\varnothing$. Most proof obligations are immediate, but it remains to show $\varnothing \in \mathsf{reb}_{\alpha}(\rho)$. Choose $\exists\, \pi$ to be $\varnothing$. Since $\mathrm{dom}(\varnothing) = \varnothing$, this simplifies to $@\varnothing \sqsupset \alpha$ and $\varnothing \geq \bullet_{\ell \in \mathrm{dom}(\pi)} \pi(\ell)$, which hold by definition. □

Lemma 6.125 ($\circlearrowright \star$). $\circlearrowright_{\alpha} P \star \circlearrowright_{\alpha} Q \vDash \circlearrowright_{\alpha} (P \star Q)$

Proof. Let ρ be arbitrary such that $\rho = \rho_1 \bullet \rho_2$, $P(\rho_1')$, and $Q(\rho_2')$ for some ρ_1, ρ_2, $\rho_1' \in \mathsf{reb}_{\alpha}(\rho_1)$, and $\rho_2' \in \mathsf{reb}_{\alpha}(\rho_2)$. By theorem 6.61, $\rho_1' \bullet \rho_2' \in \mathsf{reb}_{\alpha}(\rho_1 \bullet \rho_2)$. Choose $\exists\, \rho' \in \mathsf{reb}_{\alpha}(\rho)$ to be $\rho_1' \bullet \rho_2'$. The remaining obligations are immediate. □

Lemma 6.126 ($\circlearrowright \vee$). $\circlearrowright_{\alpha} P \vee \circlearrowright_{\alpha} Q \dashv\vDash \circlearrowright_{\alpha} (P \vee Q)$

Proof. **Case $\vDash$.** Let ρ be arbitrary such that $(\exists\, \rho' \in \mathsf{reb}_{\alpha}(\rho). P(\rho')) \vee (\exists\, \rho' \in \mathsf{reb}_{\alpha}(\rho). Q(\rho'))$.

- Case: $P(\rho')$ for some $\rho' \in \mathsf{reb}_{\alpha}(\rho)$. Choose $\exists\, \rho' \in \mathsf{reb}_{\alpha}(\rho)$ to be ρ' and discharge the disjunction via the left side.

- Case: $Q(\rho')$ for some $\rho' \in \mathsf{reb}_{\alpha}(\rho)$. Choose $\exists\, \rho' \in \mathsf{reb}_{\alpha}(\rho)$ to be ρ' and discharge the disjunction via the right side.

Case $\dashv$. Let ρ be arbitrary such that $P(\rho') \vee Q(\rho')$ for some $\rho' \in \mathsf{reb}_{\alpha}(\rho)$.

- Case: $P(\rho')$. Discharge the disjunction via the left side and choose $\exists\, \rho' \in \mathsf{reb}_{\alpha}(\rho)$ to be ρ'.

- Case: $Q(\rho')$. Discharge the disjunction via the right side and choose $\exists\, \rho' \in \mathsf{reb}_{\alpha}(\rho)$ to be ρ'.

□

Lemma 6.127 ($\circlearrowright$-WEAK). $\circlearrowright_{\alpha} (P \star Q) \vDash \circlearrowright_{\alpha} P$

Proof. Let ρ be arbitrary such that $\rho' = \rho_1' \bullet \rho_2'$ and $P(\rho_1')$ and $Q(\rho_2')$ for some $\rho' \in \mathsf{reb}_{\alpha}(\rho)$, ρ_1', and ρ_2'. Choose $\exists\, \rho' \in \mathsf{reb}_{\alpha}(\rho)$ to be ρ_1'. $P(\rho_1')$ is immediate, but it remains to show $\rho_1' \in \mathsf{reb}_{\alpha}(\rho)$.

Unfold $\rho' \in \mathsf{reb}_{\alpha}(\rho)$ and we obtain $@\rho \sqsupset \alpha^{(\mathrm{H1})}$, $\rho \geq \bullet_{\ell \in \mathrm{dom}(\pi)} \pi(\ell)^{(\mathrm{H2})}$, and $\forall\, \ell \in \mathrm{dom}(\pi), v, \rho''.\ F(\ell, v, \rho, \rho', \rho'', \pi)^{(\mathrm{H3})}$ for some $\pi : \mathrm{dom}(\rho') \to \mathrm{Res}$, where

$$\begin{aligned} F(\ell, v, \rho, \rho', \rho'', \pi) = \ell \in \mathrm{dom}(\pi(\ell)) \wedge\ & \\ & (\rho(\ell) = \mathsf{own}(v) \Rightarrow \rho'(\ell) = \mathsf{imm}(\{\alpha\}, v, \pi(\ell) \setminus \ell)) \wedge \\ & (\rho(\ell) = \mathsf{mut}(-, v, \rho'', -) \Rightarrow \rho'(\ell) = \mathsf{imm}(\{\alpha\}, v, \rho'') \wedge \mathrm{dom}(\pi(\ell)) = \{\ell\}) \wedge \\ & (\rho(\ell) = \mathsf{imm}(-, -, -) \Rightarrow \rho'(\ell) = \rho(\ell) \wedge \mathrm{dom}(\pi(\ell)) = \{\ell\}) \end{aligned}$$

Let π' be π with its domain restricted to $\mathrm{dom}(\rho_1')$. Choose $\exists\, \pi$ to be π'. It suffices if:

- $@\rho \sqsupset \alpha$: Immediate by H1.

- $\rho \geq \bullet_{\ell \in \mathrm{dom}(\pi')} \pi'(\ell)$: Since $\pi' \subseteq \pi$, $\rho \geq \bullet_{\ell \in \mathrm{dom}(\pi)} \pi(\ell) \geq \bullet_{\ell \in \mathrm{dom}(\pi')} \pi'(\ell)$.

- $\forall\, \ell \in \mathrm{dom}(\pi'), v, \rho''.\ F(\ell, v, \rho, \rho_1', \rho'', \pi')$: Let $\ell \in \mathrm{dom}(\pi'), v, \rho''$ be arbitrary. Because $\ell \in \mathrm{dom}(\pi')$ implies $\ell \in \mathrm{dom}(\pi)$, we can instantiate H3 with ℓ, v, ρ'' to obtain $F(\ell, v, \rho, \rho', \rho'', \pi)$. By inspection of F, we observe that all usages of π are of the form $\pi(\ell)$. Since $\pi(\ell) = \pi'(\ell)$, we obtain $F(\ell, v, \rho, \rho_1', \rho'', \pi')$.

□

Lemma 6.128 ($\circlearrowleft\exists$)**.** $\exists\, x.\ \circlearrowleft_\alpha P(x) \dashv\vDash \circlearrowleft_\alpha \exists\, x.\ P(x)$

Proof. **Case $\vDash$.** Let ρ be arbitrary such that $\hat{P}(x)(\rho')$ for some x and $\rho' \in \mathsf{reb}_\alpha(\rho)$. Choose $\exists\, x$ to be x and $\exists\, \rho' \in \mathsf{reb}_\alpha(\rho)$ to be ρ'. $\hat{P}(x)(\rho')$ is immediate.

Case $\dashv$. Let ρ be arbitrary such that $\hat{P}(x)(\rho')$ for some $\rho' \in \mathsf{reb}_\alpha(\rho)$ and x. Choose $\exists\, \rho' \in \mathsf{reb}_\alpha(\rho)$ to be ρ' and $\exists\, x$ to be x. $\hat{P}(x)(\rho')$ is immediate. □

Lemma 6.129 ($\circlearrowleft\forall$)**.** $\forall\, x.\ \circlearrowleft_\alpha P(x) \dashv\vDash \circlearrowleft_\alpha \forall\, x.\ P(x)$

Proof. Let ρ be arbitrary such that $\forall\, x.\ \hat{P}(x)(\rho')$ for some $\rho' \in \mathsf{reb}_\alpha(\rho)$. Let x be arbitrary and choose $\exists\, \rho' \in \mathsf{reb}_\alpha(\rho)$ to be ρ'. Instantiate $\forall\, x.\ \hat{P}(x)(\rho')$ with x to obtain $\hat{P}(x)(\rho')$. □

Lemma 6.130. $P \vDash \circlearrowleft_\alpha \mathsf{emp}$

Proof. Suppose $\rho \in P$. Then $\varnothing$ vacuously satisfies the conditions needed to be a reborrowed version of ρ, so $\rho \in \circlearrowleft_\alpha \mathsf{emp}$. □

Lemma 6.131 ($\circlearrowleft\mathcal{V}_1$)**.** $[\delta('a)]\,\mathcal{V}[\![T]\!]_\delta(v) \vDash \circlearrowleft_{\delta('a)} \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T]\!]_\delta(v)$ for all $T \neq \mathsf{Unk}$.

Proof. By induction on T. Let $\delta('a) = \alpha$.

- Case $T = 1$:
  Goal is $[\alpha]\,\mathcal{V}[\![1]\!]_\delta(v) \vDash \circlearrowleft_\alpha \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ 1]\!]_\delta(v)$.
  Unfold: $[\alpha]\ \ulcorner v = ()\urcorner \vDash \circlearrowleft_\alpha \ulcorner v = ()\urcorner$
  Apply $[\,]$-L and $\circlearrowleft$-$\ulcorner\urcorner$.

- Case $T = T_1 \otimes T_2$:
  Goal is $[\alpha]\,\mathcal{V}[\![T_1 \otimes T_2]\!]_\delta(v) \vDash \circlearrowleft_\alpha \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T_1 \otimes \underline{\mathsf{Imm}}\ 'a\ T_2]\!]_\delta(v)$.
  Unfold.
  $[\alpha]\,\exists\, v_1, v_2.\ \ulcorner v = (v_1, v_2)\urcorner \star \mathcal{V}[\![T_1]\!]_\delta(v_1) \star \mathcal{V}[\![T_2]\!]_\delta(v_2)$
  $\vDash \circlearrowleft_\alpha \exists\, v_1, v_2.\ \ulcorner v = (v_1, v_2)\urcorner \star \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T_1]\!]_\delta(v_1) \star \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T_2]\!]_\delta(v_2)$.
  Apply $[\,]\exists$, $\exists$L, $[\,]\star$, $[\,]$L.
  $\ulcorner v = (v_1, v_2)\urcorner \star [\alpha]\,\mathcal{V}[\![T_1]\!]_\delta(v_1) \star [\alpha]\,\mathcal{V}[\![T_2]\!]_\delta(v_2)$
  $\vDash \circlearrowleft_\alpha \exists\, v_1, v_2.\ \ulcorner v = (v_1, v_2)\urcorner \star \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T_1]\!]_\delta(v_1) \star \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T_2]\!]_\delta(v_2)$.
  Apply $\circlearrowleft\exists$, $\exists$R, $\circlearrowleft\star$, $\circlearrowleft\ulcorner\urcorner$.
  $\ulcorner v = (v_1, v_2)\urcorner \star [\alpha]\,\mathcal{V}[\![T_1]\!]_\delta(v_1) \star [\alpha]\,\mathcal{V}[\![T_2]\!]_\delta(v_2)$
  $\vDash \ulcorner v = (v_1, v_2)\urcorner \star \circlearrowleft_\alpha \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T_1]\!]_\delta(v_1) \star \circlearrowleft_\alpha \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T_2]\!]_\delta(v_2)$.
  Apply IH.

- Case $T = T_1 \oplus T_2$: Analogous to $T = T_1 \otimes T_2$ case, using $\circlearrowleft\vee$ in place of $\circlearrowleft\star$.

- Case $T = T_1 \multimap T_2$:
  Goal is $[\alpha]\,\mathcal{V}[\![T_1 \multimap T_2]\!]_\delta(v) \vDash \circlearrowleft_\alpha \mathcal{V}[\![\mathsf{Unk}]\!]_\delta(v)$.
  Unfold: $[\alpha]\,\mathcal{V}[\![T_1 \multimap T_2]\!]_\delta(v) \vDash \circlearrowleft_\alpha \mathsf{emp}$.
  Apply theorem 6.130.

- Case $T = \forall\, 'a \sqsubset @b.T'$: analogous to case $T = T_1 \multimap T_2$.

- Case $T = [@a]\,T$:
  Goal is $[\alpha]\,\mathcal{V}[\![[@a]\,T]\!]_\delta(v) \vDash \circlearrowleft_\alpha \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T]\!]_\delta(v)$.
  Unfold: $[\alpha]\,[@a\delta]\,\mathcal{V}[\![T]\!]_\delta(v) \vDash \circlearrowleft_\alpha \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T]\!]_\delta(v)$.
  Apply $[\,]$L: $[\alpha]\,\mathcal{V}[\![T]\!]_\delta(v) \vDash \circlearrowleft_\alpha \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T]\!]_\delta(v)$.
  Apply IH.

- Case $T = \mathsf{Ref}\ T'$:
  Goal is $[\alpha]\,\mathcal{V}[\![\mathsf{Ref}\ T']\!]_\delta(v) \vDash \circlearrowleft_\alpha \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T']\!]_\delta(v)$.
  Unfold: $[\alpha]\,\exists\, \ell, v'.\ \ulcorner v = \ell\urcorner \star l \mapsto v' \star \mathcal{V}[\![T']\!]_\delta(v') \vDash \circlearrowleft_\alpha \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T']\!]_\delta(v)$.
  Apply $[\,]\exists$, $\exists$L, $[\,]\star$, $[\,]L$ to get $\ulcorner v = \ell\urcorner \star l \mapsto v' \star [\alpha]\,\mathcal{V}[\![T']\!]_\delta(v') \vDash \circlearrowleft_\alpha \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T']\!]_\delta(v)$.
  Apply IH: $\ulcorner v = \ell\urcorner \star l \mapsto v' \star \circlearrowleft_\alpha \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T']\!]_\delta(v') \vDash \circlearrowleft_\alpha \mathcal{V}[\![\underline{\mathsf{Imm}}\ 'a\ T']\!]_\delta(v)$.

Apply theorem 6.130: $\circlearrowleft_\alpha \mathsf{emp} \star \circlearrowleft_\alpha \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'a\ T' \rrbracket_\delta(v') \vDash \circlearrowleft_\alpha \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'a\ T' \rrbracket_\delta(v)$.
Apply $\circlearrowleft\star$: $\circlearrowleft_\alpha(\mathsf{emp} \star \circlearrowleft_\alpha \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'a\ T' \rrbracket_\delta(v')) \vDash \circlearrowleft_\alpha \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'a\ T' \rrbracket_\delta(v)$.
Done because emp is a unit for $\star$.

- Case $T = \mathsf{Imm}\ @b\ T'$:
  Goal is $[\alpha]\,\mathcal{V}\llbracket \mathsf{Imm}\ @b\ T' \rrbracket_\delta(v) \vDash \circlearrowleft_\alpha \mathcal{V}\llbracket \mathsf{Imm}\ @b\ T' \rrbracket_\delta(v)$.
  Unfold: $[\alpha]\,\exists\,\ell.\ \ulcorner v = \ell \urcorner \star \ell \mapsto\mathrm{I}_{@b\delta}\ \mathcal{V}\llbracket T' \rrbracket_\delta \vDash \circlearrowleft_\alpha \mathcal{V}\llbracket \mathsf{Imm}\ @b\ T' \rrbracket_\delta(v)$.
  Apply $[\,]\exists$, $[\,]\star$, $[\,]\mathrm{L}$: $\exists\,\ell.\ \ulcorner v = \ell \urcorner \star [\alpha]\,(\ell \mapsto\mathrm{I}_{@b\delta}\ \mathcal{V}\llbracket T' \rrbracket_\delta) \vDash \circlearrowleft_\alpha \mathcal{V}\llbracket \mathsf{Imm}\ @b\ T' \rrbracket_\delta(v)$.
  Apply $\circlearrowleft\mathrm{I}$: $\exists\,\ell.\ \ulcorner v = \ell \urcorner \star \circlearrowleft_\alpha(\ell \mapsto\mathrm{I}_{@b\delta}\ \mathcal{V}\llbracket T' \rrbracket_\delta) \vDash \circlearrowleft_\alpha \mathcal{V}\llbracket \mathsf{Imm}\ @b\ T' \rrbracket_\delta(v)$.
  Apply $\circlearrowleft\ulcorner\urcorner$, $\circlearrowleft\star$, $\circlearrowleft\exists$: $\circlearrowleft_\alpha \exists\,\ell.\ \ulcorner v = \ell \urcorner \star (\ell \mapsto\mathrm{I}_{@b\delta}\ \mathcal{V}\llbracket T' \rrbracket_\delta) \vDash \circlearrowleft_\alpha \mathcal{V}\llbracket \mathsf{Imm}\ @b\ T' \rrbracket_\delta(v)$.
  Fold the definition of $\mathcal{V}\llbracket \mathsf{Imm}\ @b\ T' \rrbracket$.

