Semantic Soundness for Language Interoperability: Technical Appendix

DANIEL PATTERSON, Northeastern University, USA
NOBLE MUSHTAK, Northeastern University, USA
ANDREW WAGNER, Northeastern University, USA
AMAL AHMED, Northeastern University, USA

We organize our investigations into case studies, to both illustrate our framework and explore various types of interoperability.

Differences with the paper. In the paper that accompanies this appendix, we simplified the presentation in two ways. First, we combined the "Affine with Dynamic Safety" and "Affine with Dynamic Safety, Efficiently" case studies, effectively eliminating the former. Second, and more significantly, we presented the logical relation for that case study, and that for "Memory Management and Polymorphism" as unary relations rather than binary. While binary relations are more powerful, allowing us to express equivalences and prove parametricity theorems in the case of the latter, these issues were not explored in the paper and thus the additional complexity served only to bog down the already quite complex technical presentation.

Contents

Authors' addresses: Daniel Patterson, Northeastern University, 440 Huntington Avenue, Boston, MA, 02115, USA, dbp@dbpmail.net; Noble Mushtak, Northeastern University, 440 Huntington Avenue, Boston, MA, 02115, USA, mushtak.n@northeastern.edu; Andrew Wagner, Northeastern University, 440 Huntington Avenue, Boston, MA, 02115, USA, wagner.andr@northeastern.edu; Amal Ahmed, Northeastern University, 440 Huntington Avenue, Boston, MA, 02115, USA, amal@ccs.neu.edu.

1 CASE STUDY: REFERENCES

In this case study, we consider mutable references.

1.1 StackLang **Target Language**

Our target language is an untyped, stack-based language.

1.1.1 Syntax.

$$
\begin{array}{rcl}
\text{Stack S} & := & \mathsf{v}, \ldots, \mathsf{v} \mid \mathsf{Fail\ c} \\
\text{Error Code c} & := & \textsc{Type} \mid \textsc{Idx} \mid \textsc{Conv} \\
\text{Instruction i} & := & \mathsf{push\ v} \mid \mathsf{add} \mid \mathsf{less?} \mid \mathsf{if0\ P\ P} \mid \mathsf{lam\ x.P} \mid \mathsf{call} \\
 & & \mid \mathsf{idx} \mid \mathsf{len} \mid \mathsf{alloc} \mid \mathsf{read} \mid \mathsf{write} \mid \mathsf{fail\ c} \\
\text{Program P} & := & \cdot \mid \mathsf{i}, \mathsf{P} \\
\text{Value v} & := & \mathsf{n} \mid \mathsf{thunk\ P} \mid \ell \mid [\mathsf{v}, \ldots]
\end{array}
$$

Note that for programs, we overload the comma symbol (,) to denote both appending an instruction (i, P) and concatenating a program (P_1, P_2), which is right associative, as usual.

1.1.2 Dynamics.

$$
\begin{array}{rcll}
\langle H; S; \mathsf{push}\ v, P\rangle & \longrightarrow & \langle H; S, v; P\rangle & (S \neq \mathsf{Fail}\ c) \\
\langle H; \mathsf{Fail}\ c; \mathsf{push}\ v, P\rangle & \longrightarrow & \langle H; \mathsf{Fail}\ c; \mathsf{fail}\ \textsc{Type}\rangle & \\
\langle H; S, n_2, n_1; \mathsf{add}, P\rangle & \longrightarrow & \langle H; S, (n_1 + n_2); P\rangle & \\
\langle H; S; \mathsf{add}, P\rangle & \longrightarrow & \langle H; S; \mathsf{fail}\ \textsc{Type}\rangle & (S \neq S', n_2, n_1) \\
\langle H; S, n_2, n_1; \mathsf{less?}, P\rangle & \longrightarrow & \langle H; S, 0; P\rangle & (n_1 < n_2) \\
\langle H; S, n_2, n_1; \mathsf{less?}, P\rangle & \longrightarrow & \langle H; S, 1; P\rangle & (n_1 \geq n_2) \\
\langle H; S; \mathsf{less?}, P\rangle & \longrightarrow & \langle H; S; \mathsf{fail}\ \textsc{Type}\rangle & (S \neq S', n_2, n_1) \\
\langle H; S, 0; \mathsf{if0}\ P_1\ P_2, P\rangle & \longrightarrow & \langle H; S; P_1, P\rangle & \\
\langle H; S, n; \mathsf{if0}\ P_1\ P_2, P\rangle & \longrightarrow & \langle H; S; P_2, P\rangle & (n \neq 0) \\
\langle H; S; \mathsf{if0}\ P_1\ P_2, P\rangle & \longrightarrow & \langle H; S; \mathsf{fail}\ \textsc{Type}\rangle & (S \neq S', n) \\
\langle H; S, v; \mathsf{lam}\ x.P_1, P_2\rangle & \longrightarrow & \langle H; S; [x \mapsto v]P_1, P_2\rangle & \\
\langle H; S; \mathsf{lam}\ x.P_1, P_2\rangle & \longrightarrow & \langle H; S; \mathsf{fail}\ \textsc{Type}\rangle & (S \neq S', v) \\
\langle H; S, \mathsf{thunk}\ P_1; \mathsf{call}, P_2\rangle & \longrightarrow & \langle H; S; P_1, P_2\rangle & \\
\langle H; S; \mathsf{call}, P_2\rangle & \longrightarrow & \langle H; S; \mathsf{fail}\ \textsc{Type}\rangle & (S \neq S', \mathsf{thunk}\ P_1) \\
\langle H; S, [v_0, \ldots, v_{n_2}], n_1; \mathsf{idx}, P\rangle & \longrightarrow & \langle H; S, v_{n_1}; P\rangle & (n_1 \in [0, n_2]) \\
\langle H; S, [v_0, \ldots, v_{n_2}], n_1; \mathsf{idx}, P\rangle & \longrightarrow & \langle H; S; \mathsf{fail}\ \textsc{Idx}\rangle & (n_1 \notin [0, n_2]) \\
\langle H; S; \mathsf{idx}, P\rangle & \longrightarrow & \langle H; S; \mathsf{fail}\ \textsc{Type}\rangle & (S \neq S', [v_0, \ldots, v_{n_2}], n_1) \\
\langle H; S, [v_0, \ldots, v_n]; \mathsf{len}, P\rangle & \longrightarrow & \langle H; S, (n + 1); P\rangle & \\
\langle H; S; \mathsf{len}, P\rangle & \longrightarrow & \langle H; S; \mathsf{fail}\ \textsc{Type}\rangle & (S \neq S', [v_0, \ldots, v_n]) \\
\langle H; S, v; \mathsf{alloc}, P\rangle & \longrightarrow & \langle H \uplus \{\ell \mapsto v\}; S, \ell; P\rangle & \\
\langle H; \cdot; \mathsf{alloc}, P\rangle & \longrightarrow & \langle H; \cdot; \mathsf{fail}\ \textsc{Type}\rangle & \\
\langle H \uplus \{\ell \mapsto v\}; S, \ell; \mathsf{read}, P\rangle & \longrightarrow & \langle H \uplus \{\ell \mapsto v\}; S, v; P\rangle & \\
\langle H; S; \mathsf{read}, P\rangle & \longrightarrow & \langle H; S; \mathsf{fail}\ \textsc{Type}\rangle & (S \neq S', \ell) \\
\langle H \uplus \{\ell \mapsto \_\}; S, \ell, v; \mathsf{write}, P\rangle & \longrightarrow & \langle H \uplus \{\ell \mapsto v\}; S; P\rangle & \\
\langle H; S; \mathsf{write}, P\rangle & \longrightarrow & \langle H; S; \mathsf{fail}\ \textsc{Type}\rangle & (S \neq S', \ell, v) \\
\langle H; S; \mathsf{fail}\ c, P\rangle & \longrightarrow & \langle H; \mathsf{Fail}\ c; \cdot\rangle &
\end{array}
$$

1.1.3 Properties. We make use of the following macros:

$$\begin{aligned}
&\mathsf{SWAP} \triangleq \mathsf{lam\ x.lam\ y.(push\ x,\ \ push\ y)}\\
&\mathsf{DROP} \triangleq \mathsf{lam\ x.()}\\
&\mathsf{DUP} \triangleq \mathsf{lam\ x.(push\ x,\ \ push\ x)}
\end{aligned}$$

Lemma 1.1 (Irreducible Configurations Have Empty Programs). *If* $\langle \mathsf{H}; \mathsf{S}; \mathsf{P}\rangle \not\twoheadrightarrow$, *then* $\mathsf{P} = \cdot$.

Proof. We will prove the contrapositive: if there exist i, P' such that $\mathsf{P} = \mathsf{i}, \mathsf{P}'$, then $\langle \mathsf{H}; \mathsf{S}; \mathsf{P}\rangle \longrightarrow \langle \mathsf{H}^*; \mathsf{S}^*; \mathsf{P}^*\rangle$. This can be demonstrated by a trivial case analysis on H, S, and i, because the dynamics of StackLang are defined so that there is a reduction rule for every possible configuration with a non-empty program. □

Lemma 1.2 (Prefix Termination). *If* $\langle \mathsf{H}; \mathsf{S}; \mathsf{P}\rangle \xrightarrow{j} \langle \mathsf{H}; \mathsf{S}'; \mathsf{P}'\rangle \not\twoheadrightarrow$ *and* $\langle \mathsf{H}; \mathsf{S}; \mathsf{P}\rangle \xrightarrow{*} \langle \mathsf{H}_\bullet; \mathsf{S}_\bullet; \mathsf{P}_\bullet, \mathsf{P}_\circ\rangle$, *then* $\langle \mathsf{H}_\bullet; \mathsf{S}_\bullet; \mathsf{P}_\bullet\rangle \xrightarrow{j_\bullet} \langle \mathsf{H}'_\bullet; \mathsf{S}'_\bullet; \cdot\rangle \not\twoheadrightarrow$ *for some* $\mathsf{H}'_\bullet$, $\mathsf{S}'_\bullet$, $j_\bullet \leq j$.

Proof. There is a constructive proof using induction, but here, we will sketch an intuitive proof by contradiction.

If $\langle \mathsf{H}_\bullet; \mathsf{S}_\bullet; \mathsf{P}_\bullet\rangle$ does not step to a stuck configuration in some $j_\bullet \leq j$ steps, then $\langle \mathsf{H}_\bullet; \mathsf{S}_\bullet; \mathsf{P}_\bullet\rangle$ runs for at least $j + 1$ steps. Because StackLang is deterministic, we can then construct the reduction sequence

$$\begin{aligned}
\langle \mathsf{H}; \mathsf{S}; \mathsf{P}\rangle &\xrightarrow{*} \langle \mathsf{H}_\bullet; \mathsf{S}_\bullet; \mathsf{P}_\bullet, \mathsf{P}_\circ\rangle\\
&\xrightarrow{j+1} \langle \mathsf{H}'_\bullet; \mathsf{S}'_\bullet; \mathsf{P}'_\bullet, \mathsf{P}_\circ\rangle\\
&\xrightarrow{*} \langle \mathsf{H}; \mathsf{S}'; \mathsf{P}'\rangle\\
&\not\twoheadrightarrow
\end{aligned}$$

which is longer than j, contradicting the premise.

Finally, if $\langle \mathsf{H}_\bullet; \mathsf{S}_\bullet; \mathsf{P}_\bullet\rangle \xrightarrow{j_\bullet} \langle \mathsf{H}'_\bullet; \mathsf{S}'_\bullet; \mathsf{P}'_\bullet\rangle \not\twoheadrightarrow$, then by Lemma 1.1, $\mathsf{P}'_\bullet = \cdot$, which suffices to finish the proof. □

Note that when applying Lemma 1.2, we sometimes leave $\mathsf{P}_\circ$ implicit.

1.2 RefHL Source Language

1.2.1 Syntax.

$$\begin{array}{lll}
\text{Type } \tau & := & \mathtt{unit} \mid \mathtt{bool} \mid \tau + \tau \mid \tau \times \tau \mid \tau \rightarrow \tau \mid \mathtt{ref}\ \tau\\
\text{Expression } \mathtt{e} & := & \mathtt{()} \mid \mathtt{true} \mid \mathtt{false} \mid \mathtt{x} \mid \mathtt{inl\ e} \mid \mathtt{inr\ e} \mid \mathtt{(e, e)} \mid \mathtt{fst\ e} \mid \mathtt{snd\ e} \mid \mathtt{if\ e\ e\ e}\\
& & \mid \mathtt{match\ e\ x\{e\}\ y\{e\}} \mid \lambda \mathtt{x} : \tau.\mathtt{e} \mid \mathtt{e\ e} \mid \mathtt{ref\ e} \mid \mathtt{!e} \mid \mathtt{e := e} \mid (\!|\mathtt{e}|\!)_\tau
\end{array}$$

1.2.2 *Statics.* $\boxed{\Gamma;\Gamma \vdash \mathsf{e} : \tau}$

$$\frac{}{\Gamma;\Gamma \vdash () : \mathsf{unit}} \qquad \frac{}{\Gamma;\Gamma \vdash \mathsf{true} : \mathsf{bool}} \qquad \frac{}{\Gamma;\Gamma \vdash \mathsf{false} : \mathsf{bool}} \qquad \frac{\mathsf{x} : \tau \in \Gamma}{\Gamma;\Gamma \vdash \mathsf{x} : \tau}$$

$$\frac{\Gamma;\Gamma \vdash \mathsf{e} : \tau_1 \qquad \vdash \tau_2}{\Gamma;\Gamma \vdash \mathsf{inl}\ \mathsf{e} : \tau_1 + \tau_2} \qquad \frac{\Gamma;\Gamma \vdash \mathsf{e} : \tau_2 \qquad \vdash \tau_1}{\Gamma;\Gamma \vdash \mathsf{inr}\ \mathsf{e} : \tau_1 + \tau_2} \qquad \frac{\Gamma;\Gamma \vdash \mathsf{e} : \mathsf{bool} \qquad \Gamma;\Gamma \vdash \mathsf{e}_1 : \tau \qquad \Gamma;\Gamma \vdash \mathsf{e}_2 : \tau}{\Gamma;\Gamma \vdash \mathsf{if}\ \mathsf{e}\ \mathsf{e}_1\ \mathsf{e}_2 : \tau}$$

$$\frac{\Gamma;\Gamma \vdash \mathsf{e} : \tau_1 + \tau_2 \qquad \Gamma;\Gamma, x : \tau_1 \vdash \mathsf{e}_1 : \tau \qquad \Gamma;\Gamma, y : \tau_2 \vdash \mathsf{e}_2 : \tau}{\Gamma;\Gamma \vdash \mathsf{match}\ \mathsf{e}\ \mathsf{x}\{\mathsf{e}_1\}\ \mathsf{y}\{\mathsf{e}_2\} : \tau} \qquad \frac{\Gamma;\Gamma, x : \tau_1 \vdash \mathsf{e} : \tau_2}{\Gamma;\Gamma \vdash \lambda \mathsf{x}{:}\tau_1.\mathsf{e} : \tau_1 \rightarrow \tau_2}$$

$$\frac{\Gamma;\Gamma \vdash \mathsf{e} : \tau_1 \rightarrow \tau_2 \qquad \Gamma;\Gamma \vdash \mathsf{e}' : \tau_1}{\Gamma;\Gamma \vdash \mathsf{e}\ \mathsf{e}' : \tau_2} \qquad \frac{\Gamma;\Gamma \vdash \mathsf{e}_1 : \tau_1 \qquad \Gamma;\Gamma \vdash \mathsf{e}_2 : \tau_2}{\Gamma;\Gamma \vdash (\mathsf{e}_1, \mathsf{e}_2) : \tau_1 \times \tau_2} \qquad \frac{\Gamma;\Gamma \vdash \mathsf{e} : \tau_1 \times \tau_1}{\Gamma;\Gamma \vdash \mathsf{fst}\ \mathsf{e} : \tau_1}$$

$$\frac{\Gamma;\Gamma \vdash \mathsf{e} : \tau_1 \times \tau_1}{\Gamma;\Gamma \vdash \mathsf{snd}\ \mathsf{e} : \tau_2} \qquad \frac{\Gamma;\Gamma \vdash \mathsf{e} : \tau}{\Gamma;\Gamma \vdash \mathsf{ref}\ \mathsf{e} : \mathsf{ref}\ \tau} \qquad \frac{\Gamma;\Gamma \vdash \mathsf{e} : \mathsf{ref}\ \tau}{\Gamma;\Gamma \vdash \,!\mathsf{e} : \tau}$$

$$\frac{\Gamma;\Gamma \vdash \mathsf{e}_1 : \mathsf{ref}\ \tau \qquad \Gamma;\Gamma \vdash \mathsf{e}_2 : \tau}{\Gamma;\Gamma \vdash \mathsf{e}_1 := \mathsf{e}_2 : \mathsf{unit}} \qquad \frac{\Gamma;\Gamma \vdash \mathsf{e} : \tau \qquad \tau \sim \tau}{\Gamma;\Gamma \vdash (\!|\mathsf{e}|\!)_\tau : \tau}$$

1.2.3 *Compiler.* $\boxed{\mathsf{e} \rightsquigarrow \mathsf{P}}$

$$\begin{array}{lcl}
() & \rightsquigarrow & \text{push } 0 \\
\mathsf{true} & \rightsquigarrow & \text{push } 0 \\
\mathsf{false} & \rightsquigarrow & \text{push } 1 \\
\mathsf{x} & \rightsquigarrow & \text{push x} \\
\mathsf{inl}\ \mathsf{e} & \rightsquigarrow & \mathsf{e}^+, \text{lam x.(push } [0, \text{x}]) \\
\mathsf{inr}\ \mathsf{e} & \rightsquigarrow & \mathsf{e}^+, \text{lam x.(push } [1, \text{x}]) \\
\mathsf{if}\ \mathsf{e}\ \mathsf{e}_1\ \mathsf{e}_2 & \rightsquigarrow & \mathsf{e}^+, \text{if0 } {\mathsf{e}_1}^+\ {\mathsf{e}_2}^+ \\
\mathsf{match}\ \mathsf{e}\ \mathsf{x}\{\mathsf{e}_1\}\ \mathsf{y}\{\mathsf{e}_2\} & \rightsquigarrow & \mathsf{e}^+, \text{DUP, push 1, idx, SWAP, push 0, idx,} \\
 & & \quad \text{if0 (lam x.}{\mathsf{e}_1}^+\text{) (lam y.}{\mathsf{e}_2}^+\text{)} \\
(\mathsf{e}_1, \mathsf{e}_2) & \rightsquigarrow & {\mathsf{e}_1}^+, {\mathsf{e}_2}^+, \text{lam x}_2\text{.lam x}_1\text{.(push } [\text{x}_1, \text{x}_2]) \\
\mathsf{fst}\ \mathsf{e} & \rightsquigarrow & \mathsf{e}^+, \text{push 0, idx} \\
\mathsf{snd}\ \mathsf{e} & \rightsquigarrow & \mathsf{e}^+, \text{push 1, idx} \\
\lambda \mathsf{x} : \tau.\mathsf{e} & \rightsquigarrow & \text{push (thunk lam x.}\mathsf{e}^+) \\
\mathsf{e}_1\ \mathsf{e}_2 & \rightsquigarrow & {\mathsf{e}_1}^+, {\mathsf{e}_2}^+, \text{SWAP, call} \\
\mathsf{ref}\ \mathsf{e} & \rightsquigarrow & \mathsf{e}^+, \text{alloc} \\
!\mathsf{e} & \rightsquigarrow & \mathsf{e}^+, \text{read} \\
\mathsf{e}_1 := \mathsf{e}_2 & \rightsquigarrow & {\mathsf{e}_1}^+, {\mathsf{e}_2}^+, \text{write, push } 0 \\
(\!|\mathsf{e}|\!)_\tau & \rightsquigarrow & \mathsf{e}^+, C_{\tau \mapsto \tau}
\end{array}$$

1.3 RefLL Source Language

1.3.1 *Syntax.*

$$\begin{array}{lcl}
\text{Value Type } \tau & ::= & \text{int} \mid [\tau] \mid \tau \rightarrow \tau \mid \text{ref } \tau \\
\text{Expression } \text{e} & ::= & \text{n} \mid \text{x} \mid [\text{e}, \ldots] \mid \text{e}[\text{e}] \mid \lambda \text{x} : \tau.\text{e} \mid \text{e e} \mid \text{e} + \text{e} \mid \text{if0 e e e} \mid \text{ref e} \mid !\text{e} \mid \text{e} := \text{e} \mid (\!|\text{e}|\!)_\tau
\end{array}$$

1.3.2 *Statics.* $\boxed{\Gamma; \Gamma \vdash \mathrm{e} : \tau}$

$$\frac{}{\Gamma; \Gamma \vdash \mathrm{n} : \mathrm{int}} \qquad \frac{\Gamma; \Gamma \vdash \mathrm{e}_1 : \mathrm{int} \qquad \Gamma; \Gamma \vdash \mathrm{e}_2 : \mathrm{int}}{\Gamma; \Gamma \vdash \mathrm{e}_1 + \mathrm{e}_2 : \mathrm{int}} \qquad \frac{\mathrm{x} : \tau \in \Gamma}{\Gamma; \Gamma \vdash \mathrm{x} : \tau}$$

$$\frac{\Gamma; \Gamma \vdash \mathrm{e}_1 : \tau \qquad \ldots \qquad \Gamma; \Gamma \vdash \mathrm{e}_n : \tau}{\Gamma; \Gamma \vdash [\mathrm{e}_1, \ldots, \mathrm{e}_n] : [\tau]} \qquad \frac{\Gamma; \Gamma \vdash \mathrm{e}_1 : [\tau] \qquad \Gamma; \Gamma \vdash \mathrm{e}_2 : \mathrm{int}}{\Gamma; \Gamma \vdash \mathrm{e}_1[\mathrm{e}_2] : \tau}$$

$$\frac{\Gamma; \Gamma, \mathrm{x} : \tau_1 \vdash \mathrm{e} : \tau_2}{\Gamma; \Gamma \vdash \lambda \mathrm{x}{:}\tau_1.\mathrm{e} : \tau_1 \rightarrow \tau_2} \qquad \frac{\Gamma; \Gamma \vdash \mathrm{e} : \tau_1 \rightarrow \tau_2 \qquad \Gamma; \Gamma \vdash \mathrm{e}' : \tau_1}{\Gamma; \Gamma \vdash \mathrm{e}\ \mathrm{e}' : \tau_2}$$

$$\frac{\Gamma; \Gamma \vdash \mathrm{e} : \mathrm{int} \qquad \Gamma; \Gamma \vdash \mathrm{e}_1 : \tau \qquad \Gamma; \Gamma \vdash \mathrm{e}_2 : \tau}{\Gamma; \Gamma \vdash \mathrm{if0}\ \mathrm{e}\ \mathrm{e}_1\ \mathrm{e}_2 : \tau} \qquad \frac{\Gamma; \Gamma \vdash \mathrm{e} : \tau}{\Gamma; \Gamma \vdash \mathrm{ref}\ \mathrm{e} : \mathrm{ref}\ \tau} \qquad \frac{\Gamma; \Gamma \vdash \mathrm{e} : \mathrm{ref}\ \tau}{\Gamma; \Gamma \vdash !\mathrm{e} : \tau}$$

$$\frac{\Gamma; \Gamma \vdash \mathrm{e}_1 : \mathrm{ref}\ \tau \qquad \Gamma; \Gamma \vdash \mathrm{e}_2 : \tau}{\Gamma; \Gamma \vdash \mathrm{e}_1 := \mathrm{e}_2 : \mathrm{unit}} \qquad \frac{\Gamma; \Gamma \vdash \mathrm{e} : \tau \qquad \tau \sim \tau}{\Gamma; \Gamma \vdash (\!|\mathrm{e}|\!)_\tau}$$

1.3.3 *Compiler.* $\boxed{\mathrm{e} \rightsquigarrow \mathrm{P}}$

$$\begin{array}{lcl}
\mathrm{n} & \rightsquigarrow & \mathrm{push}\ \mathrm{n} \\
\mathrm{x} & \rightsquigarrow & \mathrm{push}\ \mathrm{x} \\
[\mathrm{e}_1, \ldots, \mathrm{e}_n] & \rightsquigarrow & \mathrm{e}_1{}^+, \ldots, \mathrm{e}_n{}^+, \mathrm{lam}\ \mathrm{x}_n. \ldots \mathrm{lam}\ \mathrm{x}_1.(\mathrm{push}\ [\mathrm{x}_1, \ldots, \mathrm{x}_n]) \\
\mathrm{e}_1[\mathrm{e}_2] & \rightsquigarrow & \mathrm{e}_1{}^+, \mathrm{e}_2{}^+, \mathrm{idx} \\
\mathrm{if0}\ \mathrm{e}\ \mathrm{e}_1\ \mathrm{e}_2 & \rightsquigarrow & \mathrm{e}^+, \mathrm{if0}\ \mathrm{e}_1{}^+\ \mathrm{e}_2{}^+ \\
\lambda \mathrm{x} : \tau.\mathrm{e} & \rightsquigarrow & \mathrm{push}\ (\mathrm{thunk}\ \mathrm{lam}\ \mathrm{x}.\mathrm{e}^+) \\
\mathrm{e}_1\ \mathrm{e}_2 & \rightsquigarrow & \mathrm{e}_1{}^+, \mathrm{e}_2{}^+, \mathrm{SWAP}, \mathrm{call} \\
\mathrm{e}_1 + \mathrm{e}_2 & \rightsquigarrow & \mathrm{e}_1{}^+, \mathrm{e}_2{}^+, \mathrm{add} \\
\mathrm{ref}\ \mathrm{e} & \rightsquigarrow & \mathrm{e}^+, \mathrm{alloc} \\
!\mathrm{e} & \rightsquigarrow & \mathrm{e}^+, \mathrm{read} \\
\mathrm{e}_1 := \mathrm{e}_2 & \rightsquigarrow & \mathrm{e}_1{}^+, \mathrm{e}_2{}^+, \mathrm{write}, \mathrm{push}\ 0 \\
(\!|\mathrm{e}|\!)_\tau & \rightsquigarrow & \mathrm{e}^+, C_{\tau \mapsto \tau}
\end{array}$$

1.4 Logical Relation

1.4.1 *Worlds.*

$$World_n = \{(k, \Psi) \mid k < n \wedge \Psi \subset HeapTy_k\}$$

$$World = \bigcup_n World_n$$

$$HeapTy_n = \{\ell \mapsto Typ_n, \ldots\}$$

$$AtomVal_n = \{(W, \mathrm{v}) \mid W \in World_n\}$$

$$
\begin{aligned}
&Typ_n = \{R \in 2^{AtomVal_n} \mid \forall (W, \mathrm{v}) \in R.\, \forall W'.\ W \sqsubseteq W' \implies (W', \mathrm{v}) \in R\}\\
&Typ = \textstyle\bigcup_n Typ_n
\end{aligned}
$$

$$\lfloor R \rfloor_j = \{(W, \mathrm{v}) \mid (W, \mathrm{v}) \in R \wedge W.k < j\}$$

$$\lfloor \Psi \rfloor_j = \{\ell \mapsto \lfloor R \rfloor_j \mid \ell \mapsto R \in \Psi\}$$

$$(k, \Psi) \sqsubseteq (j, \Psi') \triangleq \begin{array}{l} j \leq k \\ \wedge\ \forall \ell \in \mathrm{dom}(\Psi).\lfloor \Psi(\ell) \rfloor_j = \lfloor \Psi'(\ell) \rfloor_j \end{array}$$

$$W_1 \sqsubset W_2 \triangleq W_1.k > W_2.k \wedge W_1 \sqsubseteq W_2$$

$$\mathsf{H} = \{\ell \mapsto v\}$$

$$\mathsf{H} : W \triangleq\ (\forall \ell \mapsto R \in W.\Psi.\ (\triangleright W, \mathsf{H}(\ell)) \in R)$$

$$\triangleright(k, \Psi) \triangleq (k-1, \lfloor \Psi \rfloor_{k-1})$$

1.4.2 Expression Relation.

$$
\begin{aligned}
\mathcal{E}[\![\tau]\!] = \{(W, P) \mid\ & \forall \mathsf{H}{:}W, \mathsf{S}, \mathsf{H}', \mathsf{S}', j < W.k.\ \langle \mathsf{H}; \mathsf{S}; P\rangle \xrightarrow{j} \langle \mathsf{H}'; \mathsf{S}'; \cdot \rangle\\
&\implies (\mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \textsc{OkErr}) \vee \exists \mathrm{v}, W' \sqsupseteq W.\ \big(\mathsf{S}' = \mathsf{S}, \mathrm{v} \wedge \mathsf{H}' : W' \wedge (W', \mathrm{v}) \in \mathcal{V}[\![\tau]\!]\big)\}
\end{aligned}
$$

where $\textsc{OkErr} \triangleq \{\textsc{Conv}, \textsc{Idx}\}$

1.4.3 Value Relation.

$$
\begin{array}{lcl}
\mathcal{V}[\![\mathtt{unit}]\!] & = & \{(W, 0)\}\\
\mathcal{V}[\![\mathtt{bool}]\!] & = & \{(W, \mathrm{n})\}\\
\mathcal{V}[\![\tau_1 \times \tau_2]\!] & = & \{(W, [\mathrm{v}_1, \mathrm{v}_2]) \mid (W, \mathrm{v}_1) \in \mathcal{V}[\![\tau_1]\!] \wedge (W, \mathrm{v}_2) \in \mathcal{V}[\![\tau_2]\!]\}\\
\mathcal{V}[\![\tau_1 + \tau_2]\!] & = & \{(W, [0, \mathrm{v}]) \mid (W, \mathrm{v}) \in \mathcal{V}[\![\tau_1]\!]\}\\
& & \ \cup \{(W, [1, \mathrm{v}]) \mid (W, \mathrm{v}) \in \mathcal{V}[\![\tau_2]\!]\}\\
\mathcal{V}[\![\tau_1 \rightarrow \tau_2]\!] & = & \{(W, \mathsf{thunk\ lam\ x.P}) \mid \forall \mathrm{v}, W' \sqsupset W.\ (W', \mathrm{v}) \in \mathcal{V}[\![\tau_1]\!]\\
& & \implies (W', [\mathrm{x} \mapsto \mathrm{v}]\mathrm{P}) \in \mathcal{E}[\![\tau_2]\!]\}\\
\mathcal{V}[\![\mathtt{ref}\ \tau]\!] & = & \{(W, \ell) \mid W.\Psi(\ell) = \lfloor \mathcal{V}[\![\tau]\!] \rfloor_{W.k}\}\\
\\
\mathcal{V}[\![\mathrm{int}]\!] & = & \{(W, \mathrm{n})\}\\
\mathcal{V}[\![[\tau]]\!] & = & \{(W, [\mathrm{v}_1, \ldots, \mathrm{v}_n]) \mid (W, \mathrm{v}_i) \in \mathcal{V}[\![\tau]\!]\}\\
\mathcal{V}[\![\tau_1 \rightarrow \tau_2]\!] & = & \{(W, \mathsf{thunk\ lam\ x.P}) \mid \forall \mathrm{v}, W' \sqsupset W.\ (W', \mathrm{v}) \in \mathcal{V}[\![\tau_1]\!]\\
& & \implies (W', [\mathrm{x} \mapsto \mathrm{v}]\mathrm{P}) \in \mathcal{E}[\![\tau_2]\!]\}\\
\mathcal{V}[\![\mathrm{ref}\ \tau]\!] & = & \{(W, \ell) \mid W.\Psi(\ell) = \lfloor \mathcal{V}[\![\tau]\!] \rfloor_{W.k}\}
\end{array}
$$

1.4.4 *Extending to Open Terms.*

$$
\begin{aligned}
\mathcal{G}\llbracket \cdot \rrbracket_\rho &= \{(W, \cdot) \mid W \in \mathit{World}\} \\
\mathcal{G}\llbracket \Gamma, x : \tau \rrbracket &= \{(W, \gamma[\mathrm{x} \mapsto \mathrm{v}]) \mid (W, \mathrm{v}) \in \mathcal{V}\llbracket \tau \rrbracket \wedge (W, \gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket\} \\
\mathcal{G}\llbracket \Gamma, \mathrm{x} : \tau \rrbracket &= \{(W, \gamma[\mathrm{x} \mapsto \mathrm{v}]) \mid (W, \mathrm{v}) \in \mathcal{V}\llbracket \tau \rrbracket \wedge (W, \gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket\}
\end{aligned}
$$

$$\llbracket \Gamma; \Gamma \vdash \mathrm{e} : \tau \rrbracket \equiv \forall W\, \gamma_\Gamma\, \gamma_\Gamma\, .(W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket \implies (W, \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathrm{e}^+))) \in \mathcal{E}\llbracket \tau \rrbracket$$

$$\llbracket \Gamma; \Gamma \vdash \mathrm{e} : \tau \rrbracket \equiv \forall W\, \gamma_\Gamma\, \gamma_\Gamma\, .(W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket \implies (W, \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathrm{e}^+))) \in \mathcal{E}\llbracket \tau \rrbracket$$

1.5 Convertibility

$$\frac{}{\mathrm{C}_{\mathtt{bool} \mapsto \mathrm{int}}, \mathrm{C}_{\mathrm{int} \mapsto \mathtt{bool}} : \mathtt{bool} \sim \mathrm{int}} \qquad \frac{}{\mathrm{C}_{\mathtt{ref\ bool} \mapsto \mathrm{ref\ int}}, \mathrm{C}_{\mathrm{ref\ int} \mapsto \mathtt{ref\ bool}} : \mathtt{ref\ bool} \sim \mathrm{ref\ int}}$$

$$\frac{\mathrm{C}_{\tau_1 \mapsto \tau}, \mathrm{C}_{\tau \mapsto \tau_1} : \tau_1 \sim \tau \qquad \mathrm{C}_{\tau_2 \mapsto \tau}, \mathrm{C}_{\tau \mapsto \tau_2} : \tau_2 \sim \tau}{\mathrm{C}_{\tau_1 \times \tau_2 \mapsto [\tau]}, \mathrm{C}_{[\tau] \mapsto \tau_1 \times \tau_2} : \tau_1 \times \tau_2 \sim [\tau]}$$

$$\frac{\mathrm{C}_{\tau_1 \mapsto \mathrm{int}}, \mathrm{C}_{\mathrm{int} \mapsto \tau_1} : \tau_1 \sim \mathrm{int} \qquad \mathrm{C}_{\tau_2 \mapsto \mathrm{int}}, \mathrm{C}_{\mathrm{int} \mapsto \tau_2} : \tau_2 \sim \mathrm{int}}{\mathrm{C}_{\tau_1 + \tau_2 \mapsto [\mathrm{int}]}, \mathrm{C}_{[\mathrm{int}] \mapsto \tau_1 + \tau_2} : \tau_1 + \tau_2 \sim [\mathrm{int}]}$$

$$
\begin{aligned}
\mathrm{C}_{\mathtt{bool} \mapsto \mathrm{int}} &\triangleq \cdot \\
\mathrm{C}_{\mathrm{int} \mapsto \mathtt{bool}} &\triangleq \cdot \\
\mathrm{C}_{\mathtt{ref\ bool} \mapsto \mathrm{ref\ int}} &\triangleq \cdot \\
\mathrm{C}_{\mathrm{ref\ int} \mapsto \mathtt{ref\ bool}} &\triangleq \cdot \\
\mathrm{C}_{\tau_1 \times \tau_2 \mapsto [\tau]} &\triangleq \mathrm{DUP},\ \mathrm{push}\ 0,\ \mathrm{idx},\ \mathrm{C}_{\tau_1 \mapsto \tau}, \mathrm{SWAP},\ \mathrm{push}\ 1,\ \mathrm{idx},\ \mathrm{C}_{\tau_2 \mapsto \tau}, \\
&\ \ \mathrm{lam}\ \mathrm{x}_2.\mathrm{lam}\ \mathrm{x}_1.\mathrm{push}\ [\mathrm{x}_1,\ \mathrm{x}_2] \\
\mathrm{C}_{[\tau] \mapsto \tau_1 \times \tau_2} &\triangleq \mathrm{DUP},\ \mathrm{len},\ \mathrm{push}\ 2,\ \mathrm{SWAP},\ \mathrm{less?},\ \mathrm{if0\ fail\ \textsc{Conv}}, \\
&\ \ \mathrm{DUP},\ \mathrm{push}\ 0,\ \mathrm{idx},\ \mathrm{C}_{\tau \mapsto \tau_1}, \mathrm{SWAP},\ \mathrm{push}\ 1,\ \mathrm{idx},\ \mathrm{C}_{\tau \mapsto \tau_2}, \\
&\ \ \mathrm{lam}\ \mathrm{x}_2.\mathrm{lam}\ \mathrm{x}_1.\mathrm{push}\ [\mathrm{x}_1,\ \mathrm{x}_2] \\
\mathrm{C}_{\tau_1 + \tau_2 \mapsto [\mathrm{int}]} &\triangleq \mathrm{DUP},\ \mathrm{push}\ 1,\ \mathrm{idx},\ \mathrm{SWAP},\ \mathrm{push}\ 0,\ \mathrm{idx},\ \mathrm{DUP}, \\
&\ \ \mathrm{if0}\ (\mathrm{SWAP},\ \mathrm{C}_{\tau_1 \mapsto \mathrm{int}})\ (\mathrm{SWAP},\ \mathrm{C}_{\tau_2 \mapsto \mathrm{int}}), \\
&\ \ \mathrm{lam}\ \mathrm{x}_\mathrm{v}.\mathrm{lam}\ \mathrm{x}_\mathrm{t}.\mathrm{push}\ [\mathrm{x}_\mathrm{t}, \mathrm{x}_\mathrm{v}] \\
\mathrm{C}_{[\mathrm{int}] \mapsto \tau_1 + \tau_2} &\triangleq \mathrm{DUP},\ \mathrm{len},\ \mathrm{push}\ 2,\ \mathrm{SWAP},\ \mathrm{less?},\ \mathrm{if0\ fail\ \textsc{Conv}}, \\
&\ \ \mathrm{DUP}, \mathrm{push}\ 1,\ \mathrm{idx},\ \mathrm{SWAP},\ \mathrm{push}\ 0, \mathrm{idx},\ \mathrm{DUP}, \\
&\ \ \mathrm{if0}\ (\mathrm{SWAP},\ \mathrm{C}_{\mathrm{int} \mapsto \tau_1}) \\
&\ \ \qquad \big(\mathrm{DUP}, \mathrm{push}\ {-1},\ \mathrm{add},\ \mathrm{if0}\ \big(\mathrm{SWAP},\ \mathrm{C}_{\mathrm{int} \mapsto \tau_2}\big)\ \mathrm{fail\ \textsc{Conv}}\big), \\
&\ \ \mathrm{lam}\ \mathrm{x}_\mathrm{v}.\mathrm{lam}\ \mathrm{x}_\mathrm{t}.\mathrm{push}\ [\mathrm{x}_\mathrm{t}, \mathrm{x}_\mathrm{v}]
\end{aligned}
$$

Theorem 1.3 (Converibility Soundness). *If $\tau_A \sim \tau_B$ then*

(1) $\forall (W, \mathrm{P}) \in \mathcal{E}\llbracket \tau_A \rrbracket.\ \big(W, \big(\mathrm{P},\ \mathrm{C}_{\tau_\mathrm{A} \mapsto \tau_\mathrm{B}}\big)\big) \in \mathcal{E}\llbracket \tau_B \rrbracket$*; and*
(2) $\forall (W, \mathrm{P}) \in \mathcal{E}\llbracket \tau_B \rrbracket.\ \big(W, \big(\mathrm{P},\ \mathrm{C}_{\tau_\mathrm{B} \mapsto \tau_\mathrm{A}}\big)\big) \in \mathcal{E}\llbracket \tau_A \rrbracket$

Proof. By simultaneous induction on the structure of the convertibility relation.

NOTE: in the proofs in this case study, we explicitly move the world forward with $\triangleright^n$ when we take n steps. Based on how we construct our logical relations, this is not usually necessary (any future world will usually do), and we present proofs without this in later case studies.

$\boxed{\texttt{bool} \sim \texttt{int}}$

(1) $\forall\,(W, \mathsf{P}) \in \mathcal{E}\llbracket\texttt{bool}\rrbracket.\,\big(W, \big(\mathsf{P},\ \mathsf{C}_{\texttt{bool}\mapsto\mathrm{int}}\big)\big) \in \mathcal{E}\llbracket\mathrm{int}\rrbracket.$
Expanding the definition of $\mathsf{C}_{\texttt{bool}\mapsto\mathrm{int}}$, we are to show that $(W, \mathsf{P}) \in \mathcal{E}\llbracket\mathrm{int}\rrbracket$ given arbitrary W, P such that $(W, \mathsf{P}) \in \mathcal{E}\llbracket\texttt{bool}\rrbracket$. Notice that $\mathcal{V}\llbracket\texttt{bool}\rrbracket = \mathcal{V}\llbracket\mathrm{int}\rrbracket$ by definition. Then $\mathcal{E}\llbracket\texttt{bool}\rrbracket = \mathcal{E}\llbracket\mathrm{int}\rrbracket$ also by definition, so the claim is trivially true.

(2) $\forall\,(W, \mathsf{P}) \in \mathcal{E}\llbracket\mathrm{int}\rrbracket.\,\big(W, \big(\mathsf{P},\ \mathsf{C}_{\mathrm{int}\mapsto\texttt{bool}}\big)\big) \in \mathcal{E}\llbracket\texttt{bool}\rrbracket.$
As in the previous case, exchanging $\texttt{bool}$ with int where appropriate.