- Case $T = \mathsf{Mut}\ @b\ T$:
  Goal is $[\alpha]\,\mathcal{V}\llbracket \mathsf{Mut}\ @b\ T' \rrbracket_\delta(v) \vDash \circlearrowleft_\alpha \mathcal{V}\llbracket \mathsf{Imm}\ \alpha\ T' \rrbracket_\delta(v)$.
  Unfold: $[\alpha]\,\exists\,\ell.\ \ulcorner v = \ell \urcorner \star \ell \mapsto\mathrm{M}_{@b\delta}\ \mathcal{V}\llbracket T' \rrbracket_\delta \vDash \circlearrowleft_\alpha \mathcal{V}\llbracket \mathsf{Imm}\ \alpha\ T' \rrbracket_\delta(v)$.
  Apply $[\,]\exists$, $[\,]\star$, $[\,]\mathrm{L}$: $\exists\,\ell.\ \ulcorner v = \ell \urcorner \star [\alpha]\,(\ell \mapsto\mathrm{M}_{@b\delta}\ \mathcal{V}\llbracket T' \rrbracket_\delta) \vDash \circlearrowleft_\alpha \mathcal{V}\llbracket \mathsf{Imm}\ \alpha\ T' \rrbracket_\delta(v)$.
  Apply $\circlearrowleft\mathrm{M}$: $\exists\,\ell.\ \ulcorner v = \ell \urcorner \star \circlearrowleft_\alpha(\ell \mapsto\mathrm{I}_\alpha\ \mathcal{V}\llbracket T' \rrbracket_\delta) \vDash \circlearrowleft_\alpha \mathcal{V}\llbracket \mathsf{Imm}\ \alpha\ T' \rrbracket_\delta(v)$.
  Apply $\circlearrowleft\ulcorner\urcorner$, $\circlearrowleft\star$, $\circlearrowleft\exists$: $\circlearrowleft_\alpha \exists\,\ell.\ \ulcorner v = \ell \urcorner \star (\ell \mapsto\mathrm{I}_\alpha\ \mathcal{V}\llbracket T' \rrbracket_\delta) \vDash \circlearrowleft_\alpha \mathcal{V}\llbracket \mathsf{Imm}\ \alpha\ T' \rrbracket_\delta(v)$.
  Fold the definition of $\mathcal{V}\llbracket \mathsf{Imm}\ \alpha\ T' \rrbracket$.

- Case $T = \mathsf{Unk}$: impossible.

□

Lemma 6.132 ($\circlearrowleft\mathcal{V}_2$)**.** If $'a$ not free in T then $\mathcal{V}\llbracket T \rrbracket_\delta(v) \vDash \text{И}\alpha.\ \circlearrowleft_\alpha \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'a\ T \rrbracket_{\delta['a\mapsto\alpha]}(v)$

Proof.

Proof step	Current goal
Apply ИR, ИMONO and fix $\alpha \sqsubset \bigsqcap\delta$ arbitrary.	$[\alpha]\,\mathcal{V}\llbracket T \rrbracket_\delta(v) \vDash [\alpha]\ \circlearrowleft_\alpha \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'a\ T \rrbracket_{\delta['a\mapsto\alpha]}(v)$
Apply $[\,]\,\mathrm{R}$.	$[\alpha]\,\mathcal{V}\llbracket T \rrbracket_\delta(v) \vDash \circlearrowleft_\alpha \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'a\ T \rrbracket_{\delta['a\mapsto\alpha]}(v)$
Have $\mathcal{V}\llbracket T \rrbracket_\delta = \mathcal{V}\llbracket T \rrbracket_{\delta['a\mapsto\alpha]}$ because $'a$ not free in T.	$[\alpha]\,\mathcal{V}\llbracket T \rrbracket_{\delta['a\mapsto\alpha]}(v) \vDash \circlearrowleft_\alpha \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'a\ T \rrbracket_{\delta['a\mapsto\alpha]}(v)$
Apply $\circlearrowleft\mathcal{V}_1$.	□

Lemma 6.133 ($\circlearrowleft\mathcal{V}_3$)**.** If $'b$ not free in T then $\ell \mapsto\mathrm{I}_\alpha\ \mathcal{V}\llbracket T \rrbracket_\delta \vDash \ell \mapsto\mathrm{I}_\alpha\ \text{И}\beta.\ \circlearrowleft_\beta \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'b\ T \rrbracket_{\delta['b\mapsto\beta]}$

Proof. Apply $\circlearrowleft\mathcal{V}_2$ and I-MONO. □

Lemma 6.134. $\ulcorner x = y \urcorner \star \text{И}\alpha.\ \circlearrowleft_\alpha \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'a\ T \rrbracket_{\delta['a\mapsto\alpha]} \vDash \text{И}\alpha.\ \circlearrowleft_\alpha(\ulcorner x = y \urcorner \star \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'a\ T \rrbracket_{\delta['a\mapsto\alpha]})$

Proof. By unfolding and substituting for $x = y$. □

6.7 Weakest Precondition Rules

Lemma 6.135 (WP-BIND)**.** $\mathsf{wp}\,(e)\,\{v.\mathsf{wp}\,(K[v])\,\{\hat{Q}\}\} \vDash \mathsf{wp}\,(K[e])\,\{\hat{Q}\}$

Proof. Let ρ be arbitrary such that $\mathsf{wp}\,(e)\,\{v.\ \mathsf{wp}\,(K[v])\,\{\hat{Q}\}\}\,(\rho)^{(\mathrm{H1})}$. We must show $\mathsf{wp}\,(K[e])\,\{\hat{Q}\}\,(\rho)^{(\mathrm{G1})}$. Unfold wp in G1 and let $\rho_f \mathbin{\#} \rho$ be arbitrary. Instantiate H1 with ρ_f and we have $(\llbracket \rho_f \bullet \rho \rrbracket, e) \longrightarrow^* (\llbracket \rho_f \bullet \rho' \bullet \rho^+ \rrbracket, v)^{(\mathrm{H2})}$, $\rho \leftrightsquigarrow \rho' \bullet \rho^{+(\mathrm{H3})}$, $\rho^+ \mid \mathsf{own} = \varnothing^{(\mathrm{H4})}$, and $\mathsf{wp}\,(K[v])\,\{\hat{Q}\}\,(\rho)^{(\mathrm{H5})}$ for some $\rho' \mathbin{\#} \rho_f^{(\mathrm{H6})}$, $\rho^+ \mathbin{\#} \rho_f \bullet \rho'^{(\mathrm{H7})}$, v.

Instantiate H5 with $\rho_f \bullet \rho^+$. Note that we have $\rho_f \bullet \rho^+ \mathbin{\#} \rho'$ by H7 and theorem 6.46. Then we have $(\llbracket \rho_f \bullet \rho^+ \bullet \rho' \rrbracket, K[v]) \longrightarrow^* (\llbracket \rho_f \bullet \rho^+ \bullet \rho^+ + \bullet \rho'' \rrbracket, v')^{(\mathrm{H8})}$, $\rho' \leftrightsquigarrow \rho'' \bullet \rho^{++(\mathrm{H9})}$, $\rho^{++} \mid \mathsf{own} = \varnothing^{(\mathrm{H10})}$, and $\hat{Q}(v')(\rho'')^{(\mathrm{H11})}$ for some $\rho'' \mathbin{\#} \rho_f \bullet \rho^{+(\mathrm{H12})}$, $\rho^{++} \mathbin{\#} \rho_f \bullet \rho^+ \bullet \rho''^{(\mathrm{H13})}$, v'.

In G1, choose $\exists\,\rho', \rho^+, v$ to be $\rho'', \rho^+ \bullet \rho^{++}, v'$. It suffices if:

- $\rho'' \mathbin{\#} \rho_f$: By H12 and theorem 6.11.

- $\rho^+ \bullet \rho^{++} \mathbin{\#} \rho_f \bullet \rho''$: By H13 and theorem 6.46.

- $([\![\rho_f \bullet \rho]\!], K[e]) \longrightarrow^* ([\![\rho_f \bullet \rho^+ \bullet \rho'' \bullet \rho^{++}]\!], v')$: By transitivity with H2 and H8.
- $\rho \leftrightsquigarrow \rho'' \bullet \rho^+ \bullet \rho^{++}$: By H3, H9, H13, theorem 6.48, and theorem 6.49.
- $\rho^+ \bullet \rho^{++} \mid \mathsf{own} = \varnothing$: By H4 and H10.
- $\hat{Q}(v')(\rho'')$: By H11.

□

Lemma 6.136 (WP-VAL)**.** $\hat{Q}(v) \dashv\models \mathsf{wp}\,(v)\,\{\hat{Q}\}$

Proof. Let ρ be arbitrary such that $\hat{Q}(v)(\rho)^{(\mathrm{H1})}$. Let $\rho_f \# \rho^{(\mathrm{H2})}$ be arbitrary. Choose $\exists\, \rho', \rho^+, v$ to be $\rho, \varnothing, v$. It suffices if:

- $\rho \# \rho_f$: By H2.
- $\varnothing \# \rho_f \bullet \rho'$: By definition.
- $([\![\rho_f \bullet \rho]\!], v) \longrightarrow^* ([\![\rho_f \bullet \rho \bullet \varnothing]\!], v)$: By theorem 6.4 and reflexivity.
- $\rho \leftrightsquigarrow \rho \bullet \varnothing$: By theorem 6.4 and theorem 6.47.
- $\varnothing \mid \mathsf{own} = \varnothing$: By definition.
- $\hat{Q}(v)(\rho)$: By H1.

□

Lemma 6.137 (WP$\mathbb{1}$)**.** $\mathsf{wp}\,(e)\,\{\hat{Q}\} \models \mathsf{wp}\,((); e)\,\{\hat{Q}\}$

Proof. Let ρ be arbitrary such that $\mathsf{wp}\,(e)\,\{\hat{Q}\}\,(\rho)^{(\mathrm{H1})}$. Let $\rho_f \# \rho^{(\mathrm{H2})}$ be arbitrary. Instantiate H1 with ρ_f and we have $([\![\rho_f \bullet \rho]\!], e) \longrightarrow^* ([\![\rho_f \bullet \rho' \bullet \rho^+]\!], v)^{(\mathrm{H3})}$, $\rho \leftrightsquigarrow \rho' \bullet \rho^{+(\mathrm{H4})}$, $\rho^+ \mid \mathsf{own} = \varnothing^{(\mathrm{H5})}$, and $\hat{Q}(v)(\rho')^{(\mathrm{H6})}$ for some $\rho' \# \rho_f{}^{(\mathrm{H7})}$, $\rho^+ \# \rho_f \bullet \rho'^{(\mathrm{H8})}$, v.

Choose $\exists\, \rho', \rho^+, v$ to be ρ', ρ^+, v. Most of the resulting obligations are immediate, but we must show that $([\![\rho_f \bullet \rho]\!], (); e) \longrightarrow^* ([\![\rho_f \bullet \rho' \bullet \rho_f]\!], v)$. By the operational semantics, $([\![\rho_f \bullet \rho]\!], (); e) \longrightarrow ([\![\rho_f \bullet \rho]\!], e)$. Then by H3. □

Lemma 6.138 (WP$\otimes$)**.** $\mathsf{wp}\,(e[v_1/x_1, v_2/x_2])\,\{\hat{Q}\} \models \mathsf{wp}\,(\mathsf{let}\,(x_1, x_2) = (v_1, v_2); e)\,\{\hat{Q}\}$

Proof. Let ρ be arbitrary such that $\mathsf{wp}\,(e[v_1/x_1, v_2/x_2])\,\{\hat{Q}\}\,(\rho)^{(\mathrm{H1})}$. Let $\rho_f \bullet \rho^{(\mathrm{H2})}$ be arbitrary. Instantiate H1 with ρ_f and we have $([\![\rho_f \bullet \rho]\!], e[v_1/x_1, v_2/x_2]) \longrightarrow^* ([\![\rho_f \bullet \rho' \bullet \rho^+]\!], v)^{(\mathrm{H3})}$, $\rho \leftrightsquigarrow \rho' \bullet \rho^{+(\mathrm{H4})}$, $\rho^+ \mid \mathsf{own} = \varnothing^{(\mathrm{H5})}$, and $\hat{Q}(v)(\rho')^{(\mathrm{H6})}$ for some $\rho' \# \rho_f{}^{(\mathrm{H7})}$, $\rho^+ \# \rho_f \bullet \rho'^{(\mathrm{H8})}$, v.

Choose $\exists\, \rho', \rho^+, v$ to be ρ', ρ^+, v. Most of the resulting obligations are immediate, but we must show that $([\![\rho_f \bullet \rho]\!], \mathsf{let}\,(x_1, x_2) = (v_1, v_2); e) \longrightarrow^* ([\![\rho_f \bullet \rho' \bullet \rho^+]\!], v)$. By the operational semantics, $([\![\rho_f \bullet \rho]\!], \mathsf{let}\,(x_1, x_2) = (v_1, v_2); e) \longrightarrow ([\![\rho_f \bullet \rho]\!], e[v_1/x_1, v_2/x_2])$. Then by H3. □

Lemma 6.139 (WP$\oplus$)**.** $\mathsf{wp}\,(e_i[v/x_i])\,\{\hat{Q}\} \models \mathsf{wp}\,(\mathsf{match}\, i\, v\, \{1\, x_1 \Rightarrow e_1 \mid 2\, x_2 \Rightarrow e_2\})\,\{\hat{Q}\}$

Proof. Let ρ be arbitrary such that $\mathsf{wp}\,(e_i[v/x_i])\,\{\hat{Q}\}\,(\rho)^{(\mathrm{H1})}$. Let $\rho_f \# \rho^{(\mathrm{H2})}$ be arbitrary. Instantiate H1 with ρ_f and we have $([\![\rho_f \bullet \rho]\!], e_i[v/x_i]) \longrightarrow^* ([\![\rho_f \bullet \rho' \bullet \rho^+]\!], v)^{(\mathrm{H3})}$, $\rho \leftrightsquigarrow \rho' \bullet \rho^{+(\mathrm{H4})}$, $\rho^+ \mid \mathsf{own} = \varnothing^{(\mathrm{H5})}$, and $\hat{Q}(v)(\rho')^{(\mathrm{H6})}$ for some $\rho' \# \rho_f{}^{(\mathrm{H7})}$, $\rho^+ \# \rho_f \bullet \rho'^{(\mathrm{H8})}$, v.

Choose $\exists\, \rho', \rho^+, v$ to be ρ', ρ^+, v. Most of the resulting obligations are immediate, but we must show that $([\![\rho_f \bullet \rho]\!], \mathsf{match}\, iv\, \{1x_1 \Rightarrow e_1 \mid 2x_2 \Rightarrow e_2\}) \longrightarrow^* ([\![\rho_f \bullet \rho' \bullet \rho^+]\!], v)$. By the operational semantics, it follows that $([\![\rho_f \bullet \rho]\!], \mathsf{match}\, iv\, \{1x_1 \Rightarrow e_1 \mid 2x_2 \Rightarrow e_2\}) \longrightarrow ([\![\rho_f \bullet \rho]\!], e_i[v/x_i])$. Then by H3. □

Lemma 6.140 (WP$\multimap$)**.** $\mathsf{wp}\,(e[v/x])\,\{\hat{Q}\} \models \mathsf{wp}\,((\lambda x.e)\ v)\,\{\hat{Q}\}$

Proof. Let ρ be arbitrary such that $\mathsf{wp}\,(e[v/x])\,\{\hat{Q}\}\,(\rho)^{(\text{H1})}$. Let $\rho_f \# \rho^{(\text{H2})}$ be arbitrary. Instantiate H1 with ρ_f and we have $(\llbracket \rho_f \bullet \rho \rrbracket, e[v/x]) \longrightarrow^* (\llbracket \rho_f \bullet \rho' \bullet \rho^+ \rrbracket, v)^{(\text{H3})}$, $\rho \leftrightsquigarrow \rho' \bullet \rho^{+(\text{H4})}$, $\rho^+ \mid \mathsf{own} = \varnothing^{(\text{H5})}$, and $\hat{Q}(v)(\rho')^{(\text{H6})}$ for some $\rho' \# \rho_f{}^{(\text{H7})}$, $\rho^+ \# \rho_f \bullet \rho'^{(\text{H8})}$, and v.

Choose $\exists\, \rho', \rho^+, v$ to be ρ', ρ^+, v. Most of the resulting obligations are immediate, but we must show that $(\llbracket \rho_f \bullet \rho \rrbracket, (\lambda x.e)\ v) \longrightarrow^* (\llbracket \rho_f \bullet \rho' \bullet \rho^+ \rrbracket, v)$. By the operational semantics, $(\llbracket \rho_f \bullet \rho \rrbracket, (\lambda x.e)\ v) \longrightarrow (\llbracket \rho_f \bullet \rho \rrbracket, e[v/x])$. Then by H3. □

Lemma 6.141 (WP-ALLOC). $(\forall\, \ell.\ \ell \mapsto v \mathrel{-\!\!\star} \hat{Q}(\ell)) \vDash \mathsf{wp}\,(\mathsf{alloc}\ \ v)\,\{\hat{Q}\}$

Proof. Let ρ be arbitrary such that $(\forall\, \ell.\ \ell \mapsto v \mathrel{-\!\!\star} \hat{Q}(\ell))(\rho)^{(\text{H1})}$. Let $\rho_f \# \rho^{(\text{H2})}$. Choose an ℓ such that $\ell \notin \rho_f \bullet \rho^{(\text{H3})}$. Instantiate H1 with ℓ, $\ell \mapsto \mathsf{own}(v)$, $\rho \bullet \ell \mapsto \mathsf{own}(v)$ and we have $\hat{Q}(\ell)(\rho \bullet \ell \mapsto \mathsf{own}(v))^{(\text{H4})}$.

Choose $\exists\, \rho', \rho^+, v$ to be $\rho \bullet \ell \mapsto \mathsf{own}(v), \varnothing, \ell$. It suffices if:

- $\rho \bullet \ell \mapsto \mathsf{own}(v) \# \rho_f$: By H2 and H3.
- $\varnothing \# \rho_f \bullet \rho'$: By definition.
- $(\llbracket \rho_f \bullet \rho \rrbracket, \mathsf{alloc}\ v) \longrightarrow^* (\llbracket \rho_f \bullet \rho \bullet \ell \mapsto \mathsf{own}(v) \rrbracket, \ell)$: According to the operational semantics, $(\llbracket \rho_f \bullet \rho \rrbracket, \mathsf{alloc}\ v) \longrightarrow (\llbracket \rho_f \bullet \rho \rrbracket \uplus \ell \mapsto v, \ell)$. By definition, $\llbracket \rho_f \bullet \rho \rrbracket \uplus \ell \mapsto v = \llbracket \rho_f \bullet \rho \rrbracket \uplus \llbracket \ell \mapsto \mathsf{own}(v) \rrbracket = \llbracket \rho_f \bullet \rho \bullet \ell \mapsto \mathsf{own}(v) \rrbracket$.
- $\rho \leftrightsquigarrow \rho \bullet \ell \mapsto \mathsf{own}(v)$: By definition, since $\leftrightsquigarrow$ ignores own cells.
- $\varnothing \mid \mathsf{own} = \varnothing$: By definition.
- $\hat{Q}(\ell)(\rho \bullet \ell \mapsto \mathsf{own}(v))$: By H4.

□

Lemma 6.142 (WP-FREE). $\ell \mapsto v \star \hat{Q}(v) \vDash \mathsf{wp}\,(\mathsf{free}\ \ \ell)\,\{\hat{Q}\}$

Proof. Let ρ be arbitrary such that $\rho = \rho_1 \bullet \rho_2$, $\rho_1 = \ell \mapsto \mathsf{own}(v)$, and $\hat{Q}(v)(\rho_2)^{(\text{H1})}$ for some ρ_1, ρ_2. Let $\rho_f \# \rho^{(\text{H2})}$ be arbitrary. Choose $\exists\, \rho', \rho^+, v$ to be $\rho_2, \varnothing, v$. Most of the resulting proof obligations are immediate, but we must show that $(\llbracket \rho_f \bullet \ell \mapsto \mathsf{own}(v) \bullet \rho_2 \rrbracket, \mathsf{free}\ \ell) \longrightarrow^* (\llbracket \rho_f \bullet \rho_2 \rrbracket, v)$. By definition, $\llbracket \rho_f \bullet \ell \mapsto \mathsf{own}(v) \bullet \rho_2 \rrbracket = \llbracket \rho_f \bullet \rho_2 \rrbracket \uplus \ell \mapsto v$. Then by the operational semantics, $(\llbracket \rho_f \bullet \rho_2 \rrbracket \uplus \ell \mapsto v, \mathsf{free}\ \ell) \longrightarrow (\llbracket \rho_f \bullet \rho_2 \rrbracket, v)$. □

Lemma 6.143 (WP-LOAD). $\ell \mapsto v \star (\ell \mapsto v \mathrel{-\!\!\star} \hat{Q}(v)) \vDash \mathsf{wp}\,(\mathsf{load}\ \ell)\,\{\hat{Q}\}$

Proof. Let ρ be arbitrary such that $\rho = \rho_1 \bullet \rho_2$, $\rho_1 = \ell \mapsto \mathsf{own}(v)$, and $(\ell \mapsto v \mathrel{-\!\!\star} \hat{Q}(v))(\rho_2)^{(\text{H1})}$ for some ρ_1, ρ_2. Instantiate H1 with ρ_1, ρ and we have $\hat{Q}(v)(\rho)^{(\text{H2})}$.

Let $\rho_f \# \rho$ be arbitrary. Choose $\exists\, \rho', \rho^+, v$ to be $\rho, \varnothing, v$. Most of the resulting proof obligations are immediate, but we must show $(\llbracket \rho_f \bullet \rho \rrbracket, \mathsf{load}\ \ell) \longrightarrow^* (\llbracket \rho_f \bullet \rho \rrbracket, v)$. By definition, $\llbracket \rho_f \bullet \rho \rrbracket = \llbracket \rho_f \bullet \rho_1 \bullet \ell \mapsto \mathsf{own}(v) \rrbracket = \llbracket \rho_f \bullet \rho_1 \rrbracket \uplus \ell \mapsto v$. By the operational semantics, $(\llbracket \rho_f \bullet \rho_1 \rrbracket \uplus \ell \mapsto v, \mathsf{load}\ \ell) \longrightarrow (\llbracket \rho_f \bullet \rho_1 \rrbracket \uplus \ell \mapsto v, v)$. □

Lemma 6.144 (WP-LOAD-I). $\ell \mapsto\!\mathrm{I}_\alpha\ \hat{P} \star (\forall\, v.\ \ell \mapsto\!\mathrm{I}_\alpha\ (v'.\ulcorner v = v' \urcorner \star \hat{P}(v)) \mathrel{-\!\!\star} \hat{Q}(v)) \vDash \mathsf{wp}\,(\mathsf{load}\ \ell)\,\{\hat{Q}\}$

Proof. Let $R = \forall\, v.\ \ell \mapsto\!\mathrm{I}_\alpha\ (v'.\ \ulcorner v = v' \urcorner \star \hat{P}(v)) \mathrel{-\!\!\star} \hat{Q}(v)$. Suppose $\rho \in \ell \mapsto\!\mathrm{I}_\alpha\ \hat{P} \star R$, so $\rho = \ell \mapsto \mathsf{imm}(\beta, v, \rho_v) \bullet \rho_R$ for some β, v, ρ_v such that $\rho_v \in \hat{P}(v)$ and $\alpha \sqsubseteq \bigsqcup \beta$ and $\rho_R \in R$. Since $\ulcorner v = v' \urcorner \star \hat{P}(v)$ is equivalent to $\hat{P}(v)$ for v arbitrary, and $\alpha \sqsubseteq \bigsqcup \beta$, we have that $\ell \mapsto \mathsf{imm}(\beta, v, \rho_v) \in \ell \mapsto\!\mathrm{I}_\alpha\ (v'.\ulcorner v = v' \urcorner \star \hat{P}(v))$. Hence, because $\rho_R \in R$ and ρ_R is composable with $\ell \mapsto \mathsf{imm}(\beta, v, \rho_v)$ by assumption, it holds that $\ell \mapsto \mathsf{imm}(\beta, v, \rho_v) \bullet \rho_R = \rho \in \hat{Q}(v)$.

This establishes $\rho \vDash \mathsf{wp}\,(\mathsf{load}\ \ell)\,\{\hat{Q}(v)\}$: for any $\rho_f \# \rho$, choosing $\rho' := \rho$ and $\rho^+ := \varnothing$ and $v := v$ gives $(\llbracket \rho_f \bullet \rho \rrbracket, \mathsf{load}\ \ell) \longrightarrow^* (\llbracket \rho_f \bullet \rho' \rrbracket, v)$ and $\llbracket \rho_f \bullet \rho \rrbracket = \llbracket \rho_f \bullet \rho' \rrbracket$ and $\rho \leftrightsquigarrow \rho' \bullet \rho^+$ and $\rho^+|_{\text{own}} = \varnothing$ and $\rho' \in \hat{Q}(v)$ as needed. □

Lemma 6.145 (WP-STORE). $\ell \mapsto v_1 \star (\ell \mapsto v_2 \mathrel{-\!\!\star} \hat{Q}(())) \vDash \mathsf{wp}\,(\mathsf{store}\ \ell\ v_2)\,\{\hat{Q}\}$

Proof. Let ρ be arbitrary such that $\rho = \rho_1 \bullet \rho_2$, $\rho_1 = \ell \mapsto \mathsf{own}(-)$, and $(\ell \mapsto v \mathrel{-\!\!\star} \hat{Q}(()))(\rho_2)^{(\mathrm{H1})}$ for some ρ_1, ρ_2. Instantiate H1 with $\ell \mapsto \mathsf{own}(v)$, $\rho_2 \bullet \ell \mapsto \mathsf{own}(v)$ and we have $\hat{Q}(())(\rho_2 \bullet \ell \mapsto \mathsf{own}(v))^{(\mathrm{H2})}$.

Let $\rho_f \mathbin{\#} \rho^{(\mathrm{H3})}$ be arbitrary. Choose $\exists\, \rho', \rho^+, v$ to be $\rho_2 \bullet \ell \mapsto \mathsf{own}(v), \varnothing, ()$. It suffices if:

- $\rho_2 \bullet \ell \mapsto \mathsf{own}(v) \mathbin{\#} \rho_f$: By H3 and theorem 6.40.
- $\varnothing \mathbin{\#} \rho_2 \bullet \rho_2 \bullet \ell \mapsto \mathsf{own}(v)$: By definition.
- $(\llbracket \rho_f \bullet \ell \mapsto \mathsf{own}(-) \bullet \rho_2 \rrbracket, \mathsf{store}\ \ell\ v) \longrightarrow^* (\llbracket \rho_f \bullet \rho_2 \bullet \ell \mapsto \mathsf{own}(v) \rrbracket, ())$: By definition, $\ell \in \llbracket \rho_f \bullet \ell \mapsto \mathsf{own}(-) \bullet \rho_2 \rrbracket$. Thus, by the operational semantics, $(\llbracket \rho_f \bullet \ell \mapsto \mathsf{own}(-) \bullet \rho_2 \rrbracket, \mathsf{store}\ \ell\ v) \longrightarrow (\llbracket \rho_f \bullet \ell \mapsto \mathsf{own}(-) \bullet \rho_2 \rrbracket[\ell \mapsto v], ())$. By definition, $\llbracket \rho_f \bullet \ell \mapsto \mathsf{own}(-) \bullet \rho_2 \rrbracket[\ell \mapsto v] = \llbracket \rho_f \bullet \ell \mapsto \mathsf{own}(v) \bullet \rho_2 \rrbracket$.
- $\ell \mapsto \mathsf{own}(-) \bullet \rho_2 \leftrightsquigarrow \rho_2 \bullet \ell \mapsto \mathsf{own}(v)$: By definition and theorem 6.47, since $\leftrightsquigarrow$ ignores own.
- $\varnothing \mid \mathsf{own} = \varnothing$: By definition.
- $\hat{Q}(())(\rho_2 \bullet \ell \mapsto \mathsf{own}(v))$: By H2.

□

Lemma 6.146 (wp-ramify). $\mathsf{wp}\,(e)\,\{\hat{P}\} \star (\hat{P} \mathrel{-\!\!\star} \hat{Q}) \vDash \mathsf{wp}\,(e)\,\{\hat{Q}\}$

Proof. Let ρ be arbitrary such that $\rho = \rho_1 \bullet \rho_2$, $\hat{P}^{(\mathrm{H1})}(\rho_1)$, and $(\forall\,(\hat{P} \mathrel{-\!\!\star} \hat{Q}))(\rho_2)^{(\mathrm{H2})}$ for some ρ_1, ρ_2. Let $\rho_f \mathbin{\#} \rho^{(\mathrm{H3})}$ be arbitrary.

Instantiate H1 with $\rho_f \bullet \rho_2$. Note that $\rho_f \bullet \rho_2 \mathbin{\#} \rho$ by H3 and theorem 6.46. As a result, we obtain that $(\llbracket \rho_f \bullet \rho_2 \bullet \rho_1 \rrbracket, e) \longrightarrow^* (\llbracket \rho_f \bullet \rho_2 \bullet \rho' \bullet \rho^+ \rrbracket, v)^{(\mathrm{H4})}$, $\rho_1 \leftrightsquigarrow \rho' \bullet \rho^{+(\mathrm{H5})}$, $\rho^+ \mid \mathsf{own} = \varnothing^{(\mathrm{H6})}$, and $\hat{P}(v)(\rho')^{(\mathrm{H7})}$ for some $\rho' \mathbin{\#} \rho_f \bullet \rho_2{}^{(\mathrm{H8})}$, $\rho^+ \mathbin{\#} \rho_f \bullet \rho_2 \bullet \rho'^{(\mathrm{H9})}$, and v.

Instantiate H2 with v, ρ', $\rho_2 \bullet \rho'$ and we obtain $\hat{Q}(v)(\rho_2 \bullet \rho')^{(\mathrm{H10})}$.

Choose $\exists\, \rho', \rho^+, v$ to be $\rho_2 \bullet \rho', \rho^+, v$. Most proof obligations are immediate and others follow from theorem 6.46 or theorem 6.48. □

Lemma 6.147 (wp[ ]). $[\alpha]\,\mathsf{wp}\,(e)\,\{\hat{Q}\} \vDash \mathsf{wp}\,(e)\,\{[\alpha]\,\hat{Q}\}$

Proof. Let ρ be arbitrary such that $\mathsf{wp}\,(e)\,\{\hat{Q}\}\,(\rho)^{(\mathrm{H1})}$ and $@\rho \sqsupset \alpha^{(\mathrm{H2})}$. Let $\rho_f \mathbin{\#} \rho^{(\mathrm{H3})}$ be arbitrary.

Instantiate H1 with ρ_f and we obtain $(\llbracket \rho_f \bullet \rho \rrbracket, e) \longrightarrow^* (\llbracket \rho_f \bullet \rho' \bullet \rho^+ \rrbracket, v)^{(\mathrm{H4})}$, $\rho \leftrightsquigarrow \rho' \bullet \rho^{+(\mathrm{H5})}$, $\rho^+ \mid \mathsf{own} = \varnothing^{(\mathrm{H6})}$, and $\hat{Q}(v)(\rho')^{(\mathrm{H7})}$ for some $\rho' \mathbin{\#} \rho_f{}^{(\mathrm{H8})}$, $\rho^+ \mathbin{\#} \rho_f \bullet \rho'^{(\mathrm{H9})}$, and v.

Choose $\exists\, \rho', \rho^+, v$ to be ρ', ρ^+, v. All proof obligations are immediate except $@\rho' \sqsupset \alpha$. From theorem 6.50 with H2 and H5, we obtain $@(\rho' \bullet \rho^+) \sqsupset \alpha$. From theorem 6.45, we obtain $@\rho' \sqsupset \alpha$. □

Lemma 6.148 (wp-M-forget). $\ell \mapsto\!\mathrm{M}_\alpha\, \hat{P} \star \mathsf{wp}\,(e)\,\{\hat{Q}\} \vDash \mathsf{wp}\,(e)\,\{\hat{Q}\}$

Proof. Let ρ be arbitrary such that $\rho = \rho_1 \bullet \rho_2$, $\rho_1 = \ell \mapsto \mathsf{mut}(\beta, v, \rho', \hat{P})$, and $\mathsf{wp}\,(e)\,\{\hat{Q}\}\,(\rho_2)^{(\mathrm{H1})}$ for some ρ_1, ρ_2, β, v, and ρ'. Let $\rho_f \mathbin{\#} \rho^{(\mathrm{H2})}$ be arbitrary.

Instantiate H1 with $\rho_f \bullet \rho_1$. Note that $\rho_f \bullet \rho_1 \mathbin{\#} \rho_2$ by H2 and theorem 6.46. From this, we obtain that $(\llbracket \rho_f \bullet \rho_1 \bullet \rho_2 \rrbracket, e) \longrightarrow^* (\llbracket \rho_f \bullet \rho_1 \bullet \rho' \bullet \rho^+ \rrbracket, v)^{(\mathrm{H3})}$, $\rho_2 \leftrightsquigarrow \rho' \bullet \rho^{+(\mathrm{H4})}$, $\rho^+ \mid \mathsf{own} = \varnothing^{(\mathrm{H5})}$, and $\hat{Q}(v)(\rho')^{(\mathrm{H6})}$ for some $\rho' \mathbin{\#} \rho_f \bullet \rho_1{}^{(\mathrm{H7})}$, $\rho^+ \mathbin{\#} \rho_f \bullet \rho_1 \bullet \rho'^{(\mathrm{H8})}$, and v.

Choose $\exists\, \rho', \rho^+, v$ to be $\rho', \rho^+ \bullet \rho_1, v$. Note that: $\rho' \mathbin{\#} \rho_f$ by H7 and theorem 6.11; and $\rho^+ \bullet \rho_1 \mathbin{\#} \rho_f \bullet \rho'^{(\mathrm{H9})}$ by H8 and theorem 6.46. Most proof obligations are immediate, but observe that:

- $\rho^+ \bullet \rho_1 \mid \mathsf{own} = \varnothing$ follows from H5 and by definition, since ρ_1 contains only a borrow; and
- $\rho_1 \bullet \rho_2 \leftrightsquigarrow \rho' \bullet \rho^+ \bullet \rho_1$ follows from H4 and H9 and theorem 6.48.