$\boxed{\texttt{ref bool} \sim \mathrm{ref\ int}}$

(1) $\forall\,(W, \mathsf{P}) \in \mathcal{E}\llbracket\texttt{ref bool}\rrbracket.\,\big(W, \big(\mathsf{P},\ \mathsf{C}_{\texttt{ref bool}\mapsto\mathrm{ref\ int}}\big)\big) \in \mathcal{E}\llbracket\mathrm{ref\ int}\rrbracket.$
As in $\boxed{\texttt{bool} \sim \mathrm{int}}$.(1), exchanging $\texttt{bool}$, int with $\texttt{ref bool}$, $\mathrm{ref\ int}$ where appropriate.

(2) $\forall\,(W, \mathsf{P}) \in \mathcal{E}\llbracket\mathrm{ref\ int}\rrbracket.\,\big(W, \big(\mathsf{P},\ \mathsf{C}_{\mathrm{ref\ int}\mapsto\texttt{ref bool}}\big)\big) \in \mathcal{E}\llbracket\texttt{ref bool}\rrbracket.$
As in the previous case, exchanging $\texttt{ref bool}$ with $\mathrm{ref\ int}$ where appropriate.

$\boxed{\tau_1 \sim \tau \land \tau_2 \sim \tau \implies \tau_1 \times \tau_2 \sim [\tau]}$

(1) $\forall\,(W, \mathsf{P}) \in \mathcal{E}\llbracket\tau_1 \times \tau_2\rrbracket.\,\big(W, \big(\mathsf{P},\ \mathsf{C}_{\tau_1 \times \tau_2\mapsto[\tau]}\big)\big) \in \mathcal{E}\llbracket[\tau]\rrbracket.$
Expanding the definition of $\mathcal{E}\llbracket\cdot\rrbracket$ in the goal, we are to show that

$$\mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \land \mathsf{c} \in \textsc{OkErr} \lor \exists \mathsf{v},\ W' \sqsupseteq W.\big(\mathsf{S}' = \mathsf{S}, \mathsf{v} \land \mathsf{H}' : W' \land (W', \mathsf{v}) \in \mathcal{V}\llbracket[\tau]\rrbracket \qquad (1)$$

given arbitrary $W, \mathsf{P}, \mathsf{H}{:}W, \mathsf{S}, \mathsf{H}', \mathsf{S}', j < W.k$ such that $(W, \mathsf{P}) \in \mathcal{E}\llbracket\tau_1 \times \tau_2\rrbracket$ and $\langle \mathsf{H}; \mathsf{S}; \mathsf{P},\ \mathsf{C}_{\tau_1 \times \tau_2\mapsto[\tau]}\rangle \xrightarrow{j} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \not\twoheadrightarrow$. The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $\mathsf{H}_P, \mathsf{S}_P, j_P \leq j$ such that $\langle \mathsf{H}; \mathsf{S}; \mathsf{P}\rangle \xrightarrow{j_P} \langle \mathsf{H}_P; \mathsf{S}_P; \cdot\rangle \not\twoheadrightarrow$. Then by expanding the definition of $\mathcal{E}\llbracket\cdot\rrbracket$ in the premise and specializing where appropriate, either:

- $\mathsf{S}_P = \mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \land \mathsf{c} \in \textsc{OkErr}$ and $\mathsf{H}_P = \mathsf{H}'$.
  In this case, we have the left disjunct of (1).
-
  $$\exists \mathsf{v}_\mathsf{P},\ W_P \sqsupseteq W.\big(\mathsf{S}_P = \mathsf{S}, \mathsf{v}_\mathsf{P} \land \mathsf{H}_P : W_P \land (W_P, \mathsf{v}_\mathsf{P}) \in \mathcal{V}\llbracket\tau_1 \times \tau_2\rrbracket$$

  and $\langle \mathsf{H}_P; \mathsf{S}_P; \mathsf{C}_{\tau_1 \times \tau_2\mapsto[\tau]}\rangle \xrightarrow{j-j_P} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \not\twoheadrightarrow$. Expanding the definition of $\mathcal{V}\llbracket\tau_1 \times \tau_2\rrbracket$, we have that

  $$\mathsf{v}_\mathsf{P} = [\mathsf{v}_1,\ \mathsf{v}_2] \land (W_P, \mathsf{v}_1) \in \mathcal{V}\llbracket\tau_1\rrbracket \land (W_P, \mathsf{v}_2) \in \mathcal{V}\llbracket\tau_2\rrbracket$$

  for some $\mathsf{v}_1, \mathsf{v}_2$. Expanding the definition of $\mathsf{C}_{\tau_1 \times \tau_2\mapsto[\tau]}$ and applying the operational semantics of StackLang,

  $$\langle \mathsf{H}_P; \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2]; \mathsf{DUP}, \ldots\rangle \xrightarrow{5} \langle \mathsf{H}_P; \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2], \mathsf{v}_1; \mathsf{C}_{\tau_1\mapsto\tau}, \ldots\rangle$$

  Applying Lemma 1.2 again, there is $\mathsf{H}_1, \mathsf{S}_1, j_1 \leq j - j_P - 5$ such that $\langle \mathsf{H}_P; \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2], \mathsf{v}_1; \mathsf{C}_{\tau_1\mapsto\tau}\rangle \xrightarrow{j_1} \langle \mathsf{H}_1; \mathsf{S}_1; \cdot\rangle \not\twoheadrightarrow$. Appealing to the inductive hypothesis that $\tau_1 \sim \tau$, expanding the definition of $\mathcal{E}\llbracket\cdot\rrbracket$, and specialzing where appropriate, we have that

$$\begin{aligned} &\mathsf{S}_1 = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \textsc{OkErr} \vee \\ &\exists \mathsf{v}_{1c},\ W_1 \sqsupseteq W_P.\big(\mathsf{S}_1 = \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2], \mathsf{v}_{1c} \wedge \mathsf{H}_1 : W_1 \wedge (W_1, \mathsf{v}_{1c}) \in \mathcal{V}[\![\tau]\!] \end{aligned} \tag{2}$$

If we have the left disjunct, then we have the left disjunct of (1). Then suppose we have the right disjunct. By the operational semantics of StackLang, we have that

$$\begin{aligned} \langle \mathsf{H}_P; \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2], \mathsf{v}_1; \mathsf{C}_{\tau_1 \mapsto \tau}, \ldots \rangle &\xrightarrow{j_1} \langle \mathsf{H}_P; \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2], \mathsf{v}_{1c}; \mathsf{SWAP}, \ldots \rangle \\ &\xrightarrow{6} \langle \mathsf{H}_P; \mathsf{S}, \mathsf{v}_{1c}, \mathsf{v}_2; \mathsf{C}_{\tau_1 \mapsto \tau}, \ldots \rangle \end{aligned}$$

Applying Lemma 1.2 again, there is $\mathsf{H}_2, \mathsf{S}_2, j_2 \leq j - j_P - j_1 - 7$ such that $\langle \mathsf{H}_1; \mathsf{S}, \mathsf{v}_{1c}, \mathsf{v}_2; \mathsf{C}_{\tau_2 \mapsto \tau} \rangle \xrightarrow{j_2} \langle \mathsf{H}_2; \mathsf{S}_2; \cdot \rangle \not\rightarrow$. Appealing to the inductive hypothesis that $\tau_2 \sim \tau$, expanding the definition of $\mathcal{E}[\![\cdot]\!]$, and specializing where appropriate, we have that

$$\begin{aligned} &\mathsf{S}_2 = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \textsc{OkErr} \vee \\ &\exists \mathsf{v}_{2c},\ W_2 \sqsupseteq W_1.\big(\mathsf{S}_2 = \mathsf{S}, \mathsf{v}_{1c}, \mathsf{v}_{2c} \wedge \mathsf{H}_2 : W_2 \wedge (W_2, \mathsf{v}_{2c}) \in \mathcal{V}[\![\tau]\!] \end{aligned} \tag{3}$$

If we have the left disjunct, then we have the left disjunct of (1). Then suppose we have the right disjunct. By the operational semantics of StackLang, we have

$$\begin{aligned} \langle \mathsf{H}_P; \mathsf{S}, \mathsf{v}_{1c}, \mathsf{v}_2; \mathsf{C}_{\tau_2 \mapsto \tau}, \ldots \rangle &\xrightarrow{j_2} \langle \mathsf{H}_P; \mathsf{S}, \mathsf{v}_{1c}, \mathsf{v}_{2c}; \mathsf{lam}\ \mathsf{x}_2.\mathsf{lam}\ \mathsf{x}_1.\mathsf{push}\ [\mathsf{x}_1, \mathsf{x}_2] \rangle \\ &\xrightarrow{3} \langle \mathsf{H}_P; \mathsf{S}, [\mathsf{v}_{1c}, \mathsf{v}_{2c}]; \cdot \rangle \end{aligned}$$

so $\mathsf{H}' = \mathsf{H}_P$ and $\mathsf{S}' = \mathsf{S}, [\mathsf{v}_{1c}, \mathsf{v}_{2c}]$. Then we show the right disjunct of (1) by taking $\mathsf{v} = [\mathsf{v}_{1c}, \mathsf{v}_{2c}]$ and $W' = \triangleright^3 W_2$, noting that $W \sqsubseteq W_P \sqsubseteq W_1 \sqsubseteq W_2 \sqsubseteq W'$ by Lemma 1.5. All that remains is to show that $(W', [\mathsf{v}_{1c}, \mathsf{v}_{2c}]) \in \mathcal{V}[\![[\tau]]\!]$, which by definition requires that
$(W', \mathsf{v}_{1c}), (W', \mathsf{v}_{2c}) \in \mathcal{V}[\![\tau]\!]$. Recall that $(W_1, \mathsf{v}_1) \in \mathcal{V}[\![\tau_1]\!]$ by (2) and $(W_2, \mathsf{v}_2) \in \mathcal{V}[\![\tau_2]\!]$ and (3) Then we simply apply Lemmas 1.4, 1.6.

(2) $\forall (W, \mathsf{P}) \in \mathcal{E}[\![[\tau]]\!].\big(W, (\mathsf{P},\ \mathsf{C}_{[\tau] \mapsto \tau_1 \times \tau_2})\big) \in \mathcal{E}[\![\tau_1 \times \tau_2]\!]$.
Expanding the definition of $\mathcal{E}[\![\cdot]\!]$ in the goal, we are to show that

$$\mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \textsc{OkErr} \vee \exists \mathsf{v},\ W' \sqsupseteq W.\big(\mathsf{S}' = \mathsf{S}, \mathsf{v} \wedge \mathsf{H}' : W' \wedge (W', \mathsf{v}) \in \mathcal{V}[\![\tau_1 \times \tau_2]\!] \tag{4}$$

given arbitrary $W, \mathsf{P}, \mathsf{H}{:}W, \mathsf{S}, \mathsf{H}', \mathsf{S}', j < W.k$ such that $(W, \mathsf{P}) \in \mathcal{E}[\![[\tau]]\!]$ and $\langle \mathsf{H}; \mathsf{S}; \mathsf{P},\ \mathsf{C}_{[\tau] \mapsto \tau_1 \times \tau_2} \rangle \xrightarrow{j} \langle \mathsf{H}'; \mathsf{S}'; \cdot \rangle \not\rightarrow$. The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $\mathsf{H}_P, \mathsf{S}_P, j_P \leq j$ such that $\langle \mathsf{H}; \mathsf{S}; \mathsf{P} \rangle \xrightarrow{j_P} \langle \mathsf{H}_P; \mathsf{S}_P; \cdot \rangle \not\rightarrow$. Then by expanding the definition of $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing where appropriate, either:

- $\mathsf{S}_P = \mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \textsc{OkErr}$ and $\mathsf{H}_P = \mathsf{H}'$.
  In this case, we have the left disjunct of (4).
- $$\exists \mathsf{v}_\mathsf{P},\ W_P \sqsupseteq W.\big(\mathsf{S}_P = \mathsf{S}, \mathsf{v}_\mathsf{P} \wedge \mathsf{H}_P : W_P \wedge (W_P, \mathsf{v}_\mathsf{P}) \in \mathcal{V}[\![[\tau]]\!]$$

  and $\langle \mathsf{H}_P; \mathsf{S}_P; \mathsf{C}_{[\tau] \mapsto \tau_1 \times \tau_2} \rangle \xrightarrow{j - j_P} \langle \mathsf{H}'; \mathsf{S}'; \cdot \rangle \not\rightarrow$. Expanding the definition of $\mathcal{V}[\![[\tau]]\!]$, we have that

  $$\mathsf{v}_\mathsf{P} = [\mathsf{v}_1, \ldots, \mathsf{v}_\mathsf{n}] \wedge (W_P, \mathsf{v}_1) \in \mathcal{V}[\![\tau]\!] \wedge \ldots \wedge (W_P, \mathsf{v}_\mathsf{n}) \in \mathcal{V}[\![\tau]\!]$$

for some $\mathsf{v}_1, \ldots, \mathsf{v}_\mathsf{n}$. Expanding the definition of $\mathsf{C}_{[\tau] \mapsto \tau_1 \times \tau_2}$ and applying the operational semantics of StackLang,

$$\langle \mathsf{H}_P; \mathsf{S}, [\mathsf{v}_1, \ldots, \mathsf{v}_\mathsf{n}]; \mathsf{DUP}, \ldots \rangle \xrightarrow{10} \langle \mathsf{H}_P; \mathsf{S}, [\mathsf{v}_1, \ldots, \mathsf{v}_\mathsf{n}], \mathsf{n}_?; \mathsf{if0\ fail\ C\scriptsize{ONV}}, \ldots \rangle$$

where $\mathsf{n}_? \in \{0, 1\}$ is a bit indicating whether $\mathsf{n} < 2$. Here, the operational semantics gives us two cases:

- $\mathsf{n}_? = 0$. Continuing,

  $$\langle \mathsf{H}_P; \mathsf{S}, [\mathsf{v}_1, \ldots, \mathsf{v}_\mathsf{n}], 0; \mathsf{if0\ fail\ C\scriptsize{ONV}}, \ldots \rangle \xrightarrow{2} \langle \mathsf{H}_P; \mathsf{Fail\ C\scriptsize{ONV}}; \cdot \rangle$$

  In this case, $\mathsf{S}' = \mathsf{Fail\ C\scriptsize{ONV}}$ and we have the left disjunct of (4).
- $\mathsf{n}_? = 1$. Then by construction, $\mathsf{n} \geq 2$. Continuing,

$$\begin{aligned}\langle \mathsf{H}_P; \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2, \ldots, \mathsf{v}_\mathsf{n}], 1; \mathsf{if0\ fail\ C\scriptsize{ONV}}, \mathsf{DUP}, \ldots \rangle &\xrightarrow{1} \langle \mathsf{H}_P; \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2, \ldots, \mathsf{v}_\mathsf{n}]; \mathsf{DUP}, \ldots \rangle \\ &\xrightarrow{5} \langle \mathsf{H}_P; \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2, \ldots, \mathsf{v}_\mathsf{n}], \mathsf{v}_1; \mathsf{C}_{\tau \mapsto \tau_1}, \ldots \rangle\end{aligned}$$

Applying Lemma 1.2 again, there is $\mathsf{H}_1, \mathsf{S}_1, j_1 \leq j - j_P - 5$ such that $\langle \mathsf{H}_1; \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2, \ldots, \mathsf{v}_\mathsf{n}], \mathsf{v}_1; \mathsf{C}_{\tau \mapsto \tau_1} \rangle \xrightarrow{j_1} \langle \mathsf{H}_1; \mathsf{S}_1; \cdot \rangle \not\rightarrow$. Appealing to the inductive hypothesis that $\tau \sim \tau_1$ is sound, expanding the definition of $\mathcal{E}[\![\cdot]\!]$, and specializing as appropriate, we have that

$$\begin{aligned}&\mathsf{S}_1 = \mathsf{Fail\ c} \land \mathsf{c} \in \mathsf{O\scriptsize{K}\normalsize{E}\scriptsize{RR}} \lor \\ &\exists \mathsf{v}_{1\mathsf{c}},\ W_1 \sqsupseteq W_P.(\mathsf{S}_1 = \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2, \ldots, \mathsf{v}_\mathsf{n}], \mathsf{v}_{1\mathsf{c}} \land \mathsf{H}_1 : W_1 \land (W_1, \mathsf{v}_{1\mathsf{c}}) \in \mathcal{V}[\![\tau_1]\!]\end{aligned} \tag{5}$$

If we have the left disjunct, then we have the left disjunct of (4). Then suppose we have the right disjunct. By the operational semantics of StackLang, we have

$$\langle \mathsf{H}_1; \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2, \ldots, \mathsf{v}_\mathsf{n}], \mathsf{v}_{1\mathsf{c}}; \mathsf{SWAP}, \ldots, \rangle \xrightarrow{6} \langle \mathsf{H}_1; \mathsf{S}, \mathsf{v}_{1\mathsf{c}}, \mathsf{v}_2; \mathsf{C}_{\tau \mapsto \tau_2}, \rangle$$

Applying Lemma 1.2 again, there is $\mathsf{H}_2, \mathsf{S}_2, j_2 \leq j - j_P - j_1 - 6$ such that $\langle \mathsf{H}_1; \mathsf{S}, \mathsf{v}_{1\mathsf{c}}, \mathsf{v}_2; \mathsf{C}_{\tau \mapsto \tau_2} \rangle \xrightarrow{j_2} \langle \mathsf{H}_2; \mathsf{S}_2; \cdot \rangle \not\rightarrow$. Appealing to the inductive hypothesis that $\tau \sim \tau_2$ is sound, expanding the definition of $\mathcal{E}[\![\cdot]\!]$, and specializing as appropriate, we have that

$$\begin{aligned}&\mathsf{S}_2 = \mathsf{Fail\ c} \land \mathsf{c} \in \mathsf{O\scriptsize{K}\normalsize{E}\scriptsize{RR}} \lor \\ &\exists \mathsf{v}_{2\mathsf{c}},\ W_2 \sqsupseteq W_2.(\mathsf{S}_2 = \mathsf{S}, \mathsf{v}_{1\mathsf{c}}, \mathsf{v}_{2\mathsf{c}} \land \mathsf{H}_2 : W_2 \land (W_2, \mathsf{v}_{2\mathsf{c}}) \in \mathcal{V}[\![\tau_2]\!]\end{aligned} \tag{6}$$

If we have the left disjunct, then we have the left disjunct of (4). Then suppose we have the right disjunct. By the operational semantics of StackLang, we have

$$\langle \mathsf{H}_2; \mathsf{S}, \mathsf{v}_{1\mathsf{c}}, \mathsf{v}_{2\mathsf{c}}; \mathsf{lam\ x_2.lam\ x_1.push\ [x_1, x_2]} \rangle \xrightarrow{3} \langle \mathsf{H}_2; \mathsf{S}, [\mathsf{v}_{1\mathsf{c}}, \mathsf{v}_{2\mathsf{c}}]; \cdot \rangle$$

so $\mathsf{H}' = \mathsf{H}_2$ and $\mathsf{S}' = \mathsf{S}, [\mathsf{v}_{1\mathsf{c}}, \mathsf{v}_{2\mathsf{c}}]$. Then we show the right disjunct of (4) by taking $\mathsf{v} = [\mathsf{v}_{1\mathsf{c}}, \mathsf{v}_{2\mathsf{c}}]$ and $W' = \triangleright^3 W_2$, noting that $W \sqsubseteq W_P \sqsubseteq W_1 \sqsubseteq W_2 \sqsubseteq W'$ by Lemma 1.5. All that remains is to show that $(W', [\mathsf{v}_{1\mathsf{c}}, \mathsf{v}_{2\mathsf{c}}]) \in \mathcal{V}[\![\tau_1 \times \tau_2]\!]$, which by definition requires that $(W', \mathsf{v}_{1\mathsf{c}}) \in \mathcal{V}[\![\tau_1]\!]$ and $(W', \mathsf{v}_{2\mathsf{c}}) \in \mathcal{V}[\![\tau_2]\!]$. Recall that $(W_1, \mathsf{v}_{1\mathsf{c}}) \in \mathcal{V}[\![\tau_1]\!]$ by (5) and $(W_2, \mathsf{v}_{2\mathsf{c}}) \in \mathcal{V}[\![\tau_2]\!]$ by (6). Then we simply apply Lemmas 1.4, 1.6.

$\boxed{\tau_1 \sim \text{int} \land \tau_2 \sim \text{int} \implies \tau_1 + \tau_2 \sim [\text{int}]}$ □

(1) $\forall\,(W, \mathsf{P}) \in \mathcal{E}\llbracket \tau_1 + \tau_2 \rrbracket.\,\big(W, \big(\mathsf{P},\ \mathsf{C}_{\tau_1\,+\,\tau_2 \mapsto [\mathrm{int}]}\big)\big) \in \mathcal{E}\llbracket [\mathrm{int}] \rrbracket$.
Expanding the definition of $\mathcal{E}\llbracket\cdot\rrbracket$ in the goal, we are to show that

$$\mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \textsc{OkErr} \vee \exists \mathsf{v},\ W' \sqsupseteq W.\big(\mathsf{S}' = \mathsf{S}, \mathsf{v} \wedge \mathsf{H}' : W' \wedge (W', \mathsf{v}) \in \mathcal{V}\llbracket [\mathrm{int}] \rrbracket \tag{7}$$

given arbitrary $W, \mathsf{P}, \mathsf{H}{:}W, \mathsf{S}, \mathsf{H}', \mathsf{S}', j < W.k$ such that $(W, \mathsf{P}) \in \mathcal{E}\llbracket \tau_1 + \tau_2 \rrbracket$ and $\langle \mathsf{H}; \mathsf{S}; \mathsf{P},\ \mathsf{C}_{\tau_1\,+\,\tau_2 \mapsto [\tau]} \rangle \xrightarrow{j} \langle \mathsf{H}'; \mathsf{S}'; \cdot \rangle \nrightarrow$. The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $\mathsf{H}_P, \mathsf{S}_P, j_P \leq j$ such that $\langle \mathsf{H}; \mathsf{S}; \mathsf{P} \rangle \xrightarrow{j_P} \langle \mathsf{H}_P; \mathsf{S}_P; \cdot \rangle \nrightarrow$. Then by expanding the definition of $\mathcal{E}\llbracket\cdot\rrbracket$ in the premise and specializing where appropriate, either:

- $\mathsf{S}_P = \mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \textsc{OkErr}$ and $\mathsf{H}_P = \mathsf{H}'$.
  In this case, we have the left disjunct of (7).
-
  $$\exists \mathsf{v}_\mathsf{P},\ W_P \sqsupseteq W.\big(\mathsf{S}_P = \mathsf{S}, \mathsf{v}_\mathsf{P} \wedge \mathsf{H}_P : W_P \wedge (W_P, \mathsf{v}_\mathsf{P}) \in \mathcal{V}\llbracket \tau_1 + \tau_2 \rrbracket$$

  and $\langle \mathsf{H}_P; \mathsf{S}_P; \mathsf{C}_{\tau_1\,\times\,\tau_2 \mapsto [\tau]} \rangle \xrightarrow{j - j_P} \langle \mathsf{H}'; \mathsf{S}'; \cdot \rangle \nrightarrow$. Expanding the definition of $\mathcal{V}\llbracket \tau_1 \times \tau_2 \rrbracket$, we have that

  $$(\mathsf{v}_\mathsf{P} = [0,\ \mathsf{v}_1] \wedge (W_P, \mathsf{v}_1) \in \mathcal{V}\llbracket \tau_1 \rrbracket) \vee (\mathsf{v}_\mathsf{P} = [1,\ \mathsf{v}_2] \wedge (W_P, \mathsf{v}_2) \in \mathcal{V}\llbracket \tau_2 \rrbracket) \vee \tag{8}$$

  for some $\mathsf{v}_1, \mathsf{v}_2$. Without loss of generality, suppose we have the left disjunct. Expanding the definition of $\mathsf{C}_{\tau_1\,+\,\tau_2 \mapsto [\mathrm{int}]}$ and applying the operational semantics of StackLang,

  $$\langle \mathsf{H}_P; \mathsf{S}, [0, \mathsf{v}_1]; \mathsf{DUP}, \ldots \rangle \xrightarrow{19} \langle \mathsf{H}_P; \mathsf{S}, 0, \mathsf{v}_1; \mathsf{C}_{\tau_1 \mapsto \mathrm{int}}, \ldots \rangle$$

  Applying Lemma 1.2 again, there is $\mathsf{H}_1, \mathsf{S}_1, j_1 \leq j - j_P - 19$ such that $\langle \mathsf{H}_P; \mathsf{S}, 0, \mathsf{v}_1; \mathsf{C}_{\tau_1 \mapsto \mathrm{int}} \rangle \xrightarrow{j_1} \langle \mathsf{H}_1; \mathsf{S}_1; \cdot \rangle \nrightarrow$. Appealing to the inductive hypothesis that $\tau_1 \sim \mathrm{int}$, expanding the definition of $\mathcal{E}\llbracket\cdot\rrbracket$, and specialzing where appropriate, we have that

  $$\begin{aligned} &\mathsf{S}_1 = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \textsc{OkErr} \vee \\ &\exists \mathsf{v}_{1\mathsf{c}},\ W_1 \sqsupseteq W_P.\big(\mathsf{S}_1 = \mathsf{S}, 0, \mathsf{v}_{1\mathsf{c}} \wedge \mathsf{H}_1 : W_1 \wedge (W_1, \mathsf{v}_{1\mathsf{c}}) \in \mathcal{V}\llbracket \mathrm{int} \rrbracket \end{aligned} \tag{9}$$

  If we have the left disjunct, then we have the left disjunct of (7). Then suppose we have the right disjunct. By the operational semantics of StackLang, we have that

$$\langle \mathsf{H}_P; \mathsf{S}, 0, \mathsf{v}_1; \mathsf{C}_{\tau_1 \mapsto \tau}, \ldots \rangle \xrightarrow{j_1} \langle \mathsf{H}_1; \mathsf{S}, 0, \mathsf{v}_{1\mathsf{c}}; \mathsf{lam}\ \mathsf{x}_\mathsf{v}.\mathsf{lam}\ \mathsf{x}_\mathsf{t}.\mathsf{push}\ [\mathsf{x}_\mathsf{t}, \mathsf{x}_\mathsf{v}] \rangle \quad \xrightarrow{3} \langle \mathsf{H}_1; \mathsf{S}, [0, \mathsf{v}_{1\mathsf{c}}]; \cdot \rangle$$

  so $\mathsf{H}' = \mathsf{H}_1$ and $\mathsf{S}' = \mathsf{S}, [0, \mathsf{v}_{1\mathsf{c}}]$. Then we show the right disjunct of (7) by taking $\mathsf{v} = [0, \mathsf{v}_{1\mathsf{c}}]$ and $W' = \triangleright^{j_1 + 3} W_1$, noting that $W \sqsubseteq W_P \sqsubseteq W_1 \sqsubseteq W'$ by Lemma 1.5. All that remains is to show that $(W', [0, \mathsf{v}_{1\mathsf{c}}]) \in \mathcal{V}\llbracket [\mathrm{int}] \rrbracket$, which by definition requires that
  $(W', 0), (W', \mathsf{v}_{1\mathsf{c}}) \in \mathcal{V}\llbracket \mathrm{int} \rrbracket$. The former we have by definition. For the latter, recall that $(W_1, \mathsf{v}_{1\mathsf{c}}) \in \mathcal{V}\llbracket \mathrm{int} \rrbracket$ by (8). Then we simply apply Lemmas 1.4, 1.6.
  The other case is analogous, exchanging 0, 1 and τ_1, τ_2 where appropriate.

(2) $\forall\,(W, \mathsf{P}) \in \mathcal{E}\llbracket [\mathrm{int}] \rrbracket.\,\big(W, \big(\mathsf{P},\ \mathsf{C}_{[\mathrm{int}] \mapsto \tau_1\,+\,\tau_2}\big)\big) \in \mathcal{E}\llbracket \tau_1 + \tau_2 \rrbracket$.
Expanding the definition of $\mathcal{E}\llbracket\cdot\rrbracket$ in the goal, we are to show that

$$\mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \textsc{OkErr} \vee \exists \mathsf{v},\ W' \sqsupseteq W.\big(\mathsf{S}' = \mathsf{S}, \mathsf{v} \wedge \mathsf{H}' : W' \wedge (W', \mathsf{v}) \in \mathcal{V}\llbracket \tau_1 + \tau_2 \rrbracket \tag{10}$$

given arbitrary $W, \mathsf{P}, \mathsf{H}{:}W, \mathsf{S}, \mathsf{H}', \mathsf{S}', j < W.k$ such that $(W, \mathsf{P}) \in \mathcal{E}\llbracket [\mathrm{int}] \rrbracket$ and $\langle \mathsf{H}; \mathsf{S}; \mathsf{P},\ \mathsf{C}_{[\mathrm{int}] \mapsto \tau_1\,\times\,\tau_2} \rangle \xrightarrow{j} \langle \mathsf{H}'; \mathsf{S}'; \cdot \rangle \nrightarrow$. The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $\mathsf{H}_P, \mathsf{S}_P, j_P \leq j$ such that $\langle \mathsf{H}; \mathsf{S}; \mathsf{P} \rangle \xrightarrow{j_P} \langle \mathsf{H}_P; \mathsf{S}_P; \cdot \rangle \nrightarrow$.

Then by expanding the definition of $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing where appropriate, either:

- $S_P = S' = \text{Fail } c \wedge c \in \textsc{OkErr}$ and $H_P = H'$.
  In this case, we have the left disjunct of (10).
- $S_P \neq \text{Fail } c$ and $P' = \cdot$, so $\langle H_P; S_P; C_{[\text{int}]\mapsto\tau_1 + \tau_2}\rangle \xrightarrow{j-j_P} \langle H'; S'; \cdot\rangle \not\rightarrow$. Now, expanding the definition of $\mathcal{E}[\![\cdot]\!]$ in the premise, specializing as appropriate, and remembering that $S_P \neq \text{Fail } c$, we have that

  $$\exists v_P,\ W_P \sqsupseteq W. (S_P = S, v_P \wedge H_P : W_P \wedge (W_P, v_P) \in \mathcal{V}[\![[\text{int}]]\!]$$

  Expanding the definition of $\mathcal{V}[\![[\text{int}]]\!]$ and $\mathcal{V}[\![\text{int}]\!]$, we have that

  $$v_P = [n_1, \ldots, n_k]$$

  for some $n_1, \ldots, n_k$. Expanding the definition of $C_{[\text{int}]\mapsto\tau_1 + \tau_2}$ and applying the operational semantics of StackLang,

  $$\langle H_P; S, [v_1, \ldots, v_n]; \text{DUP}, \ldots\rangle \xrightarrow{10} \langle H_P; S, [v_1, \ldots, v_n], n_?; \text{if0 fail } \textsc{Conv}, \ldots\rangle$$

  where $n_? \in \{0, 1\}$ is a bit indicating whether $n < 2$. Here, the operational semantics gives us two cases:

  - $n_? = 0$. Continuing,

    $$\langle H_P; S, [n_1, \ldots, n_k], 0; \text{if0 fail } \textsc{Conv}, \ldots\rangle \xrightarrow{2} \langle H_P; \text{Fail } \textsc{Conv}; \cdot\rangle$$

    In this case, $S' = \text{Fail } \textsc{Conv}$ and we have the left disjunct of (10).
  - $n_? = 1$. Then by construction, $n \geq 2$. Continuing,

    $$\begin{aligned}\langle H_P; S, [n_1, n_2, \ldots, n_k], 1; \text{if0 fail } \textsc{Conv}, \text{DUP}, \ldots\rangle &\xrightarrow{1} \langle H_P; S, [n_1, n_2, \ldots, n_k]; \text{DUP}, \ldots\rangle \\ &\xrightarrow{5} \langle H_P; S, n_2, n_1, n_1; \text{if0 } (\ldots)\ (\ldots), \ldots\rangle\end{aligned}$$

    Here, the operational semantics gives us two cases:

    * $n_1 = 0$. Continuing,

      $$\begin{aligned}\langle H_P; S, n_2, 0, 0; \text{if0 } (\ldots)\ (\ldots), \ldots\rangle &\xrightarrow{1} \langle H_P; S, n_2, 0; \text{SWAP}, C_{\text{int}\mapsto\tau_1} \ldots\rangle \\ &\xrightarrow{4} \langle H_P; S, 0, n_2; C_{\text{int}\mapsto\tau_1} \ldots\rangle\end{aligned}$$

      Applying Lemma 1.2 again, there is $H_c, S_c, j_c \leq j - j_P - 4$ such that $\langle H_P; S, 0, n_2; C_{\text{int}\mapsto\tau_1}\rangle \xrightarrow{j_c} \langle H_c; S_c; \cdot\rangle \not\rightarrow$. Appealing to the inductive hypothesis that $\text{int} \sim \tau_1$ is sound, expanding the definition of $\mathcal{E}[\![\cdot]\!]$, and specializing as appropriate, we have that

      $$\begin{aligned}&S_c = \text{Fail } c \wedge c \in \textsc{OkErr} \vee \\ &\exists v_c,\ W_c \sqsupseteq W_P. (S_c = S, 0, v_c \wedge H_c : W_c \wedge (W_c, v_c) \in \mathcal{V}[\![\tau_1]\!]\end{aligned} \tag{11}$$

      If we have the left disjunct, then we have the left disjunct of (10). Then suppose we have the right disjunct. By the operational semantics of StackLang, we have

      $$\langle H_c; S, 0, v_c; \text{lam } x_v.\text{lam } x_t.\text{push } [x_t, x_v]\rangle \xrightarrow{3} \langle H_c; S, [0, v_c]; \cdot\rangle$$

      so $H' = H_c$ and $S' = S, [0, v_c]$. Then we show the right disjunct of (10) by taking $v = [0, v_c]$ and $W' = \triangleright^3 W_c$, noting that $W \sqsubseteq W_P \sqsubseteq W_c \sqsubseteq W'$ by Lemma 1.5. All that remains is to show that $(W', [0, v_c]) \in \mathcal{V}[\![\tau_1 + \tau_2]\!]$, which by definition requires that $(W', \mathsf{v_c}) \in \mathcal{V}\llbracket \tau_1 \rrbracket$. Recall that $(W_c, \mathsf{v_c}) \in \mathcal{V}\llbracket \tau_1 \rrbracket$ by (11). Then we simply apply Lemmas 1.4, 1.6.

- $\mathsf{n}_1 \neq 0$. Continuing,

$$\langle \mathsf{H}_P; \mathsf{S}, \mathsf{n}_2, \mathsf{n}_1, \mathsf{n}_1; \mathsf{if0}\ (\ldots)\ (\ldots), \ldots \rangle \xrightarrow{1} \langle \mathsf{H}_P; \mathsf{S}, \mathsf{n}_2, \mathsf{n}_1; \mathsf{DUP}, \ldots \rangle$$

$$\xrightarrow{6} \langle \mathsf{H}_P; \mathsf{S}, \mathsf{n}_2, \mathsf{n}_1, (\mathsf{n}_1 - 1); \mathsf{if0}\ (\ldots)\ (\mathsf{fail}\ \textsc{Conv}), \ldots \rangle$$

Here, the operational semantics again gives us two cases:

- $(\mathsf{n}_1 - 1) = 0$. That is, $\mathsf{n}_1 = 1$. Then we proceed as in the previous case, exchanging $0, 1$ and τ_1, τ_2 where appropriate.
- $(\mathsf{n}_1 - 1) \neq 0$. That is, $\mathsf{n}_1 \neq 1$. Continuing,

$$\langle \mathsf{H}_P; \mathsf{S}, \mathsf{n}_2, \mathsf{n}_1, \mathsf{n}_1; \mathsf{if0}\ (\ldots)\ \mathsf{fail}\ \textsc{Conv}, \ldots \rangle \xrightarrow{2} \langle \mathsf{H}_P; \mathsf{Fail}\ \textsc{Conv}; \cdot \rangle$$

In this case, $\mathsf{S}' = \mathsf{Fail}\ \textsc{Conv}$ and we have the left disjunct of (10).

1.6 Logical Relation Soundness

1.6.1 Supporting Lemmas.

Lemma 1.4 (World Extension).

(1) *If* $(W_1, \mathsf{v}) \in \mathcal{V}\llbracket \tau \rrbracket$ *and* $W_1 \sqsubseteq W_2$ *then* $(W_2, \mathsf{v}) \in \mathcal{V}\llbracket \tau \rrbracket$

(2) *If* $(W_1, \gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket$ *and* $W_1 \sqsubseteq W_2$ *then* $(W_2, \gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket$

Proof.

(1) By induction on τ. The only interesting cases are:

- If $(W_1, \mathsf{thunk\ lam\ x.P}) \in \mathcal{V}\llbracket \tau_1 \rightarrow \tau_2 \rrbracket$ and $(W_1 \sqsubseteq W_2)$ then $(W_2, \mathsf{thunk\ lam\ x.P}) \in \mathcal{V}\llbracket \tau_2 \rightarrow \tau_2 \rrbracket$. Expanding the definition of $\mathcal{V}\llbracket \tau_1 \rightarrow \tau_2 \rrbracket$ in the goal, we are to show that
$$(W', [\mathsf{x} \mapsto \mathsf{v}]\mathsf{P}) \in \mathcal{E}\llbracket \tau_2 \rrbracket$$
given arbitrary $W' \sqsupset W_2$ and v such that $(W', \mathsf{v}) \in \mathcal{V}\llbracket \tau_1 \rrbracket$. We have that $W_1 \sqsubseteq W_2$ and $W_2 \sqsubset W'$ so $W_1 \sqsubset W'$ by Lemma 1.5. Then we finish by expanding the definition of $\mathcal{V}\llbracket \tau_1 \rightarrow \tau_2 \rrbracket$ in the premise and specializing as appropriate.
- If $(W_1, \ell) \in \mathcal{V}\llbracket \mathrm{ref}\ \tau \rrbracket$ and $(W_1 \sqsubseteq W_2)$ then $(W_2, \ell) \in \mathcal{V}\llbracket \mathrm{ref}\ \tau \rrbracket$. Expanding the definition of $\mathcal{V}\llbracket \mathrm{ref}\ \tau \rrbracket$ in the goal, we are to show that
$$W_2.\Psi(\ell) = \lfloor \mathcal{V}\llbracket \tau \rrbracket \rfloor_{W2.k}$$
Expanding the definition of $\mathcal{V}\llbracket \mathrm{ref}\ \tau \rrbracket$ in the premise, we have
$$W_1.\Psi(\ell) = \lfloor \mathcal{V}\llbracket \tau \rrbracket \rfloor_{W1.k}$$
Expanding the definition of $\sqsubseteq$ and specializing where appropriate, we have that
$$W_2.k \leq W_1.k \wedge \lfloor W_1.\Psi(\ell) \rfloor_{W2.k} = \lfloor W_2.\Psi(\ell) \rfloor_{W2.k}$$
Then we finish by substituting $\lfloor \mathcal{V}\llbracket \tau \rrbracket \rfloor_{W1.k}$ for $W_1.\Psi(\ell)$ and expanding the definition of $\lfloor \cdot \rfloor_{\cdot}$, noting in particular that for any world W, $\lfloor W.\Psi(l) \rfloor_{W.k} = W.\Psi(l)$.

(2) By induction, appealing to the previous case where appropriate.

□

Lemma 1.5 (World Extension Transitive).
If $W_1 \sqsubseteq W_2$ *and* $W_2 \sqsubseteq W_3$ *then* $W_1 \sqsubseteq W_3$.

Proof. Suppose $(k_1, \Psi_1) \sqsubseteq (k_2, \Psi_2)$ and $(k_2, \Psi_2) \sqsubseteq (k_3, \Psi_3)$. Unfolding the definition of $\sqsubseteq$ in the goal, we are to show that

$$k_3 \leq k_1 \land \lfloor \Psi_1(\ell) \rfloor_{k_3} = \lfloor \Psi_3(\ell) \rfloor_{k_3}$$

given arbitrary $\ell \in \mathrm{dom}(\Psi_1)$. Unfolding in the premises, we have that

$$\begin{aligned} k_2 \leq k_1 \land \lfloor \Psi_1(\ell) \rfloor_{k_2} = \lfloor \Psi_2(\ell) \rfloor_{k_2} \land \\ k_3 \leq k_2 \land \lfloor \Psi_2(\ell) \rfloor_{k_3} = \lfloor \Psi_3(\ell) \rfloor_{k_3} \end{aligned}$$

where on the second line we appeal to the fact that $\mathrm{dom}(\Psi_1) \subseteq \mathrm{dom}(\Psi_2) \subseteq \mathrm{dom}(\Psi_3)$ by definition of $\sqsubseteq$. For the left disjunct, we have

$$k_3 \leq k_2 \leq k_1$$

by transitivity of $\leq$. For the right disjunct, it is sufficient to show that

$$\lfloor \Psi_1(\ell) \rfloor_{k_3} = \lfloor \Psi_2(\ell) \rfloor_{k_3}$$

because $=$ is transitive. Expanding the definition of $\lfloor \cdot \rfloor_{\cdot}$, we are to show that

$$\{(W, \mathsf{v}) \mid (W, \mathsf{v}) \in \Psi_1(\ell) \land W.k < k_3\} = \{(W, \mathsf{v}) \mid (W, \mathsf{v}) \in \Psi_2(\ell) \land W.k < k_3\}$$

and we have that

$$\{(W, \mathsf{v}) \mid (W, \mathsf{v}) \in \Psi_1(\ell) \land W.k < k_2\} = \{(W, \mathsf{v}) \mid (W, \mathsf{v}) \in \Psi_2(\ell) \land W.k < k_2\}$$

Since $k_3 \leq k_2$, $k < k_2$ if $k < k_3$, so we are done. □

Lemma 1.6 (Later Heaps). *If* $\mathsf{H} : W$ *then* $\mathsf{H} : \triangleright W$.

Proof. Suppose $\mathsf{H} : (k, \Psi)$. Expanding the definition of $\triangleright$, we are to show that

$$\mathsf{H} : (k - 1, \lfloor \Psi \rfloor_{k-1})$$

Expanding the definition of $:$, $\triangleright$, and $\lfloor \cdot \rfloor_{\cdot}$, we are to show that

$$((k - 2, \lfloor \Psi \rfloor_{k-2}), \mathsf{v}) \in R \land k - 2 < k - 1$$

for some ℓ, v, R such that $\Psi(\ell) = R$ and $\mathsf{H}(\ell) = \mathsf{v}$. The right disjunct is trivial, so we are to show the left disjunct. Expanding the definition of $:$, $\triangleright$, and $\lfloor \cdot \rfloor_{\cdot}$ in the premise and specializing where appropriate, we have that

$$((k - 1, \lfloor \Psi \rfloor_{k-1}), \mathsf{v}) \in R$$

Then since $R \in Typ$ and $(k - 1, \lfloor \Psi \rfloor_{k-1}) \sqsubseteq (k - 2, \lfloor \Psi \rfloor_{k-2})$, $((k - 2, \lfloor \Psi \rfloor_{k-2}), \mathsf{v}) \in R$ by definition of Typ_n.

□

Lemma 1.7 (Value Lifting). *If* $(W, \mathsf{v}) \in \mathcal{V}[\![\tau]\!]$, *then* $(W, \mathsf{push\ v}) \in \mathcal{E}[\![\tau]\!]$.

Proof. Expanding the definition of $\mathcal{E}[\![\tau]\!]$, we are to show that

$$\mathsf{S}' = \mathsf{Fail\ c} \land \mathsf{c} \in \textsc{OkErr} \lor \exists \mathsf{v}, W' \sqsupseteq W.\ \big(\mathsf{S}' = \mathsf{S}, \mathsf{v} \land \mathsf{H}' : W' \land (W', \mathsf{v}) \in \mathcal{V}[\![\tau]\!]\big)\big) \tag{12}$$

given arbitrary $W, \mathsf{v}, \mathsf{H}{:}W, \mathsf{S}, \mathsf{H}', \mathsf{S}', j < W.k$ such that $(W, \mathsf{v}) \in \mathcal{V}[\![\tau]\!]$ and

$$\langle \mathsf{H}; \mathsf{S}; \mathsf{push\ v} \rangle \xrightarrow{j} \langle \mathsf{H}'; \mathsf{S}'; \cdot \rangle \not\twoheadrightarrow$$

By the operational semantics of StackLang, we have that $j = 1$, $\mathsf{H}' = \mathsf{H}$, and $\mathsf{S}' = \mathsf{S}, \mathsf{v}$. Then we have the right disjunct of (12) by taking $\mathsf{v} = \mathsf{v}$, $W' = \triangleright W$ and appealing to Lemmas 1.4, 1.6. □

Theorem 1.8 (Fundamental Property). *If* $\Gamma; \Gamma \vdash \mathsf{e} : \tau$ *then* $[\![\Gamma; \Gamma \vdash \mathsf{e} : \tau]\!]$ *and if* $\Gamma; \Gamma \vdash \mathsf{e} : \tau$ *then* $[\![\Gamma; \Gamma \vdash \mathsf{e} : \tau]\!]$.

Proof. By induction on the typing derivations, using the compatibility lemmas. □

Theorem 1.9 (Type Safety for RefLL). *If* $\cdot;\cdot \vdash \mathrm{e} : \tau$ *then for any* $\mathrm{H} : W$, *if* $\langle \mathrm{H}; \cdot; \mathrm{e}^{+}\rangle \xrightarrow{*} \langle \mathrm{H}'; \mathrm{S}'; \mathrm{P}'\rangle$, *then either* $\langle \mathrm{H}'; \mathrm{S}'; \mathrm{P}'\rangle \rightarrow \langle \mathrm{H}''; \mathrm{S}''; \mathrm{P}''\rangle$, *or* $\mathrm{P}' = \cdot$ *and either* $\mathrm{S}' = \mathsf{Fail}\ \mathrm{c}$ *for some* $\mathrm{c} \in \textit{OkErr}$ *or* $\mathrm{S}' = \mathrm{v}$.

Proof. Suppose $\langle \mathrm{H}; \cdot; \mathrm{e}^{+}\rangle \xrightarrow{n} \langle \mathrm{H}'; \mathrm{S}'; \mathrm{P}'\rangle$ for some natural number n. Then, either $\langle \mathrm{H}'; \mathrm{S}'; \mathrm{P}'\rangle \rightarrow \langle \mathrm{H}''; \mathrm{S}''; \mathrm{P}''\rangle$ or $\langle \mathrm{H}'; \mathrm{S}'; \mathrm{P}'\rangle$ is irreducible. If $\langle \mathrm{H}'; \mathrm{S}'; \mathrm{P}'\rangle$ is irreducible, then $\mathrm{P}' = \cdot$ by Lemma 1.1.

Next, by the Fundamental Property, since e typechecks under empty environments, $((n + 1, \emptyset), \mathrm{e}^{+}) \in \mathcal{E}[\![\tau]\!]$.. Thus, since $n < n + 1$ and $\langle \mathrm{H}; \cdot; \mathrm{e}^{+}\rangle \xrightarrow{n} \langle \mathrm{H}'; \mathrm{S}'; \cdot\rangle$, we find that either $\mathrm{S}' = \mathsf{Fail}\ \mathrm{c}$ for some $\mathrm{c} \in \textsc{OkErr}$ or $\mathrm{S}' = \cdot, \mathrm{v}$, as was to be proven. □

Theorem 1.10 (Type Safety for RefHL). *If* $\cdot;\cdot \vdash \mathtt{e} : \tau$ *then for any* $\mathrm{H} : W$, *if* $\langle \mathrm{H}; \cdot; \mathrm{e}^{+}\rangle \xrightarrow{*} \langle \mathrm{H}'; \mathrm{S}'; \mathrm{P}'\rangle$, *then either* $\langle \mathrm{H}'; \mathrm{S}'; \mathrm{P}'\rangle \rightarrow \langle \mathrm{H}''; \mathrm{S}''; \mathrm{P}''\rangle$, *or* $\mathrm{P}' = \cdot$ *and either* $\mathrm{S}' = \mathsf{Fail}\ \mathrm{c}$ *for some* $\mathrm{c} \in \textit{OkErr}$ *or* $\mathrm{S}' = \mathrm{v}$.

Proof. This proof is identical to that of RefLL. □

1.6.2 RefHL *Compatibility Lemmas.*

Lemma 1.11 (Compat ()).

$$[\![\Gamma;\Gamma \vdash () : \mathtt{unit}]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^{+}$, we are to show that

$$(W, \mathrm{close}(\gamma_{\Gamma}, \mathrm{close}(\gamma_{\Gamma}, \mathrm{push}\ 0))) \in \mathcal{E}[\![\mathtt{unit}]\!]$$

given arbitary $W, \gamma_{\Gamma}, \gamma_{\Gamma}$ such that $(W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]$. Since push 0 is already closed, the close operators have no effect. Then we are to show that

$$(W, \mathrm{push}\ 0) \in \mathcal{E}[\![\mathtt{unit}]\!]$$

Then applying Lemma 1.7, we are to show that

$$(W, 0) \in \mathcal{V}[\![\mathtt{unit}]\!]$$

which we have by definition of $\mathcal{V}[\![\mathtt{unit}]\!]$. □

Lemma 1.12 (Compat $\mathbb{B}$).

$$\mathtt{b} \in \mathbb{B} \implies [\![\Gamma;\Gamma \vdash \mathtt{b} : \mathtt{bool}]\!]$$

Proof. As in Lemma 1.11, except that in the case where $\mathtt{b} = \mathtt{false}$, $\mathtt{b}^{+} = \mathrm{push}\ 1$ and so 1 is used as the witness for v. □

Lemma 1.13 (Compat x).

$$[\![\Gamma;\Gamma, \mathtt{x} : \tau \vdash \mathtt{x} : \tau]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^{+}$, we are to show that

$$(W, \mathrm{close}(\gamma_{\Gamma}, \mathrm{close}(\gamma_{\Gamma}, \mathrm{push}\ \mathrm{x}))) \in \mathcal{E}[\![\tau]\!]$$

given arbitary $W, \gamma_{\Gamma}, \gamma_{\Gamma}$ such that $(W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma, \mathtt{x} : \tau]\!]$. Expanding the definition of $\mathcal{G}[\![\cdot]\!]$, we have that

$$\gamma_{\Gamma} = \gamma[\mathrm{x} \mapsto \mathrm{v}] \wedge (W, \mathrm{v}) \in \mathcal{V}[\![\tau]\!] \wedge (W, \gamma) \in \mathcal{G}[\![\Gamma]\!]$$

for some γ, v. Since $\gamma_{\Gamma}(\mathrm{x}) = \mathrm{v}$ and v is closed, we are to show that

$$(W, \mathrm{push}\ \mathrm{v}) \in \mathcal{E}[\![\tau]\!]$$

Then applying Lemma 1.7, we are to show that

$$(W, \mathrm{v}) \in \mathcal{V}[\![\tau]\!]$$

which we have by assumption. □

Lemma 1.14 (Compat $\mathtt{inl}\ \mathtt{e}$).

$$[\![\Gamma;\Gamma \vdash \mathsf{e} : \tau_1]\!] \implies [\![\Gamma;\Gamma \vdash \mathtt{inl}\ \mathsf{e} : \tau_1 + \tau_2]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^+$ and pushing substitutions in the goal, we are to show that

$$\big(W, \big(\text{close}\ \big(\gamma_\Gamma, \text{close}\ \big(\gamma_\Gamma, \mathsf{e}^+\big)\big),\ \mathsf{lam}\ \mathsf{x}.\ (\mathsf{push}\ [0,\ \mathsf{x}])\big)\big) \in \mathcal{E}[\![\tau_1 + \tau_2]\!]$$

given arbitary $W, \gamma_\Gamma, \gamma_\Gamma$ such that $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]$, we are to show that

$$\mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \textsc{OkErr} \vee \exists \mathsf{v}, W' \sqsupseteq W.\ \big(\mathsf{S}' = \mathsf{S}, \mathsf{v} \wedge \mathsf{H}' : W' \wedge (W', \mathsf{v}) \in \mathcal{V}[\![\tau_1 + \tau_2]\!]\big) \tag{13}$$

given arbitrary $\mathsf{H}{:}W, \mathsf{S}, \mathsf{H}', \mathsf{S}', j < W.k$ such that

$$\langle \mathsf{H}; \mathsf{S}; \big(\text{close}\ \big(\gamma_\Gamma, \text{close}\ \big(\gamma_\Gamma, \mathsf{e}^+\big)\big),\ \mathsf{lam}\ \mathsf{x}.\ (\mathsf{push}\ [0,\ \mathsf{x}])\big)\rangle \xrightarrow{j} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \not\rightarrow$$

The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $j_e \leq j, \mathsf{H}_e, \mathsf{S}_e$ such that

$$\langle \mathsf{H}; \mathsf{S}; \big(\text{close}\ \big(\gamma_\Gamma, \text{close}\ \big(\gamma_\Gamma, \mathsf{e}^+\big)\big)\big)\rangle \xrightarrow{j_e} \langle \mathsf{H}_e; \mathsf{S}_e; \cdot\rangle \not\rightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(1) $\mathsf{S}_e = \mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \textsc{OkErr}$ and $\mathsf{H}_e = \mathsf{H}'$.
In this case, we have the left disjunct of (13).

(2)
$$\exists \mathsf{v}_\mathsf{e}, W_e \sqsupseteq W.\ \big(\mathsf{S}_e = \mathsf{S}, \mathsf{v}_\mathsf{e} \wedge \mathsf{H}_e : W_e \wedge (W_e, \mathsf{v}_\mathsf{e}) \in \mathcal{V}[\![\tau_1]\!]\big)$$
and
$$\langle \mathsf{H}_e; \mathsf{S}_e; \mathsf{lam}\ \mathsf{x}.\ (\mathsf{push}\ [0,\ \mathsf{x}])\rangle \xrightarrow{j-j_e} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \not\rightarrow$$
By the operational semantics of StackLang,
$$\begin{aligned}\langle \mathsf{H}_e; \mathsf{S}, \mathsf{v}_\mathsf{e}; \mathsf{lam}\ \mathsf{x}.\ (\mathsf{push}\ [0,\ \mathsf{x}])\rangle &\xrightarrow{1} \langle \mathsf{H}_e; \mathsf{S}; \mathsf{push}\ [0,\ \mathsf{v}_\mathsf{e}]\rangle \\ &\xrightarrow{1} \langle \mathsf{H}_e; \mathsf{S},\ [0,\ \mathsf{v}_\mathsf{e}]; \cdot\rangle \qquad \not\rightarrow\end{aligned}$$
so $\mathsf{H}' = \mathsf{H}_e$ and $\mathsf{S}' = \mathsf{S}, [0,\ \mathsf{v}_\mathsf{e}]$. Then we show the right disjunct of (13) by taking $\mathsf{v} = [0,\ \mathsf{v}_\mathsf{e}]$ and $W' = \triangleright^2 W_e$, noting that $W \sqsubseteq W_e \sqsubseteq W'$ by Lemma 1.5. All that remains is to show that $(W', [0,\ \mathsf{v}_\mathsf{e}]) \in \mathcal{V}[\![\tau_1 + \tau_2]\!]$, which, by definition, requires $(W', \mathsf{v}_\mathsf{e}) \in \mathcal{V}[\![\tau_1]\!]$. Recall that $(W_e, \mathsf{v}_\mathsf{e}) \in \mathcal{V}[\![\tau_1]\!]$. Then simply apply Lemmas 1.4, 1.6.

□

Lemma 1.15 (Compat $\mathtt{inr}\ \mathtt{e}$).

$$[\![\Gamma;\Gamma \vdash \mathsf{e} : \tau_2]\!] \implies [\![\Gamma;\Gamma \vdash \mathtt{inr}\ \mathsf{e} : \tau_1 + \tau_2]\!]$$

Proof. As in Lemma 1.14, exchanging τ_1, τ_2 and 0, 1 where appropriate. □

Lemma 1.16 (Compat $\mathtt{if}$).

$$[\![\Gamma;\Gamma \vdash \mathsf{e} : \mathtt{bool}]\!] \wedge [\![\Gamma;\Gamma \vdash \mathsf{e}_1 : \tau]\!] \wedge [\![\Gamma;\Gamma \vdash \mathsf{e}_2 : \tau]\!] \implies [\![\Gamma;\Gamma \vdash \mathtt{if}\ \mathsf{e}\ \mathsf{e}_1\ \mathsf{e}_2 : \tau]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^+$ in the goal and pushing substitutions, we are to show that

$$\big(W, \big(\text{close}\ \big(\gamma_\Gamma, \text{close}\ \big(\gamma_\Gamma, \mathsf{e}^+\big)\big),\ \text{if0 close}\ \big(\gamma_\Gamma, \text{close}\ \big(\gamma_\Gamma, \mathsf{e}_1{}^+\big)\big)\ \ \text{close}\ \big(\gamma_\Gamma, \text{close}\ \big(\gamma_\Gamma, \mathsf{e}_2{}^+\big)\big)\big)\big) \in \mathcal{E}[\![\tau]\!]$$

given arbitary $W, \gamma_\Gamma, \gamma_\Gamma$ such that $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]$, we are to show that

$$\mathsf{S}' = \mathsf{Fail\ c} \wedge \mathsf{c} \in \textsc{OkErr} \vee \exists \mathsf{v}, W' \sqsupseteq W.\ \big(\mathsf{S}' = \mathsf{S}, \mathsf{v} \wedge \mathsf{H}' : W' \wedge (W', \mathsf{v}) \in \mathcal{V}[\![\tau]\!]\big) \tag{14}$$

given arbitrary $\mathsf{H}{:}W, \mathsf{S}, \mathsf{H}', \mathsf{S}', j < W.k$ such that

$$\langle \mathsf{H}; \mathsf{S}; \mathsf{close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e}^+\right)\right),\ \mathsf{if0}\ (\ldots)\ (\ldots)\rangle \xrightarrow{j} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \nrightarrow$$

The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $j_e \leq j, \mathsf{H}_e, \mathsf{S}_e$ such that

$$\langle \mathsf{H}; \mathsf{S}; \mathsf{close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathsf{e}^+))\rangle \xrightarrow{j_e} \langle \mathsf{H}_e; \mathsf{S}_e; \cdot\rangle \nrightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(1) $\mathsf{S}_e = \mathsf{S}' = \mathsf{Fail\ c} \wedge \mathsf{c} \in \textsc{OkErr}$ and $\mathsf{H}_e = \mathsf{H}'$.
In this case, we have the left disjunct of (14).

(2)
$$\exists \mathsf{v_e}, W_e \sqsupseteq W.\ \big(\mathsf{S}_e = \mathsf{S}, \mathsf{v_e} \wedge \mathsf{H}_e : W_e \wedge (W_e, \mathsf{v_e}) \in \mathcal{V}[\![\mathtt{bool}]\!]\big)$$

and

$$\langle \mathsf{H}_e; \mathsf{S}_e; \mathsf{if0\ close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e_1}^+\right)\right)\ \mathsf{close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e_2}^+\right)\right)\rangle \xrightarrow{j-j_e} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \nrightarrow$$

Expanding the definition of $\mathcal{V}[\![\mathtt{bool}]\!]$, we have that

$$\mathsf{v_e} = \mathsf{n}$$

Without loss of generality, suppose $\mathsf{v_e} = \mathsf{n} = 0$. Then by the operational semantics of StackLang,

$$\langle \mathsf{H}_e; \mathsf{S}_e,\ 0; \mathsf{if0\ close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e_1}^+\right)\right)\ \mathsf{close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e_2}^+\right)\right)\rangle$$
$$\xrightarrow{1} \langle \mathsf{H}_e; \mathsf{S}; \mathsf{close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e_1}^+\right)\right)\ \rangle$$

Now, by expanding the definition of $[\![\cdot]\!]$ and $\mathcal{E}[\![\cdot]\!]$ in the second premise and specializing where appropriate, we have that

$$\mathsf{S}' = \mathsf{Fail\ c} \wedge \mathsf{c} \in \textsc{OkErr} \vee \exists \mathsf{v}, W' \sqsupseteq W_e.\ \big(\mathsf{S}' = \mathsf{S}, \mathsf{v} \wedge \mathsf{H}' : W' \wedge (W', \mathsf{v}) \in \mathcal{V}[\![\tau]\!]\big)$$

If we have the left disjunct, then we have the left disjunct of (14). If we have the right disjunct, then we have the right disjunct of (14) since $W \sqsubseteq W_e \sqsubseteq W'$ by Lemma 1.5.

The case in which $\mathsf{v_n} = \mathsf{n} \neq 0$ proceeds analogously over the third premise, exchanging $0, \mathsf{n}$ where appropriate.

□

Lemma 1.17 (Compat `match`).

$$[\![\Gamma; \Gamma \vdash \mathsf{e} : \tau_1 + \tau_2]\!] \wedge [\![\Gamma; \Gamma, \mathsf{x} : \tau_1 \vdash \mathsf{e_1} : \tau]\!] \wedge [\![\Gamma; \Gamma, \mathsf{y} : \tau_2 \vdash \mathsf{e_2} : \tau]\!]$$
$$\implies [\![\Gamma; \Gamma \vdash \mathtt{match\ e\ x\{e_1\}\ y\{e_2\}} : \tau_1 + \tau_2]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^+$ in the goal and pushing substitutions, we are to show that

$$(W, \big(\mathsf{close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathsf{e}^+)), \mathsf{P},$$
$$\mathsf{if0\ (lam\ x.close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathsf{e_1}^+)))\ (\mathsf{lam\ y.close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathsf{e_2}^+))))\big) \in \mathcal{E}[\![\tau]\!]$$

where $\mathsf{P} = \mathsf{DUP},\ \mathsf{push\ 1, idx},\ \mathsf{SWAP},\ \mathsf{push\ 0},\ \mathsf{idx}$

given arbitary $W, \gamma_\Gamma, \gamma_\Gamma$ such that $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]$, we are to show that

$$\mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \text{\textsc{OkErr}} \vee \exists \mathsf{v}, W' \sqsupseteq W.\ \big(\mathsf{S}' = \mathsf{S}, \mathsf{v} \wedge \mathsf{H}' : W' \wedge (W', \mathsf{v}) \in \mathcal{V}[\![\tau]\!]\big) \tag{15}$$

given arbitrary $\mathsf{H}{:}W, \mathsf{S}, \mathsf{H}', \mathsf{S}', j < W.k$ such that

$$\langle \mathsf{H}; \mathsf{S}; \mathsf{close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathsf{e}^+)),\ \mathsf{P},\ \mathsf{if0}\ (\mathsf{lam}\ \mathsf{x}.\dots)\ (\mathsf{lam}\ \mathsf{y}.\dots)\rangle \xrightarrow{j} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle$$

The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $j_e \leq j, \mathsf{H}_e, \mathsf{S}_e$ such that

$$\langle \mathsf{H}; \mathsf{S}; \mathsf{close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathsf{e}^+)),\rangle \xrightarrow{j_e} \langle \mathsf{H}_e; \mathsf{S}_e; \cdot\rangle \not\twoheadrightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(1) $\mathsf{S}_e = \mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \text{\textsc{OkErr}}$ and $\mathsf{H}_e = \mathsf{H}'$.
In this case, we have the left disjunct of (15).

(2)
$$\exists \mathsf{v}_e, W_e \sqsupseteq W.\ \big(\mathsf{S}_e = \mathsf{S}, \mathsf{v}_e \wedge \mathsf{H}_e : W_e \wedge (W_e, \mathsf{v}_e) \in \mathcal{V}[\![\tau_1 + \tau_2]\!]\big)$$

and

$$\langle \mathsf{H}_e; \mathsf{S}_e; \mathsf{P},\ \mathsf{if0}\ (\mathsf{lam}\ \mathsf{x}.\dots)\ (\mathsf{lam}\ \mathsf{y}.\dots)\rangle \xrightarrow{j-j_e} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \not\twoheadrightarrow$$

Expanding the definition of $\mathcal{V}[\![\tau_1 + \tau_2]\!]$, we have that

$$(\exists \mathsf{v}_1.\mathsf{v}_e = [0, \mathsf{v}_1] \wedge \mathsf{v}_1 \in \mathcal{V}[\![\tau_1]\!]) \vee (\exists \mathsf{v}_2.\mathsf{v}_e = [1, \mathsf{v}_2] \wedge \mathsf{v}_2 \in \mathcal{V}[\![\tau_2]\!])$$

Without loss of generality, suppose we have the left disjunct. Then by the operational semantics of StackLang,

$$\begin{aligned}
\langle \mathsf{H}_e; \mathsf{S}_e,\ [0,\ \mathsf{v}_1]; \mathsf{P},\ \mathsf{if0}\ (\mathsf{lam}\ \mathsf{x}.\dots)\ (\mathsf{lam}\ \mathsf{y}.\dots)\rangle &\xrightarrow{11} \langle \mathsf{H}_e; \mathsf{S},\ \mathsf{v}_1, 0; \mathsf{if0}\ (\mathsf{lam}\ \mathsf{x}.\dots)\ (\mathsf{lam}\ \mathsf{y}.\dots)\rangle \\
&\xrightarrow{1} \langle \mathsf{H}_e; \mathsf{S},\ \mathsf{v}_1; (\mathsf{lam}\ \mathsf{x}.\mathsf{close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathsf{e}_1{}^+)))\ \rangle \\
&\xrightarrow{1} \langle \mathsf{H}_e; \mathsf{S}; \mathsf{close}(\gamma_\Gamma, \mathsf{close}(\gamma_{\Gamma, \mathsf{x}:\tau_1}[\mathsf{x} \mapsto \mathsf{v}_1], \mathsf{e}_1{}^+))\rangle
\end{aligned}$$

where in the last step we push the substitution inside γ_Γ. Now, by expanding the definition of $[\![\cdot]\!]$ and $\mathcal{E}[\![\cdot]\!]$ in the second premise and specializing where appropriate, we have that

$$\mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \text{\textsc{OkErr}} \vee \exists \mathsf{v}, W' \sqsupseteq W_e.\ \big(\mathsf{S}' = \mathsf{S}, \mathsf{v} \wedge \mathsf{H}' : W' \wedge (W', \mathsf{v}) \in \mathcal{V}[\![\tau]\!]\big)$$

If we have the left disjunct, then we have the left disjunct of (15). If we have the right disjunct, then we have the right disjunct of (15) since $W \sqsubseteq W_e \sqsubseteq W'$ by Lemma 1.5.

The case in which $\mathsf{v}_e = [1, \mathsf{v}_2]$ proceeds analogously over the third premise, exchanging τ_1, τ_2 and 0, 1 and x, y where appropriate.

□

Lemma 1.18 (Compat $(\mathsf{e}_1,\ \mathsf{e}_2)$).

$$[\![\Gamma; \Gamma \vdash \mathsf{e}_1 : \tau_1]\!] \wedge [\![\Gamma; \Gamma \vdash \mathsf{e}_2 : \tau_2]\!] \implies [\![\Gamma; \Gamma \vdash (\mathsf{e}_1,\ \mathsf{e}_2) : \tau_1 \times \tau_2]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^+$ in the goal and pushing substitutions, we are to show that

$$\big(W, \big(\mathsf{close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathsf{e}_1{}^+)),\ \mathsf{close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e}_2{}^+\right)\right), \mathsf{lam}\ \mathsf{x}_2.\mathsf{lam}\ \mathsf{x}_1.\ (\mathsf{push}\ [\mathsf{x}_1,\ \mathsf{x}_2])\big)\big) \in \mathcal{E}[\![\tau_1 \times \tau_2]\!]$$

given arbitary $W, \gamma_\Gamma, \gamma_\Gamma$ such that $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]$, we are to show that

$$\mathsf{S}' = \mathsf{Fail\ c} \wedge \mathsf{c} \in \textsc{OkErr} \vee \exists \mathsf{v}, W' \sqsupseteq W.\ \big(\mathsf{S}' = \mathsf{S}, \mathsf{v} \wedge \mathsf{H}' : W' \wedge (W', \mathsf{v}) \in \mathcal{V}[\![\tau_1 \times \tau_2]\!]\big) \tag{16}$$

given arbitrary $\mathsf{H}{:}W, \mathsf{S}, \mathsf{H}', \mathsf{S}', j < W.k$ such that

$$\langle \mathsf{H}; \mathsf{S}; \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathsf{e}_1{}^+)),\ \mathrm{close}\left(\gamma_\Gamma, \mathrm{close}\left(\gamma_\Gamma, \mathsf{e}_2{}^+\right)\right), \ldots\rangle \xrightarrow{j} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \not\rightarrow$$

The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $j_1 \leq j, \mathsf{H}_1, \mathsf{S}_1$ such that

$$\langle \mathsf{H}; \mathsf{S}; \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathsf{e}_1{}^+))\rangle \xrightarrow{j_1} \langle \mathsf{H}_1; \mathsf{S}_1; \cdot\rangle \not\rightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(1) $\mathsf{S}_1 = \mathsf{S}' = \mathsf{Fail\ c} \wedge \mathsf{c} \in \textsc{OkErr}$ and $\mathsf{H}_1 = \mathsf{H}'$.
In this case, we have the left disjunct of (16).

(2)

$$\exists \mathsf{v}_1, W_1 \sqsupseteq W.\ \big(\mathsf{S}_1 = \mathsf{S}, \mathsf{v}_1 \wedge \mathsf{H}_1 : W_1 \wedge (W_1, \mathsf{v}_1) \in \mathcal{V}[\![\tau_1]\!]\big)$$

and

$$\langle \mathsf{H}_1; \mathsf{S}_1; \mathrm{close}\left(\gamma_\Gamma, \mathrm{close}\left(\gamma_\Gamma, \mathsf{e}_2{}^+\right)\right), \mathsf{lam\ x_2.lam\ x_1.\,(push\ [x_1,\ x_2])}\rangle \xrightarrow{j-j_1} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \not\rightarrow$$

Applying Lemma 1.2 again, there is $j_2 \leq j - j_1, \mathsf{H}_2, \mathsf{S}_2$ such that

$$\langle \mathsf{H}; \mathsf{S}; \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathsf{e}_2{}^+))\rangle \xrightarrow{j_2} \langle \mathsf{H}_2; \mathsf{S}_2; \cdot\rangle \not\rightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(a) $\mathsf{S}_2 = \mathsf{S}' = \mathsf{Fail\ c} \wedge \mathsf{c} \in \textsc{OkErr}$ and $\mathsf{H}_2 = \mathsf{H}'$.
In this case, we have the left disjunct of (16).

(b)

$$\exists \mathsf{v}_2, W_2 \sqsupseteq W_1.\ \big(\mathsf{S}_2 = \mathsf{S}_1, \mathsf{v}_2 \wedge \mathsf{H}_2 : W_2 \wedge (W_2, \mathsf{v}_2) \in \mathcal{V}[\![\tau_2]\!]\big)$$

and

$$\langle \mathsf{H}_2; \mathsf{S}_2; \mathsf{lam\ x_2.lam\ x_1.\,(push\ [x_1,\ x_2])}\rangle \xrightarrow{j-j_1-j_2} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \not\rightarrow$$

Recall that $\mathsf{S}_1 = \mathsf{S}, \mathsf{v}_1$, so $\mathsf{S}_2 = \mathsf{S}_1, \mathsf{v}_2 = \mathsf{S}, \mathsf{v}_1, \mathsf{v}_2$. Then by the operational semantics of $\mathsf{StackLang}$,

$$\langle \mathsf{H}_2; \mathsf{S}, \mathsf{v}_1, \mathsf{v}_2; \mathsf{lam\ x_2.lam\ x_1.\,(push\ [x_1,\ x_2])}\rangle \xrightarrow{3} \langle \mathsf{H}_2; \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2]; \cdot\rangle \not\rightarrow$$

so $\mathsf{H}' = \mathsf{H}_2$ and $\mathsf{S}' = \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2]$. Then we show the right disjunct of (16) by taking $\mathsf{v} = [\mathsf{v}_1, \mathsf{v}_2]$ and $W' = \triangleright^3 W_2$, noting that $W \sqsubseteq W_1 \sqsubseteq W_2 \sqsubseteq W'$ by Lemma 1.5. All that remains is to show that $(W', [\mathsf{v}_1, \mathsf{v}_2]) \in \mathcal{V}[\![\tau_1 \times \tau_2]\!]$, which requires $(W', \mathsf{v}_1) \in \mathcal{V}[\![\tau_1]\!]$ and $(W', \mathsf{v}_2) \in \mathcal{V}[\![\tau_2]\!]$. Recall that $(W_1, \mathsf{v}_1) \in \mathcal{V}[\![\tau_1]\!]$ and $(W_2, \mathsf{v}_2) \in \mathcal{V}[\![\tau_2]\!]$. Then simply apply Lemmas 1.4, 1.6.

□

Lemma 1.19 (Compat $\mathtt{fst\ e}$).

$$[\![\Gamma; \Gamma \vdash \mathtt{e} : \tau_1 \times \tau_2]\!] \implies [\![\Gamma; \Gamma \vdash \mathtt{fst\ e} : \tau_1]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^+$ and pushing substitutions in the goal, we are to show that

$$\left(W, \left(\mathsf{close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e}^+\right)\right), \mathsf{push}\ 0,\ \mathsf{idx}\right)\right) \in \mathcal{E}[\![\tau_1]\!]$$

given arbitary $W, \gamma_\Gamma, \gamma_\Gamma$ such that $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]$, we are to show that

$$\mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \textsc{OkErr} \vee \exists \mathsf{v}, W' \sqsupseteq W.\ \left(\mathsf{S}' = \mathsf{S}, \mathsf{v} \wedge \mathsf{H}' : W' \wedge (W', \mathsf{v}) \in \mathcal{V}[\![\tau_1]\!]\right) \qquad (17)$$

given arbitrary $\mathsf{H}{:}W, \mathsf{S}, \mathsf{H}', \mathsf{S}', j < W.k$ such that

$$\langle \mathsf{H}; \mathsf{S}; \mathsf{close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e}^+\right)\right),\ \mathsf{push}\ 0,\ \mathsf{idx}\rangle \xrightarrow{j} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \not\twoheadrightarrow$$

The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $j_e \leq j, \mathsf{H}_e, \mathsf{S}_e$ such that

$$\langle \mathsf{H}; \mathsf{S}; \mathsf{close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e}^+\right)\right)\rangle \xrightarrow{j_e} \langle \mathsf{H}_e; \mathsf{S}_e; \cdot\rangle \not\twoheadrightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(1) $\mathsf{S}_e = \mathsf{S}' = \mathsf{Fail}\ \mathsf{c} \wedge \mathsf{c} \in \textsc{OkErr}$ and $\mathsf{H}_e = \mathsf{H}'$.
In this case, we have the left disjunct of (17).

(2)

$$\exists \mathsf{v_e}, W_e \sqsupseteq W.\ \left(\mathsf{S}_e = \mathsf{S}, \mathsf{v_e} \wedge \mathsf{H}_e : W_e \wedge (W_e, \mathsf{v_e}) \in \mathcal{V}[\![\tau_1 \times \tau_2]\!]\right)$$

and

$$\langle \mathsf{H}_e; \mathsf{S}_e; \mathsf{push}\ 0,\ \mathsf{idx}\rangle \xrightarrow{j-j_e} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \not\twoheadrightarrow$$

Expanding the definition of $\mathcal{V}[\![\tau_1 \times \tau_2]\!]$ we have that

$$\mathsf{v_e} = [\mathsf{v}_1, \mathsf{v}_2] \wedge (W_e, \mathsf{v}_1) \in \mathcal{V}[\![\tau_1]\!] \wedge (W_e, \mathsf{v}_2) \in \mathcal{V}[\![\tau_2]\!]$$

Then by the operational semantics of StackLang,

$$\langle \mathsf{H}_e; \mathsf{S}, [\mathsf{v}_1, \mathsf{v}_2]; \mathsf{push}\ 0,\ \mathsf{idx}\rangle \xrightarrow{2} \langle \mathsf{H}; \mathsf{S}, \mathsf{v}_1; \cdot\rangle \not\twoheadrightarrow$$

so $\mathsf{H}' = \mathsf{H}_e$ and $\mathsf{S}' = \mathsf{S}, \mathsf{v}_1$. Then we show the right disjunct of (17) by taking $\mathsf{v} = \mathsf{v}_1$ and $W' = \triangleright^2 W_e$, noting that $W \sqsubseteq W_e \sqsubseteq W'$ by Lemma 1.5. All that remains is to show that $(W', \mathsf{v}_1) \in \mathcal{V}[\![\tau_1]\!]$. Recall that $(W_e, \mathsf{v}_1) \in \mathcal{V}[\![\tau_1]\!]$, so simply apply Lemmas 1.4, 1.6.

□

Lemma 1.20 (Compat $\mathsf{snd}\ \mathsf{e}$).

$$[\![\Gamma; \Gamma \vdash \mathsf{e} : \tau_1 \times \tau_2]\!] \implies [\![\Gamma; \Gamma \vdash \mathsf{snd}\ \mathsf{e} : \tau_2]\!]$$

Proof. As in Lemma 1.19, exchanging τ_1, τ_2 and 0, 1 where appropriate. □

Lemma 1.21 (Compat $\lambda \mathsf{x} : \tau.\mathsf{e}$).

$$[\![\Gamma; \Gamma, \mathsf{x} : \tau_1 \vdash \mathsf{e} : \tau_2]\!] \implies [\![\Gamma; \Gamma \vdash \lambda \mathsf{x} : \tau_1.\mathsf{e} : \tau_1 \to \tau_2]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^+$ in the goal and pushing substitutions, we are to show that

$$\left(W, \mathsf{push}\left(\mathsf{thunk}\ \mathsf{lam}\ \mathsf{x}.\mathsf{close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e}^+\right)\right)\right)\right) \in \mathcal{E}[\![\tau_1 \to \tau_2]\!]$$

given arbitary $W, \gamma_\Gamma, \gamma_\Gamma$ such that $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$. Applying Lemma 1.7, we are to show that

$$\left(W, \left(\mathsf{thunk}\ \mathsf{lam}\ \mathsf{x}.\mathsf{close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e}^+\right)\right)\right)\right) \in \mathcal{V}[\![\tau_1 \to \tau_2]\!]$$

Expanding the definition of $\mathcal{V}[\![\tau_1 \longrightarrow \tau_2]\!]$ and pushing the substitution into γ_Γ, we are to show that

$$(W',\ \mathrm{close}\ (\gamma_\Gamma, \mathrm{close}\ (\gamma_{\Gamma,\mathrm{x}:\tau_1}[\mathrm{x} \mapsto \mathrm{v}], \mathrm{e}^+))) \in \mathcal{E}[\![\tau_2]\!]$$

given arbitrary $W' \sqsupseteq W$ and v such that $(W', \mathrm{v}) \in \mathcal{V}[\![\tau_1]\!]$. We have this by expanding the definition of $[\![\cdot]\!]$ in the premise and specializing where appropriate. □

Lemma 1.22 (Compat $\mathrm{e}_1\ \mathrm{e}_2$).

$$[\![\Gamma;\Gamma \vdash \mathrm{e}_1 : \tau_1 \longrightarrow \tau_2]\!] \wedge [\![\Gamma;\Gamma \vdash \mathrm{e}_2 : \tau_1]\!] \implies [\![\Gamma;\Gamma \vdash \mathrm{e}_1\ \mathrm{e}_2 : \tau_2]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^+$ in the goal and pushing substitutions, we are to show that

$$(W, \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathrm{e}_1{}^+)), \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathrm{e}_2{}^+)), \mathrm{SWAP}, \mathrm{call}) \in \mathcal{E}[\![\tau_2]\!]$$

given arbitary $W, \gamma_\Gamma, \gamma_\Gamma$ such that $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]$, we are to show that

$$\mathrm{S}' = \mathrm{Fail}\ \mathrm{c} \wedge \mathrm{c} \in \textsc{OkErr} \vee \exists \mathrm{v}, W' \sqsupseteq W.\ \big(\mathrm{S}' = \mathrm{S}, \mathrm{v} \wedge \mathrm{H}' : W' \wedge (W', \mathrm{v}) \in \mathcal{V}[\![\tau_2]\!]\big) \tag{18}$$

given arbitrary $\mathrm{H}{:}W, \mathrm{S}, \mathrm{H}', \mathrm{S}', j < W.k$ such that

$$\langle \mathrm{H}; \mathrm{S}; \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathrm{e}_1{}^+)), \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathrm{e}_2{}^+)), \mathrm{SWAP}, \mathrm{call}\rangle \xrightarrow{j} \langle \mathrm{H}'; \mathrm{S}'; \cdot\rangle \nrightarrow$$

The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $j_1 \leq j, \mathrm{H}_1, \mathrm{S}_1$ such that

$$\langle \mathrm{H}; \mathrm{S}; \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathrm{e}_1{}^+)),\rangle \xrightarrow{j_1} \langle \mathrm{H}_1; \mathrm{S}_1; \cdot\rangle \nrightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(1) $\mathrm{S}_1 = \mathrm{S}' = \mathrm{Fail}\ \mathrm{c} \wedge \mathrm{c} \in \textsc{OkErr}$ and $\mathrm{H}_1 = \mathrm{H}'$.
In this case, we have the left disjunct of (18).

(2)

$$\exists \mathrm{v}_1, W_1 \sqsupseteq W.\ \big(\mathrm{S}_1 = \mathrm{S}, \mathrm{v}_1 \wedge \mathrm{H}_1 : W_1 \wedge (W_1, \mathrm{v}_1) \in \mathcal{V}[\![\tau_1 \longrightarrow \tau_2]\!]\big)$$

and

$$\langle \mathrm{H}_1; \mathrm{S}_1; \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathrm{e}_2{}^+)), \mathrm{SWAP}, \mathrm{call}\rangle \xrightarrow{j-j_1} \langle \mathrm{H}'; \mathrm{S}'; \cdot\rangle \nrightarrow$$

Applying Lemma 1.2 again, there is $j_2 \leq j - j_1, \mathrm{H}_2, \mathrm{S}_2$ such that

$$\langle \mathrm{H}; \mathrm{S}; \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathrm{e}_2{}^+)),\rangle \xrightarrow{j_2} \langle \mathrm{H}_2; \mathrm{S}_2; \cdot\rangle \nrightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(a) $\mathrm{S}_2 = \mathrm{S}' = \mathrm{Fail}\ \mathrm{c} \wedge \mathrm{c} \in \textsc{OkErr}$ and $\mathrm{H}_2 = \mathrm{H}'$.
In this case, we have the left disjunct of (18).