□

Lemma 6.149 (wp-I-forget). $\ell \mapsto\!\mathrm{I}_\alpha\, \hat{P} \star \mathsf{wp}\,(e)\,\{\hat{Q}\} \vDash \mathsf{wp}\,(e)\,\{\hat{Q}\}$

Proof. Proceeds almost identically to the proof of theorem 6.148. The reasoning depends only on the resource being a borrow, not on it being a mutable borrow. □

Theorem 6.150 ($\circlearrowleft$ rule)**.** $\ell \mapsto \mathsf{Imm}\ \alpha\ (\text{И}\beta.\ \circlearrowleft_\beta \hat{P}) \star (\text{И}\beta.\,\forall\, v.\, \hat{P}(v) \mathrel{-\!\!\star} \mathsf{wp}\,(e)\,\big\{[\beta]\,\hat{Q}\big\}) \vDash \mathsf{wp}\,(e)\,\big\{\hat{Q}\big\}$

Proof. Let $\rho \in \ell \mapsto \mathsf{Imm}\ \alpha\ (\text{И}\beta.\ \circlearrowleft_\beta \hat{P}) \star (\text{И}\beta.\,\forall\, v.\, \hat{P}(v) \mathrel{-\!\!\star} \mathsf{wp}\,(e)\,\big\{[\beta]\,\hat{Q}\big\})^{(\text{H1})}$.
We want to show $\rho \in \mathsf{wp}\,(e)\,\big\{\hat{Q}\big\}^{(\text{G1})}$. Unfolding wp, let $\rho_f \mathrel{\#} \rho^{(\text{H2})}$. We want to show $\exists\, \rho' \mathrel{\#} \rho_f{}^{(\text{G2})}, \rho^+ \mathrel{\#} \rho' \bullet \rho_f{}^{(\text{G3})}, v$.

- $(\llbracket \rho_f \bullet \rho \rrbracket, e) \Downarrow (\llbracket \rho_f \bullet \rho' \bullet \rho^+ \rrbracket, v)^{(\text{G4})}$
- $\rho \leftrightsquigarrow \rho' \bullet \rho^{+(\text{G5})}$
- $\rho^+|_{\mathsf{own}} = \varnothing^{(\text{G6})}$
- $\rho' \in \hat{Q}(v)^{(\text{G7})}$

Unfolding $\star$ in H1, $\exists\, \rho_i, \rho_c$ such that

- $\rho = \rho_i \bullet \rho_c{}^{(\text{H3})}$,
- $\rho_i \in \ell \mapsto \mathsf{Imm}\ \alpha\ (\text{И}\beta.\ \circlearrowleft_\beta \hat{P})^{(\text{H4})}$
- $\rho_b \in \text{И}\beta.\,\forall\, v.\, \hat{P}(v) \mathrel{-\!\!\star} \mathsf{wp}\,(e)\,\big\{[\beta]\,\hat{Q}\big\}^{(\text{H5})}$

Unfolding Imm in H4, we get there exists $\overline{\alpha}$, v', ρ' such that

- $\rho_i = \ell \mapsto \mathsf{imm}(\overline{\alpha}, v', \rho')^{(\text{H6})}$
- $\rho' \in (\text{И}\beta.\ \circlearrowleft_\beta \hat{P})(v')^{(\text{H7})}$
- $\alpha \sqsubseteq \overline{\alpha}^{(\text{H8})}$

Unfolding И in H7, we get there exists γ_i such that $\rho' \in \forall\, \beta \sqsubset \gamma_i.\, [\beta]\,(\circlearrowleft_\beta \hat{P})(v')^{(\text{H9})}$. Unfolding И in H5, we get there exists γ_b such that $\rho_b \in \forall\, \beta \sqsubset \gamma_b.\, [\beta]\,(\forall\, v.\, \hat{P}(v) \mathrel{-\!\!\star} \mathsf{wp}\,(e)\,\big\{[\beta]\,\hat{Q}\big\})^{(\text{H10})}$.
Let β be some lifetime where $\beta \sqsubset \gamma_i \sqcap \gamma_b{}^{(\text{H11})}$. Such a β always exists because for any lifetime, the set of lifetimes shorter than it is infinite. Specializing H9 and H10 to β, unfolding $[\beta]$, and specializing to v', we get

- $\rho' \in \circlearrowleft_\beta \hat{P}(v')^{(\text{H12})}$.
- $@\rho' \sqsupset \beta^{(\text{H13})}$
- $\rho_b \in \hat{P}(v') \mathrel{-\!\!\star} \mathsf{wp}\,(e)\,\big\{[\beta]\,\hat{Q}\big\}^{(\text{H14})}$
- $@\rho_b \sqsupset \beta^{(\text{H15})}$

Unfolding $\circlearrowleft_\beta$ in H12, we get there exists a $\rho_{\hat{P}(v')}$ such that $\rho_{P(\hat{v'})} \in \mathsf{reb}_\beta(\rho')^{(\text{H16})}$ and $\rho_{P(\hat{v'})} \in \hat{P}(v')^{(\text{H17})}$.
By lemma 6.10 with H2, $\checkmark\,\rho$, and therefore $\rho_i \mathrel{\#} \rho_b{}^{(\text{H18})}$. Then by lemma 6.55 with H16, $\rho_{\hat{P}(v')} \mathrel{\#} \rho_b{}^{(\text{H19})}$.
By similar reasoning, we have $\rho_{\hat{P}(v')} \mathrel{\#} \rho_b \bullet \rho_f$.
By lemma 6.55, $\rho_i \mathrel{\#} \rho_{\hat{P}(v)}$. Therefore by lemma 6.15 with H2, $\rho_{\hat{P}(v')} \mathrel{\#} \rho_i \bullet \rho_b \bullet \rho_f{}^{(\text{H20})}$.
By the definition of $\mathrel{-\!\!\star}$, $\rho_{\hat{P}(v')} \bullet \rho_b \in \mathsf{wp}\,(e)\,\big\{[\beta]\,\hat{Q}\big\}^{(\text{H21})}$. Unfolding wp in H21 and setting $\rho_f = \rho_i \bullet \rho_f$, with the compatibility constraint from H20, and $\rho = \rho_{\hat{P}(v')} \bullet \rho_b$, we have there exists $\rho_Q \mathrel{\#} \rho_i \bullet \rho_f{}^{(\text{H22})}$ and $\rho^+ \mathrel{\#} \rho_Q \bullet \rho_i \bullet \rho_f{}^{(\text{H23})}$ and v such that

- $(\left\llbracket \rho_i \bullet \rho_f \bullet \rho_{\hat{P}(v')} \bullet \rho_b \right\rrbracket, e) \Downarrow (\llbracket \rho_i \bullet \rho_f \bullet \rho_Q \bullet \rho^+ \rrbracket, v)^{(\text{H24})}$

- $\rho_{\hat{P}(v')} \bullet \rho_b \bullet\!\leftrightsquigarrow \rho_Q \bullet \rho^{+}{}^{(\mathrm{H25})}$
- $\rho^{+}|_{\mathsf{own}} = \varnothing^{(\mathrm{H26})}$
- $\rho_Q \in [\beta]\,\hat{Q}(v)^{(\mathrm{H27})}$

Unfolding $[\beta]$ in H27, we get $\rho_Q \in \hat{Q}(v)^{(\mathrm{H28})}$ and $@\rho_Q \sqsupset \beta^{(\mathrm{H29})}$.
Let $\rho^{+\prime} = \rho^{+} \boxminus \rho_{\hat{P}(v')}|_{\mathrm{dom}(\rho'|_{\mathsf{mut,own}})}$. By rewriting in H24 with lemma 6.58 applied to H16, H25, H15, H29, H18, and H23 with lemma 6.11,
$(\llbracket \rho_f \bullet \rho_i \bullet \rho_b \rrbracket, e) \Downarrow (\llbracket \rho_f \bullet \rho_Q \bullet \rho_i \bullet \rho^{+\prime} \rrbracket, v)^{(\mathrm{H30})}$.
By lemma 6.11 with H23, $\rho_Q \# \rho_f{}^{(\mathrm{H31})}$, and $\rho_i \bullet \rho^{+\prime} \# \rho_Q \bullet \rho_f{}^{(\mathrm{H32})}$.
By lemma 6.59 applied to H16, H25, H15, H29, H18, and H23, $\rho_i \bullet \rho_b \leftrightsquigarrow \rho_Q \bullet \rho_i \bullet \rho^{+\prime(\mathrm{H33})}$.
Now we can prove our goals, setting $\rho' = \rho_Q$, and $\rho^{+} = \rho_i \bullet \rho^{+\prime}$,

- G2: $\rho_Q \# \rho_f$ by H31
- G3: $\rho_i \bullet \rho^{+\prime} \# \rho_Q \bullet \rho_f$ by H32.
- G4: $(\llbracket \rho_f \bullet \rho \rrbracket, e) \Downarrow (\llbracket \rho_f \bullet \rho_Q \bullet \rho_i \bullet \rho^{+\prime} \rrbracket, v')$ by H30
- G5: $\rho_i \bullet \rho_b \leftrightsquigarrow \rho_Q \bullet \rho_i \bullet \rho^{+\prime}$ by H33
- G6: $\rho^{+}|_{\mathsf{own}} = \varnothing$ by H26
- G7: $\rho_Q \in \hat{Q}(v)$ by H28

□

6.8 Fundamental Property

Lemma 6.151 (Fundamental Property). If $\Delta; \Gamma \vdash e : T$ then $\Delta; \Gamma \vDash e : T$.

Proof. By induction on the typing derivation and appealing to the appropriate compatibility lemma (theorem 6.152 - theorem 6.176) in each case. □

Lemma 6.152 (ID-COMPAT). $\dfrac{}{\Delta; x : T \vDash x : T}\textsc{id}$

Proof. By unfolding and WP-VAL. □

Lemma 6.153 ($\mathbb{1}I$-COMPAT). $\dfrac{}{\Delta; \varnothing \vDash () : \mathbb{1}}\mathbb{1}I$

Proof. By unfolding and WP-VAL. □

Lemma 6.154 ($\mathbb{1}E$-COMPAT). $\dfrac{\Delta; \Gamma_1 \vDash e_1 : \mathbb{1} \quad \Delta; \Gamma_2 \vDash e_2 : T}{\Delta; \Gamma_1, \Gamma_2 \vDash e_1; e_2 : T}\mathbb{1}E$

Proof. Suppose $\Delta; \Gamma_1 \vDash e_1 : \mathbb{1}^{(\mathrm{H1})}$ and $\Delta; \Gamma_2 \vDash e_2 : T^{(\mathrm{H2})}$. Let $\delta \in \llbracket \Delta \rrbracket$, γ be arbitrary. Split γ into γ_1, γ_2. Apply WP-BIND. We must show:

$$\mathcal{G}\llbracket \Gamma_1 \rrbracket_\delta(\gamma_1) \star \mathcal{G}\llbracket \Gamma_2 \rrbracket_\delta(\gamma_2) \vDash \mathsf{wp}\,(e_1\gamma_1)\,\{v_1.\ \mathsf{wp}\,(v_1; e_2\gamma_2)\,\{\mathcal{V}\llbracket T \rrbracket_\delta\}\}$$

Apply H1, WP-FRAME, and WP-MONO for an arbitrary v_1.

$$\mathcal{V}\llbracket \mathbb{1} \rrbracket_\delta(v_1) \star \mathcal{G}\llbracket \Gamma_2 \rrbracket_\delta(\gamma_2) \vDash \mathsf{wp}\,(v_1; e_2\gamma_2)\,\{\mathcal{V}\llbracket T \rrbracket_\delta\}$$

By unfolding $\mathcal{V}\llbracket \mathbb{1} \rrbracket$, we have $v_1 = ()$. Follows from WP-$\mathbb{1}$ and H2. □

Lemma 6.155 ($\otimes I$-compat)**.** $\dfrac{\Delta; \Gamma_1 \vDash e_1 : T_1 \quad \Delta; \Gamma_2 \vDash e_2 : T_2}{\Delta; \Gamma_1, \Gamma_2 \vDash (e_1, e_2) : T_1 \otimes T_2}\otimes I$

Proof. Suppose $\Delta; \Gamma_1 \vDash e_1 : T_1{}^{(\mathrm{H1})}$ and $\Delta; \Gamma_2 \vDash e_2 : T_2{}^{(\mathrm{H2})}$. Let $\delta \in [\![\Delta]\!]$, γ be arbitrary. Split γ into γ_1, γ_2. Apply wp-bind. We must show:

$$\mathcal{G}[\![\Gamma_1]\!]_\delta(\gamma_1) \star \mathcal{G}[\![\Gamma_2]\!]_\delta(\gamma_2) \vDash \mathsf{wp}\,(e_1\gamma_1)\,\{v_1.\ \mathsf{wp}\,((v_1, e_2\gamma_2))\,\{\mathcal{V}[\![T_1 \otimes T_2]\!]\}\}$$

Apply H1, wp-frame, and wp-mono for an arbitrary v_1. Apply wp-bind. Repeat the previous with H2 for some v_2.

$$\mathcal{V}[\![T_1]\!]_\delta(v_1) \star \mathcal{V}[\![T_2]\!]_\delta(v_2) \vDash \mathsf{wp}\,((v_1, v_2))\,\{\mathcal{V}[\![T_1 \otimes T_2]\!]\}$$

Fold $\mathcal{V}[\![\otimes]\!]$. Follows from wp-val. □

Lemma 6.156 ($\otimes E$-compat)**.** $\dfrac{\Delta; \Gamma_1 \vDash e_1 : T_1^1 \otimes T_1^2 \quad \Delta; \Gamma_2, x_1 : T_1^1, x_2 : T_1^2 \vDash e_2 : T_2}{\Delta; \Gamma_1, \Gamma_2 \vDash \mathsf{let}\,(x_1, x_2) = e_1; e_2 : T_2}\otimes E$

Proof. Suppose $\Delta; \Gamma_1 \vDash e_1 : T_1^1 \otimes T_1^{2\,(\mathrm{H1})}$ and $\Delta; \Gamma_2, x_1 : T_1^1, x_2 : T_1^2 \vDash e_2 : T_2{}^{(\mathrm{H2})}$. Let $\delta \in [\![\Delta]\!]$, γ be arbitrary. Split γ into γ_1, γ_2. Apply wp-bind. We must show:

$$\mathcal{G}[\![\Gamma_1]\!]_\delta(\gamma_1) \star \mathcal{G}[\![\Gamma_2]\!]_\delta(\gamma_2) \vDash \mathsf{wp}\,(e_1\gamma_1)\,\{v_1.\ \mathsf{wp}\,(\mathsf{let}\,(x_1, x_2) = v_1; e_2\gamma_2)\,\{\mathcal{V}[\![T_2]\!]_\delta\}\}$$

Apply H1, wp-frame, and wp-mono for an arbitrary v_1. By unfolding $\mathcal{V}[\![\otimes]\!]$, there exist some v_1^1, v_1^2 such that $v_1 = (v_1^1, v_1^2)$.

$$\mathcal{V}\left[\!\left[T_1^1\right]\!\right]_\delta(v_1^1) \star \mathcal{V}\left[\!\left[T_1^2\right]\!\right](v_1^2) \star \mathcal{G}[\![\Gamma_2]\!]_\delta(\gamma_2) \vDash \mathsf{wp}\left(\mathsf{let}\,(x_1, x_2) = (v_1^1, v_1^2); e_2\gamma_2\right)\{\mathcal{V}[\![T_2]\!]_\delta\}$$

Follows from wp-$\otimes$ and H2 with $\gamma_2[x_1 \mapsto v_1^1, x_2 \mapsto v_1^2]$. □

Lemma 6.157 ($\oplus I$-compat)**.** $\dfrac{\Delta; \Gamma \vDash e : T_i}{\Delta; \Gamma \vDash i\ e : T_1 \oplus T_2}\oplus I$

Proof. Suppose $\Delta; \Gamma \vDash e : T_i{}^{(\mathrm{H1})}$. Let $\delta \in [\![\Delta]\!]$, γ be arbitrary. Apply wp-bind. We must show:

$$\mathcal{G}[\![\Gamma]\!]_\delta(\gamma) \vDash \mathsf{wp}\,(e\gamma)\,\{v.\ \mathsf{wp}\,(iv)\,\{\mathcal{V}[\![T_1 \oplus T_2]\!]_\delta\}\}$$