(b)

$$\exists \mathrm{v}_2, W_2 \sqsupseteq W_1.\ \big(\mathrm{S}_2 = \mathrm{S}_1, \mathrm{v}_2 \wedge \mathrm{H}_2 : W_2 \wedge (W_2, \mathrm{v}_2) \in \mathcal{V}[\![\tau_1]\!]\big)$$

and

$$\langle \mathrm{H}_2; \mathrm{S}_2; \mathrm{SWAP}, \mathrm{call}\rangle \xrightarrow{j-j_1-j_2} \langle \mathrm{H}'; \mathrm{S}'; \cdot\rangle \nrightarrow$$

Recall that $(W_1, \mathrm{v}_1) \in \mathcal{V}[\![\tau_1 \longrightarrow \tau_2]\!]$, so by expanding the definition of $\mathcal{V}[\![\tau_1 \longrightarrow \tau_2]\!]$ and specializing as appropriate, we have that

$$\mathrm{v}_1 = \mathrm{thunk}\ \mathrm{lam}\ \mathrm{x}.\mathrm{P} \wedge (W_2, [\mathrm{x} \mapsto \mathrm{v}_2]\mathrm{P}) \in \mathcal{E}[\![\tau_2]\!]$$

Recall that $\mathsf{S}_1 = \mathsf{S}, \mathsf{v}_1$, so $\mathsf{S}_2 = \mathsf{S}_1, \mathsf{v}_2 = \mathsf{S}, \mathsf{thunk\ lam\ x.P}, \mathsf{v}_2$. Then by the operational semantics of StackLang,

$$\begin{aligned}\langle \mathsf{H}_2; \mathsf{S}, \mathsf{thunk\ lam\ x.P}, \mathsf{v}_2; \mathsf{SWAP}, \mathsf{call}\rangle &\xrightarrow{4} \langle \mathsf{H}_2; \mathsf{S}, \mathsf{v}_2, \mathsf{thunk\ lam\ x.P}; \mathsf{call}\rangle\\ &\xrightarrow{1} \langle \mathsf{H}_2; \mathsf{S}, \mathsf{v}_2; \mathsf{lam\ x.P}\rangle\\ &\xrightarrow{1} \langle \mathsf{H}_2; \mathsf{S}; [\mathsf{x} \mapsto \mathsf{v}_2]\mathsf{P}\rangle\\ &\xrightarrow{j-j_1-j_2-6} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle\\ &\not\rightarrow\end{aligned}$$

Now, recall that $(W_2, [\mathsf{x} \mapsto \mathsf{v}_2]\mathsf{P}) \in \mathcal{E}[\![\tau_2]\!]$, so by expanding the definition of $\mathcal{E}[\![\cdot]\!]$ and specializing where appropriate, we have that

$$\mathsf{S}' = \mathsf{Fail\ c} \wedge \mathsf{c} \in \textsc{OkErr} \vee \exists \mathsf{v}, W' \sqsupseteq W_2.\ \big(\mathsf{S}' = \mathsf{S}, \mathsf{v} \wedge \mathsf{H}' : W' \wedge (W', \mathsf{v}) \in \mathcal{V}[\![\tau_2]\!]\big)$$

If we have the left disjunct, then we have the left disjunct of (18). If we have the right disjunct, then we have the right disjunct of (18) since $W \sqsubseteq W_1 \sqsubseteq W_2 \sqsubseteq W'$ by Lemma 1.5.

□

Lemma 1.23 (Compat $\mathtt{ref\ e}$).

$$[\![\Gamma; \Gamma \vdash \mathtt{e} : \tau]\!] \implies [\![\Gamma; \Gamma \vdash \mathtt{ref\ e} : \mathtt{ref}\ \tau]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^{+}$ in the goal and pushing substitutions, we are to show that

$$(W, \mathsf{close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathtt{e}^{+})), \mathsf{alloc}) \in \mathcal{E}[\![\mathtt{ref}\ \tau]\!]$$

given arbitary $W, \gamma_\Gamma, \gamma_\Gamma$ such that $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]$, we are to show that

$$\mathsf{S}' = \mathsf{Fail\ c} \wedge \mathsf{c} \in \textsc{OkErr} \vee \exists \mathsf{v}, W' \sqsupseteq W.\ \big(\mathsf{S}' = \mathsf{S}, \mathsf{v} \wedge \mathsf{H}' : W' \wedge (W', \mathsf{v}) \in \mathcal{V}[\![\mathtt{ref}\ \tau]\!]\big) \tag{19}$$

given arbitrary $\mathsf{H}{:}W, \mathsf{S}, \mathsf{H}', \mathsf{S}', j < W.k$ such that

$$\langle \mathsf{H}; \mathsf{S}; \mathsf{close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathtt{e}^{+})), \mathsf{alloc}\rangle \xrightarrow{j} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \not\rightarrow$$

The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $j_e \leq j, \mathsf{H}_e, \mathsf{S}_e$ such that

$$\langle \mathsf{H}; \mathsf{S}; \mathsf{close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathtt{e}^{+})),\rangle \xrightarrow{j_e} \langle \mathsf{H}_e; \mathsf{S}_e; \cdot\rangle \not\rightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(1) $\mathsf{S}_e = \mathsf{S}' = \mathsf{Fail\ c} \wedge \mathsf{c} \in \textsc{OkErr}$ and $\mathsf{H}_e = \mathsf{H}'$.
In this case, we have the left disjunct of (19).

(2)

$$\exists \mathsf{v}_\mathsf{e}, W_e \sqsupseteq W.\ \big(\mathsf{S}_e = \mathsf{S}, \mathsf{v}_\mathsf{e} \wedge \mathsf{H}_e : W_e \wedge (W_e, \mathsf{v}_\mathsf{e}) \in \mathcal{V}[\![\tau]\!]\big)$$

and

$$\langle \mathsf{H}_e; \mathsf{S}_e; \mathsf{alloc}\rangle \xrightarrow{j-j_e} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \not\rightarrow$$

By the operational semantics of StackLang,

$$\langle \mathsf{H}_e; \mathsf{S}, \mathsf{v}_\mathsf{e}; \mathsf{alloc}\rangle \xrightarrow{1} \langle \mathsf{H}_e \uplus \{\ell \mapsto \mathsf{v}_\mathsf{e}\}; \mathsf{S}, \ell; \cdot\rangle \not\rightarrow$$

for some ℓ, so $\mathrm{H}' = \mathrm{H}_e \uplus \{\ell \mapsto \mathrm{v_e}\}$ and $\mathrm{S}' = \mathrm{S}, \ell$. Then we have the right disjunct of (19) by taking $\mathrm{v} = \ell$ and $W' = (W_e.k - 1, \lfloor W_e.\Psi \rfloor_{W_e.k-1} \uplus \{\ell \mapsto \lfloor \mathcal{V}[\![\tau]\!] \rfloor_{W_e.k-1}\})$, observing that $(W', \ell) \in \mathcal{V}[\![\mathtt{ref}\ \tau]\!]$ by definition and $W \sqsubseteq W_e \sqsubseteq W'$ by Lemma 1.5.

□

Lemma 1.24 (Compat $\mathtt{!e}$).

$$[\![\Gamma; \Gamma \vdash \mathtt{e} : \mathtt{ref}\ \tau]\!] \implies [\![\Gamma; \Gamma \vdash \mathtt{!e} : \tau]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^{+}$ in the goal and pushing substitutions, we are to show that

$$(W, \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathrm{e}^{+})), \mathrm{read}) \in \mathcal{E}[\![\tau]\!]$$

given arbitary $W, \gamma_\Gamma, \gamma_\Gamma$ such that $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]$, we are to show that

$$\mathrm{S}' = \mathrm{Fail}\ \mathrm{c} \wedge \mathrm{c} \in \textsc{OkErr} \vee \exists \mathrm{v}, W' \sqsupseteq W.\ \big(\mathrm{S}' = \mathrm{S}, \mathrm{v} \wedge \mathrm{H}' : W' \wedge (W', \mathrm{v}) \in \mathcal{V}[\![\tau]\!]\big) \tag{20}$$

given arbitrary $\mathrm{H}{:}W, \mathrm{S}, \mathrm{H}', \mathrm{S}', j < W.k$ such that

$$\langle \mathrm{H}; \mathrm{S}; \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathrm{e}^{+})), \mathrm{read}\rangle \xrightarrow{j} \langle \mathrm{H}'; \mathrm{S}'; \cdot\rangle \not\rightarrow$$

The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $j_e \leq j, \mathrm{H}_e, \mathrm{S}_e$ such that

$$\langle \mathrm{H}; \mathrm{S}; \mathrm{close}(\gamma_\Gamma, \mathrm{close}(\gamma_\Gamma, \mathrm{e}^{+})),\rangle \xrightarrow{j_e} \langle \mathrm{H}_e; \mathrm{S}_e; \cdot\rangle \not\rightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(1) $\mathrm{S}_e = \mathrm{S}' = \mathrm{Fail}\ \mathrm{c} \wedge \mathrm{c} \in \textsc{OkErr}$ and $\mathrm{H}_e = \mathrm{H}'$.
In this case, we have the left disjunct of (20).

(2)

$$\exists \mathrm{v_e}, W_e \sqsupseteq W.\ (\mathrm{S}_e = \mathrm{S}, \mathrm{v_e} \wedge \mathrm{H}_e : W_e \wedge (W_e, \mathrm{v_e}) \in \mathcal{V}[\![\mathtt{ref}\ \tau]\!])$$

and

$$\langle \mathrm{H}_e; \mathrm{S}_e; \mathrm{read}\rangle \xrightarrow{j - j_e} \langle \mathrm{H}'; \mathrm{S}'; \cdot\rangle \not\rightarrow$$

Expanding the definition of $\mathcal{V}[\![\cdot]\!]$, we have that

$$\mathrm{v_e} = \ell \wedge W_e.\Psi(\ell) = \lfloor \mathcal{V}[\![\tau]\!] \rfloor_{We.k}$$

so $\mathrm{H}_e = \mathrm{H}'_e \uplus \{\ell \mapsto \mathrm{v}_\ell\}$ for some v_ℓ such that $\mathrm{v}_\ell \in \lfloor \mathcal{V}[\![\tau]\!] \rfloor_{We.k}$. Then by the operational semantics of StackLang,

$$\langle \mathrm{H}'_e \uplus \{\ell \mapsto \mathrm{v}_\ell\}; \mathrm{S}, \ell; \mathrm{read}\rangle \xrightarrow{1} \langle \mathrm{H}'_e \uplus \{\ell \mapsto \mathrm{v}_\ell\}; \mathrm{S}, \mathrm{v}_\ell; \cdot\rangle \not\rightarrow$$

so $\mathrm{H}' = \mathrm{H}'_e \uplus \{\ell \mapsto \mathrm{v}_\ell\}$ and $\mathrm{S}' = \mathrm{S}, \mathrm{v}_\ell$. Then we have the right disjunct of (20) by taking $\mathrm{v} = \mathrm{v}_\ell$ and $W' = \triangleright W_e$, noting that $W \sqsubseteq W_e \sqsubseteq W' = \triangleright W_e$ by Lemma 1.5.

□

Lemma 1.25 (Compat $\mathtt{e_1} := \mathtt{e_2}$).

$$[\![\Gamma; \Gamma \vdash \mathtt{e_1} : \mathtt{ref}\ \tau]\!] \wedge [\![\Gamma; \Gamma \vdash \mathtt{e_2} : \tau]\!] \implies [\![\Gamma; \Gamma \vdash \mathtt{e_1} := \mathtt{e_2} : \mathtt{unit}]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^{+}$ in the goal and pushing substitutions, we are to show that

$$(W, \left(\mathsf{close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathsf{e_1}^{+})),\ \mathsf{close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e_2}^{+}\right)\right), \mathsf{write},\ \mathsf{push}\ 0\right)) \in \mathcal{E}[\![\texttt{unit}]\!]$$

given arbitary $W, \gamma_\Gamma, \gamma_\Gamma$ such that $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]$, we are to show that

$$\mathsf{S}' = \mathsf{Fail\ c} \wedge \mathsf{c} \in \textsc{OkErr} \vee \exists \mathsf{v}, W' \sqsupseteq W.\ \left(\mathsf{S}' = \mathsf{S}, \mathsf{v} \wedge \mathsf{H}' : W' \wedge (W', \mathsf{v}) \in \mathcal{V}[\![\texttt{unit}]\!]\right) \qquad (21)$$

given arbitrary $\mathsf{H}{:}W, \mathsf{S}, \mathsf{H}', \mathsf{S}', j < W.k$ such that

$$\langle \mathsf{H}; \mathsf{S}; \mathsf{close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathsf{e_1}^{+})),\ \mathsf{close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e_2}^{+}\right)\right), \mathsf{write},\ \mathsf{push}\ 0\rangle \xrightarrow{j} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \nrightarrow$$

The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $j_1 \leq j, \mathsf{H}_1, \mathsf{S}_1$ such that

$$\langle \mathsf{H}; \mathsf{S}; \mathsf{close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathsf{e_1}^{+})),\rangle \xrightarrow{j_1} \langle \mathsf{H}_1; \mathsf{S}_1; \cdot\rangle \nrightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(1) $\mathsf{S}_1 = \mathsf{S}' = \mathsf{Fail\ c} \wedge \mathsf{c} \in \textsc{OkErr}$ and $\mathsf{H}_1 = \mathsf{H}'$.
In this case, we have the left disjunct of (21).

(2)
$$\exists \mathsf{v}_1, W_1 \sqsupseteq W.\ \left(\mathsf{S}_1 = \mathsf{S}, \mathsf{v}_1 \wedge \mathsf{H}_1 : W_1 \wedge (W_1, \mathsf{v}_1) \in \mathcal{V}[\![\texttt{ref}\ \tau]\!]\right)$$
and
$$\langle \mathsf{H}_1; \mathsf{S}_1; \mathsf{close}\left(\gamma_\Gamma, \mathsf{close}\left(\gamma_\Gamma, \mathsf{e_2}^{+}\right)\right), \mathsf{write},\ \mathsf{push}\ 0\rangle \xrightarrow{j-j_1} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \nrightarrow$$
Expanding the definition of $\mathcal{V}[\![\texttt{ref}\ ]\!]$, we have that
$$\mathsf{v}_1 = \ell \wedge W_1.\Psi(\ell) = \lfloor \mathcal{V}[\![\tau]\!] \rfloor_{W1.k}$$
for some ℓ.
Applying Lemma 1.2 again, there is $j_2 \leq j - j_1, \mathsf{H}_2, \mathsf{S}_2$ such that
$$\langle \mathsf{H}_1; \mathsf{S}_1; \mathsf{close}(\gamma_\Gamma, \mathsf{close}(\gamma_\Gamma, \mathsf{e_2}^{+})),\rangle \xrightarrow{j_2} \langle \mathsf{H}_2; \mathsf{S}_2; \cdot\rangle \nrightarrow$$
Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

  (a) $\mathsf{S}_2 = \mathsf{S}' = \mathsf{Fail\ c} \wedge \mathsf{c} \in \textsc{OkErr}$ and $\mathsf{H}_2 = \mathsf{H}'$.
  In this case, we have the left disjunct of (21).

  (b)
  $$\exists \mathsf{v}_2, W_2 \sqsupseteq W_1.\ \left(\mathsf{S}_2 = \mathsf{S}_1, \mathsf{v}_2 \wedge \mathsf{H}_2 : W_2 \wedge (W_2, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]\right)$$
  and
  $$\langle \mathsf{H}_2; \mathsf{S}_2; \mathsf{write},\ \mathsf{push}\ 0\rangle \xrightarrow{j-j_1-j_2} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \nrightarrow$$
  Recall that $W_1.\Psi(\ell) = \lfloor \mathcal{V}[\![\tau]\!] \rfloor_{W1.k}$. Then since $W_1 \sqsubseteq W_2$, we also have that $W_2.\Psi(\ell) = \lfloor \mathcal{V}[\![\tau]\!] \rfloor_{W2.k}$. Then since $\mathsf{H}_2 : W_2$, we may write $\mathsf{H}_2 = \mathsf{H}_2' \uplus \{\ell \mapsto \mathsf{v}_\ell\}$ for some v_ℓ such that $\mathsf{v}_\ell \in \lfloor \mathcal{V}[\![\tau]\!] \rfloor_{W2.k}$.
  Recall that $\mathsf{S}_1 = \mathsf{S}, \ell$, so $\mathsf{S}_2 = \mathsf{S}_1, \mathsf{v}_2 = \mathsf{S}, \ell, \mathsf{v}_2$. Then by the operational semantics of StackLang,
  $$\langle \mathsf{H}_2' \uplus \{\ell \mapsto \mathsf{v}_\ell\}; \mathsf{S}, \ell, \mathsf{v}_2; \mathsf{write},\ \mathsf{push}\ 0\rangle \xrightarrow{2} \langle \mathsf{H}_2' \uplus \{\ell \mapsto \mathsf{v}_2\}; \mathsf{S}, 0; \cdot\rangle$$
  so $\mathsf{H}' = \mathsf{H}_2' \uplus \{\ell \mapsto \mathsf{v}_2\}$ and $\mathsf{S}' = \mathsf{S}, 0$. Then we show the right disjunct of (19) by taking $\mathsf{v} = 0$ and $W' = \triangleright^2 W_2$, noting that $W \sqsubseteq W_1 \sqsubseteq W_2 \sqsubseteq W'$ by Lemma 1.5. All that remains is to show that $(W', 0) \in \mathcal{V}[\![\texttt{unit}]\!]$, which we have by definition.

□

Lemma 1.26 (Compat $(\!|\mathrm{e}|\!)_{\tau}$).

$$[\![\Gamma;\Gamma \vdash \mathrm{e} : \tau]\!] \wedge \tau \sim \tau \implies [\![\Gamma;\Gamma \vdash (\!|\mathrm{e}|\!)_{\tau} : \tau]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^{+}$ and pushing substitutions in the goal, we are to show that

$$\left(W, \left(\mathrm{close}\left(\gamma_{\Gamma}, \mathrm{close}\left(\gamma_{\Gamma}, \mathrm{e}^{+}\right)\right), \mathrm{C}_{\tau \mapsto \tau}\right)\right) \in \mathcal{E}[\![\tau]\!]$$

given arbitary $W, \gamma_{\Gamma}, \gamma_{\Gamma}$ such that $(W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]$.

We proceed by appealing to Theorem 1.3, which says that it suffices to show that:

$$\left(W, \left(\mathrm{close}\left(\gamma_{\Gamma}, \mathrm{close}\left(\gamma_{\Gamma}, \mathrm{e}^{+}\right)\right)\right)\right) \in \mathcal{E}[\![\tau]\!]$$

But this is exactly what our hypothesis tells us, appropriately applied. □

1.6.3 RefLL Compatibility Lemmas.

Lemma 1.27 (Compat n).

$$[\![\Gamma;\Gamma \vdash \mathrm{n} : \mathrm{int}]\!]$$

Proof. As in Lemma 1.11, exchanging `unit`, int and 0, n where appropriate. □

Lemma 1.28 (Compat x).

$$[\![\Gamma;\Gamma, \mathrm{x} : \tau \vdash \mathrm{x} : \tau]\!]$$

Proof. As in Lemma 1.13, exchanging τ, τ where appropriate. □

Lemma 1.29 (Compat $[\mathrm{e}_1, \ldots, \mathrm{e}_n]$).

$$[\![\Gamma;\Gamma \vdash \mathrm{e}_1 : \tau]\!] \wedge \ldots \wedge [\![\Gamma;\Gamma \vdash \mathrm{e}_n : \tau]\!] \implies [\![\Gamma;\Gamma \vdash [\mathrm{e}_1, \ldots, \mathrm{e}_n] : [\tau]]\!]$$

Proof. As in Lemma 1.18, exchanging τ_1, τ_2 with $[\tau]$ and generalizing $n \neq 2$ where appropriate. □

Lemma 1.30 (Compat $\mathrm{e}_1[\mathrm{e}_2]$).

$$[\![\Gamma;\Gamma \vdash \mathrm{e}_1 : [\tau]]\!] \wedge [\![\Gamma;\Gamma \vdash \mathrm{e}_2 : \mathrm{int}]\!] \implies [\![\Gamma;\Gamma \vdash \mathrm{e}_1[\mathrm{e}_2] : \tau]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^{+}$ and pushing substitutions in the goal, we are to show that

$$\left(W, \left(\mathrm{close}\left(\gamma_{\Gamma}, \mathrm{close}\left(\gamma_{\Gamma}, \mathrm{e_1}^{+}\right)\right),\ \mathrm{close}\left(\gamma_{\Gamma}, \mathrm{close}\left(\gamma_{\Gamma}, \mathrm{e_2}^{+}\right)\right),\ \mathrm{idx}\right)\right) \in \mathcal{E}[\![\tau]\!]$$

given arbitary $W, \gamma_{\Gamma}, \gamma_{\Gamma}$ such that $(W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]$, we are to show that

$$\mathrm{S}' = \mathsf{Fail}\ \mathrm{c} \wedge \mathrm{c} \in \textsc{OkErr} \vee \exists \mathrm{v}, W' \sqsupseteq W.\ \left(\mathrm{S}' = \mathrm{S}, \mathrm{v} \wedge \mathrm{H}' : W' \wedge (W', \mathrm{v}) \in \mathcal{V}[\![\tau]\!]\right) \tag{22}$$

given arbitrary $\mathrm{H}{:}W, \mathrm{S}, \mathrm{H}', \mathrm{S}', j < W.k$ such that

$$\langle \mathrm{H}; \mathrm{S}; \mathrm{close}\left(\gamma_{\Gamma}, \mathrm{close}\left(\gamma_{\Gamma}, \mathrm{e_1}^{+}\right)\right),\ \mathrm{close}\left(\gamma_{\Gamma}, \mathrm{close}\left(\gamma_{\Gamma}, \mathrm{e_2}^{+}\right)\right),\ \mathrm{idx}\rangle \xrightarrow{j} \langle \mathrm{H}'; \mathrm{S}'; \cdot\rangle \nrightarrow$$

The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $j_1 \leq j, \mathrm{H}_1, \mathrm{S}_1$ such that

$$\langle \mathrm{H}; \mathrm{S}; \mathrm{close}\left(\gamma_{\Gamma}, \mathrm{close}\left(\gamma_{\Gamma}, \mathrm{e_1}^{+}\right)\right),\ \mathrm{close}\left(\gamma_{\Gamma}, \mathrm{close}\left(\gamma_{\Gamma}, \mathrm{e_2}^{+}\right)\right),\ \mathrm{idx}\rangle \xrightarrow{j_1} \langle \mathrm{H}_1; \mathrm{S}_1; \cdot\rangle \nrightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(1) $\mathrm{S}_1 = \mathrm{S}' = \mathsf{Fail}\ \mathrm{c} \wedge \mathrm{c} \in \textsc{OkErr}$ and $\mathrm{H}_1 = \mathrm{H}'$.
In this case, we have the left disjunct of (22).

(2)

$$\exists \mathsf{v}_1, W_1 \sqsupseteq W.\ \big(\mathsf{S}_1 = \mathsf{S}, \mathsf{v}_1 \wedge \mathsf{H}_1 : W_1 \wedge (W_1, \mathsf{v}_1) \in \mathcal{V}[\![[\tau]]\!]\big)$$

and

$$\langle \mathsf{H}_1; \mathsf{S}_1; \text{close}\,\big(\gamma_\Gamma, \text{close}\,\big(\gamma_\Gamma, \mathrm{e}_2{}^+\big)\big)\,,\ \mathsf{idx}\rangle \xrightarrow{j-j_1} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \not\rightarrow$$

Expanding the definition of $\mathcal{V}[\![[\tau]]\!]$ we have that

$$\mathsf{v}_1 = [\mathsf{v}'_1, \dots, \mathsf{v}'_n] \wedge (W_1, \mathsf{v}'_1) \in \mathcal{V}[\![\tau]\!] \wedge \dots \wedge (W_1, \mathsf{v}'_n) \in \mathcal{V}[\![\tau]\!]$$

Applying Lemma 1.2 again, there is $j_2 \leq j - j_1, \mathsf{H}_2, \mathsf{S}_2$ such that

$$\langle \mathsf{H}_1; \mathsf{S}_1; \text{close}\,\big(\gamma_\Gamma, \text{close}\,\big(\gamma_\Gamma, \mathrm{e}_2{}^+\big)\big)\,,\ \mathsf{idx}\rangle \xrightarrow{j_2} \langle \mathsf{H}_2; \mathsf{S}_2; \cdot\rangle \not\rightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(a) $\mathsf{S}_2 = \mathsf{S}' = \mathsf{Fail\ c} \wedge \mathsf{c} \in \textsc{OkErr}$ and $\mathsf{H}_2 = \mathsf{H}'$.
In this case, we have the left disjunct of (22).

(b)

$$\exists \mathsf{v}_2, W_2 \sqsupseteq W_1.\ \big(\mathsf{S}_2 = \mathsf{S}, \mathsf{v}_2 \wedge \mathsf{H}_2 : W_2 \wedge (W_2, \mathsf{v}_2) \in \mathcal{V}[\![\mathrm{int}]\!]\big)$$

and

$$\langle \mathsf{H}_2; \mathsf{S}_2; \mathsf{idx}\rangle \xrightarrow{j-j_1-j_2} \langle \mathsf{H}'; \mathsf{S}'; \cdot\rangle \not\rightarrow$$

Expanding the definition of $\mathcal{V}[\![\mathrm{int}]\!]$ we have that

$$\mathsf{v}_2 = \mathsf{n_i}$$

for some $\mathsf{n_i}$.

Recall that $\mathsf{S}_1 = \mathsf{S}, [\mathsf{v}'_1, \dots, \mathsf{v}'_n]$, so $\mathsf{S}_2 = \mathsf{S}_1, \mathsf{n_i} = \mathsf{S}, [\mathsf{v}'_1, \dots, \mathsf{v}'_n], \mathsf{n_i}$. Then there are two cases:

(i) $\mathsf{n_i} \in [1, \dots, \mathsf{n}]$. Then by the operational semantics of StackLang,

$$\langle \mathsf{H}_2; \mathsf{S}, [\mathsf{v}'_1, \dots, \mathsf{v}'_n], \mathsf{n_i}; \mathsf{idx}\rangle \xrightarrow{1} \langle \mathsf{H}_2; \mathsf{S}, \mathsf{v_{ni}}; \cdot\rangle$$

so $\mathsf{H}' = \mathsf{H}_2$ and $\mathsf{S}' = \mathsf{S}, \mathsf{v}'_{\mathsf{ni}}$. Then we have the right disjunct of (22) by taking $\mathsf{v} = \mathsf{v_{ni}}$ and $W' = \triangleright W_2$, noting that $W \sqsubseteq W_1 \sqsubseteq W_2 \sqsubseteq W'$ by Lemma 1.5 All that remains is to show that $(W', \mathsf{v}'_{\mathsf{ni}}) \in \mathcal{V}[\![\tau]\!]$. Recall that $(W_1, \mathsf{v}'_{\mathsf{ni}}) \in \mathcal{V}[\![\tau]\!]$, so simply apply Lemmas 1.4, 1.6.

(ii) $\mathsf{n_i} \notin [1, \dots, \mathsf{n}]$. Then by the operational semantics of StackLang,

$$\begin{aligned}\langle \mathsf{H}_2; \mathsf{S}, [\mathsf{v}'_1, \dots, \mathsf{v}'_n], \mathsf{n_i}; \mathsf{idx}\rangle &\xrightarrow{1} \langle \mathsf{H}_2; \mathsf{S}; \mathsf{error}\rangle \\ &\xrightarrow{1} \langle \mathsf{H}_2; \mathsf{Fail\ c}; \cdot\rangle\end{aligned}$$

so $\mathsf{S}' = \mathsf{Fail\ c} \wedge \mathsf{c} \in \textsc{OkErr}$. Then we have the left disjunct of (22).

□

Lemma 1.31 (Compat if0).

$$[\![\Gamma; \Gamma \vdash \mathrm{e} : \mathrm{int}]\!] \wedge [\![\Gamma; \Gamma \vdash \mathrm{e}_1 : \tau]\!] \wedge [\![\Gamma; \Gamma \vdash \mathrm{e}_2 : \tau]\!] \implies [\![\Gamma; \Gamma \vdash \mathrm{if0\ e\ e_1\ e_2} : \tau]\!]$$

Proof. As in Lemma 1.22, exchanging $\mathtt{bool}, \tau$ with int, τ where appropriate. □

Lemma 1.32 (Compat $\lambda \mathrm{x} : \tau.\mathrm{e}$).

$$[\![\Gamma; \Gamma, \mathrm{x} : \tau_1 \vdash \mathrm{e} : \tau_2]\!] \implies [\![\Gamma; \Gamma \vdash \lambda \mathrm{x} : \tau_1.\mathrm{e} : \tau_1 \to \tau_2]\!]$$

Proof. As in Lemma 1.21, exchanging τ_1, τ_2 with τ_1, τ_2 where appropriate. □

Lemma 1.33 (Compat $e_1\ e_2$).

$$[\![\Gamma;\Gamma \vdash e_1 : \tau_1 \to \tau_2]\!] \wedge [\![\Gamma;\Gamma \vdash e_2 : \tau_1]\!] \implies [\![\Gamma;\Gamma \vdash e_1\ e_2 : \tau_2]\!]$$

Proof. As in Lemma 1.22, exchanging τ_1, τ_2 with τ_1, τ_2 where appropriate. □

Lemma 1.34 (Compat $e_1 + e_2$).

$$[\![\Gamma;\Gamma \vdash e_1 : \mathrm{int}]\!] \wedge [\![\Gamma;\Gamma \vdash e_2 : \mathrm{int}]\!] \implies [\![\Gamma;\Gamma \vdash e_1 + e_2 : \mathrm{int}]\!]$$

Proof. Expanding the definition of $[\![\cdot]\!]$ and $\cdot^+$ and pushing substitutions in the goal, we are to show that

$$\left(W, \left(\mathrm{close}\left(\gamma_\Gamma, \mathrm{close}\left(\gamma_\Gamma, {e_1}^+\right)\right),\ \mathrm{close}\left(\gamma_\Gamma, \mathrm{close}\left(\gamma_\Gamma, {e_2}^+\right)\right),\ \mathrm{add}\right)\right) \in \mathcal{E}[\![\mathrm{int}]\!]$$

given arbitary $W, \gamma_\Gamma, \gamma_\Gamma$ such that $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]$, we are to show that

$$\mathrm{S}' = \mathrm{Fail\ c} \wedge \mathrm{c} \in \textsc{OkErr} \vee \exists \mathrm{v}, W' \sqsupseteq W.\ \left(\mathrm{S}' = \mathrm{S}, \mathrm{v} \wedge \mathrm{H}' : W' \wedge (W', \mathrm{v}) \in \mathcal{V}[\![\mathrm{int}]\!]\right) \tag{23}$$

given arbitrary $\mathrm{H}{:}W, \mathrm{S}, \mathrm{H}', \mathrm{S}', j < W.k$ such that

$$\langle \mathrm{H}; \mathrm{S}; \mathrm{close}\left(\gamma_\Gamma, \mathrm{close}\left(\gamma_\Gamma, {e_1}^+\right)\right),\ \mathrm{close}\left(\gamma_\Gamma, \mathrm{close}\left(\gamma_\Gamma, {e_2}^+\right)\right),\ \mathrm{add}\rangle \xrightarrow{j} \langle \mathrm{H}'; \mathrm{S}'; \cdot\rangle$$

The claim is vacuous when $W.k = 0$, so consider $W.k > 0$. Applying Lemma 1.2, there is $j_1 \leq j, \mathrm{H}_1, \mathrm{S}_1$ such that

$$\langle \mathrm{H}; \mathrm{S}; \mathrm{close}\left(\gamma_\Gamma, \mathrm{close}\left(\gamma_\Gamma, {e_1}^+\right)\right),\ \mathrm{close}\left(\gamma_\Gamma, \mathrm{close}\left(\gamma_\Gamma, {e_2}^+\right)\right),\ \mathrm{add}\rangle \xrightarrow{j_1} \langle \mathrm{H}_1; \mathrm{S}_1; \cdot\rangle \not\twoheadrightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(1) $\mathrm{S}_1 = \mathrm{S}' = \mathrm{Fail\ c} \wedge \mathrm{c} \in \textsc{OkErr}$ and $\mathrm{H}_1 = \mathrm{H}'$.
In this case, we have the left disjunct of (23).

(2)

$$\exists \mathrm{v}_1, W_1 \sqsupseteq W.\ \left(\mathrm{S}_1 = \mathrm{S}, \mathrm{v}_1 \wedge \mathrm{H}_1 : W_1 \wedge (W_1, \mathrm{v}_1) \in \mathcal{V}[\![\mathrm{int}]\!]\right)$$

and

$$\langle \mathrm{H}_1; \mathrm{S}_1; \mathrm{close}\left(\gamma_\Gamma, \mathrm{close}\left(\gamma_\Gamma, {e_2}^+\right)\right),\ \mathrm{add}\rangle \xrightarrow{j-j_1} \langle \mathrm{H}'; \mathrm{S}'; \cdot\rangle \not\twoheadrightarrow$$

Expanding the definition of $\mathcal{V}[\![\mathrm{int}]\!]$ we have that

$$\mathrm{v}_1 = \mathrm{n}_1$$

for some n_1. Applying Lemma 1.2 again, there is $j_2 \leq j - j_1, \mathrm{H}_2, \mathrm{S}_2$ such that

$$\langle \mathrm{H}_1; \mathrm{S}_1; \mathrm{close}\left(\gamma_\Gamma, \mathrm{close}\left(\gamma_\Gamma, {e_2}^+\right)\right),\ \mathrm{add}\rangle \xrightarrow{j_2} \langle \mathrm{H}_2; \mathrm{S}_2; \cdot\rangle \not\twoheadrightarrow$$

Then by expanding $\mathcal{E}[\![\cdot]\!]$ in the premise and specializing as appropriate, either:

(a) $\mathrm{S}_2 = \mathrm{S}' = \mathrm{Fail\ c} \wedge \mathrm{c} \in \textsc{OkErr}$ and $\mathrm{H}_2 = \mathrm{H}'$.
In this case, we have the left disjunct of (23).

(b)

$$\exists \mathrm{v}_2, W_2 \sqsupseteq W_1.\ \left(\mathrm{S}_2 = \mathrm{S}, \mathrm{v}_2 \wedge \mathrm{H}_2 : W_2 \wedge (W_2, \mathrm{v}_2) \in \mathcal{V}[\![\mathrm{int}]\!]\right)$$

and

$$\langle \mathrm{H}_2; \mathrm{S}_2; \mathrm{add}\rangle \xrightarrow{j-j_1-j_2} \langle \mathrm{H}'; \mathrm{S}'; \cdot\rangle \not\twoheadrightarrow$$

Expanding the definition of $\mathcal{V}[\![\mathrm{int}]\!]$ we have that

$$\mathrm{v}_2 = \mathrm{n}_2$$

for some n_2.

Recall that $S_1 = S, n_1$, so $S_2 = S_1, n_2 = S, n_1, n_2$. Then by the operational semantics of StackLang,

$$\langle H_2; S, n_1, n_2; \mathsf{add}\rangle \xrightarrow{1} \langle H_2; S, (n_1 + n_2); \cdot\rangle \not\rightarrow$$

so $H' = H_2$ and $S' = S, (n_1 + n_2)$. Then we have the right disjunct of (23) by taking $v = n_1 + n_2$ and $W' = \triangleright W_2$, noting that $W \sqsubseteq W_1 \sqsubseteq W_2 \sqsubseteq W'$ by Lemma 1.5 and that $(W', n_1 + n_2) \in \mathcal{V}[\![\tau]\!]$ by definition.

□

Lemma 1.35 (Compat ref e).

$$[\![\Gamma; \Gamma \vdash e : \tau]\!] \implies [\![\Gamma; \Gamma \vdash \mathrm{ref}\ e : \mathrm{ref}\ \tau]\!]$$

Proof. As in Lemma 1.23, exchanging τ, τ where appropriate. □

Lemma 1.36 (Compat !e).

$$[\![\Gamma; \Gamma \vdash e : \mathrm{ref}\ \tau]\!] \implies [\![\Gamma; \Gamma \vdash !e : \tau]\!]$$

Proof. As in Lemma 1.24, exchanging τ, τ where appropriate. □

Lemma 1.37 (Compat $e_1 := e_2$).

$$[\![\Gamma; \Gamma \vdash e_1 : \mathrm{ref}\ \tau]\!] \wedge [\![\Gamma; \Gamma \vdash e_2 : \tau]\!] \implies [\![\Gamma; \Gamma \vdash e_1 := e_2 : \mathrm{int}]\!]$$

Proof. As in Lemma 1.25, exchanging τ, τ where appropriate. □

Lemma 1.38 (Compat $(\!|e|\!)_\tau$).

$$[\![\Gamma; \Gamma \vdash e : \tau]\!] \wedge \tau \sim \tau \implies [\![\Gamma; \Gamma \vdash (\!|e|\!)_\tau : \tau]\!]$$

Proof. As in 1.26, exchanging τ, τ where appropriate. □

2 CASE STUDY: AFFINE WITH DYNAMIC SAFETY

In this setting, we have two source languages: MiniML and Affi. The former is a functional language with polymorphism and mutable references: a scaled down ML, essentially. The latter is an affine lambda calculus, built by allowing weakening at the base out of a linear lambda calculus.

2.1 MiniML Language

$$\begin{array}{lcl} \text{Type } \tau & ::= & \mathtt{unit} \mid \mathtt{int} \mid \tau \times \tau \mid \tau + \tau \mid \tau \rightarrow \tau \mid \forall \alpha.\tau \mid \alpha \mid \mathtt{ref}\ \tau \\ \text{Expression } \mathtt{e} & ::= & () \mid \mathbb{Z} \mid \mathtt{x} \mid (\mathtt{e}, \mathtt{e}) \mid \mathtt{fst}\ \mathtt{e} \mid \mathtt{snd}\ \mathtt{e} \mid \mathtt{inl}\ \mathtt{e} \mid \mathtt{inr}\ \mathtt{e} \mid \mathtt{match}\ \mathtt{e}\ \mathtt{x}\{\mathtt{e}\}\ \mathtt{y}\{\mathtt{e}\} \\ & & \mid \lambda \mathtt{x} : \tau.\mathtt{e} \mid \mathtt{e}\ \mathtt{e} \mid \Lambda \alpha.\mathtt{e} \mid \mathtt{e}[\tau] \mid \mathtt{ref}\ \mathtt{e} \mid !\mathtt{e} \mid \mathtt{e} := \mathtt{e} \mid \llparenthesis \mathtt{e} \rrparenthesis_{\tau} \end{array}$$

This is a functional language with higher-order mutable state and polymorphism. Note that we have syntax for an embedding the foreign (Affi language) terms at a native type τ (written $\llparenthesis \mathtt{e} \rrparenthesis_{\tau}$). In order to support open terms within boundaries, we write the typing judgments including a typing context from Affi, written as shorthand $\mathfrak{C}$ (though standing for $\Gamma; \Omega$), which is threaded through the typing judgments of MiniML – a simpler model of interoperability takes this to be empty, retains nearly identical typing rules to the original source, and thus only allows closed terms to be embedded.

Typing.

$$\frac{}{\mathfrak{C}; \Delta; \Gamma \vdash () : \mathtt{unit} \rightsquigarrow \mathfrak{C}} \qquad \frac{}{\mathfrak{C}; \Delta; \Gamma \vdash \mathbb{Z} : \mathtt{int} \rightsquigarrow \mathfrak{C}} \qquad \frac{\Delta \vdash \tau \qquad \mathtt{x} : \tau \in \Gamma}{\mathfrak{C}; \Delta; \Gamma \vdash \mathtt{x} : \tau \rightsquigarrow \mathfrak{C}}$$

$$\frac{\mathfrak{C}_1; \Delta; \Gamma \vdash \mathtt{e}_1 : \tau_1 \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2; \Delta; \Gamma \vdash \mathtt{e}_2 : \tau_2 \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1; \Delta; \Gamma \vdash (\mathtt{e}_1, \mathtt{e}_2) : \tau_1 \times \tau_2 \rightsquigarrow \mathfrak{C}_3} \qquad \frac{\mathfrak{C}; \Delta; \Gamma \vdash \mathtt{e} : \tau_1 \times \tau_2 \rightsquigarrow \mathfrak{C}'}{\mathfrak{C}; \Delta; \Gamma \vdash \mathtt{fst}\ \mathtt{e} : \tau_1 \rightsquigarrow \mathfrak{C}'}$$

$$\frac{\mathfrak{C}; \Delta; \Gamma \vdash \mathtt{e} : \tau_1 \times \tau_2 \rightsquigarrow \mathfrak{C}'}{\mathfrak{C}; \Delta; \Gamma \vdash \mathtt{snd}\ \mathtt{e} : \tau_2 \rightsquigarrow \mathfrak{C}'} \qquad \frac{\Delta \vdash \tau_2 \qquad \mathfrak{C}; \Delta; \Gamma \vdash \mathtt{e} : \tau_1 \rightsquigarrow \mathfrak{C}'}{\mathfrak{C}; \Delta; \Gamma \vdash \mathtt{inl}\ \mathtt{e} : \tau_1 + \tau_2 \rightsquigarrow \mathfrak{C}'} \qquad \frac{\Delta \vdash \tau_1 \qquad \mathfrak{C}; \Delta; \Gamma \vdash \mathtt{e} : \tau_2 \rightsquigarrow \mathfrak{C}'}{\mathfrak{C}; \Delta; \Gamma \vdash \mathtt{inr}\ \mathtt{e} : \tau_1 + \tau_2 \rightsquigarrow \mathfrak{C}'}$$

$$\frac{\mathfrak{C}_1; \Delta; \Gamma \vdash \mathtt{e} : \tau_1 + \tau_2 \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2; \Delta; \Gamma[\mathtt{x} : \tau_1] \vdash \mathtt{e}_1 : \tau \rightsquigarrow \mathfrak{C}_3 \qquad \mathfrak{C}_2; \Delta; \Gamma[\mathtt{y} : \tau_2] \vdash \mathtt{e}_2 : \tau \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1; \Delta; \Gamma \vdash \mathtt{match}\ \mathtt{e}\ \mathtt{x}\{\mathtt{e}_1\}\ \mathtt{y}\{\mathtt{e}_2\} : \tau \rightsquigarrow \mathfrak{C}_3}$$

$$\frac{\mathfrak{C}; \Delta; \Gamma[\mathtt{x} : \tau_1] \vdash \mathtt{e} : \tau_2 \rightsquigarrow \mathfrak{C}'}{\mathfrak{C}; \Delta; \Gamma \vdash \lambda \mathtt{x} : \tau_1.\mathtt{e} : \tau_1 \rightarrow \tau_2 \rightsquigarrow \mathfrak{C}'} \qquad \frac{\mathfrak{C}_1; \Delta; \Gamma \vdash \mathtt{e} : \tau' \rightarrow \tau \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2; \Delta; \Gamma \vdash \mathtt{e}' : \tau \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1; \Delta; \Gamma \vdash \mathtt{e}\ \mathtt{e}' : \tau \rightsquigarrow \mathfrak{C}_3}$$

$$\frac{\mathfrak{C}; \Delta, \alpha; \Gamma \vdash \mathtt{e} : \tau \rightsquigarrow \mathfrak{C}'}{\mathfrak{C}; \Delta; \Gamma \vdash \Lambda \alpha.\mathtt{e} : \forall \alpha.\tau \rightsquigarrow \mathfrak{C}'} \qquad \frac{\mathfrak{C}; \Delta \vdash \tau \qquad \mathfrak{C}; \Delta; \Gamma \vdash \mathtt{e} : \forall \alpha.\tau \rightsquigarrow \mathfrak{C}'}{\mathfrak{C}; \Delta; \Gamma \vdash \mathtt{e}[\tau'] : \tau[\tau'/\alpha] \rightsquigarrow \mathfrak{C}'}$$

$$\frac{\mathfrak{C}; \Delta; \Gamma \vdash \mathtt{e} : \tau \rightsquigarrow \mathfrak{C}'}{\mathfrak{C}; \Delta; \Gamma \vdash \mathtt{ref}\ \mathtt{e} : \mathtt{ref}\ \tau \rightsquigarrow \mathfrak{C}'} \qquad \frac{\mathfrak{C}; \Delta; \Gamma \vdash \mathtt{e} : \mathtt{ref}\ \tau \rightsquigarrow \mathfrak{C}'}{\mathfrak{C}; \Delta; \Gamma \vdash !\mathtt{e} : \tau \rightsquigarrow \mathfrak{C}'}$$

$$\frac{\mathfrak{C}_1; \Delta; \Gamma \vdash \mathtt{e}_1 : \mathtt{ref}\ \tau \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2; \Delta; \Gamma \vdash \mathtt{e}_2 : \tau \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1; \Delta; \Gamma \vdash \mathtt{e}_1 := \mathtt{e}_2 : \mathtt{unit} \rightsquigarrow \mathfrak{C}_3} \qquad \frac{\mathfrak{C}; \Delta; \Gamma \vdash \mathtt{e} : \tau \rightsquigarrow \mathfrak{C}' \qquad \_ : \tau \sim \tau}{\mathfrak{C}; \Delta; \Gamma \vdash \llparenthesis \mathtt{e} \rrparenthesis_{\tau} : \tau \rightsquigarrow \mathfrak{C}'}$$

where the typing rule for foreign terms uses the following macro in its assumptions:

$$\mathfrak{C}; \Delta; \Gamma \vdash \mathtt{e} : \tau \rightsquigarrow \mathfrak{C}' \triangleq \exists \Omega_{\mathtt{e}}.\Omega = \Omega_{\mathtt{e}} \uplus \Omega' \land \Gamma = \Gamma' \land \Delta; \Gamma; \Gamma; \Omega_{\mathtt{e}} \vdash \mathtt{e} : \tau \rightsquigarrow \Delta; \Gamma$$

2.2 Affi Language

$$\begin{array}{lcl}
\tau & ::= & \mathrm{unit} \mid \mathrm{bool} \mid \mathrm{int} \mid \tau \multimap \tau \mid !\tau \mid \tau \& \tau \mid \tau \otimes \tau \\
e & ::= & () \mid \mathrm{true} \mid \mathrm{false} \mid n \mid x \mid a \mid \lambda a : \tau.e \mid e\ e \mid (\!| e |\!)_\tau \mid !v \mid \mathrm{let}\ !x = e\ \mathrm{in}\ e' \mid \\
 & & \langle e, e' \rangle \mid e.1 \mid e.2 \mid (e, e) \mid \mathrm{let}\ (a, a') = e\ \mathrm{in}\ e' \\
v & ::= & () \mid \lambda a : \tau.e \mid !v \mid \langle e, e' \rangle \mid (v, v')
\end{array}$$

Typing.

$$\frac{a : \tau \in \Omega}{\mathfrak{C};\Gamma;\Omega \vdash a : \tau \rightsquigarrow \mathfrak{C}} \qquad \frac{x : \tau \in \Gamma}{\mathfrak{C};\Gamma;\Omega \vdash x : \tau \rightsquigarrow \mathfrak{C}} \qquad \frac{}{\mathfrak{C};\Gamma;\Omega \vdash () : \mathrm{unit} \rightsquigarrow \mathfrak{C}} \qquad \frac{}{\mathfrak{C};\Gamma;\Omega \vdash n : \mathrm{int} \rightsquigarrow \mathfrak{C}}$$

$$\frac{}{\mathfrak{C};\Gamma;\Omega \vdash \mathrm{true} : \mathrm{bool} \rightsquigarrow \mathfrak{C}} \qquad \frac{}{\mathfrak{C};\Gamma;\Omega \vdash \mathrm{false} : \mathrm{bool} \rightsquigarrow \mathfrak{C}}$$

$$\frac{\mathfrak{C};\Gamma;\Omega[a := \tau_1] \vdash e : \tau_2 \rightsquigarrow \mathfrak{C}'}{\mathfrak{C};\Gamma;\Omega \vdash \lambda a : \tau_1.e : \tau_1 \multimap \tau_2 \rightsquigarrow \mathfrak{C}'}$$

$$\frac{\Omega = \Omega_1 \uplus \Omega_2 \qquad \mathfrak{C}_1;\Gamma;\Omega_1 \vdash e_1 : \tau_1 \multimap \tau_2 \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2;\Gamma;\Omega_2 \vdash e_2 : \tau_1 \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1;\Gamma;\Omega \vdash e_1\ e_2 : \tau_2 \rightsquigarrow \mathfrak{C}_3}$$

$$\frac{\mathfrak{C};\Gamma;\cdot \vdash v : \tau \rightsquigarrow \mathfrak{C}'}{\mathfrak{C};\Gamma;\cdot \vdash !v : !\tau \rightsquigarrow \mathfrak{C}'}$$

$$\frac{\Omega = \Omega_1 \uplus \Omega_2 \qquad \mathfrak{C}_1;\Gamma;\Omega_1 \vdash e : !\tau \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2;\Gamma[x := \tau];\Omega_2 \vdash e' : \tau' \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1;\Gamma;\Omega \vdash \mathrm{let}\ !x = e\ \mathrm{in}\ e' \rightsquigarrow \mathfrak{C}_3}$$

$$\frac{\mathfrak{C}_1;\Gamma;\Omega \vdash e_1 : \tau_1 \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2;\Gamma;\Omega \vdash e_2 : \tau_2 \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1;\Gamma;\Omega \vdash \langle e_1, e_2 \rangle : \tau_1 \& \tau_2 \rightsquigarrow \mathfrak{C}_3} \qquad \frac{\mathfrak{C};\Gamma;\Omega \vdash e : \tau_1 \& \tau_2 \rightsquigarrow \mathfrak{C}'}{\mathfrak{C};\Gamma;\Omega \vdash e.1 : \tau_1 \rightsquigarrow \mathfrak{C}'}$$

$$\frac{\mathfrak{C};\Gamma;\Omega \vdash e : \tau_1 \& \tau_2 \rightsquigarrow \mathfrak{C}'}{\mathfrak{C};\Gamma;\Omega \vdash e.2 : \tau_2 \rightsquigarrow \mathfrak{C}'}$$

$$\frac{\Omega = \Omega_1 \uplus \Omega_2 \qquad \mathfrak{C}_1;\Gamma;\Omega_1 \vdash e_1 : \tau_1 \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2;\Gamma;\Omega_2 \vdash e_2 : \tau_2 \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1;\Gamma;\Omega \vdash (e_1, e_2) : \tau_1 \otimes \tau_2 \rightsquigarrow \mathfrak{C}_3}$$

$$\frac{\Omega = \Omega_1 \uplus \Omega_2 \qquad \mathfrak{C}_1;\Gamma;\Omega_1 \vdash e : \tau_1 \otimes \tau_2 \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2;\Gamma;\Omega_2[a := \tau_1, a' := \tau_1] \vdash e' : \tau' \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1;\Gamma;\Omega \vdash \mathrm{let}\ (a, a') = e\ \mathrm{in}\ e' : \tau' \rightsquigarrow \mathfrak{C}_3}$$

$$\frac{\mathfrak{C};\Gamma;\Omega \vdash e : \tau \rightsquigarrow \mathfrak{C}' \qquad \_ : \tau \sim \tau}{\mathfrak{C};\Gamma;\Omega \vdash (\!| e |\!)_\tau : \tau \rightsquigarrow \mathfrak{C}'}$$

where the typing rule for foreign terms uses the following macro in its assumptions:

$$\mathfrak{C};\Gamma;\Omega \vdash e : \tau \rightsquigarrow \mathfrak{C}' \triangleq \exists \Omega'.\Delta = \Delta' \wedge \Gamma = \Gamma' \wedge \Gamma;\Omega;\Delta;\Gamma \vdash e : \tau \rightsquigarrow \Gamma;\Omega'$$

2.3 LCVM Language

$$\begin{array}{lcl}
\text{Expressions } e & := & () \mid \mathbb{Z} \mid \ell \mid x \mid (e, e) \mid \text{fst } e \mid \text{snd } e \mid \text{inl } e \mid \text{inr } e \mid \text{if } e\ \{e\}\ \{e\} \\
 & & \mid \text{match } e\ x\{e\}\ y\{e\} \mid \text{let } x = e \text{ in } e \mid \lambda x\{e\} \mid e\ e \mid \text{ref } e \mid\ !e \mid e := e \\
 & & \mid \text{fail } c \\
\text{Values } v & ::= & () \mid \mathbb{Z} \mid \ell \mid (v, v) \mid \lambda x.e \\
\text{Error Code } c & ::= & \textsc{Type} \mid \textsc{Conv} \\
\text{Heap } H & ::= & \ell \mapsto v, \ldots \\
\text{Evaluation Context } K & ::= & [\cdot] \mid (K, e) \mid (v, K) \mid \text{inl } K \mid \text{inr } K \mid \text{match } K\ x\{e\}\ y\{e\} \mid \text{if } K\ \{e\}\ \{e\} \mid \\
 & & \text{let } x = K \text{ in } e \mid K\ e \mid v\ K \mid \text{ref } K \mid\ \ K \mid K := e \mid v := K
\end{array}$$

This is an untyped lambda calculus with pairs, sums, and references. Our operational semantics is presented, below, using evaluation contexts to lift steps on subterms into steps on whole programs.

2.3.1 Operational Semantics.

$$\frac{}{\langle H, \text{fst } (v, v')\rangle \longrightarrow \langle H, v\rangle} \qquad \frac{v \neq (v_1, v_2)}{\langle H, \text{fst } v\rangle \longrightarrow \langle H, \text{fail } \textsc{Type}\rangle} \qquad \frac{}{\langle H, \text{snd } (v', v)\rangle \longrightarrow \langle H, v\rangle}$$

$$\frac{v \neq (v_1, v_2)}{\langle H, \text{snd } v\rangle \longrightarrow \langle H, \text{fail } \textsc{Type}\rangle} \qquad \frac{}{\langle H, \text{if } 0\ \{e_1\}\ \{e_2\}\rangle \longrightarrow \langle H, e_1\rangle} \qquad \frac{n \neq 0}{\langle H, \text{if } n\ \{e_1\}\ \{e_2\}\rangle \longrightarrow \langle H, e_2\rangle}$$

$$\frac{v \notin \mathbb{Z}}{\langle H, \text{if } v\ \{e_1\}\ \{e_2\}\rangle \longrightarrow \langle H, \text{fail } \textsc{Type}\rangle} \qquad \frac{}{\langle H, \text{match inl } v\ x\{e_1\}\ y\{e_2\}\rangle \longrightarrow \langle H, [x \mapsto v]e_1\rangle}$$

$$\frac{}{\langle H, \text{match inr } v\ x\{e_1\}\ y\{e_2\}\rangle \longrightarrow \langle H, [y \mapsto v]e_2\rangle} \qquad \frac{v \notin \{\text{inr } v', \text{inl } v'\}}{\langle H, \text{match } v\ x\{e_1\}\ y\{e_2\}\rangle \longrightarrow \langle H, \text{fail } \textsc{Type}\rangle}$$

$$\frac{}{\langle H, \text{let } x = v \text{ in } e\rangle \longrightarrow \langle H, [x \mapsto v]e\rangle} \qquad \frac{}{\langle H, \lambda x\{e_b\}\ v\rangle \longrightarrow \langle H, [x \mapsto v]e_b\rangle}$$

$$\frac{v \neq \lambda x\{e\}}{\langle H, v\ v'\rangle \longrightarrow \langle H, \text{fail } \textsc{Type}\rangle} \qquad \frac{\text{fresh } \ell}{\langle H, \text{ref } v\rangle \longrightarrow \langle H[\ell \mapsto v], \ell\rangle} \qquad \frac{H[\ell] = v}{\langle H, !\ell\rangle \longrightarrow \langle H, v\rangle}$$

$$\frac{v \neq \ell}{\langle H, !v\rangle \longrightarrow \langle H, \text{fail } \textsc{Type}\rangle} \qquad \frac{}{\langle H, \ell := v\rangle \longrightarrow \langle H[\ell \mapsto v], ()\rangle} \qquad \frac{v \neq \ell}{\langle H, v := v'\rangle \longrightarrow \langle H, \text{fail } \textsc{Type}\rangle}$$

$$\frac{\langle H, e\rangle \longrightarrow \langle H', e'\rangle}{\langle H, K[e]\rangle \longrightarrow \langle H', K[e']\rangle} \qquad \frac{K \neq [\cdot]}{\langle H, K[\text{fail } c]\rangle \longrightarrow \langle H, \text{fail } c\rangle}$$

2.4 Compilers

For MiniML, we take the standard approach of erasing types. That means that most terms are translated to syntactically analogous terms without type annotations (where present). The only exceptions have to do with the type-only feature: polymorphism. There, we take a simple approach: translate α to type unit (our target is untyped, so this guides our translation, rather than showing up in target types), so that $\Lambda\alpha.\text{e}$ turns into a normal value-level target lambda and $\text{e}[\tau]$ turns into

$e^+()$. For foreign wrapper terms, we insert appropriate target-level wrappers ; we will describe in much more detail what these mean and where they come from later on.

$$
\begin{array}{lcl}
() & \leadsto & () \\
\mathbb{Z} & \leadsto & \mathbb{Z} \\
x & \leadsto & x \\
(e_1, e_2) & \leadsto & ({e_1}^+, {e_2}^+) \\
\mathtt{fst}\ e & \leadsto & \mathsf{fst}\ e^+ \\
\mathtt{snd}\ e & \leadsto & \mathsf{snd}\ e^+ \\
\mathtt{inl}\ e & \leadsto & \mathsf{inl}\ e^+ \\
\mathtt{inr}\ e & \leadsto & \mathsf{inr}\ e^+ \\
\mathtt{match}\ e\ x\{e_1\}\ y\{e_2\} & \leadsto & \mathsf{match}\ e^+\ x\{{e_1}^+\}\ y\{{e_2}^+\} \\
\lambda x : \tau.e & \leadsto & \lambda x.\{e^+\} \\
e_1\ e_2 & \leadsto & {e_1}^+\ {e_2}^+ \\
\Lambda\alpha.e & \leadsto & \lambda\_.\{e^+\} \\
e[\tau] & \leadsto & e^+\ () \\
\mathtt{ref}\ e & \leadsto & \mathsf{ref}\ e^+ \\
!e & \leadsto & !e^+ \\
e_1 := e_2 & \leadsto & {e_1}^+ := {e_2}^+ \\
(\!|e|\!)_\tau & \leadsto & C_{\tau\mapsto\tau}(e^+)
\end{array}
$$

For **Affi**, the compilation is again primarily about erasing types, but there are places where we need to account for affinity and it is not directly achievable. Note in particular that ! is a no-op, as statically we know that the term it is applied to is (affinely-)closed, which means there are no affine variables in it and thus nothing we have to do with it. Our lazy products have to compile to explicit thunks, to ensure that the resources (affine variables) that can be shared between both are not evaluated twice, since the pair should only have one component used.

$$\mathsf{thunk}(e) \triangleq \mathsf{let}\ r_{\mathsf{fresh}} = \mathsf{ref}\ 1\ \mathsf{in}\ \lambda\_.\{\mathsf{if}\ !r_{\mathsf{fresh}}\ \{\mathsf{fail}\ \textsc{Conv}\}\ \{r_{\mathsf{fresh}} := 0; e\}\}$$

$$
\begin{array}{lcl}
() & \leadsto & () \\
x & \leadsto & x \\
\mathrm{true} & \leadsto & 0 \\
\mathrm{false} & \leadsto & 1 \\
n & \leadsto & n \\
a & \leadsto & a\ () \\
\lambda a : \tau.e & \leadsto & \lambda a.\{e^+\} \\
e_1\ e_2 & \leadsto & {e_1}^+\ (\mathsf{let}\ x = {e_2}^+\ \mathsf{in}\ \mathsf{thunk}(x)) \\
!v & \leadsto & v^+ \\
\mathrm{let}\ !x = e\ \mathrm{in}\ e' & \leadsto & \mathsf{let}\ x = e^+\ \mathsf{in}\ e'^+ \\
\langle e, e' \rangle & \leadsto & (\lambda\_.\{e^+\}, \lambda\_.\{e'^+\}) \\
e.1 & \leadsto & (\mathsf{fst}\ e^+)\ () \\
e.2 & \leadsto & (\mathsf{snd}\ e^+)\ () \\
(e, e') & \leadsto & (e^+, e'^+) \\
\mathrm{let}\ (a, a') = e\ \mathrm{in}\ e' & \leadsto & \mathsf{let}\ x_{\mathsf{fresh}} = e^+\ \mathsf{in}\ \mathsf{let}\ x'_{\mathsf{fresh}} = \mathsf{fst}\ x_{\mathsf{fresh}}\ \mathsf{in}\ \mathsf{let}\ x''_{\mathsf{fresh}} = \mathsf{snd}\ x_{\mathsf{fresh}}\ \mathsf{in} \\
 & & \mathsf{let}\ a = \mathsf{thunk}(x'_{\mathsf{fresh}})\ \mathsf{in}\ \mathsf{let}\ a' = \mathsf{thunk}(x''_{\mathsf{fresh}})\ \mathsf{in}\ e'^+ \\
(\!|e|\!)_\tau & \leadsto & C_{\tau\mapsto\tau}(e^+)
\end{array}
$$

2.5 Convertibility

We incorporate type checking of embedded foreign terms by means of a convertibility relation that defines when we can safely convert between (terms of) a type in one language to (terms of) a type in the other language, which is defined up to the possibility of (well-defined) operational failure. This is written as $\tau \sim \tau$, which indicates that we can convert from τ to τ and the reverse, though either can produce a (well-defined) runtime failure.

The above descriptions are our informal description. Formally, we split the definition into two steps: first, we define declarative rules for the judgment. Second, we prove that these are sound with respect to the logical relation. These are in the form of compatibility lemmas for our new rules, which we appeal to in the typing rule for a embedded foreign term. A type checking algorithm could then use the syntactic rules, knowing, based on the proof of soundness, that the result would be sound. Our rules are the following:

$$\dfrac{}{C_{\mathtt{unit}\mapsto\mathrm{unit}}, C_{\mathrm{unit}\mapsto\mathtt{unit}} : \mathtt{unit} \sim \mathrm{unit}} \qquad \dfrac{}{C_{\mathtt{int}\mapsto\mathrm{bool}}, C_{\mathrm{bool}\mapsto\mathtt{int}} : \mathtt{int} \sim \mathrm{bool}}$$

$$\dfrac{C_{\tau_1\mapsto\tau_1}, C_{\tau_1\mapsto\tau_1} : \tau_1 \sim \tau_1 \qquad C_{\tau_2\mapsto\tau_2}, C_{\tau_2\mapsto\tau_2} : \tau_2 \sim \tau_2}{C_{\tau_1\otimes\tau_2\mapsto\tau_1 \times \tau_2}, C_{\tau_1 \times \tau_2\mapsto\tau_1\otimes\tau_2} : \tau_1 \otimes \tau_2 \sim \tau_1 \times \tau_2}$$

$$\dfrac{C_{\tau_1\mapsto\tau_1}, C_{\tau_1\mapsto\tau_1} : \tau_1 \sim \tau_1 \qquad C_{\tau_2\mapsto\tau_2}, C_{\tau_2\mapsto\tau_2} : \tau_2 \sim \tau_2}{C_{\tau_1\multimap\tau_2\mapsto(\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2}, C_{(\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2\mapsto\tau_1\multimap\tau_2} : \tau_1 \multimap \tau_2 \sim (\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2}$$

$$\begin{array}{lcl}
C_{\mathtt{unit}\mapsto\mathrm{unit}}(\mathrm{e}) & \triangleq & \mathrm{e} \\
C_{\mathrm{unit}\mapsto\mathtt{unit}}(\mathrm{e}) & \triangleq & \mathrm{e} \\
C_{\mathtt{int}\mapsto\mathrm{bool}}(\mathrm{e}) & \triangleq & \mathrm{e} \\
C_{\mathrm{bool}\mapsto\mathtt{int}}(\mathrm{e}) & \triangleq & \mathrm{if\ e\ 0\ 1} \\
\mathrm{C}_{\tau_1\otimes\tau_2\mapsto\tau_1 \times \tau_2}(\mathrm{e}) & \triangleq & \mathrm{let\ x = e\ in\ (C}_{\tau_1\mapsto\tau_1}(\mathrm{fst\ x}), \mathrm{C}_{\tau_2\mapsto\tau_2}(\mathrm{snd\ x})) \\
\mathrm{C}_{\tau_1 \times \tau_2\mapsto\tau_1\otimes\tau_2}(\mathrm{e}) & \triangleq & \mathrm{let\ x = e\ in\ (C}_{\tau_1\mapsto\tau_1}(\mathrm{fst\ x}), \mathrm{C}_{\tau_2\mapsto\tau_2}(\mathrm{snd\ x})) \\
\mathrm{C}_{\tau_1\multimap\tau_2\mapsto(\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2}(\mathrm{e}) & \triangleq & \mathrm{let\ x = e\ in\ } \lambda \mathrm{x_{thnk}.let\ x_{conv} = C}_{\tau_1\mapsto\tau_1}(\mathrm{x_{thnk}\ ()}) \\
 & & \qquad\qquad \mathrm{in\ let\ x_{access} = thunk(x_{conv})\ in\ C}_{\tau_2\mapsto\tau_2}(\mathrm{x\ x_{access}}) \\
\mathrm{C}_{(\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2\mapsto\tau_1\multimap\tau_2}(\mathrm{e}) & \triangleq & \mathrm{let\ x = e\ in\ } \lambda \mathrm{x_{thnk}.let\ x_{access} = thunk(C}_{\tau_1\mapsto\tau_1}(\mathrm{x_{thnk}\ ()))\ in\ C}_{\tau_2\mapsto\tau_2}(\mathrm{x\ x_{access}})
\end{array}$$

2.6 Logical Relation

Our MiniML language has state, and so our relation contains worlds W that are made up of a step-index k, a heap typing Ψ that captures the invariants of our heap, and an affine variable flag set Θ.

2.6.1 Worlds.

A world W is drawn from:

$$World_n = \{(k, \Psi, \Theta) \mid k < n \wedge \Psi \subset HeapTy_k \wedge \mathrm{dom}(\Psi) \# \mathrm{dom}(\Theta)\}$$

$$World = \bigcup_n World_n$$

Where k is the step index, Ψ is a heap typing, and Θ is the set of pairs of locations that are affine variable flags. To be well-formed, $\mathrm{dom}(W.\Theta)$ is disjoint from $\mathrm{dom}(W.\Psi)$.

This heap typing has the following shape:

$$HeapTy_n = \{(\ell, \ell) \mapsto Typ_n, \ldots\}$$

Where ℓ are heap locations. This is a simplified model as compared to the complex models for state, but sufficient for our motivation. The locations map to the following relations:

$$Atom_n = \{(W, \mathrm{e}_1, \mathrm{e}_2) \mid W \in World_n\}$$

where for any expression e, $FL(\mathrm{e})$ denotes all of the locations which appear in e. This condition ensures that all locations which appear in e also appear in the world.

$$AtomVal_n = \{(W, \mathrm{v}_1, \mathrm{v}_2) \in Atom_n\}$$

$$Atom = \bigcup_n Atom_n$$

$$AtomVal = \bigcup_n AtomVal_n$$

$$Typ_n = \{R \in 2^{AtomVal_n} \mid \forall (W, \mathrm{v}_1, \mathrm{v}_2) \in R.\ \forall W'.\ W \sqsubseteq W' \implies (W', \mathrm{v}_1, \mathrm{v}_2) \in R\}$$
$$Typ = \{R \in 2^{AtomVal} \mid \forall k. \lfloor R \rfloor_k \in Typ_k\}$$

The affine flag set maps pairs of locations to $\{0, 1\}$, which we interpret as booleans. Let USED denote 0 and UNUSED denote 1.

Restrictions. We define restriction based on indexing over relations as:

$$\lfloor R \rfloor_j = \{(W, \mathrm{e}_1, \mathrm{e}_2) \mid (W, \mathrm{e}_1, \mathrm{e}_2) \in R \land W.k < j\}$$

$$\lfloor \Psi \rfloor_j = \{(\ell_1, \ell_2) \mapsto \lfloor R \rfloor_j \mid (\ell_1, \ell_2) \mapsto R \in \Psi\}$$

Later. We define a $\triangleright$ (later) modality defined as restricting the index to the current one, which forces the worlds "forward" one step (as it cuts out everything with the current step index). On a world W, $\triangleright W = (W.k - 1, \lfloor W.\Psi \rfloor_{W.k-1}, W.\Theta)$, and $\triangleright$ naturally extends to other definitions with step indexes.

World Extension. We next define world extension, $(k, \Psi, \Theta) \sqsubseteq (j, \Psi', \Theta')$ (between well-formed worlds), as:

$$\begin{aligned} & j \leq k \\ & \land \forall (\ell_1, \ell_2) \in \mathrm{dom}(\Psi). \lfloor \Psi(\ell_1, \ell_2) \rfloor_j = \Psi'(\ell_1, \ell_2) \\ & \land \forall (\ell_1, \ell_2) \in \mathrm{dom}(\Theta). (\ell_1, \ell_2) \in \mathrm{dom}(\Theta') \land (\Theta(\ell_1, \ell_2) = 0 \implies \Theta'(\ell_1, \ell_2) = 0) \end{aligned}$$

As in, the step index can shrink, modulo loss of information due to decreasing step index.

We also define a strict version, that requires that the step index actually decreased:

$$W_1 \sqsubset W_2 \triangleq W_1.k > W_2.k \land W_1 \sqsubseteq W_2$$

Heaps. A heap H is:

$$\mathrm{H} = \{\ell \mapsto v\}$$

And we define when a pair of heaps $\mathrm{H}_1, \mathrm{H}_2$ satisfy a world as $\mathrm{H}_1, \mathrm{H}_2 : W$:

$$(\forall(\ell_1, \ell_2) \mapsto R \in W.\Psi.\ (\triangleright W, \mathrm{H}_1(\ell_1), \mathrm{H}_2(\ell_2)) \in R) \wedge\ (\forall(\ell_1, \ell_2) \mapsto b \in W.\Theta.\forall i \in \{1,2\}.\ \mathrm{H}_i(\ell_i) = b)$$

i.e., locations must point to closed values that are in the relation specified by the heap typing and the affine flags must be in the heap.

Expression Relation. We define an expression relation on closed terms as follows:

$$\begin{aligned}\mathcal{E}[\![\tau]\!]_\rho = \{(W, \mathrm{e}_1, \mathrm{e}_2) \mid \mathrm{freevars}(\mathrm{e}_1) = \mathrm{freevars}(\mathrm{e}_2) = \emptyset \wedge \\ \forall \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.\ \langle \mathrm{H}_1, \mathrm{e}_1\rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1'\rangle \nrightarrow \\ \implies \mathrm{e}_1' = \mathrm{fail}\ \textsc{Conv} \vee (\exists \mathrm{v}_2 \mathrm{H}_2' W'. \\ \langle \mathrm{H}_2, \mathrm{e}_2\rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{v}_2\rangle \wedge W \sqsubseteq W' \wedge \mathrm{H}_1', \mathrm{H}_2' : W' \wedge (W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!]_\rho)\}\end{aligned}$$

This relation is entirely standard – all of the interesting bits (capturing the semantics of affine references at runtime) is captured in our operational semantics, which is described by our world.

In order to properly close the terms, we need to separately interpret environments from our two source languages, and separate the affine and unrestricted environments from **Affi**.

For any binary substitution γ:

$$\gamma^1 \triangleq \{\ell \rightarrow \mathrm{v}_1 \mid \ell \rightarrow (\mathrm{v}_1, \mathrm{v}_2) \in \gamma\}$$
$$\gamma^2 \triangleq \{\ell \rightarrow \mathrm{v}_2 \mid \ell \rightarrow (\mathrm{v}_1, \mathrm{v}_2) \in \gamma\}$$

$$\mathrm{guard}(e, \ell) \triangleq \lambda\_.\{\mathrm{if}\ !\ell\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell := \textsc{used}; \mathrm{e}\}\}$$

$$\begin{aligned}
\mathcal{G}[\![\cdot]\!]_\rho &= \{(W, \cdot) \mid W \in \mathit{World}\}\\
\mathcal{G}[\![\Gamma, x : \tau]\!]_\rho &= \{(W, \gamma; x{\mapsto}(\mathrm{v}_1, \mathrm{v}_2)) \mid (W, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!]_\rho \wedge (W, \gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho\}\\
\mathcal{G}[\![\Gamma, \mathrm{x} : \tau]\!]_\rho &= \{(W, \gamma; x{\mapsto}(\mathrm{v}_1, \mathrm{v}_2)) \mid (W, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!]_\rho \wedge (W, \gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho\}\\
\mathcal{G}[\![\Omega, \mathrm{a} : \tau]\!]_\rho &= \{(W, \gamma; a{\mapsto}(\mathrm{guard}(\mathrm{v}_1, \ell_1), \mathrm{guard}(\mathrm{v}_2, \ell_2))) \mid \\
&\quad (\ell_1, \ell_2) \in W.\Theta \wedge (W, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!]_\rho \wedge (W, \gamma) \in \mathcal{G}[\![\Omega]\!]_\rho\\
&\quad \wedge \ell_1 \notin \mathit{FL}(\mathrm{v}_1) \cup \mathit{FL}(\mathrm{cod}(\gamma^1)) \wedge \ell_2 \notin \mathit{FL}(\mathrm{v}_2) \cup \mathit{FL}(\mathrm{cod}(\gamma^2))\}
\end{aligned}$$

Our interpretation of type environments is typical. Note that we write this in `MiniML` colors because **Affi** does not have polymorphism, so the only type environment we will be interpreting will be a `MiniML` one.

$$\begin{aligned}\mathcal{D}[\![\cdot]\!] &= \{\cdot\}\\ \mathcal{D}[\![\Delta, \alpha]\!] &= \{\rho[\alpha \mapsto R] \mid R \in \mathit{Typ} \wedge \rho \in \mathcal{D}[\![\Delta]\!]\}\end{aligned}$$

Where Typ was defined earlier as an arbitrary relation on pairs of target values.

Then we define an interpretation for each source typing judgment (as these judgments have different shapes).

$$\begin{aligned}&\Gamma;\Omega;\Delta;\Gamma \vdash \mathrm{e}_1 \precsim \mathrm{e}_2 : \tau \equiv \forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega\\ &\quad \rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W,\gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W,\gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket. \wedge (W,\gamma_\Omega) \in \mathcal{G}\llbracket\Omega\rrbracket.\\ &\quad \Longrightarrow\ (W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, {\mathrm{e}_1}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, {\mathrm{e}_2}^+)))) \in \mathcal{E}\llbracket\tau\rrbracket_\rho\end{aligned}$$

$$\begin{aligned}&\Gamma;\Omega;\Delta;\Gamma \vdash \mathrm{e}_1 \precsim \mathrm{e}_2 : \tau \equiv \forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega\\ &\quad \rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W,\gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W,\gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket. \wedge (W,\gamma_\Omega) \in \mathcal{G}\llbracket\Omega\rrbracket.\\ &\quad \Longrightarrow\ (W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, {\mathrm{e}_1}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, {\mathrm{e}_2}^+)))) \in \mathcal{E}\llbracket\tau\rrbracket_\rho\end{aligned}$$

$$\begin{aligned}&\Delta;\Gamma;\Gamma;\Omega \vdash \mathrm{e}_1 \precsim \mathrm{e}_2 : \tau \rightsquigarrow \Delta';\Gamma' \equiv\\ &\quad \Delta;\Gamma;\Gamma;\Omega \vdash \mathrm{e}_1 : \tau \rightsquigarrow \Delta';\Gamma'\\ &\wedge\ \Delta;\Gamma;\Gamma;\Omega \vdash \mathrm{e}_2 : \tau \rightsquigarrow \Delta';\Gamma'\\ &\wedge\ \Delta = \Delta' \wedge \Gamma = \Gamma' \wedge \Gamma;\Omega;\Delta;\Gamma \vdash \mathrm{e}_1 \precsim \mathrm{e}_2 : \tau\end{aligned}$$

$$\begin{aligned}&\Gamma;\Omega;\Delta;\Gamma \vdash \mathrm{e}_1 \precsim \mathrm{e}_2 : \tau \rightsquigarrow \Gamma';\Omega' \equiv\\ &\quad \Gamma;\Omega;\Delta;\Gamma \vdash \mathrm{e}_1 : \tau \rightsquigarrow \Gamma';\Omega'\\ &\wedge\ \Gamma;\Omega;\Delta;\Gamma \vdash \mathrm{e}_2 : \tau \rightsquigarrow \Gamma';\Omega'\\ &\wedge\ \exists \Omega_\mathrm{e}.\Omega = \Omega_\mathrm{e} \uplus \Omega' \wedge \Gamma = \Gamma' \wedge \Gamma;\Omega_\mathrm{e};\Delta;\Gamma \vdash \mathrm{e}_1 \precsim \mathrm{e}_2 : \tau\end{aligned}$$

We will use these shorthands frequently when stating compatibility rules about our type systems.

2.6.2 *Value Relation.* Our value relation is indexed by the source types of both MiniML and AFFI. Note, however, that what inhabits the relation is just the target: these source types are purely logical constructs.

$$\begin{array}{lcl}
\mathcal{V}\llbracket\mathtt{unit}\rrbracket_\rho & = & \{(W, (), ())\}\\
\mathcal{V}\llbracket\mathtt{int}\rrbracket_\rho & = & \{(W, \mathrm{n}, \mathrm{n}) \mid \mathrm{n} \in \mathbb{Z}\}\\
\mathcal{V}\llbracket\tau_1 \times \tau_2\rrbracket_\rho & = & \{(W, (\mathrm{v}_{1a}, \mathrm{v}_{2a}), (\mathrm{v}_{1b}, \mathrm{v}_{2b})) \mid (W, \mathrm{v}_{1a}, \mathrm{v}_{1b}) \in \mathcal{V}\llbracket\tau_1\rrbracket_\rho \wedge (W, \mathrm{v}_{2a}, \mathrm{v}_{2b}) \in \mathcal{V}\llbracket\tau_2\rrbracket_\rho\}\\
\mathcal{V}\llbracket\tau_1 + \tau_2\rrbracket_\rho & = & \{(W, \mathrm{inl}\ \mathrm{v}_1, \mathrm{inl}\ \mathrm{v}_2) \mid (W, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}\llbracket\tau_1\rrbracket_\rho\}\\
 & & \quad \cup \{(W, \mathrm{inr}\ \mathrm{v}_1, \mathrm{inr}\ \mathrm{v}_2) \mid (W, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}\llbracket\tau_2\rrbracket_\rho\}\\
\mathcal{V}\llbracket\tau_1 \rightarrow \tau_2\rrbracket_\rho & = & \{(W, \lambda \mathrm{x}.\{\mathrm{e}_1\}, \lambda \mathrm{x}.\{\mathrm{e}_2\}) \mid \forall \mathrm{v}_1\ \mathrm{v}_2\ W'.W \sqsubset W' \ \wedge\ (W', \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}\llbracket\tau_1\rrbracket_\rho\\
 & & \Longrightarrow\ (W', [x \mapsto \mathrm{v}_1]\mathrm{e}_1, [x \mapsto \mathrm{v}_2]\mathrm{e}_2) \in \mathcal{E}\llbracket\tau_2\rrbracket_\rho\}\\
\mathcal{V}\llbracket\mathtt{ref}\ \tau\rrbracket_\rho & = & \{(W, \ell_1, \ell_2) \mid W.\Psi(\ell_1, \ell_2) = \lfloor \mathcal{V}\llbracket\tau\rrbracket_\rho \rfloor_{W.k}\}\\
\mathcal{V}\llbracket\forall \alpha.\tau\rrbracket_\rho & = & \{(W, \lambda\_.\mathrm{e}_1, \lambda\_.\mathrm{e}_2) \mid \forall R \in \mathit{Typ},\ W'.W \sqsubset W' \ \Longrightarrow\ (W', \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}\llbracket\tau\rrbracket_{\rho[\alpha \mapsto R]}\}\\
\mathcal{V}\llbracket\alpha\rrbracket_\rho & = & \rho(\alpha)
\end{array}$$

Our relation for types from AFFI is similar.

$$\begin{array}{lcl}
\mathcal{V}[\![\mathrm{unit}]\!]_{.} & = & \{(W, (), ())\} \\
\mathcal{V}[\![\mathrm{bool}]\!]_{\rho} & = & \{(W, 0, 0)\} \cup \{(W, \mathrm{n}_1, \mathrm{n}_2) \mid \mathrm{n}_1 \neq 0 \wedge \mathrm{n}_2 \neq 0\} \\
\mathcal{V}[\![\mathrm{int}]\!]_{.} & = & \{(W, \mathrm{n}, \mathrm{n}) \mid \mathrm{n} \in \mathbb{Z}\} \\
\mathcal{V}[\![\tau_1 \multimap \tau_2]\!]_{.} & = & \{(W, \lambda\, \mathrm{a.e}_1, \lambda\, \mathrm{a.e}_2) \mid \forall \mathrm{v}_1\ \mathrm{v}_2\ W'\ \ell_1\ \ell_2. \\
 & & \quad W \sqsubset W' \wedge (W', \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau_1]\!]_{.} \wedge (\ell_1, \ell_2) \notin \mathrm{dom}(W'.\Psi) \cup \mathrm{dom}(W'.\Theta) \\
 & & \quad \Longrightarrow\ ((W'.k, W'.\Psi, W'.\Theta \uplus (\ell_1, \ell_2) \mapsto \textsc{unused}), \\
 & & \qquad [\mathrm{a} \mapsto \mathrm{guard}(\mathrm{v}_1, \ell_1)]\mathrm{e}_1, [\mathrm{a} \mapsto \mathrm{guard}(\mathrm{v}_2, \ell_2)]\mathrm{e}_2) \in \mathcal{E}[\![\tau_2]\!]_{.}\} \\
\mathcal{V}[\![!\tau]\!]_{.} & = & \{(W, \mathrm{v}_1, \mathrm{v}_2) \mid (W, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!]_{.}\} \\
\mathcal{V}[\![\tau_1 \otimes \tau_2]\!]_{.} & = & \{(W, (\mathrm{v}_{1a}, \mathrm{v}_{2a}), (\mathrm{v}_{1b}, \mathrm{v}_{2b})) \mid (W, \mathrm{v}_{1a}, \mathrm{v}_{1b}) \in \mathcal{V}[\![\tau_1]\!]_{.} \wedge (W, \mathrm{v}_{2a}, \mathrm{v}_{2b}) \in \mathcal{V}[\![\tau_2]\!]_{.}\} \\
\mathcal{V}[\![\tau_1 \& \tau_2]\!]_{.} & = & \{(W, (\lambda\_.\{\mathrm{e}_{1a}\}, \lambda\_.\{\mathrm{e}_{2a}\}), (\lambda\_.\{\mathrm{e}_{1b}\}, \lambda\_.\{\mathrm{e}_{2b}\})) \\
 & & \qquad \mid (W, \mathrm{e}_{1a}, \mathrm{e}_{1b}) \in \mathcal{E}[\![\tau_1]\!]_{.} \wedge (W, \mathrm{e}_{2a}, \mathrm{e}_{2b}) \in \mathcal{E}[\![\tau_2]\!]_{.}\}
\end{array}$$

2.7 Logical Relation Soundness

Lemma 2.1 (Expression Relation Contains Value Relation).

$$\mathcal{V}[\![\tau]\!]_{\rho} \subseteq \mathcal{E}[\![\tau]\!]_{\rho}$$

Proof. All terms in the value relation are irreducible, and thus are trivially in the expression relation. □

Lemma 2.2 (Split Substitutions). *For any world W and substitution γ such that*

$$(W, \gamma) \in \mathcal{G}[\![\Omega_1 \uplus \Omega_2]\!]_{\rho}$$

there exist substitutions γ_1, γ_2 such that $\gamma = \gamma_1 \uplus \gamma_2$ and

$$(W, \gamma_1) \in \mathcal{G}[\![\Omega_1]\!]_{\rho}$$

and

$$(W, \gamma_2) \in \mathcal{G}[\![\Omega_2]\!]_{\rho}$$

Moreover, for any $i, j \in \{1, 2\}$, for any $\Gamma; \Omega_j; \Delta; \Gamma \vdash \mathrm{e} : \tau \rightsquigarrow \Gamma'; \Omega'$,

$$close_i(\gamma, \mathrm{e}^+) = close_i(\gamma_j, \mathrm{e}^+)$$

and for any $\Delta; \Gamma; \Gamma; \Omega_j \vdash \mathrm{e} : \tau \rightsquigarrow \Delta'; \Gamma'$,

$$close_i(\gamma, \mathrm{e}^+) = close_i(\gamma_j, \mathrm{e}^+)$$

Proof. First, we need to show that there exist substitutions γ_1 and γ_2. This follows from the inductive structure of $\mathcal{G}[\![\Omega]\!]_{\rho}$, where we can separate the parts that came from $\mathcal{G}[\![\Omega_1]\!]_{\rho}$ and $\mathcal{G}[\![\Omega_2]\!]_{\rho}$. The second follows from the fact that the statics means that the rest of the substitution must not occur in the term, and thus $\mathrm{close}_i(\gamma, \mathrm{e}^+) = \mathrm{close}_i(\gamma_1, \mathrm{close}_i(\gamma_2, \mathrm{e}^+)) = \mathrm{close}_i(\gamma_1, \mathrm{e}^+)$ (for example). □

Lemma 2.3 (World Extension).