Apply H1 and wp-mono. Fold $\mathcal{V}[\![\oplus]\!]$. Follows from wp-val. □

Lemma 6.158 ($\oplus E$-compat)**.** $\dfrac{\Delta; \Gamma_1 \vDash e_1 : T_1^1 \oplus T_1^2 \quad \Delta; \Gamma_2, x_i : T_1^i \vDash e_2^i : T_2 \quad i \in \{1, 2\}}{\Delta; \Gamma_1, \Gamma_2 \vDash \mathsf{match}\, e_1\, \{x_1 \Rightarrow e_2^1, x_2 \Rightarrow e_2^2\} : T_2}\oplus E$

Proof. Suppose $\Delta; \Gamma_1 \vDash e_1 : T_1^1 \oplus T_1^{2\,(\mathrm{H1})}$ and $\forall\, i \in \{1, 2\}.\ \Delta; \Gamma_2, x_i : T_1^i \vDash e_2^i : T_2{}^{(\mathrm{H2})}$. Let $\delta \in [\![\Delta]\!]$, γ be arbitrary. Split γ into γ_1, γ_2. Apply wp-bind. We must show:

$$\mathcal{G}[\![\Gamma_1]\!]_\delta(\gamma_1) \star \mathcal{G}[\![\Gamma_2]\!]_\delta(\gamma_2) \vDash \mathsf{wp}\,(e_1\gamma_1)\left\{v_1.\ \mathsf{wp}\left(\mathsf{match}\, v_1\, \{x_1 \Rightarrow e_2^1\gamma_2, x_2 \Rightarrow e_2^2\gamma_2\}\right)\{\mathcal{V}[\![T_2]\!]_\delta\}\right\}$$

Apply H1, wp-frame, and wp-mono for an arbitrary v_1. By unfolding $\mathcal{V}[\![\oplus]\!]$, there exists some i and v_1'.

$$\mathcal{V}\left[\!\left[T_1^i\right]\!\right]_\delta(v_1') \star \mathcal{G}[\![\Gamma_2]\!]_\delta(\gamma_2) \vDash \mathsf{wp}\left(\mathsf{match}\, iv_1'\, \{x_1 \Rightarrow e_2^1\gamma_2, x_2 \Rightarrow e_2^2\gamma_2\}\right)\{\mathcal{V}[\![T_2]\!]_\delta\}$$

Follows from wp-$\oplus$ and H2 with $\gamma_2[x_i \mapsto v_1']$. □

Lemma 6.159 ($\multimap I$-compat)**.** $\dfrac{\Delta; \Gamma, x : T_1 \vDash e : T_2}{\Delta; \Gamma \vDash \lambda x.e : T_1 \multimap T_2}\multimap I$

Proof. Suppose $\Delta; \Gamma, x : T_1 \vDash e : T_2{}^{(\mathrm{H1})}$. Let $\delta \in [\![\Delta]\!]$, γ be arbitrary. Apply wp-val. Unfold $\mathcal{V}[\![\multimap]\!]$ and let v' be arbitrary. We must show:

$$\mathcal{G}[\![\Gamma]\!]_\delta(\gamma) \star \mathcal{V}[\![T_1]\!]_\delta(v') \vDash \mathsf{wp}\,((\lambda x.e\gamma)\ v')\,\{\mathcal{V}[\![T_2]\!]_\delta\}$$

Follows from wp-$\multimap$ and H1. □

Lemma 6.160 ($\multimap E$-compat)**.** $\dfrac{\Delta;\Gamma_1 \vDash e_1 : T_1 \quad \Delta;\Gamma_2 \vDash e_2 : T_1 \multimap T_2}{\Delta;\Gamma_1,\Gamma_2 \vDash e_2 e_1 : T_2}\multimap E$

Proof. Suppose $\Delta;\Gamma_1 \vDash e_1 : T_1{}^{(\mathrm{H1})}$ and $\Delta;\Gamma_2 \vDash e_2 : T_1 \multimap T_2{}^{(\mathrm{H2})}$. Let $\delta \in [\![\Delta]\!]$, γ be arbitrary. Split γ into γ_1, γ_2. Apply wp-bind. We must show:

$$\mathcal{G}[\![\Gamma_1]\!]_\delta(\gamma_1) \star \mathcal{G}[\![\Gamma_2]\!]_\delta(\gamma_2) \vDash \mathsf{wp}\,(e_1\gamma_1)\,\{v_1.\ \mathsf{wp}\,(e_2\gamma_2\ v_1)\,\{\mathcal{V}[\![T_2]\!]_\delta\}\}$$

Apply H1, wp-frame, and wp-mono for an arbitrary v_1. Apply wp-bind.

$$\mathcal{V}[\![T_1]\!]_\delta(v_1) \star \mathcal{G}[\![\Gamma_2]\!]_\delta(\gamma_2) \vDash \mathsf{wp}\,(e_2\gamma_2)\,\{v_2.\ \mathsf{wp}\,(v_2\ v_1)\,\{\mathcal{V}[\![T_2]\!]_\delta\}\}$$

Apply H2, wp-frame, and wp-mono for an arbitrary v_2.

$$\mathcal{V}[\![T_1]\!]_\delta(v_1) \star \mathcal{V}[\![T_1 \multimap T_2]\!](v_2) \vDash \mathsf{wp}\,(v_2\ v_1)\,\{\mathcal{V}[\![T_2]\!]_\delta\}$$

Follows from unfolding $\mathcal{V}[\![\multimap]\!]$. □

Lemma 6.161 ($\forall\, I$-compat)**.** $\dfrac{\Delta, ('a \sqsubset @b);\Gamma \vDash e : T}{\Delta;\Gamma \vDash \lambda e : \forall\,('a \sqsubset @b).T}\forall\, I$

Proof. Suppose $\Delta, ('a \sqsubset @b);\Gamma \vDash e : T^{(\mathrm{H1})}$. Let $\delta \in [\![\Delta]\!]$, γ be arbitrary. Apply wp-val. We must show:

$$\mathcal{G}[\![\Gamma]\!]_\delta(\gamma) \vDash \mathcal{V}[\![\forall\,('a \sqsubset @b).\ T]\!]_\delta(\lambda\_.e\gamma)$$

Unfold $\mathcal{V}[\![\forall\,]\!]$ and let $\alpha \sqsubset @b\delta$ be arbitrary. By Δ-extend, $\delta['a \mapsto \alpha] \in [\![\Delta, ('a \sqsubset @b)]\!]$. Extend $\mathcal{G}[\![\Gamma]\!]_\delta$ with $\delta['a \mapsto \alpha]$.

$$\mathcal{G}[\![\Gamma]\!]_{\delta['a\mapsto\alpha]}(\gamma) \vDash \mathsf{wp}\,((\lambda\_.e\gamma)\ ())\left\{\mathcal{V}[\![T]\!]_{\delta['a\mapsto\alpha]}\right\}$$

Follows from wp-$\multimap$ and H1. □

Lemma 6.162 ($\forall\, E$-compat)**.** $\dfrac{\Delta;\Gamma \vDash e : \forall\,('a \sqsubset @b).T \quad \Delta \vDash @a \sqsubset @b}{\Delta;\Gamma \vDash e\ () : T[@a/'a]}\forall\, E$

Proof. Suppose $\Delta;\Gamma \vDash e : \forall\,('a \sqsubset @b).\ T^{(\mathrm{H1})}$ and $\Delta \vDash @a \sqsubset @b^{(\mathrm{H2})}$. Let $\delta \in [\![\Delta]\!]$, γ be arbitrary. Apply wp-bind. We must show:

$$\mathcal{G}[\![\Gamma]\!]_\delta(\gamma) \vDash \mathsf{wp}\,(e\gamma)\,\{v.\ \mathsf{wp}\,(v\ ())\,\{\mathcal{V}[\![T[@a/'a]]\!]_\delta\}\}$$

Apply H1 and wp-mono for an arbitrary v.

$$\mathcal{V}[\![\forall\,('a \sqsubset @b).\ T]\!]_\delta(v) \vDash \mathsf{wp}\,(v\ ())\,\{\mathcal{V}[\![T[@a/'a]]\!]_\delta\}$$

Unfold $\mathcal{V}[\![\forall\,]\!]$ and instantiate with $@a\delta$. Note that $@a\delta \sqsubset @b\delta$ by H2. Apply wp-mono for an arbitrary v'.

$$\mathcal{V}[\![T]\!]_{\delta['a\mapsto @a\delta]}(v') \vDash \mathcal{V}[\![T[@a/'a]]\!]_\delta(v')$$

Follows from Δ-subst. □

Lemma 6.163 ($[\,]\,I$-compat)**.** $\dfrac{\Delta;\Gamma \vDash e : T \quad \Delta \vDash \Gamma \sqsupset @a}{\Delta;\Gamma \vDash e : [@a]\,T}[\,]\,I$

Proof. Suppose $\Delta;\Gamma \vDash e : T^{(\mathrm{H1})}$ and $\Delta \vdash \Gamma \sqsupset @a^{(\mathrm{H2})}$. Let $\delta \in [\![\Delta]\!]$, γ be arbitrary. We must show:

$$\mathcal{G}[\![\Gamma]\!]_\delta(\gamma) \vDash \mathsf{wp}\,(e)\,\{\mathcal{V}[\![[@a]\,T]\!]_\delta\}$$

Apply theorem 6.62 with H2. Unfold $\mathcal{V}[\![[\,]\,]\!]$.

$$[@a\delta]\,\mathcal{G}[\![\Gamma]\!]_\delta(\gamma) \vDash \mathsf{wp}\,(e)\,\{[@a\delta]\,\mathcal{V}[\![T]\!]_\delta\}$$

Follows from wp-$[\,]$, $[\,]$-mono, and H1. □

Lemma 6.164 ($[\,]\,E$-compat)**.** $\dfrac{\Delta;\Gamma \vDash e : [@a]\,T}{\Delta;\Gamma \vDash e : T}[\,]\,E$

Proof. Suppose $\Delta;\Gamma \vDash e : [@a]\,T^{(\mathrm{H1})}$. Let $\delta \in \llbracket\Delta\rrbracket$, γ be arbitrary. Follows from H1, wp-mono, unfolding $\mathcal{V}\llbracket[\,]\,\rrbracket$, and $[\,]$-l □

Lemma 6.165 (alloc-compat)**.** $\dfrac{}{\Delta;\varnothing \vDash \mathsf{alloc}\ : T \multimap \mathsf{Ref}\ T}\mathsf{alloc}$

Proof. Let $\delta \in \llbracket\varnothing\rrbracket$, γ be arbitrary. Apply wp-val and unfold $\mathcal{V}\llbracket\multimap\rrbracket$ for an arbitrary v. We must show:

$$\mathcal{V}\llbracket T\rrbracket_\delta(v) \vDash \mathsf{wp}\,(\mathsf{alloc}\ \ v)\,\{\mathcal{V}\llbracket *T\rrbracket_\delta\}$$

Follows from wp-alloc and unfolding $\mathcal{V}\llbracket *\rrbracket$. □

Lemma 6.166 (free-compat)**.** $\dfrac{}{\Delta;\varnothing \vDash \mathsf{free}\ : \mathsf{Ref}\ T \multimap T}\mathsf{free}$

Proof. Let $\delta \in \llbracket\varnothing\rrbracket$, γ be arbitrary. Apply wp-val and unfold $\mathcal{V}\llbracket\multimap\rrbracket$ for an arbitrary v. We must show:

$$\mathcal{V}\llbracket *T\rrbracket_\delta(v) \vDash \mathsf{wp}\,(\mathsf{free}\ \ v)\,\{\mathcal{V}\llbracket T\rrbracket_\delta\}$$

Follows from unfolding $\mathcal{V}\llbracket *\rrbracket$ and wp-free. □

Lemma 6.167 ($\sqsubseteq$imm-compat)**.** $\dfrac{\Delta;\Gamma \vDash e : \mathsf{Imm}\ @b\ T \quad \Delta \vDash @a \sqsubseteq @b}{\Delta;\Gamma \vDash e : \mathsf{Imm}\ @a\ T}\sqsubseteq\text{IMM}$

Proof. Suppose $\Delta;\Gamma \vDash e : \mathsf{Imm}\ @b\ T^{(\mathrm{H1})}$ and $\Delta \vDash @a \sqsubseteq @b^{(\mathrm{H2})}$. Let $\delta \in \llbracket\Delta\rrbracket$, γ be arbitrary. We must show:

$$\mathcal{G}\llbracket\Gamma\rrbracket_\delta(\gamma) \vDash \mathsf{wp}\,(e)\,\{\mathcal{V}\llbracket\mathsf{Imm}\ @a\ T\rrbracket_\delta\}$$

Apply H1 to $\mathcal{G}\llbracket\Gamma\rrbracket_\delta(\gamma)$, then apply wp-mono for an arbitrary v.

$$\mathcal{V}\llbracket\mathsf{Imm}\ @b\ T\rrbracket_\delta(v) \vDash \mathcal{V}\llbracket\mathsf{Imm}\ @a\ T\rrbracket_\delta(v)$$

Unfold $\mathcal{V}\llbracket\mathsf{Imm}\ \ \rrbracket_\delta$. There exists some ℓ such that $v = \ell$.

$$\ell \mapsto\mathrm{I}_{@b\delta}\ \mathcal{V}\llbracket T\rrbracket_\delta \vDash \exists\,\ell.\ \ulcorner v = \ell \urcorner \star \ell \mapsto\mathrm{I}_{@a\delta}\ \mathcal{V}\llbracket T\rrbracket_\delta$$

Apply $\mathsf{I} \sqsupseteq$ with H2. Then choose $\exists\,\ell$ to be ℓ. □

Lemma 6.168 ($\sqsubseteq$mut-compat)**.** $\dfrac{\Delta;\Gamma \vDash e : \mathsf{Mut}\ @b\ T \quad \Delta \vDash @a \sqsubseteq @b}{\Delta;\Gamma \vDash e : \mathsf{Mut}\ @a\ T}\sqsubseteq\text{MUT}$

Proof. Suppose $\Delta;\Gamma \vDash e : \mathsf{Mut}\ @b\ T^{(\mathrm{H1})}$ and $\Delta \vDash @a \sqsubseteq @b^{(\mathrm{H2})}$. Let $\delta \in \llbracket\Delta\rrbracket$, γ be arbitrary. We must show:

$$\mathcal{G}\llbracket\Gamma\rrbracket_\delta(\gamma) \vDash \mathsf{wp}\,(e)\,\{\mathcal{V}\llbracket\mathsf{Mut}\ @a\ T\rrbracket_\delta\}$$

Apply H1 to $\mathcal{G}\llbracket\Gamma\rrbracket_\delta(\gamma)$, then apply wp-mono for an arbitrary v.

$$\mathcal{V}\llbracket\mathsf{Mut}\ @b\ T\rrbracket_\delta(v) \vDash \mathcal{V}\llbracket\mathsf{Mut}\ @a\ T\rrbracket_\delta(v)$$

Unfold $\mathcal{V}\llbracket\mathsf{Mut}\ \ \rrbracket_\delta$. There exists some ℓ such that $v = \ell$.

$$\ell \mapsto\mathrm{M}_{@b\delta}\ \mathcal{V}\llbracket T\rrbracket_\delta \vDash \exists\,\ell.\ \ulcorner v = \ell \urcorner \star \ell \mapsto\mathrm{M}_{@a\delta}\ \mathcal{V}\llbracket T\rrbracket_\delta$$

Apply $\mathsf{M} \sqsupseteq$ with H2. Then choose $\exists\,\ell$ to be ℓ. □

Lemma 6.169 (swap-COMPAT). $\dfrac{}{\Delta;\varnothing \vDash \mathsf{swap} : \mathsf{Ref}\ T_1 \multimap T_2 \multimap \mathsf{Ref}\ T_2 \otimes T_1}\,\mathsf{swap}$

Proof. Let $\delta \in \llbracket\varnothing\rrbracket$, γ be arbitrary. Apply WP-VAL. We must show:

$$\vDash \mathcal{V}\llbracket \mathsf{Ref}\ T_1 \multimap T_2 \multimap \mathsf{Ref}\ T_2 \otimes T_1 \rrbracket_\delta(\mathsf{swap})$$

Unfold $\mathcal{V}\llbracket\multimap\rrbracket$. Let v_1 be arbitrary. Apply WP-$\multimap$.

$$\mathcal{V}\llbracket \mathsf{Ref}\ T_1\rrbracket_\delta(v_1) \vDash \mathsf{wp}\,(\lambda y.\mathsf{let}\, z = \mathsf{load}\ v_1; \mathsf{store}\ v_1\ y; (x,z))\,\{\mathcal{V}\llbracket T_2 \multimap \mathsf{Ref}\ T_2 \otimes T_1\rrbracket_\delta\}$$

Apply WP-VAL. Unfold $\mathcal{V}\llbracket\multimap\rrbracket$. Let v_2 be arbitrary. Apply WP-$\multimap$.

$$\mathcal{V}\llbracket \mathsf{Ref}\ T_1\rrbracket_\delta(v_1) \star \mathcal{V}\llbracket T_2\rrbracket_\delta(v_2) \vDash \mathsf{wp}\,(\mathsf{let}\, z = \mathsf{load}\ v_1; \mathsf{store}\ v_1\ v_2; (v_1,z))\,\{\mathcal{V}\llbracket \mathsf{Ref}\ T_2 \otimes T_1\rrbracket_\delta\}$$

Unfold let.

$$\mathcal{V}\llbracket \mathsf{Ref}\ T_1\rrbracket_\delta(v_1) \star \mathcal{V}\llbracket T_2\rrbracket_\delta(v_2) \vDash \mathsf{wp}\,((\lambda z.\mathsf{store}\ v_1\ v_2; (v_1,z))\ (\mathsf{load}\ v_1))\,\{\mathcal{V}\llbracket \mathsf{Ref}\ T_2 \otimes T_1\rrbracket_\delta\}$$

Apply WP-BIND.

$$\mathcal{V}\llbracket \mathsf{Ref}\ T_1\rrbracket_\delta(v_1) \star \mathcal{V}\llbracket T_2\rrbracket_\delta(v_2) \vDash \mathsf{wp}\,(\mathsf{load}\ v)\,\{v_3.\ \mathsf{wp}\,((\lambda z.\mathsf{store}\ v_1\ v_2; (v_1,z))\ v_3)\,\{\mathcal{V}\llbracket \mathsf{Ref}\ T_2 \otimes T_1\rrbracket_\delta\}\}$$

Unfold $\mathcal{V}\llbracket\mathsf{Ref}\ \rrbracket$. There exists some ℓ, v_1' such that $v_1 = \ell$.

$$\ell \mapsto v_1' \star \mathcal{V}\llbracket T_1\rrbracket_\delta(v_1') \star \mathcal{V}\llbracket T_2\rrbracket_\delta(v_2) \vDash \mathsf{wp}\,(\mathsf{load}\ v)\,\{v_3.\ \mathsf{wp}\,((\lambda z.\mathsf{store}\ v_1\ v_2; (\ell,z))\ v_3)\,\{\mathcal{V}\llbracket \mathsf{Ref}\ T_2 \otimes T_1\rrbracket_\delta\}\}$$

Apply WP-LOAD, WP-$\multimap$, and WP-BIND.

$$\ell \mapsto v_1' \star \mathcal{V}\llbracket T_1\rrbracket_\delta(v_1') \star \mathcal{V}\llbracket T_2\rrbracket_\delta(v_2) \vDash \mathsf{wp}\,(\mathsf{store}\ v_1\ v_2)\,\{\_.\ \mathsf{wp}\,((\ell,v_1'))\,\{\mathcal{V}\llbracket \mathsf{Ref}\ T_2 \otimes T_1\rrbracket_\delta\}\}$$

Apply WP-STORE and WP-VAL.

$$\ell \mapsto v_2 \star \mathcal{V}\llbracket T_1\rrbracket_\delta(v_1') \star \mathcal{V}\llbracket T_2\rrbracket_\delta(v_2) \vDash \mathcal{V}\llbracket \mathsf{Ref}\ T_2 \otimes T_1\rrbracket_\delta((\ell,v_1'))$$

This follows from folding and unfolding $\mathcal{V}$ definitions. □

Lemma 6.170 (copy-COMPAT). $\Delta \vDash \mathsf{copy} : \mathsf{Imm}\ @a\ T \multimap (\mathsf{Imm}\ @a\ T \otimes \mathsf{Imm}\ @a\ T)$.

Proof.

Proof step	Current goal
Let $\delta \in \llbracket\Delta\rrbracket$ be arbitrary.	$\vDash \mathcal{V}\llbracket \mathsf{Imm}\ @a\ T_1 \multimap (\mathsf{Imm}\ @a\ T \otimes \mathsf{Imm}\ @a\ T)\rrbracket_\delta(\mathsf{copy})$
Apply WP-VAL.	
Let v be arbitrary.	
Apply WP-$\multimap$.	$\mathcal{V}\llbracket \mathsf{Imm}\ @a\ T\rrbracket_\delta(v) \vDash \mathcal{V}\llbracket \mathsf{Imm}\ @a\ T \otimes \mathsf{Imm}\ @a\ T\rrbracket_\delta(v,v)$.
Unfold.	$\mathcal{V}\llbracket \mathsf{Imm}\ @a\ T\rrbracket_\delta(v) \vDash \exists\, v_1, v_2.\ \ulcorner (v,v) = (v_1,v_2)\urcorner \star \mathcal{V}\llbracket T\rrbracket_\delta(v_1) \star \mathcal{V}\llbracket T_2\rrbracket_\delta(v_2)$
Choose $v_1 = v_2 = v$.	$\mathcal{V}\llbracket \mathsf{Imm}\ @a\ T\rrbracket_\delta(v) \vDash \mathcal{V}\llbracket \mathsf{Imm}\ @a\ T\rrbracket_\delta(v) \star \mathcal{V}\llbracket \mathsf{Imm}\ @a\ T\rrbracket_\delta(v)$
Unfold.	$\exists\, \ell.\ \ulcorner v = \ell\urcorner \star \ell \mapsto\mathrm{I}_{@a\delta}\ \mathcal{V}\llbracket T\rrbracket \vDash \mathcal{V}\llbracket \mathsf{Imm}\ @a\ T\rrbracket_\delta(v) \star \mathcal{V}\llbracket \mathsf{Imm}\ @a\ T\rrbracket_\delta(v)$
Substitute $v = \ell$.	$\ell \mapsto\mathrm{I}_{@a\delta}\ \mathcal{V}\llbracket T\rrbracket \vDash \mathcal{V}\llbracket \mathsf{Imm}\ @a\ T\rrbracket_\delta(\ell) \star \mathcal{V}\llbracket \mathsf{Imm}\ @a\ T\rrbracket_\delta(\ell)$
Unfold and simplify.	$\ell \mapsto\mathrm{I}_{@a\delta}\ \mathcal{V}\llbracket T\rrbracket \vDash (\ell \mapsto\mathrm{I}_{@a\delta}\ \mathcal{V}\llbracket T\rrbracket) \star (\ell \mapsto\mathrm{I}_{@a\delta}\ \mathcal{V}\llbracket T\rrbracket)$
Apply I-DUP.	□

Lemma 6.171 (forget-COMPAT). $\Delta \vDash \mathsf{forget} : B \multimap \mathbb{1}$ for all $B \in \{\mathsf{Imm}\ @a\ T, \mathsf{Mut}\ @a\ T, \mathsf{Unk}\}$.

Proof.

Proof step	Current goal
Let $\delta \in \llbracket\Delta\rrbracket$ be arbitrary.	$\vDash \mathcal{V}\llbracket B \multimap \mathbb{1}\rrbracket_\delta(\mathsf{forget})$
Apply WP-VAL.	
Let v be arbitrary.	
Apply WP-$\multimap$.	$\mathcal{V}\llbracket B\rrbracket_\delta(v) \vDash \mathsf{wp}\,(())\,\{\mathcal{V}\llbracket\mathbb{1}\rrbracket_\delta\}$

Now there are three cases:

- Case $B = \mathsf{Imm}\ @a\ T$:

Proof step	Current goal
	$\mathcal{V}[\![\mathsf{Imm}\ @a\ T]\!]_\delta(v) \vDash \mathsf{wp}\,(())\,\{\mathcal{V}[\![\mathbb{1}]\!]_\delta\}$
Unfold.	$\exists\,\ell.\ \ulcorner v = \ell \urcorner \star \ell \mapsto\mathrm{I}\ \mathcal{V}[\![T]\!] \vDash \mathsf{wp}\,(())\,\{\mathcal{V}[\![\mathbb{1}]\!]_\delta\}$
Substitute $v = \ell$.	$\ell \mapsto\mathrm{I}\ \mathcal{V}[\![T]\!] \vDash \mathsf{wp}\,(())\,\{\mathcal{V}[\![\mathbb{1}]\!]_\delta\}$
Apply wp-I-forget.	$\ell \mapsto\mathrm{I}\ \mathcal{V}[\![T]\!] \vDash \ell \mapsto\mathrm{I}\ \mathcal{V}[\![T]\!] \star \mathsf{wp}\,(())\,\{\mathcal{V}[\![\mathbb{1}]\!]_\delta\}$
Cancel $\ell \mapsto\mathrm{I}\ \mathcal{V}[\![T]\!]$.	$\mathsf{emp} \vDash \mathsf{wp}\,(())\,\{\mathcal{V}[\![\mathbb{1}]\!]_\delta\}$
Apply wp-val.	$\mathsf{emp} \vDash \mathcal{V}[\![\mathbb{1}]\!]_\delta()$
Unfold.	$\mathsf{emp} \vDash \ulcorner () = () \urcorner$

- Case $B = \mathsf{Mut}\ @a\ T$:

Proof step	Current goal
	$\mathcal{V}[\![\mathsf{Mut}\ @a\ T]\!]_\delta(v) \vDash \mathsf{wp}\,(())\,\{\mathcal{V}[\![\mathbb{1}]\!]_\delta\}$
Unfold.	$\exists\,\ell.\ \ulcorner v = \ell \urcorner \star \ell \mapsto\mathrm{M}\ \mathcal{V}[\![T]\!] \vDash \mathsf{wp}\,(())\,\{\mathcal{V}[\![\mathbb{1}]\!]_\delta\}$
Substitute $v = \ell$.	$\ell \mapsto\mathrm{M}\ \mathcal{V}[\![T]\!] \vDash \mathsf{wp}\,(())\,\{\mathcal{V}[\![\mathbb{1}]\!]_\delta\}$
Apply wp-M-forget.	$\ell \mapsto\mathrm{M}\ \mathcal{V}[\![T]\!] \vDash \ell \mapsto\mathrm{M}\ \mathcal{V}[\![T]\!] \star \mathsf{wp}\,(())\,\{\mathcal{V}[\![\mathbb{1}]\!]_\delta\}$
Cancel $\ell \mapsto\mathrm{M}\ \mathcal{V}[\![T]\!]$.	$\mathsf{emp} \vDash \mathsf{wp}\,(())\,\{\mathcal{V}[\![\mathbb{1}]\!]_\delta\}$
Apply wp-val.	$\mathsf{emp} \vDash \mathcal{V}[\![\mathbb{1}]\!]_\delta()$
Unfold.	$\mathsf{emp} \vDash \ulcorner () = () \urcorner$

- Case $B = \mathsf{Unk}$:

Proof step	Current goal
	$\mathcal{V}[\![\mathsf{Unk}]\!]_\delta(v) \vDash \mathsf{wp}\,(())\,\{\mathcal{V}[\![\mathbb{1}]\!]_\delta\}$
Unfold.	$\mathsf{emp} \vDash \mathsf{wp}\,(())\,\{\mathcal{V}[\![\mathbb{1}]\!]_\delta\}$
Apply wp-val.	$\mathsf{emp} \vDash \mathcal{V}[\![\mathbb{1}]\!]_\delta()$
Unfold.	$\mathsf{emp} \vDash \ulcorner () = () \urcorner$

□

Lemma 6.172 (withbor-compat1)**.** $\Delta \vDash \mathsf{withbor} : \mathsf{Ref}\ T_1 \multimap (\forall\, 'a \sqsubset \bigsqcap\Delta.\ \mathsf{Imm}\ 'a\ T_1 \multimap ['a]\, T_2) \multimap \mathsf{Ref}\ T_1 \otimes T_2$

Proof. Let $T_f := (\forall\, 'a \sqsubset \bigsqcap\Delta.\ \mathsf{Imm}\ 'a\ T_1 \multimap ['a]\, T_2)$. Fix $\delta \in [\![\Delta]\!]$.

$$\vDash \mathcal{V}[\![\mathsf{Ref}\ T_1 \multimap T_f \multimap \mathsf{Ref}\ T_1 \otimes T_2]\!]_\delta(\mathsf{withbor})$$

Apply wp-val,wp-$\multimap$ and fix v, v_f.

$$\mathcal{V}[\![\mathsf{Ref}\ T_1]\!]_\delta(v) \star \mathcal{V}[\![T_f]\!]_\delta(v_f) \vDash \mathsf{wp}\,(v, v_f\ \ ()\ \ v)\,\{\mathcal{V}[\![\mathsf{Ref}\ T_1 \otimes T_2]\!]_\delta\}$$

Unfold.

$$(\exists\,\ell\ v_\ell.\ulcorner v = \ell \urcorner \star \ell \mapsto v_\ell \star \mathcal{V}[\![T_1]\!]_\delta(v_\ell)) \star \mathcal{V}[\![T_f]\!](v_f) \vDash \mathsf{wp}\,(v, v_f\ \ ()\ \ v)\,\{\mathcal{V}[\![\mathsf{Ref}\ T_1 \otimes T_2]\!]_\delta\}$$

Substitute.

$$\ell \mapsto v_\ell \star \mathcal{V}[\![T_1]\!]_\delta(v_\ell) \star \mathcal{V}[\![T_f]\!]_\delta(v_f) \vDash \mathsf{wp}\,(\ell, v_f\ \ ()\ \ \ell)\,\{\mathcal{V}[\![\mathsf{Ref}\ T_1 \otimes T_2]\!]_\delta\}$$

Apply ImmFrame.

$$\mathcal{V}[\![T_f]\!](v_f) \vDash \reflectbox{N}\alpha.\,\ell \mapsto\mathrm{I}_\alpha\ \mathcal{V}[\![T_1]\!]_\delta(v_\ell) \mathrel{-\!\!\star} \mathsf{wp}\,(\ell, v_f\ \ ()\ \ \ell)\,\{[\alpha]\,(\ell \mapsto v_\ell \mathrel{-\!\!\star} \mathcal{V}[\![T_1]\!]_\delta(v_\ell) \mathrel{-\!\!\star} \mathcal{V}[\![\mathsf{Ref}\ T_1 \otimes T_2]\!]_\delta)\}$$

Unfold $\mathcal{V}[\![\mathsf{Ref}\ T_1 \otimes T_2]\!]_\delta$.

$$\mathcal{V}[\![T_f]\!]_\delta(v_f) \vDash \reflectbox{N}\alpha.\,\ell \mapsto\mathrm{I}_\alpha\ \mathcal{V}[\![T_1]\!]_\delta(v_\ell) \mathrel{-\!\!\star} \mathsf{wp}\,(\ell, v_f\ \ ()\ \ \ell)\,\big\{[\alpha]\,(\ell \mapsto v_\ell \mathrel{-\!\!\star} \mathcal{V}[\![T_1]\!]_\delta(v_\ell) \mathrel{-\!\!\star} \hat{P})\big\}$$
$$\text{where } \hat{P}(v') = \exists\, v_1, v_2.\ \ulcorner v' = (v_1, v_2) \urcorner \star \mathcal{V}[\![\mathsf{Ref}\ T_1]\!]_\delta(v_1) \star \mathcal{V}[\![T_2]\!]_\delta(v_2)$$

Apply wp-bind.

$$\mathcal{V}[\![T_f]\!]_\delta(v_f) \vDash \reflectbox{N}\alpha.\,\ell \mapsto\mathrm{I}_\alpha\ \mathcal{V}[\![T_1]\!]_\delta(v_\ell) \mathrel{-\!\!\star} \mathsf{wp}\,(v_f\ \ ()\ \ \ell)\,\big\{v_2.\mathsf{wp}\,(\ell, v_2)\,\big\{[\alpha]\,(\ell \mapsto v_\ell \mathrel{-\!\!\star} \mathcal{V}[\![T_1]\!]_\delta(v_\ell) \mathrel{-\!\!\star} \hat{P}(\ell, v_2))\big\}\big\}$$
$$\text{where } \hat{P}(v') = \exists\, v_1, v_2.\ \ulcorner v' = (v_1, v_2) \urcorner \star \mathcal{V}[\![\mathsf{Ref}\ T_1]\!]_\delta(v_1) \star \mathcal{V}[\![T_2]\!]_\delta(v_2)$$

Choose $v_1 \coloneqq \ell, v_2 \coloneqq v_2$.

$$\begin{aligned}&\mathcal{V}\llbracket T_f \rrbracket_\delta(v_f) \vDash \text{И}\alpha.\, \ell \mapsto\!\mathrm{I}_\alpha\, \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_\ell) \mathrel{-\!\!*} \mathsf{wp}\,(v_f\ ()\ \ell)\,\{v_2.\mathsf{wp}\,(\ell, v_2)\,\{[\alpha]\,(\ell \mapsto v_\ell \mathrel{-\!\!*} \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_\ell) \mathrel{-\!\!*} Q)\}\}\\ &\text{where } Q = \mathcal{V}\llbracket \mathsf{Ref}\ T_1 \rrbracket_\delta(\ell) \star \mathcal{V}\llbracket T_2 \rrbracket_\delta(v_2)\end{aligned}$$

Unfold $\mathcal{V}\llbracket \mathsf{Ref}\ T_1 \rrbracket_\delta$.