(1) *If $(W_1, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!]_{\rho}$ and $W_1 \sqsubseteq W_2$ then $(W_2, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!]_{\rho}$*
(2) *If $(W_1, \gamma_1, \gamma_2) \in \mathcal{G}[\![\Gamma]\!]_{\rho}$ and $W_1 \sqsubseteq W_2$ then $(W_2, \gamma_1, \gamma_2) \in \mathcal{G}[\![\Gamma]\!]_{\rho}$*

Proof. We note that world extension allows three things: the step index to decrease, the heap typing to add bindings (holding all existing bindings at same relation, module decreasing step index), and add flag references (ensuring existing flag references can go from unused to used, but not the other way). In all cases, this is straightforward based on the definition (relying on Lemma 2.4 in some cases). □

Lemma 2.4 (World Extension Transitive). *If $W_1 \sqsubseteq W_2$ and $W_2 \sqsubseteq W_3$ then $W_1 \sqsubseteq W_3$.*

Proof. Straightforward based on the definition. □

Lemma 2.5 (Heaps in Later World). *For any $W \in World$ and $\mathsf{H}_1, \mathsf{H}_2 : W$, it holds that $\mathsf{H}_1, \mathsf{H}_2 : \triangleright W$.*

Proof. Since heap typings map to relations that are by definition closed under world extension, and world extension cannot remove locations, only restrict them to future step indices, this holds by definition. □

Lemma 2.6 (Logical Relations for `MiniML` in Typ). *For any Δ, $\rho \in \mathcal{D}[\![\Delta]\!]$, and τ, if $\Delta \vdash \tau$, then $\mathcal{V}[\![\tau]\!]_\rho \in Typ$.*

Proof. By the definition of Typ, it suffices to show, for all natural numbers n, $\lfloor \mathcal{V}[\![\tau]\!]_\rho \rfloor_n \in Typ_n$. This requires us to show two things: first, that it is in $2^{AtomVal_n}$, and second that it is closed under world extension. The latter holds by Lemma 2.3. For the former, we note that we are required to show that the worlds are in $World_n$, which holds by definition. □

Lemma 2.7 (Compositionality). $(W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]_{\rho[\alpha \mapsto \mathcal{V}[\![\tau']\!]_\rho]} \iff (W, \mathsf{v}_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau[\tau'/\alpha]]\!]_\rho$

Proof. It suffices to show $\mathcal{V}[\![\tau]\!]_{\rho[\alpha \mapsto \mathcal{V}[\![\tau']\!]_\rho]} = \mathcal{V}[\![\tau[\tau'/\alpha]]\!]_\rho$, which we will do by induction on τ. We show the interesting cases:

Case $\tau = \alpha$.

$$\begin{aligned}
\mathcal{V}[\![[\alpha \mapsto \tau']\alpha]\!]_\rho &= \mathcal{V}[\![\tau']\!]_\rho && \text{(by sub)}\\
&= \rho[\alpha \mapsto \mathcal{V}[\![\tau']\!]_\rho](\alpha) && \text{(by lookup)}\\
&= \mathcal{V}[\![\alpha]\!]_{\rho[\alpha \mapsto \mathcal{V}[\![\tau']\!]_\rho]} && \text{(by def } \mathcal{V}[\![\cdot]\!]\text{.)}
\end{aligned}$$

Case $\tau = \beta \neq \alpha$.

$$\begin{aligned}
\mathcal{V}[\![[\alpha \mapsto \tau']\beta]\!]_\rho &= \mathcal{V}[\![\beta]\!]_\rho && \text{(by sub)}\\
&= \rho(\beta) && \text{(by def } \mathcal{V}[\![\cdot]\!]\text{.)}\\
&= \rho[\alpha \mapsto \mathcal{V}[\![\tau']\!]_\rho](\beta) && \text{(by lookup)}\\
&= \mathcal{V}[\![\beta]\!]_{\rho[\alpha \mapsto \mathcal{V}[\![\tau']\!]_\rho]} && \text{(by def } \mathcal{V}[\![\cdot]\!]\text{.)}
\end{aligned}$$

The other cases are straightforward by expanding the definitions of $\mathcal{V}[\![\cdot]\!]_\cdot, \mathcal{E}[\![\cdot]\!]_\cdot$ and applying the induction hypotheses. □

Lemma 2.8 (Expression Relation for Closed Types). *For any `MiniML` type τ where $\cdot \vdash \tau$ and any ρ,*

$$\mathcal{E}[\![\tau]\!]_\rho = \mathcal{E}[\![\tau]\!]_\cdot$$

Proof. Since $\mathcal{E}[\![\tau]\!]_\rho$ is defined in terms of $\mathcal{V}[\![\tau]\!]_\rho$, this proof is analogous to Lemma 2.7, though since what we are substituting is not used, the interpretation can be arbitrary. □

Lemma 2.9 (Closing `MiniML` Terms). *For any `MiniML` term e where $\Gamma; \Omega; \Delta; \Gamma \vdash \mathsf{e} : \tau \rightsquigarrow \Gamma'; \Omega'$, for any $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$ where $\rho \in \mathcal{D}[\![\Delta]\!]$, $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho$, $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\cdot$, and $(W, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!]_\cdot$, it holds that*

$$close_1(\gamma_\Gamma, close_1(\gamma_\Gamma, close_1(\gamma_\Omega, \mathsf{e}^+)))$$

and

$$close_2(\gamma_\Gamma, close_2(\gamma_\Gamma, close_2(\gamma_\Omega, \mathsf{e}^+)))$$

are closed terms.

Proof. Since free variables are compiled to free variables, and no other free variables are introduced via compilation, this follows trivially from the structure of $\mathcal{G}\llbracket\Gamma\rrbracket_\rho$. □

Lemma 2.10 (Closing Affi Terms). *For any* Affi *term* e *where* $\Delta;\Gamma;\Gamma;\Omega \vdash \mathrm{e} : \tau \rightsquigarrow \Delta';\Gamma'$, *for any* $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$ *where* $\rho \in \mathcal{D}\llbracket\Delta\rrbracket$, $(W, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho$, $(W, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\cdot$, *and* $(W, \gamma_\Omega) \in \mathcal{G}\llbracket\Omega\rrbracket_\cdot$, *it holds that*

$$close_1(\gamma_\Gamma, close_1(\gamma_\Gamma, close_1(\gamma_\Omega, \mathrm{e}^+)))$$

and

$$close_2(\gamma_\Gamma, close_2(\gamma_\Gamma, close_2(\gamma_\Omega, \mathrm{e}^+)))$$

are closed terms.

Proof. Since free variables are compiled to free variables, and no other free variables are introduced via compilation, this follows trivially from the structure of $\mathcal{G}\llbracket\Gamma\rrbracket_\rho$. □

Lemma 2.11 (Anti-reduction). *If* $(W', \mathrm{e}_1', \mathrm{e}_2') \in \mathcal{E}\llbracket\tau\rrbracket_\rho$, *then* $\forall j\ \mathrm{e}_1\ \mathrm{e}_2\ W\ \mathrm{H}_1\ \mathrm{H}_2\ \mathrm{H}_1'\ \mathrm{H}_2'. W \sqsubseteq W' \land j < W.k \land \mathrm{H}_1, \mathrm{H}_2 : W \land \langle \mathrm{H}_1, \mathrm{e}_1 \rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1' \rangle \land \langle \mathrm{H}_2, \mathrm{e}_2 \rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{e}_2' \rangle \land \mathrm{H}_1', \mathrm{H}_2' : W' \land W'.k \geq W.k - j \land freevars(\mathrm{e}_1) = freevars(\mathrm{e}_2) = \emptyset \implies (W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}\llbracket\tau\rrbracket_\rho$

Proof. Expanding the expression relation, given

$$\forall \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1^*,\ \mathrm{H}_1^*,\ j' < W.k.\ \langle \mathrm{H}_1, \mathrm{e}_1 \rangle \xrightarrow{j'} \langle \mathrm{H}_1^*, \mathrm{e}_1^* \rangle \nrightarrow$$

we must show either e_1^* is fail Conv or there exist v_2, H_2^*, W^* such that

$$\langle \mathrm{H}_2, \mathrm{e}_2 \rangle \xrightarrow{*} \langle \mathrm{H}_2^*, \mathrm{v}_2 \rangle \land W \sqsubseteq W^* \land \mathrm{H}_1^*, \mathrm{H}_2^* : W^* \land (W^*, \mathrm{e}_1^*, \mathrm{v}_2) \in \mathcal{V}\llbracket\tau\rrbracket_\rho$$

By confluence, if $\langle \mathrm{H}_1, \mathrm{e}_1 \rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1' \rangle$ and $\langle \mathrm{H}_1, \mathrm{e}_1 \rangle \xrightarrow{j'} \langle \mathrm{H}_1^*, \mathrm{e}_1^* \rangle \nrightarrow$, then

$$\langle \mathrm{H}_1', \mathrm{e}_1' \rangle \xrightarrow{j'-j} \langle \mathrm{H}_1^*, \mathrm{e}_1^* \rangle \nrightarrow$$

Thus, by applying $(W', \mathrm{e}_1', \mathrm{e}_2') \in \mathcal{E}\llbracket\tau\rrbracket_\rho$, since $j' - j < W.k - j \leq W'.k$, we find either e_1^* is fail Conv, in which case we are done, or there exist v_2, H_2^*, W^* such that

$$\langle \mathrm{H}_2', \mathrm{e}_2' \rangle \xrightarrow{*} \langle \mathrm{H}_2^*, \mathrm{v}_2 \rangle \land W' \sqsubseteq W^* \land \mathrm{H}_1^*, \mathrm{H}_2^* : W^* \land (W^*, \mathrm{e}_1^*, \mathrm{v}_2) \in \mathcal{V}\llbracket\tau\rrbracket_\rho$$

Now, since $W \sqsubseteq W'$ and $W' \sqsubseteq W^*$, we have $W \sqsubseteq W^*$ by Lemma 2.4. Moreover, since $\langle \mathrm{H}_2, \mathrm{e}_2 \rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{e}_2' \rangle$ and $\langle \mathrm{H}_2', \mathrm{e}_2' \rangle \xrightarrow{*} \langle \mathrm{H}_2^*, \mathrm{v}_2 \rangle$, we have $\langle \mathrm{H}_2, \mathrm{e}_2 \rangle \xrightarrow{*} \langle \mathrm{H}_2^*, \mathrm{v}_2 \rangle$. This suffices to finish the proof. □

Theorem 2.12 (Convertibility Soundness). *If* $\tau_A \sim \tau_B$ *then*
$\forall\, (W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}\llbracket\tau_A\rrbracket_\cdot \implies (W, C_{\tau_A \mapsto \tau_B}(\mathrm{e}_1), C_{\tau_A \mapsto \tau_B}(\mathrm{e}_2)) \in \mathcal{E}\llbracket\tau_B\rrbracket_\cdot \land \forall\, (W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}\llbracket\tau_B\rrbracket_\cdot \implies (W, C_{\tau_B \mapsto \tau_A}(\mathrm{e}_1), C_{\tau_B \mapsto \tau_A}(\mathrm{e}_2)) \in \mathcal{E}\llbracket\tau_A\rrbracket_\cdot.$

Proof. We prove this by simultaneous induction on the structure of the convertibility relation.

$\boxed{\texttt{unit} \sim \mathrm{unit}}$ There are two directions to this proof:

$$\forall\, (W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}\llbracket\texttt{unit}\rrbracket_\cdot \implies (W, C_{\texttt{unit} \mapsto \mathrm{unit}}(\mathrm{e}_1), C_{\texttt{unit} \mapsto \mathrm{unit}}(\mathrm{e}_2)) \in \mathcal{E}\llbracket\mathrm{unit}\rrbracket_\cdot$$

and:

$$\forall\, (W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}\llbracket\mathrm{unit}\rrbracket_\cdot \implies (W, C_{\mathrm{unit} \mapsto \texttt{unit}}(\mathrm{e}_1), C_{\mathrm{unit} \mapsto \texttt{unit}}(\mathrm{e}_2)) \in \mathcal{E}\llbracket\texttt{unit}\rrbracket_\cdot$$

Both directions are trivially similar to each other, so we will only prove the first direction. Expanding the definition of the convertibility boundaries, we refine this to:

$$\forall\,(W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}[\![\texttt{unit}]\!]. \implies (W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}[\![\mathrm{unit}]\!].$$

From the expression relation, we first need to show $\mathrm{e}_1, \mathrm{e}_2$ are closed. This follows directly from the fact the assumption that $(W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}[\![\texttt{unit}]\!].$, and all terms in the expression relation are closed. Next, we need to show that given:

$$\forall \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.\ \langle \mathrm{H}_1, \mathrm{e}_1\rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1'\rangle \not\twoheadrightarrow$$

then it holds that:

$$\mathrm{e}_1' = \mathrm{fail}\ \textsc{Conv} \vee (\exists \mathrm{v}_2 \mathrm{H}_2' W'.\langle \mathrm{H}_2, \mathrm{e}_2\rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{v}_2\rangle \wedge W \sqsubseteq W' \wedge \mathrm{H}_1', \mathrm{H}_2' : W' \wedge (W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![\mathrm{unit}]\!].)$$

By instantiating the assumption $(W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}[\![\texttt{unit}]\!].$ with $\mathrm{H}_1, \mathrm{H}_2$, we find that

$$\mathrm{e}_1' = \mathrm{fail}\ \textsc{Conv} \vee (\exists \mathrm{v}_2 \mathrm{H}_2' W'.\langle \mathrm{H}_2, \mathrm{e}_2\rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{v}_2\rangle \wedge W \sqsubseteq W' \wedge \mathrm{H}_1', \mathrm{H}_2' : W' \wedge (W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![\texttt{unit}]\!].)$$

Ergo, it suffices to show that if $(W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![\texttt{unit}]\!].$, then $(W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![\mathrm{unit}]\!]..$ However, this is trivial because $\mathcal{V}[\![\texttt{unit}]\!]. = \mathcal{V}[\![\mathrm{unit}]\!]. = \{(W, (), ())\}$.

$\boxed{\texttt{int} \sim \mathrm{bool}}$ There are two directions to this proof:

$$\forall\,(W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}[\![\texttt{int}]\!]. \implies (W, C_{\texttt{int}\mapsto\mathrm{bool}}(\mathrm{e}_1), C_{\texttt{int}\mapsto\mathrm{bool}}(\mathrm{e}_2)) \in \mathcal{E}[\![\mathrm{bool}]\!].$$

and:

$$\forall\,(W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}[\![\mathrm{bool}]\!]. \implies (W, C_{\mathrm{bool}\mapsto\texttt{int}}(\mathrm{e}_1), C_{\mathrm{bool}\mapsto\texttt{int}}(\mathrm{e}_2)) \in \mathcal{E}[\![\texttt{int}]\!].$$

Consider the first direction.

Expanding the definition of the convertibility boundaries, we refine this to:

$$\forall\,(W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}[\![\texttt{int}]\!]. \implies (W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}[\![\mathrm{bool}]\!].$$

From the expression relation, we first need to show $\mathrm{e}_1, \mathrm{e}_2$ are closed. This follows directly from the fact the assumption that $(W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}[\![\texttt{int}]\!].$, and all terms in the expression relation are closed. Next, we need to show that given:

$$\forall \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.\ \langle \mathrm{H}_1, \mathrm{e}_1\rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1'\rangle \not\twoheadrightarrow$$

then it holds that:

$$\mathrm{e}_1' = \mathrm{fail}\ \textsc{Conv} \vee (\exists \mathrm{v}_2 \mathrm{H}_2' W'.\langle \mathrm{H}_2, \mathrm{e}_2\rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{v}_2\rangle \wedge W \sqsubseteq W' \wedge \mathrm{H}_1', \mathrm{H}_2' : W' \wedge (W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![\mathrm{bool}]\!].)$$

By instantiating the assumption $(W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}[\![\texttt{int}]\!].$ with $\mathrm{H}_1, \mathrm{H}_2$, we find that

$$\mathrm{e}_1' = \mathrm{fail}\ \textsc{Conv} \vee (\exists \mathrm{v}_2 \mathrm{H}_2' W'.\langle \mathrm{H}_2, \mathrm{e}_2\rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{v}_2\rangle \wedge W \sqsubseteq W' \wedge \mathrm{H}_1', \mathrm{H}_2' : W' \wedge (W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![\texttt{int}]\!].)$$

Ergo, it suffices to show that if $(W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![\texttt{int}]\!].$, then $(W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![\mathrm{bool}]\!]..$ However, this is trivial because $\mathcal{V}[\![\texttt{int}]\!]. \subseteq \mathcal{V}[\![\mathrm{bool}]\!]..$

Next, consider the second direction. Expanding the convertibility boundaries, we must show:

$$\forall\,(W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}[\![\mathrm{bool}]\!]. \implies (W, \mathrm{if}\ \mathrm{e}_1\ 0\ 1, \mathrm{if}\ \mathrm{e}_2\ 0\ 1) \in \mathcal{E}[\![\texttt{int}]\!].$$

Expanding the expression relation, we must show that given

$$\forall \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.\ \langle \mathrm{H}_1, \mathrm{if}\ \mathrm{e}_1\ 0\ 1\rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1'\rangle \not\twoheadrightarrow$$

it holds that:

$e_1' = \text{fail Conv} \vee (\exists v_2 H_2' W'. \langle H_2, \text{if } e_2\ 0\ 1\rangle \xrightarrow{*} \langle H_2', v_2\rangle \wedge W \sqsubseteq W' \wedge H_1', H_2' : W' \wedge (W', e_1', v_2) \in \mathcal{V}[\![\texttt{int}]\!]_\rho)\}$

By $(W, e_1, e_2) \in \mathcal{E}[\![\text{bool}]\!]_.$, we find that either $\langle H_1, e_1\rangle$ either steps to fail Conv, in which case $\langle H_1, \text{if } e_1\ 0\ 1\rangle$ takes another step to fail Conv and we are done, or steps to an irreducible configuration $\langle H_1^*, e_1^*\rangle$, in which case $\langle H_2, e_2\rangle$ steps to an irreducible configuration $\langle H_2^*, e_2^*\rangle$ and there exists some world W' such that $W \sqsubseteq W'$, $H_1^*, H_2^* : W'$, and $(W', e_1^*, e_2^*) \in \mathcal{V}[\![\text{bool}]\!]_.$. There are then two cases:

(1) $e_1^* = e_2^* = 0$. In this scenario, we have

$$\langle H_1, \text{if } e_1\ 0\ 1\rangle \xrightarrow{*} \langle H_1^*, \text{if } 0\ 0\ 1\rangle \longrightarrow \langle H_1^*, 0\rangle$$

and

$$\langle H_2, \text{if } e_2\ 0\ 1\rangle \xrightarrow{*} \langle H_2^*, \text{if } 0\ 0\ 1\rangle \longrightarrow \langle H_2^*, 0\rangle$$

Then, we have from before that $W \sqsubseteq W'$ and $H_1^*, H_2^* : W'$, and one can easily see that $(W', 0, 0) \in \mathcal{V}[\![\texttt{int}]\!]_.$, which suffices to finish the proof.

(2) $e_1^* = n_1$ and $e_2^* = n_2$ with $n_1, n_2 \neq 0$. In this scenario, we have

$$\langle H_1, \text{if } e_1\ 0\ 1\rangle \xrightarrow{*} \langle H_1^*, \text{if } n_1\ 0\ 1\rangle \longrightarrow \langle H_1^*, 1\rangle$$

and

$$\langle H_2, \text{if } e_2\ 0\ 1\rangle \xrightarrow{*} \langle H_2^*, \text{if } n_2\ 0\ 1\rangle \longrightarrow \langle H_2^*, 1\rangle$$

Then, we have from before that $W \sqsubseteq W'$ and $H_1^*, H_2^* : W'$, and one can easily see that $(W', 1, 1) \in \mathcal{V}[\![\texttt{int}]\!]_.$, which suffices to finish the proof.

$\boxed{\tau_1 \otimes \tau_2 \sim \tau_1 \times \tau_2}$ There are two directions to this proof:

$$\forall\,(W, e_1, e_2) \in \mathcal{E}[\![\tau_1 \otimes \tau_2]\!]_. \implies (W, C_{\tau_1 \otimes \tau_2 \mapsto \tau_1 \times \tau_2}(e_1), C_{\tau_1 \otimes \tau_2 \mapsto \tau_1 \times \tau_2}(e_2)) \in \mathcal{E}[\![\tau_1 \times \tau_2]\!]_.$$

and:

$$\forall\,(W, e_1, e_2) \in \mathcal{E}[\![\tau_1 \times \tau_2]\!]_. \implies (W, C_{\tau_1 \times \tau_2 \mapsto \tau_1 \otimes \tau_2}(e_1), C_{\tau_1 \times \tau_2 \mapsto \tau_1 \otimes \tau_2}(e_2)) \in \mathcal{E}[\![\tau_1 \otimes \tau_2]\!]_.$$

Both directions are trivially similar to each other, so we will only prove the first direction. Expanding the definition of the convertibility boundaries, we refine this to:

$$\begin{aligned}
&\forall\,(W, e_1, e_2) \in \mathcal{E}[\![\tau_1 \otimes \tau_2]\!]_. \implies \\
&\quad (W, \\
&\quad \text{let } x = e_1 \text{ in } (C_{\tau_1 \mapsto \tau_1}(\text{fst } x), C_{\tau_2 \mapsto \tau_2}(\text{snd } x)), \\
&\quad \text{let } x = e_2 \text{ in } (C_{\tau_1 \mapsto \tau_1}(\text{fst } x), C_{\tau_2 \mapsto \tau_2}(\text{snd } x))) \in \mathcal{E}[\![\tau_1 \times \tau_2]\!]_.
\end{aligned}$$

From the expression relation, we first need to show the two expressions in the conclusion are closed. This follows from the fact that e_1, e_2 are closed, by the assumption that $(W, e_1, e_2) \in \mathcal{E}[\![\tau_1 \otimes \tau_2]\!]_.$, and that the new expressions do not introduce any new free variables. Next, we need to show that given:

$$\forall H_1, H_2{:}W,\ e_1',\ H_1',\ j < W.k.\ \langle H_1, \text{let } x = e_1 \text{ in } (C_{\tau_1 \mapsto \tau_1}(\text{fst } x), C_{\tau_2 \mapsto \tau_2}(\text{snd } x))\rangle \xrightarrow{j} \langle H_1', e_1'\rangle \nrightarrow$$

then it holds that:

$$\begin{aligned}
&e_1' = \text{fail Conv} \vee \\
&\quad (\exists v_2 H_2' W'. \langle H_2, \text{let } x = e_2 \text{ in } (C_{\tau_1 \mapsto \tau_1}(\text{fst } x), C_{\tau_2 \mapsto \tau_2}(\text{snd } x))\rangle \xrightarrow{*} \langle H_2', v_2\rangle \\
&\quad \wedge W \sqsubseteq W' \wedge H_1', H_2' : W' \wedge (W', e_1', v_2) \in \mathcal{V}[\![\tau_1 \times \tau_2]\!]_.)
\end{aligned}$$

First, since the let expression in the first configuration terminates to an irreducible configuration, by inspection on the operational semantic, it must be the case that $\langle \mathsf{H}_1, \mathsf{e}_1\rangle$ terminates to some irreducible configuration $\langle \mathsf{H}_1^*, \mathsf{e}_1^*\rangle$. Then, by assumption, it follows that either $\mathsf{e}_1^* = \mathsf{fail}\ \textsc{Conv}$, in which case the whole let expression steps to $\mathsf{fail}\ \textsc{Conv}$, or that e_1^* is a value, in which case $\langle \mathsf{H}_2, \mathsf{e}_2\rangle$ also steps to some irreducible configuration $\langle \mathsf{H}_2^*, \mathsf{e}_2^*\rangle$ and there exists some world W_1 where $W \sqsubseteq W_1$, $\mathsf{H}_1^*, \mathsf{H}_2^* : W_1$, and $(W_1, \mathsf{e}_1^*, \mathsf{e}_2^*) \in \mathcal{V}[\![\tau_1 \otimes \tau_2]\!]_{.}.$ By expanding the value relation definition, we find that $\mathsf{e}_1^* = (\mathsf{v}_1^*, \mathsf{v}_2^*)$ and $\mathsf{e}_2^* = (\mathsf{v}_1^\dagger, \mathsf{v}_2^\dagger)$ where $(W_1, \mathsf{v}_1^*, \mathsf{v}_1^\dagger) \in \mathcal{V}[\![\tau_1]\!]_{.}$ and $(W_1, \mathsf{v}_2^*, \mathsf{v}_2^\dagger) \in \mathcal{V}[\![\tau_2]\!]_{.}.$

Thus, the first configuration steps as follows:

$$\begin{aligned}
&\langle \mathsf{H}_1, \mathsf{let}\ \mathsf{x} = \mathsf{e}_1\ \mathsf{in}\ (\mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{fst}\ \mathsf{x}), \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{snd}\ \mathsf{x}))\rangle \xrightarrow{*}\\
&\langle \mathsf{H}_1^*, \mathsf{let}\ \mathsf{x} = (\mathsf{v}_1^*, \mathsf{v}_2^*)\ \mathsf{in}\ (\mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{fst}\ \mathsf{x}), \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{snd}\ \mathsf{x}))\rangle \longrightarrow\\
&\langle \mathsf{H}_1^*, (\mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{fst}\ (\mathsf{v}_1^*, \mathsf{v}_2^*)), \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{snd}\ (\mathsf{v}_1^*, \mathsf{v}_2^*)))\rangle \longrightarrow\\
&\langle \mathsf{H}_1^*, (\mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{v}_1^*), \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_2^*))\rangle
\end{aligned}$$

By a similar argument, the configuration on the other side with H_2 steps to

$$\langle \mathsf{H}_2^*, (\mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{v}_1^\dagger), \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_2^\dagger))\rangle$$

Since $(W_1, \mathsf{v}_1^*, \mathsf{v}_1^\dagger) \in \mathcal{V}[\![\tau_1]\!]_{.} \subseteq \mathcal{E}[\![\tau_1]\!]_{.}$ and $(W_1, \mathsf{v}_2^*, \mathsf{v}_2^\dagger) \in \mathcal{V}[\![\tau_2]\!]_{.} \subseteq \mathcal{E}[\![\tau_2]\!]_{.}$, by the induction hypothesis, we have that

$$(W_1, \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{v}_1^*), \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{v}_1^\dagger)) \in \mathcal{E}[\![\tau_1]\!]_{.}$$

and

$$(W_1, \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_2^*), \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_2^\dagger)) \in \mathcal{E}[\![\tau_2]\!]_{.}$$

By the first fact, either $\langle \mathsf{H}_1^*, \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{v}_1^*)\rangle$ steps to $\mathsf{fail}\ \textsc{Conv}$, in which case the original configuration with H_1 steps to $\mathsf{fail}\ \textsc{Conv}$, or it steps to an irreudicble configuration $\langle \mathsf{H}_1^\dagger, \mathsf{v}_1^{**}\rangle$, in which case $\langle \mathsf{H}_2^*, \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{v}_1^\dagger)\rangle$ also steps to an irreducible configuration $\langle \mathsf{H}_2^\dagger, \mathsf{v}_2^{**}\rangle$ and there exists some world W_2 where $W_1 \sqsubseteq W_2$, $\mathsf{H}_1^\dagger, \mathsf{H}_2^\dagger : W_2$, and $(W_2, \mathsf{v}_1^{**}, \mathsf{v}_2^{**}) \in \mathcal{V}[\![\tau_1]\!]_{.}.$

Once the first component of the pair in the configurations above have stepped to values v_1^{**} and v_2^{**}, the pair will continue reducing on the second component. Then, by Lemma 2.3, since $W_1 \sqsubseteq W_2$,

$$(W_2, \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_2^*), \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_2^\dagger)) \in \mathcal{E}[\![\tau_2]\!]_{.}$$

Thus, either $\langle \mathsf{H}_1^\dagger, \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_2^*)\rangle$ steps to $\mathsf{fail}\ \textsc{Conv}$, in which case the original configuration also takes a step to $\mathsf{fail}\ \textsc{Conv}$, or it steps to an irreducible configuration $\langle \mathsf{H}_1^f, \mathsf{v}_1^{***}\rangle$, in which case $\langle \mathsf{H}_2^\dagger, \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_2^\dagger)\rangle$ also steps to an irreducible configuration $\langle \mathsf{H}_2^f, \mathsf{v}_2^{***}\rangle$ and there exists some world W_3 where $W_2 \sqsubseteq W_3$, $\mathsf{H}_1^f, \mathsf{H}_2^f : W_3$, and $(W_3, \mathsf{v}_1^{***}, \mathsf{v}_2^{***}) \in \mathcal{V}[\![\tau_2]\!]_{.}.$

Thus, the original configuration with H_1 steps to $\langle \mathsf{H}_1^f, (\mathsf{v}_1^{**}, \mathsf{v}_1^{***})\rangle$ and the original configuration with H_2 steps to $\langle \mathsf{H}_2^f, (\mathsf{v}_2^{**}, \mathsf{v}_2^{***})\rangle$. We have $\mathsf{H}_1^f, \mathsf{H}_2^f : W_3$ and, since $W \sqsubseteq W_1$, $W_1 \sqsubseteq W_2$, and $W_2 \sqsubseteq W_3$, it follows that $W \sqsubseteq W_3$. Moreover, since $W_2 \sqsubseteq W_3$ and $(W_2, \mathsf{v}_1^{**}, \mathsf{v}_2^{**}) \in \mathcal{V}[\![\tau_1]\!]_{.}$, we have $(W_3, \mathsf{v}_1^{**}, \mathsf{v}_2^{**}) \in \mathcal{V}[\![\tau_1]\!]_{.}.$ Finally, we also have $(W_3, \mathsf{v}_1^{***}, \mathsf{v}_2^{***}) \in \mathcal{V}[\![\tau_2]\!]_{.}.$ Ergo,

$$(W_3, (\mathsf{v}_1^{**}, \mathsf{v}_1^{***}), (\mathsf{v}_2^{**}, \mathsf{v}_2^{***})) \in \mathcal{V}[\![\tau_1 \times \tau_2]\!]_{.}$$

which suffices to finish the proof.

$\boxed{\tau_1 \multimap \tau_2 \sim (\texttt{unit} \to \tau_1) \to \tau_2}$

There are two directions, we first prove the former implication, that is, that:

$$\begin{aligned}
&\forall\, (W, \mathsf{e}_1, \mathsf{e}_2) \in \mathcal{E}[\![\tau_1 \multimap \tau_2]\!]_{.} \implies\\
&(W, C_{\tau_1 \multimap \tau_2 \mapsto (\texttt{unit} \to \tau_1) \to \tau_2}(\mathsf{e}_1), C_{\tau_1 \multimap \tau_2 \mapsto (\texttt{unit} \to \tau_1) \to \tau_2}(\mathsf{e}_2)) \in \mathcal{E}[\![(\texttt{unit} \to \tau_1) \to \tau_2]\!]_{.}
\end{aligned}$$

Expanding the definition of the convertibility boundaries, we refine our goal to:

$$\begin{aligned}(W, &\text{let } \mathsf{x} = \mathsf{e}_1 \text{ in } \lambda \mathsf{x}_{\mathsf{thnk}}.\text{let } \mathsf{x}_{\mathsf{conv}} = \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{x}_{\mathsf{thnk}}\ ())\\ &\qquad\qquad \text{in let } \mathsf{x}_{\mathsf{access}} = \mathsf{thunk}(\mathsf{x}_{\mathsf{conv}}) \text{ in } \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{x}\ \mathsf{x}_{\mathsf{access}}),\\ &\text{let } \mathsf{x} = \mathsf{e}_2 \text{ in } \lambda \mathsf{x}_{\mathsf{thnk}}.\text{let } \mathsf{x}_{\mathsf{conv}} = \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{x}_{\mathsf{thnk}}\ ())\\ &\qquad\qquad \text{in let } \mathsf{x}_{\mathsf{access}} = \mathsf{thunk}(\mathsf{x}_{\mathsf{conv}}) \text{ in } \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{x}\ \mathsf{x}_{\mathsf{access}}))\\ &\in \mathcal{E}[\![(\texttt{unit} \to \tau_1) \to \tau_2]\!].\end{aligned}$$

From the expression relation, we must show first that the terms are closed, which follows from out hypothesis given we did not introduce any new free variables. Then, we need to show that given:

$$\forall \mathsf{H}_1, \mathsf{H}_2{:}W,\ \mathsf{e}_1',\ \mathsf{H}_1',\ j < W.k.$$

$$\begin{aligned}\langle \mathsf{H}_1,\ &\text{let } \mathsf{x} = \mathsf{e}_1 \text{ in } \lambda \mathsf{x}_{\mathsf{thnk}}.\text{let } \mathsf{x}_{\mathsf{conv}} = \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{x}_{\mathsf{thnk}}\ ()) \\ &\qquad\qquad \text{in let } \mathsf{x}_{\mathsf{access}} = \mathsf{thunk}(\mathsf{x}_{\mathsf{conv}}) \text{ in } \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{x}\ \mathsf{x}_{\mathsf{access}})\rangle \xrightarrow{j} \langle \mathsf{H}_1', \mathsf{e}_1'\rangle \nrightarrow\end{aligned}$$

We can demonstrate that either e_1' is fail Conv, or there exists $\mathsf{v}_2, \mathsf{H}_2', W'$ such that:

$$\begin{aligned}\langle \mathsf{H}_2,\ &\text{let } \mathsf{x} = \mathsf{e}_2 \text{ in } \lambda \mathsf{x}_{\mathsf{thnk}}.\text{let } \mathsf{x}_{\mathsf{conv}} = \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{x}_{\mathsf{thnk}}\ ()) \\ &\qquad\qquad \text{in let } \mathsf{x}_{\mathsf{access}} = \mathsf{thunk}(\mathsf{x}_{\mathsf{conv}}) \text{ in } \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{x}\ \mathsf{x}_{\mathsf{access}})\rangle \xrightarrow{*} \langle \mathsf{H}_2', \mathsf{v}_2\rangle\\ &\wedge W \sqsubseteq W' \wedge \mathsf{H}_1', \mathsf{H}_2' : W' \wedge (W', \mathsf{e}_1', \mathsf{v}_2) \in \mathcal{V}[\![(\texttt{unit} \to \tau_1) \to \tau_2]\!].\end{aligned}$$

To figure out what e_1' is, we know from the operational semantics that first we will evaluate e_1 until it is a value and then will substitute. From our hypothesis, which we can instantiate with H_1 and H_2, we know that e_1 will run with H_1 to either fail Conv (in which case this will lift into the entire term running to fail Conv) or will run to a value v_1 related at a future world $W^{\dagger}$ to another value v_2 that e_2 will run with H_2 to, where the heaps have evolved to $\mathsf{H}_1^{\dagger}, \mathsf{H}_2^{\dagger} : W^{\dagger}$.

Now, our original term will take another step and substitute v_1 for x (note that the operational semantics lifts steps on the subterm to steps on the whole term), which results in the following term:

$$\lambda \mathsf{x}_{\mathsf{thnk}}.\text{let } \mathsf{x}_{\mathsf{conv}} = \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{x}_{\mathsf{thnk}}\ ()) \text{ in let } \mathsf{x}_{\mathsf{access}} = \mathsf{thunk}(\mathsf{x}_{\mathsf{conv}}) \text{ in } \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_1\ \mathsf{x}_{\mathsf{access}})$$

This is clearly irreducible (it is a value), so we now need to show that the other side similarly reduces to a value, which follows in the same way from our hypothesis, and thus what remains to show is that these two values are related at $W^{\dagger}$ in $\mathcal{V}[\![(\texttt{unit} \to \tau_1) \to \tau_2]\!]$..

The definition of $\mathcal{V}[\![(\texttt{unit} \to \tau_1) \to \tau_2]\!]$. says that we need to take any $W^{\dagger} \sqsubset W'$, v_1', and v_2' that are in $\mathcal{V}[\![\texttt{unit} \to \tau_1]\!]$. and show that

$$\begin{aligned}(W', &[\mathsf{x}_{\mathsf{thnk}} \mapsto \mathsf{v}_1']\text{let } \mathsf{x}_{\mathsf{conv}} = \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{x}_{\mathsf{thnk}}\ ()) \text{ in let } \mathsf{x}_{\mathsf{access}} = \mathsf{thunk}(\mathsf{x}_{\mathsf{conv}}) \text{ in } \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_1\ \mathsf{x}_{\mathsf{access}}),\\ &[\mathsf{x}_{\mathsf{thnk}} \mapsto \mathsf{v}_2']\text{let } \mathsf{x}_{\mathsf{conv}} = \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{x}_{\mathsf{thnk}}\ ()) \text{ in let } \mathsf{x}_{\mathsf{access}} = \mathsf{thunk}(\mathsf{x}_{\mathsf{conv}}) \text{ in } \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_2\ \mathsf{x}_{\mathsf{access}})) \in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

Where if we substitute, we get:

$$\begin{aligned}(W', &\text{let } \mathsf{x}_{\mathsf{conv}} = \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{v}_1'\ ()) \text{ in let } \mathsf{x}_{\mathsf{access}} = \mathsf{thunk}(\mathsf{x}_{\mathsf{conv}}) \text{ in } \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_1\ \mathsf{x}_{\mathsf{access}}),\\ &\text{let } \mathsf{x}_{\mathsf{conv}} = \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{v}_2'\ ()) \text{ in let } \mathsf{x}_{\mathsf{access}} = \mathsf{thunk}(\mathsf{x}_{\mathsf{conv}}) \text{ in } \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_2\ \mathsf{x}_{\mathsf{access}})) \in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

Now we can expand the definition of thunk$(\cdot)$, to get:

$$\begin{aligned}&(W', \mathrm{let}\ \mathrm{x_{conv}} = \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{v}_1'\ ())\ \mathrm{in}\ \mathrm{let}\ \mathrm{x_{access}} =\\ &\qquad(\mathrm{let}\ \mathrm{r_{fresh}} = \mathrm{ref}\ 1\ \mathrm{in}\ \lambda\_.\{\mathrm{if}\ !\mathrm{r_{fresh}}\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\mathrm{r_{fresh}} := 0; \mathrm{x_{conv}}\}\})\ \mathrm{in}\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{v}_1\ \mathrm{x_{access}}),\\ &\quad \mathrm{let}\ \mathrm{x_{conv}} = \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{v}_2'\ ())\ \mathrm{in}\ \mathrm{let}\ \mathrm{x_{access}} =\\ &\qquad(\mathrm{let}\ \mathrm{r_{fresh}} = \mathrm{ref}\ 1\ \mathrm{in}\ \lambda\_.\{\mathrm{if}\ !\mathrm{r_{fresh}}\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\mathrm{r_{fresh}} := 0; \mathrm{x_{conv}}\}\})\ \mathrm{in}\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{v}_2\ \mathrm{x_{access}}))\\ &\quad \in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

From our induction hypothesis, instantiated with W', we know that, if they don't run forever or fail, $(W', \mathrm{C}_{\tau_1 \mapsto \tau_1}(v_1'\ ()), \mathrm{C}_{\tau_1 \mapsto \tau_1}(v_2'\ ()))$ will be in $\mathcal{E}[\![\tau_1]\!]$. if $(W', \mathrm{v}_1'\ (), \mathrm{v}_2'\ ())$ is in $\mathcal{E}[\![\tau_1]\!]$. Since we got v_1' and v_2' from $\mathcal{V}[\![\mathtt{unit} \to \tau_1]\!]$., the latter holds, and thus we know the converted terms will eventually run to related values vc_1 and vc_2 at some future world W'' of W' in $\mathcal{V}[\![\tau_1]\!]$. We can further step, substituting those values and reducing to a future world W''' that has in $W'''.\Theta$ a pair of fresh locations (ℓ_1, ℓ_2) pointing to UNUSED:

$$\begin{aligned}&(W''', \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{v}_1\ (\lambda\_.\{\mathrm{if}\ !\ell_1\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1 := 0; \mathrm{vc}_1\}\})),\\ &\quad \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{v}_2\ (\lambda\_.\{\mathrm{if}\ !\ell_2\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2 := 0; \mathrm{vc}_2\}\}))) \in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

Our induction hypothesis reduces this to proving that:

$$(W''', \mathrm{v}_1(\lambda\_.\{\mathrm{if}\ !\ell_1\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1 := 0; \mathrm{vc}_1\}\}), \mathrm{v}_2(\lambda\_.\{\mathrm{if}\ !\ell_2\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2 := 0; \mathrm{vc}_2\}\})) \in \mathcal{E}[\![\tau_2]\!].$$

If we return to how we got v_1 and v_2, we know they are in $\mathcal{V}[\![\tau_1 \multimap \tau_2]\!]$. with world $W^\dagger$, but via Lemma 2.3, they are also related under W'''. From that definition, we know that $\mathrm{v_i}$ has the form $\lambda\ \mathrm{a.e_i}$, and that:

$$\begin{aligned}&((W^*.k, W^*.\Psi, W^*.\Theta \uplus (\ell_1, \ell_2) \mapsto \textsc{unused}),\\ &\quad \mathrm{close}(\{a \mapsto \mathrm{guard}(\mathrm{v_1}^*, \ell_1)\}, e_1), \mathrm{close}(\{a \mapsto \mathrm{guard}(\mathrm{v_2}^*, \ell_2)\}, e_2)) \in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

Given any related values $\mathrm{v_1}^*$ and $\mathrm{v_2}^*$ at a future world W^* of W'''. If we expand out the definition of guard(·), we note that it exactly matches the terms that we have, and thus our vc_1 and vc_2 are exactly $\mathrm{v_1}^*$ and $\mathrm{v_1}^*$, which we already know are related at $\mathcal{V}[\![\tau_1]\!]$., and due to Lemma 2.3, they are related not only at W'' but also at W^*. Thus, we are done with the first direction.

Now we have to prove the other direction, that is, that:

$$\begin{aligned}&\forall\ (W, \mathrm{e}_1, \mathrm{e}_2) \in \mathcal{E}[\![(\mathtt{unit} \to \tau_1) \to \tau_2]\!].\ \implies\\ &(W, C_{(\mathtt{unit} \to \tau_1) \to \tau_2 \mapsto \tau_1 \multimap \tau_2}(\mathrm{e}_1), C_{(\mathtt{unit} \to \tau_1) \to \tau_2 \mapsto \tau_1 \multimap \tau_2}(\mathrm{e}_2)) \in \mathcal{E}[\![\tau_1 \multimap \tau_2]\!].\end{aligned}$$

Expanding the definition of the convertibility boundaries, we refine our goal to:

$$\begin{aligned}&(W, \mathrm{let}\ \mathrm{x}\ =\ \mathrm{e}_1\ \mathrm{in}\ \lambda \mathrm{x_{thnk}}.\mathrm{let}\ \mathrm{x_{access}}\ =\ \mathrm{thunk}(\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}}\ ()))\ \mathrm{in}\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{x}\ \mathrm{x_{access}}),\\ &\quad \mathrm{let}\ \mathrm{x}\ =\ \mathrm{e}_2\ \mathrm{in}\ \lambda \mathrm{x_{thnk}}.\mathrm{let}\ \mathrm{x_{access}}\ =\ \mathrm{thunk}(\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}}\ ()))\ \mathrm{in}\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{x}\ \mathrm{x_{access}}))\\ &\quad \in \mathcal{E}[\![\tau_1 \multimap \tau_2]\!].\end{aligned}$$

From the expression relation, we must show first that the terms are closed, which follows from out hypothesis given we did not introduce any new free variables. Then, we need to show that given:

$$\begin{gathered}\forall \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.\\ \langle \mathrm{H}_1, \mathrm{let}\ \mathrm{x}\ =\ \mathrm{e}_1\ \mathrm{in}\ \lambda \mathrm{x_{thnk}}.\mathrm{let}\ \mathrm{x_{access}}\ =\ \mathrm{thunk}(\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}}\ ()))\ \mathrm{in}\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{x}\ \mathrm{x_{access}})\rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1'\rangle \not\rightarrow\end{gathered}$$

We can demonstrate that either e_1' is fail Conv, or there exists $\mathsf{v}_2, \mathsf{H}_2', W'$ such that:

$$\begin{aligned}&\langle \mathsf{H}_2, \mathsf{let\ x\ =\ e_2\ in\ } \lambda \mathsf{x_{thnk}}.\mathsf{let\ x_{access}\ =\ thunk}(\mathsf{C}_{\tau_1\mapsto\tau_1}(\mathsf{x_{thnk}}\ ()))\ \mathsf{in}\ \mathsf{C}_{\tau_2\mapsto\tau_2}(\mathsf{x\ x_{access}})\rangle \xrightarrow{*} \langle \mathsf{H}_2', \mathsf{v}_2\rangle\\ &\quad \wedge W \sqsubseteq W' \wedge \mathsf{H}_1', \mathsf{H}_2' : W' \wedge (W', \mathsf{e}_1', \mathsf{v}_2) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!].\end{aligned}$$

To figure out what e_1' is, we know from the operational semantics that first we will evaluate e_1 until it is a value and then will substitute. From our hypothesis, which we can instantiate with H_1 and H_2, we know that e_1 will run with H_1 to either fail Conv (in which case this will lift into the entire term running to fail Conv) or will run to a value v_1 related at a future world $W^\dagger$ to another value v_2 that e_2 will run with H_2 to, where the heaps have evolved to $\mathsf{H}_1^\dagger, \mathsf{H}_2^\dagger : W^\dagger$.

Now, our original term will take another step and substitute v_1 for x (note that the operational semantics lifts steps on the subterm to steps on the whole term), which results in the following term:

$$\lambda \mathsf{x_{thnk}}.\mathsf{let\ x_{access}\ =\ thunk}(\mathsf{C}_{\tau_1\mapsto\tau_1}(\mathsf{x_{thnk}}\ ()))\ \mathsf{in}\ \mathsf{C}_{\tau_2\mapsto\tau_2}(\mathsf{v_1\ x_{access}})$$

This is clearly irreducible (it is a value), so we now need to show that the other side similarly reduces to a value v_2, which follows in the same way from our hypothesis, and thus what remains to show is that:

$$\begin{aligned}(W^\dagger, &\lambda \mathsf{x_{thnk}}.\mathsf{let\ x_{access}\ =\ thunk}(\mathsf{C}_{\tau_1\mapsto\tau_1}(\mathsf{x_{thnk}}\ ()))\ \mathsf{in}\ \mathsf{C}_{\tau_2\mapsto\tau_2}(\mathsf{v_1\ x_{access}}),\\ &\lambda \mathsf{x_{thnk}}.\mathsf{let\ x_{access}\ =\ thunk}(\mathsf{C}_{\tau_1\mapsto\tau_1}(\mathsf{x_{thnk}}\ ()))\ \mathsf{in}\ \mathsf{C}_{\tau_2\mapsto\tau_2}(\mathsf{v_2\ x_{access}}))\\ &\in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!].\end{aligned}$$

The definition of $\mathcal{V}[\![\tau_1 \multimap \tau_2]\!]$. says that we need to take any $W^\dagger \sqsubset W', \mathsf{v}_1', \mathsf{v}_2', \ell_1, \ell_2$ where $(W^\dagger, \mathsf{v}_1', \mathsf{v}_2')$ are in $\mathcal{V}[\![\tau_1]\!]$. and (ℓ_1, ℓ_2) are not in either $W'.\Psi$ or $W'.\Theta$ and show that

$$\begin{aligned}(W', &[\mathsf{x_{thnk}} \mapsto \mathsf{guard}(\mathsf{v}_1', \ell_1)]\mathsf{let\ x_{access}\ =\ thunk}(\mathsf{C}_{\tau_1\mapsto\tau_1}(\mathsf{x_{thnk}}\ ()))\ \mathsf{in}\ \mathsf{C}_{\tau_2\mapsto\tau_2}(\mathsf{v_1\ x_{access}}),\\ &[\mathsf{x_{thnk}} \mapsto \mathsf{guard}(\mathsf{v}_2', \ell_2)]\mathsf{let\ x_{access}\ =\ thunk}(\mathsf{C}_{\tau_1\mapsto\tau_1}(\mathsf{x_{thnk}}\ ()))\ \mathsf{in}\ \mathsf{C}_{\tau_2\mapsto\tau_2}(\mathsf{v_2\ x_{access}}))\\ &\in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

Where if we substitute, we get:

$$\begin{aligned}(W', &\mathsf{let\ x_{access}\ =\ thunk}(\mathsf{C}_{\tau_1\mapsto\tau_1}(\mathsf{guard}(\mathsf{v}_1', \ell_1)\ ()))\ \mathsf{in}\ \mathsf{C}_{\tau_2\mapsto\tau_2}(\mathsf{v_1\ x_{access}}),\\ &\mathsf{let\ x_{access}\ =\ thunk}(\mathsf{C}_{\tau_1\mapsto\tau_1}(\mathsf{guard}(\mathsf{v}_2', \ell_2)\ ()))\ \mathsf{in}\ \mathsf{C}_{\tau_2\mapsto\tau_2}(\mathsf{v_2\ x_{access}}))\\ &\in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

First, let's expand the definition of $\mathsf{thunk}(\cdot)$:

$$\begin{aligned}(W',\ &\mathsf{let\ x_{access}\ =\ let\ r_{fresh} = ref\ \textsc{unused}\ in}\\ &\qquad \lambda\_.\{\mathsf{if}\ !\mathsf{r_{fresh}}\ \{\mathsf{fail\ Conv}\}\ \{\mathsf{r_{fresh}} := \textsc{used}; \mathsf{C}_{\tau_1\mapsto\tau_1}(\mathsf{guard}(\mathsf{v}_1', \ell_1)\ ())\}\})\ \mathsf{in}\ \mathsf{C}_{\tau_2\mapsto\tau_2}(\mathsf{v_1\ x_{access}}) \quad ,\\ &\mathsf{let\ x_{access}\ =\ let\ r_{fresh} = ref\ \textsc{unused}\ in}\\ &\qquad \lambda\_.\{\mathsf{if}\ !\mathsf{r_{fresh}}\ \{\mathsf{fail\ Conv}\}\ \{\mathsf{r_{fresh}} := \textsc{used}; \mathsf{C}_{\tau_1\mapsto\tau_1}(\mathsf{guard}(\mathsf{v}_2', \ell_2)\ ())\})\}\ \mathsf{in}\ \mathsf{C}_{\tau_2\mapsto\tau_2}(\mathsf{v_2\ x_{access}}) \quad)\\ &\in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

From Lemma 2.11 we can take three steps forward: allocating a new reference (ℓ_i'), substituting it for $\mathsf{r_{fresh}}$, and then substituting all of $\mathsf{x_{access}}$, and thus suffices to show that:

$$\begin{aligned}(W^\dagger, &\mathsf{C}_{\tau_2\mapsto\tau_2}(\mathsf{v}_1\ (\lambda\_.\{\mathsf{if}\ !\ell_1'\ \{\mathsf{fail\ Conv}\}\ \{\ell_1' := \textsc{used}; \mathsf{C}_{\tau_1\mapsto\tau_1}(\mathsf{guard}(\mathsf{v}_1', \ell_1)\ ())\}\})),\\ &\mathsf{C}_{\tau_2\mapsto\tau_2}(\mathsf{v}_2\ (\lambda\_.\{\mathsf{if}\ !\ell_2'\ \{\mathsf{fail\ Conv}\}\ \{\ell_2' := \textsc{used}; \mathsf{C}_{\tau_1\mapsto\tau_1}(\mathsf{guard}(\mathsf{v}_2', \ell_2)\ ())\}\}))\\ &\in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

Where $W^\dagger$ has a new pair of references in $W^\dagger.\Theta$ (set to UNUSED), a smaller step index, but otherwise is identical to W'.

For this, we can appeal to our induction hypothesis, which requires us to show that:

$$\begin{aligned}(\,&W^\dagger, \mathrm{v}_1\ (\lambda\_.\{\mathrm{if}\ !\ell_1'\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1' := \textsc{used}; \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{guard}(\mathrm{v}_1', \ell_1)\ ())\}\}),\\ &\mathrm{v}_2\ (\lambda\_.\{\mathrm{if}\ !\ell_2'\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2' := \textsc{used}; \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{guard}(\mathrm{v}_2', \ell_2)\ ())\}\}))\\ &\in \mathcal{E}[\![\tau_2]\!]_{.}\end{aligned}$$

Recalling that v_1 and v_2 came from $\mathcal{V}[\![(\texttt{unit} \to \tau_1) \to \tau_2]\!]_{.}$, we can proceed by appealing to the definition of that relation, which tells us that for any arguments in $\mathcal{V}[\![\texttt{unit} \to \tau_1]\!]_{.}$, the result of substituting will be in $\mathcal{E}[\![\tau_2]\!]_{.}$. It thus remains to show that:

$$\begin{aligned}(\,&W^*, \lambda\_.\{\mathrm{if}\ !\ell_1'\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1' := \textsc{used}; \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{guard}(\mathrm{v}_1', \ell_1)\ ())\}\},\\ &\lambda\_.\{\mathrm{if}\ !\ell_2'\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2' := \textsc{used}; \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{guard}(\mathrm{v}_2', \ell_2)\ ())\}\})\\ &\in \mathcal{V}[\![\texttt{unit} \to \tau_1]\!]_{.}\end{aligned}$$

Where W^* is some future world of $W^\dagger$. From the definition of $\mathcal{V}[\![\texttt{unit} \to \tau_1]\!]_{.}$, we have to show that substituting () for the unused argument results in terms in $\mathcal{E}[\![\tau_1]\!]_{.}$, at some arbitrary future world W^{**}.

We proceed first by case analysis on whether the affine flags (ℓ_1', ℓ_2') have been set to USED, which they can be in a future world. If they have been, we can expand the definition of the expression relation, choose heaps $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : W^{**}$, and show that

$$\langle \mathrm{H}_1, \mathrm{if}\ !\ell_1'\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1' := \textsc{used}; \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{guard}(\mathrm{v}_1', \ell_1)\ ())\rangle \xrightarrow{2} \langle \mathrm{H}_1, \mathrm{fail}\ \textsc{Conv}\rangle$$

At which point we are done.

Thus, we now consider if (ℓ_1', ℓ_2') are still set to UNUSED. If that's the case, we instead appeal to Lemma 2.11, taking three steps to move into the else branches and update the affine flags to USED. That means we reduce our task to showing that in a world W^{***}, which now has those locations marked used in Θ, we need to show:

$$(\,W^{***}, \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{guard}(\mathrm{v}_1', \ell_1)\ ()), \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{guard}(\mathrm{v}_2', \ell_2)\ ())) \in \mathcal{E}[\![\tau_1]\!]_{.}$$

We now again appeal to our induction hypothesis, expanding the definition of $\mathrm{guard}(\cdot)$ at the same time to yield the following obligation:

$$(\,W^{***}, (\lambda\_.\{\mathrm{if}\ !\ell_1\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1 := \textsc{used}; \mathrm{v}_1'\}\})\ (), (\lambda\_.\{\mathrm{if}\ !\ell_2\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2 := \textsc{used}; \mathrm{v}_2'\}\})\ ()) \in \mathcal{E}[\![\tau_1]\!]_{.}$$

We can appeal to Lemma 2.11 to take one step, eliminating the pointless beta-reduction (for simplicity, we use the same name for the world, even though it is a future world):

$$(\,W^{***}, \mathrm{if}\ !\ell_1\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1 := \textsc{used}; \mathrm{v}_1'\}, \mathrm{if}\ !\ell_2\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2 := \textsc{used}; \mathrm{v}_2'\}) \in \mathcal{E}[\![\tau_1]\!]_{.}$$

Now we again do case analysis on whether (ℓ_1, ℓ_2) is USED in $W^{***}.\Theta$. If it is, then, as before, we trivially reduce the left side to failure and are done. If it is not, then we update those affine flags and reduce both sides to the values v_1' and v_2', at a future world W^{final}. Now we knew, originally, that those values were in $\mathcal{V}[\![\tau_1]\!]_{.}$ at world $W^\dagger$, but since, through many applications of Lemma 2.4 and Lemma 2.3, that also means that they are related at W^{final}, we are finally done.

□

THEOREM 2.13 (FUNDAMENTAL PROPERTY). *If* $\Gamma; \Omega; \Delta; \Gamma \vdash \mathrm{e} : \tau \rightsquigarrow \Gamma'; \Omega'$ *then* $\Gamma; \Omega; \Delta; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \tau \rightsquigarrow \Gamma'; \Omega'$ *and if* $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{e} : \tau \rightsquigarrow \Delta'; \Gamma'$ *then* $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{e} \preceq \mathrm{e} : \tau \rightsquigarrow \Delta'; \Gamma'$.

Proof. By induction on typing derivation, relying on the following compatibility lemmas, which have to exist for every typing rule in both source languages. □

Theorem 2.14 (Type Safety for MiniML). *For any* MiniML *term* e *where* $\cdot;\cdot;\cdot;\cdot \vdash \mathsf{e} : \tau \leadsto \cdot;\cdot$ *and for any heap* H*, if* $\langle \mathsf{H}, \mathsf{e}^{+} \rangle \xrightarrow{*} \langle \mathsf{H}', \mathsf{e}' \rangle$*, then either* $\mathsf{e}' = \mathsf{fail}\ \textsc{Conv}$*,* e' *is a value, or there exist* $\mathsf{H}'', \mathsf{e}''$ *such that* $\langle \mathsf{H}', \mathsf{e}' \rangle \longrightarrow \langle \mathsf{H}'', \mathsf{e}'' \rangle$*.*

Proof. This follows as a consequence of the fundamental property and the definition of the logical relation, as follows: if $\langle \mathsf{H}, \mathsf{e}^{+} \rangle \xrightarrow{n} \langle \mathsf{H}', \mathsf{e}' \rangle$, then consider a trivial world W with $k > n$, an empty heap typing and empty affine store. Then, since the term is closed, the fundamental property says that $(W, \mathsf{e}^{+}, \mathsf{e}^{+}) \in \mathcal{E}\llbracket\tau\rrbracket_{\cdot}$. This means that it runs to a stuck state, which is either at n or greater than n. If it's greater than n, then we have a further step that can be taken. If it gets stuck at n, then we know that is either fail Conv or a value. □

Theorem 2.15 (Type Safety for Affi). *For any* Affi *term* e *where* $\cdot;\cdot;\cdot;\cdot \vdash \mathsf{e} : \tau \leadsto \cdot;\cdot$ *and for any heap* H*, if* $\langle \mathsf{H}, \mathsf{e}^{+} \rangle \xrightarrow{*} \langle \mathsf{H}', \mathsf{e}' \rangle$*, then we know from the logical relation that either* $\mathsf{e}' = \mathsf{fail}\ \textsc{Conv}$*,* e' *is a value, or there exist* $\mathsf{H}'', \mathsf{e}''$ *such that* $\langle \mathsf{H}', \mathsf{e}' \rangle \longrightarrow \langle \mathsf{H}'', \mathsf{e}'' \rangle$*.*

Proof. This proof is identical to that of MiniML. □

Lemma 2.16 (Compat unit).

$$\Gamma;\Omega;\Delta;\Gamma \vdash () \preceq () : \mathtt{unit} \leadsto \Gamma;\Omega$$

Proof. One can see that $\Omega = \cdot \uplus \Omega$ and $\Gamma = \Gamma$. Moreover, $\Gamma;\Omega;\Delta;\Gamma \vdash () : \mathtt{unit} \leadsto \Gamma;\Omega$ by the unit typing rule. Ergo, it suffices to show that $\Gamma;\cdot;\Delta;\Gamma \vdash () \preceq () : \mathtt{unit}$.

Expanding the conclusion, given

$$\forall W.\forall \rho\, \gamma_{\Gamma}\, \gamma_{\Gamma}\, \gamma_{\Omega}.\rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \gamma_{\Gamma}) \in \mathcal{G}\llbracket\Gamma\rrbracket_{\rho} \wedge (W, \gamma_{\Gamma}) \in \mathcal{G}\llbracket\Gamma\rrbracket_{\cdot} \wedge (W, \gamma_{\Omega}) \in \mathcal{G}\llbracket\cdot\rrbracket_{\cdot}$$

we must show

$$(W, \mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Omega}, ()^{+}))), \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Omega}, ()^{+})))) \in \mathcal{E}\llbracket\mathtt{unit}\rrbracket_{\rho}$$

$()^{+} = ()$ is a closed term, so the closings have no effect. Ergo,

$$\mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Omega}, ()^{+}))) = \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Omega}, ()^{+}))) = ()$$

One can easily see $(W, (), ()) \in \mathcal{V}\llbracket\mathtt{unit}\rrbracket_{\rho}$, which suffices to show $(W, (), ()) \in \mathcal{E}\llbracket\mathtt{unit}\rrbracket_{\rho}$ by Lemma 2.1. This suffices to finish the proof.

□

Lemma 2.17 (Compat int).

$$\Gamma;\Omega;\Delta;\Gamma \vdash \mathbb{Z} \preceq \mathbb{Z} : \mathtt{int} \leadsto \Gamma;\Omega$$

Proof. One can see that $\Omega = \cdot \uplus \Omega$ and $\Gamma = \Gamma$. Moreover, $\Gamma;\Omega;\Delta;\Gamma \vdash \mathbb{Z} : \mathtt{int} \leadsto \Gamma;\Omega$ from the int typing rule. Ergo, it suffices to show that $\Gamma;\cdot;\Delta;\Gamma \vdash \mathsf{n} \preceq \mathsf{n} : \mathtt{int}$ for any $n \in \mathbb{Z}$.

Expanding the conclusion, given

$$\forall W.\forall \rho\, \gamma_{\Gamma}\, \gamma_{\Gamma}\, \gamma_{\Omega}.\rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \gamma_{\Gamma}) \in \mathcal{G}\llbracket\Gamma\rrbracket_{\rho} \wedge (W, \gamma_{\Gamma}) \in \mathcal{G}\llbracket\Gamma\rrbracket_{\cdot} \wedge (W, \gamma_{\Omega}) \in \mathcal{G}\llbracket\cdot\rrbracket_{\cdot}$$

we must show

$$(W, \mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Omega}, \mathsf{n}^{+}))), \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Omega}, \mathsf{n}^{+})))) \in \mathcal{E}\llbracket\mathtt{int}\rrbracket_{\rho}$$

$\mathsf{n}^{+} = \mathsf{n}$ is a closed term, so the closings have no effect. Ergo,

$$\mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Omega}, \mathsf{n}^{+}))) = \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Omega}, \mathsf{n}^{+}))) = \mathsf{n}$$

Since $\mathsf{n} \in \mathbb{Z}$, one can easily see $(W, \mathsf{n}, \mathsf{n}) \in \mathcal{V}\llbracket\mathtt{int}\rrbracket_{\rho}$, which suffices to show $(W, \mathsf{n}, \mathsf{n}) \in \mathcal{E}\llbracket\mathtt{int}\rrbracket_{\rho}$ by Lemma 2.1. This suffices to finish the proof. □

Lemma 2.18 (Compat x).

$$\Delta \vdash \tau \land \mathsf{x} : \tau \in \Gamma \implies \Gamma; \Omega; \Delta; \Gamma \vdash \mathsf{x} \preceq \mathsf{x} : \tau \rightsquigarrow \Gamma; \Omega$$

Proof. One can see that $\Omega = \cdot \uplus \Omega$ and $\Gamma = \Gamma$. Moreover, $\Gamma; \Omega; \Delta; \Gamma \vdash \mathsf{x} : \tau \rightsquigarrow \Gamma; \Omega$ from the variable typing rule. Ergo, it suffices to show that $\Gamma; \cdot; \Delta; \Gamma \vdash \mathsf{x} \preceq \mathsf{x} : \tau$.

Second, expanding this conclusion, given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}[\![\Delta]\!] \land (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \land (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_{.} \land (W, \gamma_\Omega) \in \mathcal{G}[\![\cdot]\!]_{.}$$

we must show

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{x}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{x}^+)))) \in \mathcal{E}[\![\tau]\!]_\rho$$

Notice that $\mathsf{x}^+ = \mathrm{x}$. Then, since $\mathsf{x} \notin \cdot$ and $(W, \gamma_\Omega) \in \mathcal{G}[\![\cdot]\!]_{.}$, we have

$$\mathrm{close}_1(\gamma_\Omega, \mathrm{x}) = \mathrm{close}_2(\gamma_\Omega, \mathrm{x}) = \mathrm{x}$$

Next, since $\mathsf{x} \notin \Gamma$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_{.}$, we have

$$\mathrm{close}_1(\gamma_\Gamma, \mathrm{x}) = \mathrm{close}_2(\gamma_\Gamma, \mathrm{x}) = \mathrm{x}$$

Finally, since $\mathsf{x} : \tau \in \Gamma$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_{.}$, there must exist $\mathrm{v}_1, \mathrm{v}_2$ such that

$$\gamma_\Gamma(\mathsf{x}) = (\mathrm{v}_1, \mathrm{v}_2) \land (W, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!]_\rho$$

Thus,

$$\mathrm{close}_1(\gamma_\Gamma, \mathrm{x}) = \mathrm{v}_1 \land \mathrm{close}_2(\gamma_\Gamma, \mathrm{x}) = \mathrm{v}_2$$

Ergo, since $(W, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!]_\rho$, this suffices to show that

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{x}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{x}^+)))) \in \mathcal{V}[\![\tau]\!]_\rho$$

By Lemma 2.1, $\mathcal{V}[\![\tau]\!]_\rho \subseteq \mathcal{E}[\![\tau]\!]_\rho$, so this suffices to finish the proof. □

Lemma 2.19 (Compat $\times$).

$$\begin{gathered} \Gamma_1; \Omega_1; \Delta; \Gamma \vdash \mathsf{e}_1 \preceq \mathsf{e}_1 : \tau_1 \rightsquigarrow \Gamma_2; \Omega_2 \\ \land \Gamma_2; \Omega_2; \Delta; \Gamma \vdash \mathsf{e}_2 \preceq \mathsf{e}_2 : \tau_2 \rightsquigarrow \Gamma_3; \Omega_3 \\ \implies \Gamma_1; \Omega_1; \Delta; \Gamma \vdash (\mathsf{e}_1, \mathsf{e}_2) \preceq (\mathsf{e}_1, \mathsf{e}_2) : \tau_1 \times \tau_2 \rightsquigarrow \Gamma_3; \Omega_3 \end{gathered}$$

Proof. Expanding the hypotheses, we find that $\Gamma_1 = \Gamma_2 = \Gamma_3$ and there exist Ω_e, Ω'_e such that $\Omega_1 = \Omega_e \uplus \Omega_2$ where $\Gamma_1; \Omega_e; \Delta; \Gamma \vdash \mathsf{e}_1 \preceq \mathsf{e}_1 : \tau_1$ and $\Omega_2 = \Omega'_e \uplus \Omega_3$ where $\Gamma_1; \Omega'_e; \Delta; \Gamma \vdash \mathsf{e}_2 \preceq \mathsf{e}_2 : \tau_2$. Therefore, $\Omega_1 = (\Omega_e \uplus \Omega'_e) \uplus \Omega_3$. Moreover, $\Gamma_1; \Omega_1; \Delta; \Gamma \vdash (\mathsf{e}_1, \mathsf{e}_2) \preceq (\mathsf{e}_1, \mathsf{e}_2) : \tau_1 \times \tau_2 \rightsquigarrow \Gamma_3; \Omega_3$ by the pair typing rule. It thus suffices to show that $\Gamma_1; \Omega_e \uplus \Omega'_e; \Delta; \Gamma \vdash (\mathsf{e}_1, \mathsf{e}_2) \preceq (\mathsf{e}_1, \mathsf{e}_2) : \tau_1 \times \tau_2$.

Expanding the conclusion, we must show that given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}[\![\Delta]\!] \land (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \land (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_{.} \land (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega_e \uplus \Omega'_e]\!]_{.}$$

then

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, (\mathsf{e}_1, \mathsf{e}_2)^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, (\mathsf{e}_1, \mathsf{e}_2)^+)))) \in \mathcal{E}[\![\tau_1 \times \tau_2]\!]_\rho$$

Notice that both of the expressions have no free variables by Lemma 2.9.

We can push the compiler and substitutions through the pair to refine that to:

$$\begin{gathered} (W, (\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_1{}^+))), \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_2{}^+)))), \\ (\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}_1{}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}_2{}^+))))) \in \mathcal{E}[\![\tau_1 \times \tau_2]\!]_\rho \end{gathered}$$

Then, we can expand the definition of the expression relation to get that given:

$$\begin{gathered} \forall \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}'_1,\ \mathrm{H}'_1,\ j < W.k. \\ \langle \mathrm{H}_1, (\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_1{}^+))), \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_2{}^+))))\rangle \xrightarrow{j} \langle \mathrm{H}'_1, \mathrm{e}'_1 \rangle \nrightarrow \end{gathered}$$

we need to show that either e_1' is fail Conv, or there exists v_2, H_2', W' such that:

$$\langle H_2, (\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, e_1{}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, e_2{}^+))))\rangle \overset{*}{\longrightarrow} \langle H_2', v_2\rangle$$
$$\wedge W \sqsubseteq W' \wedge H_1', H_2' : W' \wedge (W', e_1', v_2) \in \mathcal{V}[\![\tau_1 \times \tau_2]\!]_\rho$$

In order to proceed, first notice that, by Lemma 2.2, $\gamma_\Omega = \gamma_1 \uplus \gamma_2$ where

$$(W, \gamma_1) \in \mathcal{G}[\![\Omega_e]\!]_\cdot$$

and

$$(W, \gamma_2) \in \mathcal{G}[\![\Omega_e']\!]_\cdot$$

and, for any $i \in \{1, 2\}$

$$\mathrm{close}_i(\gamma_\Omega, e_1) = \mathrm{close}_i(\gamma_1, e_1)$$

and

$$\mathrm{close}_i(\gamma_\Omega, e_2) = \mathrm{close}_i(\gamma_2, e_2)$$

Next, we need to know what e_1' is. From the operational semantic, we know that our pair will first run its first component using the heap H_1 until it reaches a target value (or gets stuck). By appealing to our first induction hypothesis, instantiated it with W, γ_Γ, γ_Γ, γ_1, ρ, we get that:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, e_1{}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, e_1{}^+)))) \in \mathcal{E}[\![\tau_1]\!]_\rho$$

And in particular, can then use this, choosing the heaps to be H_1, and H_2 (which satisfy W), to conclude that either $\langle H_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, e_1{}^+)))\rangle$ reduces to fail Conv (with any heap, as it doesn't matter), in which case the entire term will take another step to fail Conv, or it will reduce to some irreducible intermediate configuration $\langle H_1^*, e_1^*\rangle$, at which point the other side will reduce to a corresponding intermediate configuration $\langle H_2^*, e_1^\dagger\rangle$ and both will be in $\mathcal{V}[\![\tau_1]\!]_\rho$ for some world W_1 that is a future world of W such that $H_1^*, H_2^* : W_1$.

Since terms in the value relation are target values, our original pair will continue reducing on the other subexpression according to the operational semantics. To figure out what happens, we can appeal to our other induction hypothesis, this time using W_1, which we can do since $\mathcal{G}[\![\Gamma]\!]_\rho, \mathcal{G}[\![\Gamma]\!]_\cdot, \mathcal{G}[\![\Omega_e']\!]_\cdot$ is closed under world extension (Lemma 2.3), and choosing heaps H_1^*, H_2^*.

From that hypothesis, we again either get that

$$\langle H_1^*, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, e_2{}^+)))\rangle$$

either runs to fail Conv, in which case the entire term takes another step to fail Conv, or to an irreducible configuration $\langle H_1', e_2{}^*\rangle$ such that the other side runs to some configuration $\langle H_2', e_2^\dagger\rangle$ and both are in $\mathcal{V}[\![\tau_2]\!]_\rho$ for some world W_2 that is a future world of W_1, with $H_1', H_2' : W_2$. Since terms in the value relation are values, our original pair, with H_1, has now run to the configuration $\langle H_1', (e_1^*, e_2^*)\rangle$, which is a pair of values and thus is irreducible.

Now we just need to show that there is a value on the other side, corresponding heap, and extended world such that the resulting pairs are in $\mathcal{V}[\![\tau_1 \times \tau_2]\!]_\rho$. The former two we have gotten along the way, from our induction hypotheses, which composed together give us that

$$\langle H_2, (\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, e_1{}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, e_2{}^+))))\rangle$$

runs to the irreducible configuration $\langle H_2', (e_1^\dagger, e_2^\dagger)\rangle$. The future world that satisfies the resulting heaps H_1' and H_2' is W_2. Because world extension is transitive (Lemma 2.4), this is a future world not only of W_1 but of W, as needed.

Finally, to show that our pairs are in the value relation at that world, we need to show that each corresponding component is in the value relation at the component type. For τ_2, this is by definition. For τ_1, we know that e_1^* and e_2^* are related at W_1, but need to show that they are related at W_2. But this is exactly Lemma 2.3, and so we are done. □

Lemma 2.20 (Compat `fst`).

$$\Gamma;\Omega;\Delta;\Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau_1 \times \tau_2 \rightsquigarrow \Gamma';\Omega' \implies \Gamma;\Omega;\Delta;\Gamma \vdash \mathtt{fst}\ \mathsf{e} \preceq \mathtt{fst}\ \mathsf{e} : \tau_1 \rightsquigarrow \Gamma';\Omega'$$

Proof. Expanding the hypotheses, we find that $\Gamma = \Gamma'$ and there exists Ω_e such that $\Omega = \Omega_\mathsf{e} \uplus \Omega'$ where $\Gamma;\Omega_\mathsf{e};\Delta;\Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau_1 \times \tau_2$. Moreover, $\Gamma;\Omega;\Delta;\Gamma \vdash \mathtt{fst}\ \mathsf{e} : \tau_1 \rightsquigarrow \Gamma';\Omega'$ by the `fst` typing rule. It thus suffices to show that $\Gamma;\Omega_\mathsf{e};\Delta;\Gamma \vdash \mathtt{fst}\ \mathsf{e} \preceq \mathtt{fst}\ \mathsf{e} : \tau_1$.

Expanding the conclusion, we must show that given

$$\forall W.\forall \rho\ \gamma_\Gamma\ \gamma_\Gamma\ \gamma_\Omega.\rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]. \wedge (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega_\mathsf{e}]\!].$$

then

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathtt{fst}\ \mathsf{e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathtt{fst}\ \mathsf{e}^+)))) \in \mathcal{E}[\![\tau_1]\!]_\rho$$

Notice that both of these expressions have no free variables by Lemma 2.9.

We can push the compiler and substitutions through `fst` to refine that to:

$$(W, \mathrm{fst}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+))), \mathrm{fst}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))) \in \mathcal{E}[\![\tau_1]\!]_\rho$$

Expanding the expression relation definition, we find that given

$$\forall \mathsf{H}_1, \mathsf{H}_2{:}W,\ \mathsf{e}_1',\ \mathsf{H}_1',\ j < W.k.$$
$$\langle \mathsf{H}_1, \mathrm{fst}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+)))\rangle \xrightarrow{j} \langle \mathsf{H}_1', \mathsf{e}_1'\rangle \nrightarrow$$

we must show either $\mathsf{e}_1' = \mathsf{fail}\ \textsc{Conv}$ or there exist $\mathsf{v}_2, \mathsf{H}_2', W'$ such that:

$$\langle \mathsf{H}_2, \mathrm{fst}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))\rangle \xrightarrow{*} \langle \mathsf{H}_2', \mathsf{v}_2\rangle$$
$$\wedge W \sqsubseteq W' \wedge \mathsf{H}_1', \mathsf{H}_2' : W' \wedge (W', \mathsf{e}_1', \mathsf{v}_2) \in \mathcal{V}[\![\tau_1]\!]_\rho$$

To proceed, we must find what e_1' is. From the operational semantic, we know fst will run its argument using H_1 until it reaches a target value or gets stuck. From the induction hypothesis instantiated with W, γ_Γ, γ_Γ, γ_Ω, ρ, we find that:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))) \in \mathcal{E}[\![\tau_1 \times \tau_2]\!]_\rho$$

By instantiating this fact with $\mathsf{H}_1, \mathsf{H}_2$, we find that $\langle \mathsf{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+)))\rangle$ either reduces to $\mathsf{fail}\ \textsc{Conv}$, in which case the entire term reduced to $\mathsf{fail}\ \textsc{Conv}$, or it will reduce to some $\langle \mathsf{H}_1^*, \mathsf{e}_1{}^*\rangle$, in which case the other side with H_2 will reduce to some $\langle \mathsf{H}_2^*, \mathsf{e}_1{}^\dagger\rangle$ and $(W_1, \mathsf{e}_1{}^*, \mathsf{e}_1{}^\dagger) \in \mathcal{V}[\![\tau_1 \times \tau_2]\!]_\rho$ for some world W_1 where $W \sqsubseteq W_1$ and $\mathsf{H}_1^*, \mathsf{H}_2^* : W_1$.

Then, by expanding the definition of the value relation, we find there exist $\mathsf{v}_{1a}, \mathsf{v}_{1b}, \mathsf{v}_{2a}, \mathsf{v}_{2b}$ such that $\mathsf{e}_1^* = (\mathsf{v}_{1a}, \mathsf{v}_{2a})$, $\mathsf{e}_1^\dagger = (\mathsf{v}_{1b}, \mathsf{v}_{2b})$, $(W_1, \mathsf{v}_{1a}, \mathsf{v}_{1b}) \in \mathcal{V}[\![\tau_1]\!]_\rho$, and $(W_1, \mathsf{v}_{2a}, \mathsf{v}_{2b}) \in \mathcal{V}[\![\tau_2]\!]_\rho$.

Thus, the original configuration with H_1 runs to the configuration $\langle \mathsf{H}_1^*, \mathrm{fst}\ (\mathsf{v}_{1a}, \mathsf{v}_{2a})\rangle$, which steps to $\langle \mathsf{H}_1^*, \mathsf{v}_{1a}\rangle$, which is a value and thus irreducible. Ergo, we have $\mathsf{e}_1' = \mathsf{v}_{1a}$.

Moreover, on the other side, the original pair with H_2 runs to the configuration $\langle \mathsf{H}_2^*, \mathrm{fst}\ (\mathsf{v}_{1b}, \mathsf{v}_{2b})\rangle$, which steps to $\langle \mathsf{H}_2^*, \mathsf{v}_{1b}\rangle$, which is a value and thus irreducible.

Then, since H_1^* and H_2^* both satisfy the world W_1, it suffices to show $(W_1, \mathsf{v}_{1a}, \mathsf{v}_{1b}) \in \mathcal{V}[\![\tau_1]\!]_\rho$. This is true by definition of $\mathsf{v}_{1a}, \mathsf{v}_{1b}$, which suffices to finish the proof. □

Lemma 2.21 (Compat `snd`).

$$\Gamma;\Omega;\Delta;\Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau_1 \times \tau_2 \rightsquigarrow \Gamma';\Omega' \implies \Gamma;\Omega;\Delta;\Gamma \vdash \mathsf{snd}\ \mathsf{e} \preceq \mathsf{snd}\ \mathsf{e} : \tau_2 \rightsquigarrow \Gamma';\Omega'$$

Proof. This proof is essentially identical to that of `fst`. □

Lemma 2.22 (Compat $\mathtt{inl}$).

$$\Delta \vdash \tau_2 \land \Gamma; \Omega; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau_1 \rightsquigarrow \Gamma'; \Omega' \implies \Gamma; \Omega; \Delta; \Gamma \vdash \mathtt{inl}\ \mathsf{e} \preceq \mathtt{inl}\ \mathsf{e} : \tau_1 + \tau_2 \rightsquigarrow \Gamma'; \Omega'$$

Proof. Expanding the hypotheses, we find that $\Gamma = \Gamma'$ and there exists Ω_e such that $\Omega = \Omega_\mathsf{e} \uplus \Omega'$ where $\Gamma; \Omega_\mathsf{e}; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau_1$. Moreover, $\Gamma; \Omega; \Delta; \Gamma \vdash \mathtt{inl}\ \mathsf{e} : \tau_1 + \tau_2 \rightsquigarrow \Gamma'; \Omega'$ by the $\mathtt{inl}$ typing rule. It thus suffices to show that $\Gamma; \Omega_\mathsf{e}; \Delta; \Gamma \vdash \mathtt{inl}\ \mathsf{e} \preceq \mathtt{inl}\ \mathsf{e} : \tau_1 + \tau_2$.

Expanding the conclusion, we must show that given

$$\forall W. \forall \rho\ \gamma_\Gamma\ \gamma_\Gamma\ \gamma_\Omega. \rho \in \mathcal{D}[\![\Delta]\!] \land (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \land (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]. \land (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega_\mathsf{e}]\!].$$

then

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathtt{inl}\ \mathsf{e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathtt{inl}\ \mathsf{e}^+)))) \in \mathcal{E}[\![\tau_1 + \tau_2]\!]_\rho$$

Notice that both of these expressions have no free variables by Lemma 2.9.