$$\begin{aligned}&\mathcal{V}\llbracket T_f \rrbracket_\delta(v_f) \vDash \text{И}\alpha.\, \ell \mapsto\!\mathrm{I}_\alpha\, \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_\ell) \mathrel{-\!\!*} \mathsf{wp}\,(v_f\ ()\ \ell)\,\big\{v_2.\mathsf{wp}\,(\ell, v_2)\,\big\{[\alpha]\,(\ell \mapsto v_\ell \mathrel{-\!\!*} \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_\ell) \mathrel{-\!\!*} \hat{Q})\big\}\big\}\\ &\text{where } \hat{Q}(\ell, v_2) = (\exists\, v_\ell.\ \ell \mapsto v_\ell \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_\ell)) \star \mathcal{V}\llbracket T_2 \rrbracket_\delta(v_2)\end{aligned}$$

Choose $v_\ell \coloneqq v_\ell$ in $\hat{Q}$.
Cancel $\ell \mapsto v_\ell, \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_\ell)$.

$$\mathcal{V}\llbracket T_f \rrbracket_\delta(v_f) \vDash \text{И}\alpha.\, \ell \mapsto\!\mathrm{I}_\alpha\, \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_\ell) \mathrel{-\!\!*} \mathsf{wp}\,(v_f\ ()\ \ell)\,\{v_2.\mathsf{wp}\,(\ell, v_2)\,\{(\ell, v_2).\ [\alpha]\,\mathcal{V}\llbracket T_2 \rrbracket_\delta(v_2)\}\}$$

Apply WP-VAL.

$$\mathcal{V}\llbracket T_f \rrbracket_\delta(v_f) \vDash \text{И}\alpha.\, \ell \mapsto\!\mathrm{I}_\alpha\, \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_\ell) \mathrel{-\!\!*} \mathsf{wp}\,(v_f\ ()\ \ell)\,\{v_2.[\alpha]\,\mathcal{V}\llbracket T_2 \rrbracket_\delta(v_2)\}$$

Unfold T_f.

$$\mathcal{V}\big\llbracket \forall\, 'a \sqsubset \bigsqcap\Delta.\ \mathsf{Imm}\ 'a\ T_1 \multimap [\,'a\,]\,T_2 \big\rrbracket_\delta(v_f) \vDash \text{И}\alpha.\, \ell \mapsto\!\mathrm{I}_\alpha\, \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_\ell) \mathrel{-\!\!*} \mathsf{wp}\,(v_f\ ()\ \ell)\,\{v_2.[\alpha]\,\mathcal{V}\llbracket T_2 \rrbracket_\delta(v_2)\}$$

Apply $\text{И}R$ on LHS.
Fix $\alpha \sqsubset \bigsqcap\delta$ by И-MONO.
Apply $\mathrel{-\!\!*}$R.

$$\mathcal{V}\big\llbracket \forall\, 'a \sqsubset \bigsqcap\Delta.\ \mathsf{Imm}\ 'a\ T_1 \multimap [\,'a\,]\,T_2 \big\rrbracket_\delta(v_f) \star \ell \mapsto\!\mathrm{I}_\alpha\, \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_\ell) \vDash \mathsf{wp}\,(v_f\ ()\ \ell)\,\{v_2.[\alpha]\,\mathcal{V}\llbracket T_2 \rrbracket_\delta(v_2)\}$$

Fold and simplify, using that $'b$ does not occur free in T_1 or T_2.

$$\mathcal{V}\big\llbracket \forall\, 'a \sqsubset \bigsqcap\Delta.\ \mathsf{Imm}\ 'a\ T_1 \multimap [\,'a\,]\,T_2 \big\rrbracket_\delta(v_f) \star \mathcal{V}\llbracket \mathsf{Imm}\ 'a\ T_1 \rrbracket_{\delta['a \mapsto \alpha]}(\ell) \vDash \mathsf{wp}\,(v_f\ ()\ \ell)\,\Big\{v_2.\mathcal{V}\llbracket [\,'a\,]\,T_2 \rrbracket_{\delta['a \mapsto \alpha]}(v_2)\Big\}$$

Follows from $\forall\, E$-COMPAT and $\multimap E$-COMPAT. □

Lemma 6.173 (withbor-COMPAT2)**.** If $\Delta \vdash T_1 \sqsupset @b$ then

$$\Delta \vDash \mathsf{withbor} : \mathsf{Ref}\ T_1 \multimap (\forall\, 'a \sqsubset \bigsqcap\Delta.\ \mathsf{Mut}\ 'a\ T_1 \multimap [\,'a\,]\,T_2) \multimap \mathsf{Ref}\ T_1 \otimes T_2$$

Proof. Let $T_f = (\forall\, 'a \sqsubset \bigsqcap\Delta.\ \mathsf{Mut}\ 'a\ T_1 \multimap [\,'a\,]\,T_2)$. Follow the proof of theorem 6.172 up to the point where IMMFRAME is applied. The proof state is:

$$\ell \mapsto v_\ell \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_\ell) \star \mathcal{V}\llbracket T_f \rrbracket_\delta(v_f) \vDash \mathsf{wp}\,(\ell, v_f\ ()\ \ell)\,\{\mathcal{V}\llbracket \mathsf{Ref}\ T_1 \otimes T_2 \rrbracket_\delta\}$$

Since $\Delta \vdash T_1 \sqsupset @b$, theorem 6.60 gives $\mathcal{V}\llbracket T_1 \rrbracket_\delta \vDash [@b\delta]\,\mathcal{V}\llbracket T_1 \rrbracket_\delta$, so MUTFRAME applies.

$$\mathcal{V}\llbracket T_f \rrbracket_\delta(v_f) \vDash \text{И}\alpha.\, \ell \mapsto\!\mathrm{M}_\alpha\, \mathcal{V}\llbracket T_1 \rrbracket_\delta \mathrel{-\!\!*} \mathsf{wp}\,(\ell, v_f\ ()\ \ell)\,\{[\alpha]\,\forall\, v'.\ \ell \mapsto v' \mathrel{-\!\!*} \mathcal{V}\llbracket T_1 \rrbracket_\delta(v') \mathrel{-\!\!*} \mathcal{V}\llbracket \mathsf{Ref}\ T_1 \otimes T_2 \rrbracket_\delta\}$$

Apply WP-BIND, WP-RET.

$$\mathcal{V}\llbracket T_f \rrbracket_\delta(v_f) \vDash \text{И}\alpha.\, \ell \mapsto\!\mathrm{M}_\alpha\, \mathcal{V}\llbracket T_1 \rrbracket_\delta \mathrel{-\!\!*} \mathsf{wp}\,(v_f\ ()\ \ell)\,\{v''.[\alpha]\,\forall\, v'.\ \ell \mapsto v' \mathrel{-\!\!*} \mathcal{V}\llbracket T_1 \rrbracket_\delta(v') \mathrel{-\!\!*} \mathcal{V}\llbracket \mathsf{Ref}\ T_1 \otimes T_2 \rrbracket_\delta(\ell, v'')\}$$

Unfold $\mathcal{V}\llbracket \mathsf{Ref}\ T_1 \otimes T_2 \rrbracket_\delta$ and simplify.

$$\begin{aligned}&\mathcal{V}\llbracket T_f \rrbracket_\delta(v_f) \vDash \text{И}\alpha.\, \ell \mapsto\!\mathrm{M}_\alpha\, \mathcal{V}\llbracket T_1 \rrbracket_\delta \mathrel{-\!\!*} \mathsf{wp}\,(v_f\ ()\ \ell)\,\{v''.[\alpha]\,\forall\, v'.\ \ell \mapsto v' \mathrel{-\!\!*} \mathcal{V}\llbracket T_1 \rrbracket_\delta(v') \mathrel{-\!\!*} P(v', v'')\}\\ &\text{where } P(v', v'') = \exists\, v_1, v_2.\ \ulcorner(\ell, v'') = (v_1, v_2)\urcorner \star (\exists\, v_\ell.\ \ell \mapsto v_\ell \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_\ell)) \star \mathcal{V}\llbracket T_2 \rrbracket_\delta(v'')\end{aligned}$$

Choose $v_1 \coloneqq \ell, v_2 \coloneqq v'', v_\ell \coloneqq v'$.

$$\begin{aligned}&\mathcal{V}\llbracket T_f \rrbracket_\delta(v_f) \vDash \text{И}\alpha.\, \ell \mapsto\!\mathrm{M}_\alpha\, \mathcal{V}\llbracket T_1 \rrbracket_\delta \mathrel{-\!\!*} \mathsf{wp}\,(v_f\ ()\ \ell)\,\{v''.[\alpha]\,\forall\, v'.\ \ell \mapsto v' \mathrel{-\!\!*} \mathcal{V}\llbracket T_1 \rrbracket_\delta(v') \mathrel{-\!\!*} P(v', v'')\}\\ &\text{where } P(v', v'') = \ell \mapsto v' \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v') \star \mathcal{V}\llbracket T_2 \rrbracket_\delta(v'')\end{aligned}$$

Cancel $\ell \mapsto v', \mathcal{V}\llbracket T_1 \rrbracket_\delta(v')$.

$$\mathcal{V}\llbracket T_f \rrbracket_\delta(v_f) \vDash \text{И}\alpha.\, \ell \mapsto\!\mathrm{M}_\alpha\, \mathcal{V}\llbracket T_1 \rrbracket_\delta \mathrel{-\!\!*} \mathsf{wp}\,(v_f\ ()\ \ell)\,\{v''.[\alpha]\,\mathcal{V}\llbracket T_2 \rrbracket_\delta(v'')\}$$

The remainder of the proof follows the proof of theorem 6.172, from the step "Unfold T_f" onwards. □

Lemma 6.174 ($\mathsf{withbor}$-COMPAT3)**.** $\Delta \vDash \mathsf{withbor} : \mathsf{Mut}\ @a\ T_1 \multimap (\forall\, 'b \sqsubset \bigsqcap\Delta.\ \mathsf{Mut}\ 'b\ T_1 \multimap ['b]\, T_2) \multimap \mathsf{Mut}\ @a\ T_1 \otimes T_2$

Proof. Let $T_f = (\forall\, 'b \sqsubset \bigsqcap\Delta.\ \mathsf{Mut}\ 'b\ T_1 \multimap ['b]\, T_2)$. Fix $\delta \in [\![\Delta]\!]$.

$$\vDash \mathcal{V}[\![\mathsf{Mut}\ @a\ T_1 \multimap T_f \multimap \mathsf{Mut}\ @a\ T_1 \otimes T_2]\!]_\delta(\mathsf{withbor})$$

Apply WP-VAL,WP$\multimap$ and fix v, v_f.

$$\mathcal{V}[\![\mathsf{Mut}\ @a\ T_1]\!]_\delta(v) \star \mathcal{V}[\![T_f]\!]_\delta(v_f) \vDash \mathsf{wp}\,(v, v_f\ \ ()\ v)\,\{\mathcal{V}[\![\mathsf{Mut}\ @a\ T_1 \otimes T_2]\!]_\delta\}$$

Unfold and let $\alpha \coloneqq @a\delta$.

$$\exists\, \ell.\ulcorner v = \ell \urcorner \star \ell \mapsto\mathrm{M}_\alpha\ \mathcal{V}[\![T_1]\!]_\delta \star \mathcal{V}[\![T_f]\!](v_f) \vDash \mathsf{wp}\,(v, v_f\ \ ()\ v)\,\{\mathcal{V}[\![\mathsf{Mut}\ @a\ T_1 \otimes T_2]\!]_\delta\}$$

Substitute.

$$\ell \mapsto\mathrm{M}_\alpha\ \mathcal{V}[\![T_1]\!]_\delta \star \mathcal{V}[\![T_f]\!](v_f) \vDash \mathsf{wp}\,(\ell, v_f\ \ ()\ \ell)\,\{\mathcal{V}[\![\mathsf{Mut}\ @a\ T_1 \otimes T_2]\!]_\delta\}$$

Apply ANTIFRAME.

$$\mathcal{V}[\![T_f]\!](v_f) \vDash \begin{pmatrix}\forall\, v.\, \ell \mapsto v \mathrel{-\!\!\star} \mathcal{V}[\![T_1]\!]_\delta(v) \mathrel{-\!\!\star} \\ \mathsf{wp}\,(\ell, v_f\ \ ()\ \ell)\,\{v'.\exists\, v.\, \ell \mapsto v \star \mathcal{V}[\![T_1]\!]_\delta(v) \star (\ell \mapsto\mathrm{M}_\alpha\ \mathcal{V}[\![T_1]\!]_\delta(v) \mathrel{-\!\!\star} \mathcal{V}[\![\mathsf{Mut}\ @a\ T_1 \otimes T_2]\!]_\delta)\}\end{pmatrix}$$

Apply $\forall$ R, $\mathrel{-\!\!\star}$R.

$$\begin{aligned}&\mathcal{V}[\![T_f]\!](v_f) \star \ell \mapsto v \star \mathcal{V}[\![T_1]\!]_\delta(v)\\ &\quad\vDash \mathsf{wp}\,(\ell, v_f\ \ ()\ \ell)\,\{v'.\exists\, v.\, \ell \mapsto v \star \mathcal{V}[\![T_1]\!]_\delta(v) \star (\ell \mapsto\mathrm{M}_\alpha\ \mathcal{V}[\![T_1]\!]_\delta(v) \mathrel{-\!\!\star} \mathcal{V}[\![\mathsf{Mut}\ @a\ T_1 \otimes T_2]\!]_\delta(v'))\}\end{aligned}$$

Apply WP-BIND.

$$\begin{aligned}&\mathcal{V}[\![T_f]\!](v_f) \star \ell \mapsto v \star \mathcal{V}[\![T_1]\!]_\delta(v)\\ &\quad\vDash \mathsf{wp}\,(v_f\ \ ()\ \ell)\,\{v''.\mathsf{wp}\,(\ell, v'')\,\{v'.\exists\, v.\, \ell \mapsto v \star \mathcal{V}[\![T_1]\!]_\delta(v) \star (\ell \mapsto\mathrm{M}_\alpha\ \mathcal{V}[\![T_1]\!]_\delta(v) \mathrel{-\!\!\star} \mathcal{V}[\![\mathsf{Mut}\ @a\ T_1 \otimes T_2]\!]_\delta(v'))\}\}\end{aligned}$$

Apply WP-VAL.

$$\begin{aligned}&\mathcal{V}[\![T_f]\!](v_f) \star \ell \mapsto v \star \mathcal{V}[\![T_1]\!]_\delta(v)\\ &\quad\vDash \mathsf{wp}\,(v_f\ \ ()\ \ell)\,\{v''.\exists\, v.\, \ell \mapsto v \star \mathcal{V}[\![T_1]\!]_\delta(v) \star (\ell \mapsto\mathrm{M}_\alpha\ \mathcal{V}[\![T_1]\!]_\delta(v) \mathrel{-\!\!\star} \mathcal{V}[\![\mathsf{Mut}\ @a\ T_1 \otimes T_2]\!]_\delta(\ell, v''))\}\end{aligned}$$

Simplify $\mathcal{V}[\![\mathsf{Mut}\ @a\ T_1 \otimes T_2]\!]_\delta(\ell, v'')$.

$$\begin{aligned}&\mathcal{V}[\![T_f]\!](v_f) \star \ell \mapsto v \star \mathcal{V}[\![T_1]\!]_\delta(v)\\ &\quad\vDash \mathsf{wp}\,(v_f\ \ ()\ \ell)\,\{v''.\exists\, v.\, \ell \mapsto v \star \mathcal{V}[\![T_1]\!]_\delta(v) \star (\ell \mapsto\mathrm{M}_\alpha\ \mathcal{V}[\![T_1]\!]_\delta(v) \mathrel{-\!\!\star} \ell \mapsto\mathrm{M}_\alpha\ \mathcal{V}[\![T_1]\!] \star \mathcal{V}[\![T_2]\!]_\delta(v''))\}\end{aligned}$$

Cancel $\ell \mapsto\mathrm{M}_\alpha\ \mathcal{V}[\![T_1]\!]_\delta(v)$.

$$\mathcal{V}[\![T_f]\!](v_f) \star \ell \mapsto v \star \mathcal{V}[\![T_1]\!]_\delta(v) \vDash \mathsf{wp}\,(v_f\ \ ()\ \ell)\,\{v''.\exists\, v.\, \ell \mapsto v \star \mathcal{V}[\![T_1]\!]_\delta(v) \star \mathcal{V}[\![T_2]\!]_\delta(v'')\}$$

Have $\Delta \vdash T_1 \sqsupset @a$ by well-formedness of the type $\mathsf{Mut}\ @a\ T_1$, hence $\mathcal{V}[\![T_1]\!]_\delta \vDash [\alpha]\,\mathcal{V}[\![T_1]\!]_\delta$ by theorem 6.60, so MUTFRAME applies.

$$\mathcal{V}[\![T_f]\!](v_f) \vDash \text{И}\alpha.\, \ell \mapsto\mathrm{M}_\alpha\ \mathcal{V}[\![T_1]\!]_\delta \mathrel{-\!\!\star} \mathsf{wp}\,(v_f\ \ ()\ \ell)\,\{v''.[\alpha]\,\forall\, v'.\ \ell \mapsto v' \mathrel{-\!\!\star} \mathcal{V}[\![T_1]\!]_\delta(v') \mathrel{-\!\!\star} \exists\, v.\, \ell \mapsto v \star \mathcal{V}[\![T_1]\!]_\delta(v) \star \mathcal{V}[\![T_2]\!]_\delta(v'')\}$$

In the postcondition, choose $v \coloneqq v'$ and cancel.

$$\mathcal{V}[\![T_f]\!](v_f) \vDash \text{И}\alpha.\, \ell \mapsto\mathrm{M}_\alpha\ \mathcal{V}[\![T_1]\!]_\delta \mathrel{-\!\!\star} \mathsf{wp}\,(v_f\ \ ()\ \ell)\,\{v''.[\alpha]\,\mathcal{V}[\![T_2]\!]_\delta(v'')\}$$

The remainder of the proof follows the proof of theorem 6.172, from the step "Unfold T_f" onwards. □

Lemma 6.175 ($\mathsf{withload}$-COMPAT)**.** $\Delta \vDash \mathsf{withload} : \mathsf{Imm}\ @a\ T_1 \multimap (\forall\, 'b \sqsubset \bigsqcap\Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \multimap ['b]\, T_2) \multimap T_2$

Proof. Let $\delta \in \llbracket\Delta\rrbracket$ be arbitrary. We must show

$$\vDash \mathcal{V}\left\llbracket \mathsf{Imm}\ @a\ T_1 \multimap (\forall\, 'b \sqsubset \bigsqcap\Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \multimap ['b]\, T_2) \multimap T_2 \right\rrbracket_\delta(\mathsf{withload})$$

Unfold $\mathcal{V}\llbracket\multimap\rrbracket$. Let v be arbitrary. Apply WP-$\multimap$ and WP-VAL.

$$\mathcal{V}\llbracket \mathsf{Imm}\ @a\ T_1\rrbracket_\delta(v) \vDash \mathcal{V}\left\llbracket (\forall\, 'b \sqsubset \bigsqcap\Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \multimap ['b]\, T_2) \multimap T_2 \right\rrbracket_\delta(\lambda f.f\ ()\ (\mathsf{load}\ v))$$

Unfold $\mathcal{V}\llbracket\multimap\rrbracket$. Let v_f be arbitrary. Apply WP-$\multimap$.

$$\mathcal{V}\llbracket \mathsf{Imm}\ @a\ T_1\rrbracket_\delta(v) \star \mathcal{V}\left\llbracket \forall\, 'b \sqsubset \bigsqcap\Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \multimap ['b]\, T_2 \right\rrbracket_\delta(v_f) \vDash \mathsf{wp}\,(v_f\ ()\ (\mathsf{load}\ v))\,\{\mathcal{V}\llbracket T_2\rrbracket_\delta\}$$

Unfold $\mathcal{V}\llbracket\mathsf{Imm}\rrbracket$. There exists some ℓ such that $v = \ell$.

$$\ell \mapsto\mathrm{I}_{@a\delta}\ \mathcal{V}\llbracket T_1\rrbracket_\delta \star \mathcal{V}\left\llbracket \forall\, 'b \sqsubset \bigsqcap\Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \multimap ['b]\, T_2 \right\rrbracket_\delta(v_f) \vDash \mathsf{wp}\,(v_f\ ()\ (\mathsf{load}\ \ell))\,\{\mathcal{V}\llbracket T_2\rrbracket_\delta\}$$

Apply WP-BIND.

$$\ell \mapsto\mathrm{I}_{@a\delta}\ \mathcal{V}\llbracket T_1\rrbracket_\delta \star \mathcal{V}\left\llbracket \forall\, 'b \sqsubset \bigsqcap\Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \multimap ['b]\, T_2 \right\rrbracket_\delta(v_f) \vDash \mathsf{wp}\,(\mathsf{load}\ \ell)\,\{v_\ell.\,\mathsf{wp}\,(v_f\ ()\ v_\ell)\,\{\mathcal{V}\llbracket T_2\rrbracket_\delta\}\}$$

Apply WP-LOAD-I. Let v_ℓ be arbitrary.

$$\ell \mapsto\mathrm{I}_{@a\delta}\ (v'.\ (v' = v_\ell) \star \mathcal{V}\llbracket T_1\rrbracket_\delta(v')) \star \mathcal{V}\left\llbracket \forall\, 'b \sqsubset \bigsqcap\Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \multimap ['b]\, T_2 \right\rrbracket_\delta(v_f) \vDash \mathsf{wp}\,(v_f\ ()\ v_\ell)\,\{\mathcal{V}\llbracket T_2\rrbracket_\delta\}$$

Apply $\circlearrowleft\mathcal{V}_2$.

$$\ell \mapsto\mathrm{I}_{@a\delta}\ (v'.\ (v' = v_\ell) \star \text{И}\beta.\ \circlearrowleft_\beta \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'b\ T_1\rrbracket_{\delta['b\mapsto\beta]}(v')) \star \mathcal{V}\left\llbracket \forall\, 'b \sqsubset \bigsqcap\Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \multimap ['b]\, T_2 \right\rrbracket_\delta(v_f) \vDash \mathsf{wp}\,(v_f\ ()\ v_\ell)\,\{\mathcal{V}\llbracket T_2\rrbracket_\delta\}$$

Apply theorem 6.134.

$$\ell \mapsto\mathrm{I}_{@a\delta}\ (v'.\ \text{И}\beta.\ \circlearrowleft_\beta((v' = v_\ell) \star \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'b\ T_1\rrbracket_{\delta['b\mapsto\beta]}(v'))) \star \mathcal{V}\left\llbracket \forall\, 'b \sqsubset \bigsqcap\Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \multimap ['b]\, T_2 \right\rrbracket_\delta(v_f) \vDash \mathsf{wp}\,(v_f\ ()\ v_\ell)\,\{\mathcal{V}\llbracket T_2\rrbracket_\delta\}$$

Apply theorem 6.150.

$$\mathcal{V}\left\llbracket \forall\, 'b \sqsubset \bigsqcap\Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \multimap ['b]\, T_2 \right\rrbracket_\delta(v_f) \vDash \text{И}\beta.\ \forall\, v'.v' = v_\ell \star \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'b\ T_1\rrbracket_{\delta['b\mapsto\beta]}(v') \mathrel{-\!\!\star} \mathsf{wp}\,(v_f\ ()\ v')\,\{[\beta]\,\mathcal{V}\llbracket T_2\rrbracket_\delta\}$$

Substitute v_ℓ for v'.

$$\mathcal{V}\left\llbracket \forall\, 'b \sqsubset \bigsqcap\Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \multimap ['b]\, T_2 \right\rrbracket_\delta(v_f) \vDash \text{И}\beta.\ \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'b\ T_1\rrbracket_{\delta['b\mapsto\beta]}(v_\ell) \mathrel{-\!\!\star} \mathsf{wp}\,(v_f\ ()\ v_\ell)\,\{[\beta]\,\mathcal{V}\llbracket T_2\rrbracket_\delta\}$$

Apply $\text{И}R$ on the left-hand side. By И-MONO, let $\beta \sqsubset \bigsqcap\delta$ be arbitrary. Apply $-\!\!\star$R.

$$\mathcal{V}\left\llbracket \forall\, 'b \sqsubset \bigsqcap\Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \multimap ['b]\, T_2 \right\rrbracket_\delta(v_f) \star \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'b\ T_1\rrbracket_{\delta['b\mapsto\beta]}(v') \vDash \mathsf{wp}\,(v_f\ ()\ v_\ell)\,\{[\beta]\,\mathcal{V}\llbracket T_2\rrbracket_\delta\}$$

Have $\mathcal{V}\llbracket T_2\rrbracket_\delta = \mathcal{V}\llbracket T_2\rrbracket_{\delta['b\mapsto\beta]}$ because $'b$ does not occur free in T_2.

$$\mathcal{V}\left\llbracket \forall\, 'b \sqsubset \bigsqcap\Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \multimap ['b]\, T_2 \right\rrbracket_\delta(v_f) \star \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'b\ T_1\rrbracket_{\delta['b\mapsto\beta]}(v') \vDash \mathsf{wp}\,(v_f\ ()\ v_\ell)\left\{[\beta]\,\mathcal{V}\llbracket T_2\rrbracket_{\delta['b\mapsto\beta]}\right\}$$

Fold $\mathcal{E}\llbracket-\rrbracket$.

$$\mathcal{V}\left\llbracket \forall\, 'b \sqsubset \bigsqcap\Delta.\ \underline{\mathsf{Imm}}\ 'b\ T_1 \multimap ['b]\, T_2 \right\rrbracket_\delta(v_f) \star \mathcal{V}\llbracket \underline{\mathsf{Imm}}\ 'b\ T_1\rrbracket_{\delta['b\mapsto\beta]}(v') \vDash \mathcal{E}\llbracket ['b]\, T_2\rrbracket_{\delta['b\mapsto\beta]}(v_f\ ()\ v_\ell)$$

Follows from $\forall\,E$-COMPAT and $\multimap E$-COMPAT. □

Lemma 6.176 (withswap-COMPAT). $\dfrac{}{\Delta; \varnothing \vDash \mathsf{withswap} : \mathsf{Mut}\ @a\ T_1 \multimap (T_1 \multimap T_1 \otimes T_2) \multimap \mathsf{Mut}\ @a\ T_1 \otimes T_2}\,\mathsf{withswap}$

Proof. Let $\delta \in \llbracket \Delta \rrbracket$ be arbitrary. We must show

$$\vDash \mathcal{V}\llbracket \mathsf{Mut}\ @a\ T_1 \multimap (T_1 \multimap T_1 \otimes T_2) \multimap \mathsf{Mut}\ @a\ T_1 \otimes T_2 \rrbracket_\delta(\mathsf{withswap})$$

Unfold $\mathcal{V}\llbracket \multimap \rrbracket$. Let v_1 be arbitrary.

$$\mathcal{V}\llbracket \mathsf{Mut}\ @a\ T_1 \rrbracket_\delta(v_1) \vDash \mathsf{wp}\,(\mathsf{withswap}\ v_1)\,\{\mathcal{V}\llbracket (T_1 \multimap T_2 \otimes T_2) \multimap \mathsf{Mut}\ @a\ T_1 \otimes T_2 \rrbracket_\delta\}$$

Apply wp-$\multimap$ and wp-val. Unfold $\mathcal{V}\llbracket \multimap \rrbracket$. Let v_f be arbitrary. Apply wp-$\multimap$.

$$\mathcal{V}\llbracket \mathsf{Mut}\ @a\ T_1 \rrbracket_\delta(v_1) \star \mathcal{V}\llbracket T_1 \multimap T_1 \otimes T_2 \rrbracket_\delta(v_f) \vDash \mathsf{wp}\,(\mathsf{let}\,(y,z) = v_f\ (\mathsf{load}\ v_1); \mathsf{store}\ v_1\ y; (v_1, z))\,\{\mathcal{V}\llbracket \mathsf{Mut}\ @a\ T_1 \otimes T_2 \rrbracket_\delta\}$$

Unfold $\mathcal{V}\llbracket \mathsf{Mut}\ \ \rrbracket$. There exists some ℓ such that $v_1 = \ell$.

$$\ell \mapsto\mathrm{M}_{@a\delta}\ \mathcal{V}\llbracket T_1 \rrbracket_\delta \star \mathcal{V}\llbracket T_1 \multimap T_1 \otimes T_2 \rrbracket_\delta(v_f) \vDash \mathsf{wp}\,(\mathsf{let}\,(y,z) = v_f\ (\mathsf{load}\ \ell); \mathsf{store}\ \ell\ y; (\ell, z))\,\{\mathcal{V}\llbracket \mathsf{Mut}\ @a\ T_1 \otimes T_2 \rrbracket_\delta\}$$

Apply wp-m-anti-frame. Let v_2 be arbitrary.

$$\begin{array}{l} \ell \mapsto v_2 \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_2) \star \mathcal{V}\llbracket T_1 \multimap T_1 \otimes T_2 \rrbracket_\delta(v_f) \vDash \\ \mathsf{wp}\,(\mathsf{let}\,(y,z) = v_f\ (\mathsf{load}\ \ell); \mathsf{store}\ \ell\ y; (\ell, z))\,\{\exists\, v.\ \ell \mapsto v \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v) \star (\ell \mapsto\mathrm{M}_{@a\delta}\ \mathcal{V}\llbracket T_1 \rrbracket_\delta \mathrel{-\!\!\star} \mathcal{V}\llbracket \mathsf{Mut}\ @a\ T_1 \otimes T_2 \rrbracket_\delta)\} \end{array}$$

Apply wp-bind to focus on $\mathsf{load}\ \ell$. Apply wp-load.

$$\begin{array}{l} \ell \mapsto v_2 \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_2) \star \mathcal{V}\llbracket T_1 \multimap T_1 \otimes T_2 \rrbracket_\delta(v_f) \vDash \\ \mathsf{wp}\,(\mathsf{let}\,(y,z) = v_f\ v_2; \mathsf{store}\ \ell\ y; (\ell, z))\,\{\exists\, v.\ \ell \mapsto v \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v) \star (\ell \mapsto\mathrm{M}_{@a\delta}\ \mathcal{V}\llbracket T_1 \rrbracket_\delta \mathrel{-\!\!\star} \mathcal{V}\llbracket \mathsf{Mut}\ @a\ T_1 \otimes T_2 \rrbracket_\delta)\} \end{array}$$

Instantiate $\mathcal{V}\llbracket T_1 \multimap T_1 \otimes T_2 \rrbracket_\delta(v_f)$ with $\mathcal{V}\llbracket T_1 \rrbracket_\delta(v_2)$.

$$\begin{array}{l} \ell \mapsto v_2 \star \mathsf{wp}\,(v_f\ v_2)\,\{\mathcal{V}\llbracket T_1 \otimes T_2 \rrbracket\} \vDash \\ \mathsf{wp}\,(\mathsf{let}\,(y,z) = v_f\ v_2; \mathsf{store}\ \ell\ y; (\ell, z))\,\{\exists\, v.\ \ell \mapsto v \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v) \star (\ell \mapsto\mathrm{M}_{@a\delta}\ \mathcal{V}\llbracket T_1 \rrbracket_\delta \mathrel{-\!\!\star} \mathcal{V}\llbracket \mathsf{Mut}\ @a\ T_1 \otimes T_2 \rrbracket_\delta)\} \end{array}$$

Apply wp-bind to focus on $f\ v_2$. Apply wp-mono. Unfold $\mathcal{V}\llbracket \otimes \rrbracket$ for some v_3, v_4.

$$\begin{array}{l} \ell \mapsto v_2 \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_3) \star \mathcal{V}\llbracket T_2 \rrbracket_\delta(v_4) \vDash \\ \mathsf{wp}\,(\mathsf{let}\,(y,z) = (v_3, v_4); \mathsf{store}\ \ell\ y; (\ell, z))\,\{\exists\, v.\ \ell \mapsto v \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v) \star (\ell \mapsto\mathrm{M}_{@a\delta}\ \mathcal{V}\llbracket T_1 \rrbracket_\delta \mathrel{-\!\!\star} \mathcal{V}\llbracket \mathsf{Mut}\ @a\ T_1 \otimes T_2 \rrbracket_\delta)\} \end{array}$$

Apply wp-$\otimes$.

$$\begin{array}{l} \ell \mapsto v_2 \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_3) \star \mathcal{V}\llbracket T_2 \rrbracket_\delta(v_4) \vDash \\ \mathsf{wp}\,(\mathsf{store}\ \ell\ v_3; (\ell, v_4))\,\{\exists\, v.\ \ell \mapsto v \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v) \star (\ell \mapsto\mathrm{M}_{@a\delta}\ \mathcal{V}\llbracket T_1 \rrbracket_\delta \mathrel{-\!\!\star} \mathcal{V}\llbracket \mathsf{Mut}\ @a\ T_1 \otimes T_2 \rrbracket_\delta)\} \end{array}$$

Apply wp-bind to focus on $\mathsf{store}\ \ell\ v_3$. Apply wp-store, wp-$\mathbb{1}$, and wp-val.

$$\ell \mapsto v_3 \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v_3) \star \mathcal{V}\llbracket T_2 \rrbracket_\delta(v_4) \vDash \exists\, v.\ \ell \mapsto v \star \mathcal{V}\llbracket T_1 \rrbracket_\delta(v) \star (\ell \mapsto\mathrm{M}_{@a\delta}\ \mathcal{V}\llbracket T_1 \rrbracket_\delta \mathrel{-\!\!\star} \mathcal{V}\llbracket \mathsf{Mut}\ @a\ T_1 \otimes T_2 \rrbracket_\delta((\ell, v_4)))$$

Choose $\exists\, v$ to be v_3.

$$\mathcal{V}\llbracket T_2 \rrbracket_\delta(v_4) \star \ell \mapsto\mathrm{M}_{@a\delta}\ \mathcal{V}\llbracket T_1 \rrbracket_\delta \vDash \mathcal{V}\llbracket \mathsf{Mut}\ @a\ T_1 \otimes T_2 \rrbracket_\delta((\ell, v_4))$$

This follows from the $\mathcal{V}$ definitions. □