We can push the compiler and substitutions through $\mathtt{inl}$ to refine that to:

$$(W, \mathsf{inl}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+))), \mathsf{inl}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))) \in \mathcal{E}[\![\tau_1 + \tau_2]\!]_\rho$$

Then, expanding the expression relation definition, we find that given

$$\forall \mathsf{H}_1, \mathsf{H}_2{:}W,\ \mathsf{e}_1',\ \mathsf{H}_1',\ j < W.k.$$
$$\langle \mathsf{H}_1, \mathsf{inl}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+)))\rangle \xrightarrow{j} \langle \mathsf{H}_1', \mathsf{e}_1' \rangle \nrightarrow$$

we must show either $\mathsf{e}_1' = \mathsf{fail}\ \textsc{Conv}$ or there exist $\mathsf{v}_2, \mathsf{H}_2', W'$ such that:

$$\langle \mathsf{H}_2, \mathsf{inl}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))\rangle \xrightarrow{*} \langle \mathsf{H}_2', \mathsf{v}_2 \rangle$$
$$\land W \sqsubseteq W' \land \mathsf{H}_1', \mathsf{H}_2' : W' \land (W', \mathsf{e}_1', \mathsf{v}_2) \in \mathcal{V}[\![\tau_1 + \tau_2]\!]_\rho$$

To proceed, we must find what e_1' is. From the operational semantic, we know inl will run its argument using H_1 until it reaches a target value or gets stuck. From the induction hypothesis instantiated with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$, we find that:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))) \in \mathcal{E}[\![\tau_1]\!]_\rho$$

By instantiating this fact with $\mathsf{H}_1, \mathsf{H}_2$, we find that $\langle \mathsf{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+)))\rangle$ either reduces to $\mathsf{fail}\ \textsc{Conv}$, in which case the entire term reduced to $\mathsf{fail}\ \textsc{Conv}$, or it will reduce to some $\langle \mathsf{H}_1^*, \mathsf{e}_1{}^* \rangle$, in which case the other side with H_2 will reduce to some $\langle \mathsf{H}_2^*, \mathsf{e}_1{}^\dagger \rangle$ and $(W_1, \mathsf{e}_1{}^*, \mathsf{e}_1{}^\dagger) \in \mathcal{V}[\![\tau_1]\!]_\rho$ for some world W_1 where $W \sqsubseteq W_1$ and $\mathsf{H}_1^*, \mathsf{H}_2^* : W_1$.

Thus, the original pair with H_1 runs to the configuration $\langle \mathsf{H}_1^*, \mathsf{inl}\ \mathsf{e}_1^* \rangle$, which is a value and thus irreducible. Ergo, we have $\mathsf{e}_1' = \mathsf{inl}\ \mathsf{e}_1^*$.

Moreover, on the other side, the original pair with H_2 runs to the configuration $\langle \mathsf{H}_2^*, \mathsf{inl}\ \mathsf{e}_1^\dagger \rangle$, which is also a value and thus irreducible.

Then, since H_1^* and H_2^* both satisfy the world W_1, it suffices to show $(W_1, \mathsf{inl}\ \mathsf{e}_1^*, \mathsf{inl}\ \mathsf{e}_1^\dagger) \in \mathcal{V}[\![\tau_1 + \tau_2]\!]_\rho$. This holds true because $(W_1, \mathsf{e}_1^*, \mathsf{e}_1^\dagger) \in \mathcal{V}[\![\tau_1]\!]_\rho$, which suffices to finish the proof. □

Lemma 2.23 (Compat $\mathtt{inr}$).

$$\Delta \vdash \tau_1 \land \Gamma; \Omega; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau_2 \rightsquigarrow \Gamma'; \Omega' \implies \Gamma; \Omega; \Delta; \Gamma \vdash \mathtt{inr}\ \mathsf{e} \preceq \mathtt{inr}\ \mathsf{e} : \tau_1 + \tau_2 \rightsquigarrow \Gamma'; \Omega'$$

Proof. This proof is essentially identical to that of $\mathtt{inl}$. □

Lemma 2.24 (Compat $\mathtt{match}$).

$$\Gamma_1; \Omega_1; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau_1 + \tau_2 \rightsquigarrow \Gamma_2; \Omega_2$$
$$\land \Gamma_2; \Omega_2; \Delta; \Gamma[\mathsf{x} : \tau_1] \vdash \mathsf{e}_1 \preceq \mathsf{e}_1 : \tau \rightsquigarrow \Gamma_3; \Omega_3$$
$$\land \Gamma_2; \Omega_2; \Delta; \Gamma[\mathsf{y} : \tau_2] \vdash \mathsf{e}_2 \preceq \mathsf{e}_2 : \tau \rightsquigarrow \Gamma_3; \Omega_3$$
$$\implies \Gamma_1; \Omega_1; \Delta; \Gamma \vdash \mathtt{match}\ \mathsf{e}\ \mathsf{x}\{\mathsf{e}_1\}\ \mathsf{y}\{\mathsf{e}_2\} \preceq \mathtt{match}\ \mathsf{e}\ \mathsf{x}\{\mathsf{e}_1\}\ \mathsf{y}\{\mathsf{e}_2\} : \tau \rightsquigarrow \Gamma_3; \Omega_3$$

Proof. Expanding the hypotheses, we find $\Gamma_1 = \Gamma_2 = \Gamma_3$ and there exist Ω_e, Ω'_e such that $\Omega_1 = \Omega_e \uplus \Omega_2$ where $\Gamma_1; \Omega_1; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau_1 + \tau_2$ and $\Omega_2 = \Omega'_e \uplus \Omega_3$ where $\Gamma_2; \Omega_2; \Delta; \Gamma[\mathsf{x} : \tau_1] \vdash \mathsf{e}_1 \preceq \mathsf{e}_1 : \tau$ and $\Gamma_2; \Omega_2; \Delta; \Gamma[\mathsf{y} : \tau_2] \vdash \mathsf{e}_2 \preceq \mathsf{e}_2 : \tau$. Moreover, $\Gamma_1; \Omega_1; \Delta; \Gamma \vdash \mathtt{match}\ \mathsf{e}\ \mathsf{x}\{\mathsf{e}_1\}\ \mathsf{y}\{\mathsf{e}_2\} : \tau \rightsquigarrow \Gamma_3; \Omega_3$ by the $\mathtt{match}$ typing rule. It thus suffices to show that

$$\Gamma_1; \Omega_1; \Delta; \Gamma \vdash \mathtt{match}\ \mathsf{e}\ \mathsf{x}\{\mathsf{e}_1\}\ \mathsf{y}\{\mathsf{e}_2\} \preceq \mathtt{match}\ \mathsf{e}\ \mathsf{x}\{\mathsf{e}_1\}\ \mathsf{y}\{\mathsf{e}_2\} : \tau$$

Expanding the conclusion, we must show that given

$$\forall W. \forall \rho\ \gamma_\Gamma\ \gamma_\Gamma\ \gamma_\Omega. \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]. \wedge (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega_e \uplus \Omega'_e]\!].$$

then

$$\begin{aligned}&(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathtt{match}\ \mathsf{e}\ \mathsf{x}\{\mathsf{e}_1\}\ \mathsf{y}\{\mathsf{e}_2\}^+))),\\ &\quad \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathtt{match}\ \mathsf{e}\ \mathsf{x}\{\mathsf{e}_1\}\ \mathsf{y}\{\mathsf{e}_2\}^+)))) \in \mathcal{E}[\![\tau]\!]_\rho\end{aligned}$$

Notice that both of the expressions have no free variables by Lemma 2.9.

We can push the compiler and substitutions through the match to refine that to:

$$\begin{aligned}&(W, \mathsf{match}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+)))\\ &\quad \mathsf{x}\{\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_1{}^+)))\}\ \mathsf{y}\{\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_2{}^+)))\},\\ &\quad \mathsf{match}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))\\ &\quad \mathsf{x}\{\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}_1{}^+)))\}\ \mathsf{y}\{\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}_2{}^+)))\}, \in \mathcal{E}[\![\tau]\!]_\rho\end{aligned}$$

We can expand the definition of the expression relation to get that given:

$$\begin{gathered}\forall \mathsf{H}_1, \mathsf{H}_2{:}W,\ \mathsf{e}'_1,\ \mathsf{H}'_1,\ j < W.k.\\ \langle \mathsf{H}_1, \mathsf{match}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+)))\\ \mathsf{x}\{\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_1{}^+)))\}\ \mathsf{y}\{\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_2{}^+)))\}\rangle \xrightarrow{j} \langle \mathsf{H}'_1, \mathsf{e}'_1\rangle \nrightarrow\end{gathered}$$

we need to show that either e'_1 is fail Conv, or there exists $\mathsf{v}_2, \mathsf{H}'_2, W'$ such that:

$$\begin{aligned}&\langle \mathsf{H}_2, \mathsf{match}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))\\ &\quad \mathsf{x}\{\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}_1{}^+)))\}\ \mathsf{y}\{\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}_2{}^+)))\}\rangle \xrightarrow{*} \langle \mathsf{H}'_2, \mathsf{v}_2\rangle\\ &\quad \wedge W \sqsubseteq W' \wedge \mathsf{H}'_1, \mathsf{H}'_2 : W' \wedge (W', \mathsf{e}'_1, \mathsf{v}_2) \in \mathcal{V}[\![\tau]\!]_\rho\end{aligned}$$

In order to proceed, first notice that, by applying Lemma 2.2 twice, we find that $\gamma_\Omega = \gamma_1 \uplus \gamma_2$ where

$$(W, \gamma_1) \in \mathcal{G}[\![\Omega_e]\!].$$

and

$$(W, \gamma_2) \in \mathcal{G}[\![\Omega'_e]\!].$$

and for any $i \in \{1, 2\}$,

$$\mathrm{close}_i(\gamma_\Omega, \mathsf{e}) = \mathrm{close}_i(\gamma_1, \mathsf{e})$$

and

$$\mathrm{close}_i(\gamma_\Omega, \mathsf{e}) = \mathrm{close}_i(\gamma_2, \mathsf{e}_1)$$

and

$$\mathrm{close}_i(\gamma_\Omega, \mathsf{e}) = \mathrm{close}_i(\gamma_2, \mathsf{e}_2)$$

Next, we need to know what e'_1 is. From the operational semantics, we know that the match expression will run its first subexpression using the heap H_1 until it reaches a target value or gets stuck. From our first induction hypothesis, instantiated with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_1, \rho$, we find that

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))) \in \mathcal{E}[\![\tau_1 + \tau_2]\!]_\rho$$

We can instatiate this with the heaps $\mathsf{H}_1, \mathsf{H}_2$ (which satisfy W) to conclude that either

$$\langle \mathsf{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+)))\rangle$$

reduces to fail Conv, in which case the entire term will take another step to fail Conv, or it will reduce to some irreducible configuration $\langle \mathsf{H}_1^*, \mathsf{e}_1^* \rangle$, at which point the other side will reduce to another intermediate configuration $\langle \mathsf{H}_2^*, \mathsf{e}_1^\dagger \rangle$, and both will be in $\mathcal{V}\llbracket \tau_1 + \tau_2 \rrbracket_\rho$ for some future world W_1 where $W \sqsubseteq W_1$ and $\mathsf{H}_1^*, \mathsf{H}_2^* : W_1$.

Given $(W_1, \mathsf{e}_1^*, \mathsf{e}_1^\dagger) \in \mathcal{V}\llbracket \tau_1 + \tau_2 \rrbracket_\rho$, there must exist $\mathsf{v}_1^*, \mathsf{v}_1^\dagger$ such that either $e_1^* = \mathsf{inl}\ \mathsf{v}_1^*$, $e_1^\dagger = \mathsf{inl}\ \mathsf{v}_1^\dagger$, and $(W_1, \mathsf{v}_1^*, \mathsf{v}_1^\dagger) \in \mathcal{V}\llbracket \tau_1 \rrbracket_\rho$ or $e_1^* = \mathsf{inr}\ \mathsf{v}_1^*$, $e_1^\dagger = \mathsf{inr}\ \mathsf{v}_1^\dagger$, and $(W_1, \mathsf{v}_1^*, \mathsf{v}_1^\dagger) \in \mathcal{V}\llbracket \tau_2 \rrbracket_\rho$.

First, consider the case where $\mathsf{e}_1^* = \mathsf{inl}\ \mathsf{v}_1^*$ and $\mathsf{e}_1^\dagger = \mathsf{inl}\ \mathsf{v}_1^\dagger$. Then, by the operational semantic, the configuration with H_1 and the original match expression must step to

$$\langle \mathsf{H}_1^*, [\mathsf{x} \to \mathsf{v}_1^*]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathsf{e}_1{}^+))) \rangle$$

and, on the other side, the configuration with H_2 must step to

$$\langle \mathsf{H}_2^*, [\mathsf{x} \to \mathsf{v}_1^\dagger]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathsf{e}_1{}^+))) \rangle$$

Next, notice that $(W_1, \gamma_2[x \to (\mathsf{v}_1^*, \mathsf{v}_1^\dagger)]) \in \mathcal{G}\llbracket \Gamma[\mathsf{x} : \tau_1] \rrbracket_\rho$ because $(W_1, \gamma_2) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho$ (by $W \sqsubseteq W_1$ and Lemma 2.3) and $(W_1, \mathsf{v}_1^*, \mathsf{v}_1^\dagger) \in \mathcal{V}\llbracket \tau_1 \rrbracket_\rho$. Therefore, we can instantiate the second induction hypothesis with $W_1, \gamma_\Gamma, \gamma_\Gamma, \gamma_2[x \to (\mathsf{v}_1^*, \mathsf{v}_1^\dagger)], \rho$, because $W \sqsubseteq W_1$ and $\mathcal{G}\llbracket \Gamma \rrbracket_\rho, \mathcal{G}\llbracket \Gamma \rrbracket_\cdot, \mathcal{G}\llbracket \Omega \rrbracket_\cdot$ are closed under world extension by Lemma 2.3. We then find that:

$$(W_1, [\mathsf{x} \to \mathsf{v}_1^*]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathsf{e}_1{}^+))), [\mathsf{x} \to \mathsf{v}_1^\dagger]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathsf{e}_1{}^+)))) \in \mathcal{E}\llbracket \tau \rrbracket_\rho$$

Ergo, since $\mathsf{H}_1^* : W_1$, the configuration above with H_1^* must either step to fail Conv, in which case the whole expression steps to fail Conv, or it must step to $\langle \mathsf{H}_1^\dagger, \mathsf{e}_1^{**} \rangle$ for some $\mathsf{H}_1^\dagger : W_2$ where $W_1 \sqsubseteq W_2$. Moreover, on the other side, the configuration above with H_2^* must step to $\langle \mathsf{H}_2^\dagger, \mathsf{e}_1^{\dagger\dagger} \rangle$ for some $\mathsf{H}_2^\dagger : W_2$, with $(W_2, \mathsf{e}_1^{**}, \mathsf{e}_1^{\dagger\dagger}) \in \mathcal{V}\llbracket \tau \rrbracket_\rho$. Then, since $W \sqsubseteq W_1$ and $W_1 \sqsubseteq W_2$, we have $W \sqsubseteq W_2$ (by Lemma 2.4), which suffices to finish the proof for this case.

Now, consider the case where $\mathsf{e}_1^* = \mathsf{inr}\ \mathsf{v}_1^*$ and $\mathsf{e}_1^\dagger = \mathsf{inr}\ \mathsf{v}_1^\dagger$. Then, by the operational semantics, the configuration with H_1 and the original match expression must step to

$$\langle \mathsf{H}_1^*, [\mathsf{y} \to \mathsf{v}_1^*]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathsf{e}_2{}^+))) \rangle$$

and, on the other side, the configuration with H_2 must step to

$$\langle \mathsf{H}_2^*, [\mathsf{y} \to \mathsf{v}_1^\dagger]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathsf{e}_2{}^+))) \rangle$$

The rest of the proof for this case is trivially similar to the proof for the first case, where x, x, τ_1, e_1 is replaced with y, y, τ_2, e_2, respectively. □

Lemma 2.25 (Compat ⟶).

$$\Gamma; \Omega; \Delta; \Gamma[\mathsf{x} : \tau_1] \vdash \mathsf{e} \preceq \mathsf{e} : \tau_2 \rightsquigarrow \Gamma'; \Omega' \implies \Gamma; \Omega; \Delta; \Gamma \vdash \lambda\mathsf{x} : \tau_1.\mathsf{e} \preceq \lambda\mathsf{x} : \tau_1.\mathsf{e} : \tau_1 \to \tau_2 \rightsquigarrow \Gamma'; \Omega'$$

Proof. Expanding the hypotheses, we find that $\Gamma = \Gamma'$ and there exists Ω_e such that $\Omega = \Omega_\mathsf{e} \uplus \Omega'$ where $\Gamma; \Omega_\mathsf{e}; \Delta; \Gamma[\mathsf{x} : \tau_1] \vdash \mathsf{e} \preceq \mathsf{e} : \tau_2$. Moreover, $\Gamma; \Omega; \Delta; \Gamma \vdash \lambda\mathsf{x} : \tau_1.\mathsf{e} : \tau_1 \to \tau_2 \rightsquigarrow \Gamma'; \Omega'$ by the λ typing rule. It thus suffices to show that $\Gamma; \Omega_\mathsf{e}; \Delta; \Gamma \vdash \lambda\mathsf{x} : \tau_1.\mathsf{e} \preceq \lambda\mathsf{x} : \tau_1.\mathsf{e} : \tau_1 \to \tau_2$.

Expanding the conclusion, we must show that given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}\llbracket \Delta \rrbracket \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\cdot \wedge (W, \gamma_\Omega) \in \mathcal{G}\llbracket \Omega_\mathsf{e} \rrbracket_\cdot$$

then

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \lambda\mathsf{x} : \tau_1.\mathsf{e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \lambda\mathsf{x} : \tau_1.\mathsf{e}^+)))) \in \mathcal{E}\llbracket \tau_1 \to \tau_2 \rrbracket_\rho$$

Notice that both of the expressions have no free variables by Lemma 2.9.

We can push the compiler and substitutions through the lambda to refine that to:

$$(W, \lambda x.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, e^+))), \lambda x.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, e^+)))) \in \mathcal{E}\llbracket \tau_1 \rightarrow \tau_2 \rrbracket_\rho$$

Expanding the expression relation definition, we find that given

$$\forall H_1, H_2{:}W,\ e_1',\ H_1',\ j < W.k.$$
$$\langle H_1, \lambda x.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, e^+)))\rangle \xrightarrow{j} \langle H_1', e_1'\rangle \nrightarrow$$

we must show either $e_1' = \mathrm{fail}\ \textsc{Conv}$ or there exist v_2, H_2', W' such that:

$$\langle H_2, \lambda x.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, e^+)))\rangle \xrightarrow{*} \langle H_2', v_2\rangle$$
$$\wedge W \sqsubseteq W' \wedge H_1', H_2' : W' \wedge (W', e_1', v_2) \in \mathcal{V}\llbracket \tau_1 \rightarrow \tau_2 \rrbracket_\rho$$

Clearly, $\langle H_1, \lambda x.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, e^+)))\rangle \nrightarrow$ because this expression is a target value. Therefore, $e_1' = \lambda x.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, e^+)))$. Moreover, we trivially have

$$\langle H_2, \lambda x.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, e^+)))\rangle \xrightarrow{0} \langle H_2, \lambda x.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, e^+)))\rangle$$

and $H_1, H_2 : W$ and trivially, $W \sqsubseteq W$. Therefore, it suffices to prove that

$$(W, \lambda x.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, e^+))), \lambda x.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, e^+)))) \in \mathcal{V}\llbracket \tau_1 \rightarrow \tau_2 \rrbracket_\rho$$

Consider arbitrary v_1, v_2, W' where $W \sqsubset W'$ and $(W', v_1, v_2) \in \mathcal{V}\llbracket \tau_1 \rrbracket_\rho$. Then, we must show

$$(W', [x \rightarrow v_1]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, e^+))),$$
$$[x \rightarrow v_2]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, e^+)))) \in \mathcal{E}\llbracket \tau_2 \rrbracket_\rho$$

Notice that $\gamma_\Gamma[x \rightarrow (v_1, v_2)] \in \mathcal{G}\llbracket \Gamma[x : \tau_1] \rrbracket_\rho$ because $(W', \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho$ (by $W \sqsubseteq W'$ and Lemma 2.3) and $(W', v_1, v_2) \in \mathcal{V}\llbracket \tau_1 \rrbracket_\rho$. Then, we can instantiate the first induction hypothesis with $W', \gamma_\Gamma[x \rightarrow (v_1, v_2)], \gamma_\Gamma, \gamma_\Omega, \rho$ because $W \sqsubseteq W'$ and $\mathcal{G}\llbracket \Gamma \rrbracket_\rho, \mathcal{G}\llbracket \Gamma \rrbracket_\cdot, \mathcal{G}\llbracket \Omega \rrbracket_\cdot$ are closed under world extension by Lemma 2.3. Therefore,

$$(W', \mathrm{close}_1(\gamma_\Gamma[x \rightarrow (v_1, v_2)], \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, e^+))),$$
$$\mathrm{close}_2(\gamma_\Gamma[x \rightarrow (v_1, v_2)], \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, e^+)))) \in \mathcal{E}\llbracket \tau_2 \rrbracket_\rho$$

We can simplify the above statement by bringing $x \rightarrow v_1$ out of the close_1 on the left side and bringing $x \rightarrow v_2$ out of the close_2 on the right side. This suffices to finish the proof. □

Lemma 2.26 (Compat app).

$$\Gamma_1; \Omega_1; \Delta; \Gamma \vdash e_1 \preceq e_1 : \tau_1 \rightarrow \tau_2 \rightsquigarrow \Gamma_2; \Omega_2 \wedge \Gamma_2; \Omega_2; \Delta; \Gamma \vdash e_2 \preceq e_2 : \tau_1 \rightsquigarrow \Gamma_3; \Omega_3 \implies$$
$$\Gamma_1; \Omega_1; \Delta; \Gamma \vdash e_1\ e_2 \preceq e_1\ e_2 : \tau_2 \rightsquigarrow \Gamma_3; \Omega_3$$

Proof. Expanding the hypotheses, we find that $\Gamma_1 = \Gamma_2 = \Gamma_3$ and there exist Ω_e, Ω_e' such that $\Omega_1 = \Omega_e \uplus \Omega_2$ where $\Gamma_1; \Omega_e; \Delta; \Gamma \vdash e_1 \preceq e_1 : \tau_1 \rightarrow \tau_2$ and $\Omega_2 = \Omega_e' \uplus \Omega_3$ where $\Gamma_2; \Omega_e'; \Delta; \Gamma \vdash e_2 \preceq e_2 : \tau_1$. Therefore, $\Omega_1 = (\Omega_e \uplus \Omega_e') \uplus \Omega_3$. Moreover, $\Gamma_1; \Omega_1; \Delta; \Gamma \vdash e_1\ e_2 \preceq e_1\ e_2 : \tau_2 \rightsquigarrow \Gamma_3; \Omega_3$ by the application typing rule. It thus suffices to show that $\Gamma_1; \Omega_e \uplus \Omega_e'; \Delta; \Gamma \vdash e_1\ e_2 \preceq e_1\ e_2 : \tau_2$.

Expanding the conclusion, we must show that given

$$\forall W.\forall \rho\ \gamma_\Gamma\ \gamma_\Gamma\ \gamma_\Omega.\rho \in \mathcal{D}\llbracket \Delta \rrbracket \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\cdot \wedge (W, \gamma_\Omega) \in \mathcal{G}\llbracket \Omega_e \uplus \Omega_e' \rrbracket_\cdot$$

then

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, e_1\ {e_2}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, e_1\ {e_2}^+)))) \in \mathcal{E}\llbracket \tau_2 \rrbracket_\rho$$

Notice that both of the expressions have no free variables by Lemma 2.9.

We can push the compiler and substitutions through to refine that to:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^{+}))) \ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^{+}))), \\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1{}^{+}))) \ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^{+})))) \in \mathcal{E}\llbracket \tau_2 \rrbracket_\rho$$

Expanding the expression relation definition, we find that:

$$\forall \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.$$

$$\langle \mathrm{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^{+}))) \ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^{+})))\rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1'\rangle \not\rightarrow$$

we must show either $\mathrm{e}_1' = \mathrm{fail}\ \textsc{Conv}$ or there exist $\mathrm{v}_2, \mathrm{H}_2', W'$ such that:

$$\langle \mathrm{H}_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1{}^{+}))) \ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^{+})))\rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{v}_2\rangle \\ \wedge W \sqsubseteq W' \wedge \mathrm{H}_1', \mathrm{H}_2' : W' \wedge (W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}\llbracket \tau_2 \rrbracket_\rho$$

In order to proceed, first notice that, by Lemma 2.2, $\gamma_\Omega = \gamma_1 \uplus \gamma_2$ where

$$(W, \gamma_1) \in \mathcal{G}\llbracket \Omega_{\mathrm{e}} \rrbracket.$$

and

$$(W, \gamma_2) \in \mathcal{G}\llbracket \Omega_{\mathrm{e}}' \rrbracket.$$

and, for any $i \in \{1, 2\}$

$$\mathrm{close}_i(\gamma_\Omega, \mathrm{e}_1) = \mathrm{close}_i(\gamma_1, \mathrm{e}_1)$$

and

$$\mathrm{close}_i(\gamma_\Omega, \mathrm{e}_2) = \mathrm{close}_i(\gamma_2, \mathrm{e}_2)$$

Next, we need to know what e_1' is. From the operational semantics, the application will run the first subexpression using the heap H_1 until it reaches a target value or gets stuck. By appealing to our first induction hypothesis, instantiated with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_1, \rho$, we get that:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e}_1{}^{+}))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathrm{e}_1{}^{+})))) \in \mathcal{E}\llbracket \tau_1 \longrightarrow \tau_2 \rrbracket_\rho$$

We can instantiate this fact with H_1 and H_2, both of which satisfy W, to find that

$$\langle \mathrm{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e}_1{}^{+})))\rangle$$

either reduces to fail Conv, in which case the whole expression steps to fail Conv, or to some irreducible configuration $\langle \mathrm{H}_1^*, \mathrm{e}_1^*\rangle$, in which case on the other side, the configuration reduces to some irreducible configuration $\langle \mathrm{H}_2^*, \mathrm{e}_1^\dagger\rangle$, and there exists some W_1 such that $W \sqsubseteq W_1$, $\mathrm{H}_1^*, \mathrm{H}_2^* : W_1$, and $(W_1, e_1^*, e_1^\dagger) \in \mathcal{V}\llbracket \tau_1 \longrightarrow \tau_2 \rrbracket_\rho$.

Since terms in the value relation are target values, the original application will continue reducing on the second subexpression according to the operational semantics. Then, we can appeal to the second induction hypothesis instantiated with $W_1, \gamma_\Gamma, \gamma_\Gamma, \gamma_2, \rho$, because $W \sqsubseteq W_1$ and $\mathcal{G}\llbracket \Gamma \rrbracket_\rho, \mathcal{G}\llbracket \Gamma \rrbracket_\cdot, \mathcal{G}\llbracket \Gamma \rrbracket_\cdot$ are closed under world extension by Lemma 2.3. Thus,

$$(W_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e}_2{}^{+}))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e}_2{}^{+})))) \in \mathcal{E}\llbracket \tau_1 \rrbracket_\rho$$

We can instantiate this fact with H_1^* and H_2^*, both of which satisfy W_1, to find that

$$\langle \mathrm{H}_1^*, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e}_2{}^{+})))\rangle$$

either reduces to fail Conv, in which case the whole expression steps to fail Conv, or to some irreducible configuration $\langle \mathrm{H}_1^{**}, \mathrm{e}_2^*\rangle$, in which case on the other side, the configuration reduces to some irreducible configuration $\langle \mathrm{H}_2^{**}, \mathrm{e}_2^\dagger\rangle$, and there exists some W_2 such that $W_1 \sqsubseteq W_2$, $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : W_2$, and $(W_2, \mathrm{e}_2^*, \mathrm{e}_2^\dagger) \in \mathcal{V}\llbracket \tau_1 \rrbracket_\rho$.

Then, instantiate $(W_1, \mathrm{e}_1^*, \mathrm{e}_1^\dagger) \in \mathcal{V}\llbracket\tau_1 \rightarrow \tau_2\rrbracket_\rho$ with $\mathrm{e}_2^*, \mathrm{e}_2^\dagger, \triangleright W_2$. Because $W_1 \sqsubseteq W_2$ and $W_2 \sqsubset \triangleright W_2$, it follows that $W_1 \sqsubset \triangleright W_2$. Moreover, $(\triangleright W_2, \mathrm{e}_2^*, \mathrm{e}_2^\dagger) \in \mathcal{V}\llbracket\tau_1\rrbracket_\rho$ (because $(W_2, \mathrm{e}_2^*, \mathrm{e}_2^\dagger) \in \mathcal{V}\llbracket\tau_1\rrbracket_\rho$ and $W_2 \sqsubseteq \triangleright W_2$), so we find that there exist $\mathrm{e}_\mathrm{b}^*, \mathrm{e}_\mathrm{b}^\dagger$ such that

$$e_1^* = \lambda \mathrm{x}.\mathrm{e}_\mathrm{b}^*$$

and

$$e_1^\dagger = \lambda \mathrm{x}.\mathrm{e}_\mathrm{b}^\dagger$$

and

$$(\triangleright W_2, [\mathrm{x} \mapsto \mathrm{e}_2^*]e_b^*), [\mathrm{x} \rightarrow \mathrm{e}_2^\dagger]e_b^\dagger)) \in \mathcal{E}\llbracket\tau_2\rrbracket_\rho$$

Now, by the operational semantics, the original configuration with heap H_1 steps to $\langle \mathrm{H}_1^{**}, \lambda x.\mathrm{e}_\mathrm{b}^*\ \mathrm{e}_2^* \rangle$ and, on the other side, the original configuration with H_2 steps to $\langle \mathrm{H}_2^{**}, \lambda x.\mathrm{e}_\mathrm{b}^\dagger\ \mathrm{e}_2^\dagger \rangle$. Both of these configurations step to $\langle \mathrm{H}_1^{**}, [\mathrm{x} \rightarrow \mathrm{e}_2^*]\mathrm{e}_\mathrm{b}^* \rangle$ and $\langle \mathrm{H}_2^{**}, [\mathrm{x} \rightarrow \mathrm{e}_2^\dagger]\mathrm{e}_\mathrm{b}^\dagger \rangle$, respectively. Then, since $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : W_2$, by Lemma 2.5, it follows that $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : \triangleright W_2$, so we can instantiate the above fact with $\mathrm{H}_1^{**}, \mathrm{H}_2^{**}$ to deduce that either the first configuration steps to fail Conv, in which case the original configuration with H_1 steps to fail Conv, or the first configuration steps to some irreducible configuration $\langle \mathrm{H}_1^f, \mathrm{e}_\mathrm{f}^* \rangle$, in which case the configuration on the other side steps to some irreducible configuration $\langle \mathrm{H}_2^f, \mathrm{e}_\mathrm{f}^\dagger \rangle$, and there exists some W_3 such that $\triangleright W_2 \sqsubseteq W_3$, $\mathrm{H}_1^f, \mathrm{H}_2^f : W_3$, and $(W_3, \mathrm{e}_\mathrm{f}^*, \mathrm{e}_\mathrm{f}^\dagger) \in \mathcal{V}\llbracket\tau_2\rrbracket_\rho$. This suffices to show that $\mathrm{e}_1' = \mathrm{e}_\mathrm{f}^*$ and that e_1' is in the value relation at τ_2 along with the value that is stepped to by the original configuration on the right hand side. Then, since $W \sqsubseteq W_1$, $W_1 \sqsubseteq W_2$, $W_2 \sqsubseteq \triangleright W_2$, $W_2 \sqsubseteq W_3$, we have $W \sqsubseteq W_3$, which suffices to finish the proof. □

Lemma 2.27 (Compat $\forall$).

$$\Gamma; \Omega; \Delta, \alpha; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \tau \rightsquigarrow \Gamma'; \Omega' \implies \Gamma; \Omega; \Delta; \Gamma \vdash \Lambda\alpha.e \preceq \Lambda\alpha.e : \forall\alpha.\tau \rightsquigarrow \Gamma'; \Omega'$$

Proof. Expanding the hypotheses, we find that $\Gamma = \Gamma'$ and there exists Ω_e such that $\Omega = \Omega_\mathrm{e} \uplus \Omega'$ where $\Gamma; \Omega_\mathrm{e}; \Delta, \alpha; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \tau$. Moreover, $\Gamma; \Omega; \Delta; \Gamma \vdash \Lambda\alpha.e : \forall\alpha.\tau \rightsquigarrow \Gamma'; \Omega'$ by the type abstraction typing rule. It thus suffices to show that $\Gamma; \Omega_\mathrm{e}; \Delta; \Gamma \vdash \Lambda\alpha.e \preceq \Lambda\alpha.e : \forall\alpha.\tau$.

Expanding the conclusion, we must show that given

$$\forall W. \forall\rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_. \wedge (W, \gamma_\Omega) \in \mathcal{G}\llbracket\Omega_\mathrm{e}\rrbracket_.$$

then

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \Lambda\alpha.\mathrm{e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \Lambda\alpha.\mathrm{e}^+)))) \in \mathcal{E}\llbracket\forall\alpha.\tau\rrbracket_\rho$$

Notice that both of the expressions have no free variables by Lemma 2.9.

We can push the compiler and substitutions through the pair to refine that to:

$$(W, \lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+))), \lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+)))) \in \mathcal{E}\llbracket\forall\alpha.\tau\rrbracket_\rho$$

Expanding the expression relation definition, we find that given

$$\forall \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.$$
$$\langle \mathrm{H}_1, \lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+))) \rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1' \rangle \nrightarrow$$

we must show either $\mathrm{e}_1' =$ fail Conv or there exist $\mathrm{v}_2, \mathrm{H}_2', W'$ such that:

$$\langle \mathrm{H}_2, \lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))) \rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{v}_2 \rangle$$
$$\wedge W \sqsubseteq W' \wedge \mathrm{H}_1', \mathrm{H}_2' : W' \wedge (W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}\llbracket\forall\alpha.\tau\rrbracket_\rho$$

Clearly, $\langle \mathrm{H}_1, \lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+))) \rangle \nrightarrow$ because this expression is a target value. Therefore, $\mathrm{e}_1' = \lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))$. Moreover, we trivially have

$$\langle \mathrm{H}_2, \lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))) \rangle \xrightarrow{0} \langle \mathrm{H}_2, \lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))) \rangle$$

and $\mathsf{H}_1, \mathsf{H}_2 : W$ and trivially, $W \sqsubseteq W$. Therefore, it suffices to prove that

$$(W, \lambda\_.\mathsf{close}_1(\gamma_\Gamma, \mathsf{close}_1(\gamma_\Gamma, \mathsf{close}_1(\gamma_\Omega, \mathsf{e}^+))), \lambda\_.\mathsf{close}_2(\gamma_\Gamma, \mathsf{close}_2(\gamma_\Gamma, \mathsf{close}_2(\gamma_\Omega, \mathsf{e}^+)))) \in \mathcal{V}[\![\forall\alpha.\tau]\!]_\rho$$

Consider some arbitrary $R \in \mathit{Typ}$ and W' such that $W \sqsubset W'$. We must prove that

$$(W', \mathsf{close}_1(\gamma_\Gamma, \mathsf{close}_1(\gamma_\Gamma, \mathsf{close}_1(\gamma_\Omega, \mathsf{e}^+))), \mathsf{close}_2(\gamma_\Gamma, \mathsf{close}_2(\gamma_\Gamma, \mathsf{close}_2(\gamma_\Omega, \mathsf{e}^+)))) \in \mathcal{E}[\![\tau]\!]_{\rho[\alpha\mapsto R]}$$

Since $R \in \mathit{Typ}$ and $\rho \in \mathcal{D}[\![\Delta]\!]$, it follows that $\rho[\alpha \mapsto R] \in \mathcal{D}[\![\Delta, \alpha]\!]$. Thus, we can instantiate the first induction hypothesis with $W', \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho[\alpha \mapsto R]$, because $W \sqsubseteq W'$ and $\mathcal{G}[\![\Gamma]\!]_\rho, \mathcal{G}[\![\Gamma]\!]_{\cdot}, \mathcal{G}[\![\Omega]\!]_{\cdot}$ is closed under world extension by Lemma 2.3. This suffices to prove the above fact. □

Lemma 2.28 (Compat $[\tau/\alpha]$).

$$\Delta \vdash \tau' \land \Gamma;\Omega;\Delta;\Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \forall\alpha.\tau \rightsquigarrow \Gamma';\Omega' \implies \Gamma;\Omega;\Delta;\Gamma \vdash \mathsf{e}[\tau'] \preceq \mathsf{e}[\tau'] : \tau[\tau'/\alpha] \rightsquigarrow \Gamma';\Omega'$$

Proof. Expanding the hypotheses, we find that $\Gamma = \Gamma'$ and there exists Ω_e such that $\Omega = \Omega_\mathsf{e} \uplus \Omega'$ where $\Gamma;\Omega_\mathsf{e};\Delta;\Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau$. Moreover, $\Gamma;\Omega;\Delta;\Gamma \vdash \mathsf{e}[\tau'] : \tau[\tau'/\alpha] \rightsquigarrow \Gamma';\Omega'$ by the type application typing rule. It thus suffices to show that $\Gamma;\Omega_\mathsf{e};\Delta;\Gamma \vdash \mathsf{e}[\tau'] \preceq \mathsf{e}[\tau'] : \tau[\tau'/\alpha]$.

Expanding the conclusion, we must show that given

$$\forall W.\forall\rho\,\gamma_\Gamma\,\gamma_\Gamma\,\gamma_\Omega.\rho \in \mathcal{D}[\![\Delta]\!] \land (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \land (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_{\cdot} \land (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega_\mathsf{e}]\!]_{\cdot}$$

then

$$(W, \mathsf{close}_1(\gamma_\Gamma, \mathsf{close}_1(\gamma_\Gamma, \mathsf{close}_1(\gamma_\Omega, \mathsf{e}[\tau']^+))), \mathsf{close}_2(\gamma_\Gamma, \mathsf{close}_2(\gamma_\Gamma, \mathsf{close}_2(\gamma_\Omega, \mathsf{e}[\tau']^+)))) \in \mathcal{E}[\![\tau[\tau'/\alpha]]\!]_\rho$$

Notice that both of the expressions have no free variables by Lemma 2.9.

We can push the compiler and substitutions through the type application to refine this to:

$$(W, \mathsf{close}_1(\gamma_\Gamma, \mathsf{close}_1(\gamma_\Gamma, \mathsf{close}_1(\gamma_\Omega, \mathsf{e}^+)))\ (), \mathsf{close}_2(\gamma_\Gamma, \mathsf{close}_2(\gamma_\Gamma, \mathsf{close}_2(\gamma_\Omega, \mathsf{e}^+)))\ ()) \in \mathcal{E}[\![\tau[\tau'/\alpha]]\!]_\rho$$

Expanding the expression relation definition, we find that given

$$\forall \mathsf{H}_1, \mathsf{H}_2{:}W,\ \mathsf{e}_1',\ \mathsf{H}_1',\ j < W.k.$$
$$\langle \mathsf{H}_1, \mathsf{close}_1(\gamma_\Gamma, \mathsf{close}_1(\gamma_\Gamma, \mathsf{close}_1(\gamma_\Omega, \mathsf{e}^+)))\ ()\rangle \xrightarrow{j} \langle \mathsf{H}_1', \mathsf{e}_1'\rangle \not\rightarrow$$

we must show either $\mathsf{e}_1' = \mathsf{fail}\ \textsc{Conv}$ or there exist $\mathsf{v}_2, \mathsf{H}_2', W'$ such that:

$$\langle \mathsf{H}_2, \mathsf{close}_2(\gamma_\Gamma, \mathsf{close}_2(\gamma_\Gamma, \mathsf{close}_2(\gamma_\Omega, \mathsf{e}^+)))\ ()\rangle \xrightarrow{*} \langle \mathsf{H}_2', \mathsf{v}_2\rangle$$
$$\land W \sqsubseteq W' \land \mathsf{H}_1', \mathsf{H}_2' : W' \land (W', \mathsf{e}_1', \mathsf{v}_2) \in \mathcal{V}[\![\tau[\tau'/\alpha]]\!]_\rho$$

To proceed, we must find what e_1' is. From the operational semantic, we know the application will run its subexpression using H_1 until it reaches a target value or gets stuck. From the induction hypothesis instantiated with W, γ_Γ, γ_Γ, γ_Ω, ρ, we find that:

$$(W, \mathsf{close}_1(\gamma_\Gamma, \mathsf{close}_1(\gamma_\Gamma, \mathsf{close}_1(\gamma_\Omega, \mathsf{e}^+))), \mathsf{close}_2(\gamma_\Gamma, \mathsf{close}_2(\gamma_\Gamma, \mathsf{close}_2(\gamma_\Omega, \mathsf{e}^+)))) \in \mathcal{E}[\![\forall\alpha.\tau]\!]_\rho$$

By instantiating this fact with $\mathsf{H}_1, \mathsf{H}_2$, we find that $\langle \mathsf{H}_1, \mathsf{close}_1(\gamma_\Gamma, \mathsf{close}_1(\gamma_\Gamma, \mathsf{close}_1(\gamma_\Omega, \mathsf{e}^+)))\rangle$ either reduces to fail Conv, in which case the entire term reduced to fail Conv, or it will reduce to some $\langle \mathsf{H}_1^*, \mathsf{e}_1{}^*\rangle$, in which case the other side with H_2 will reduce to some $\langle \mathsf{H}_2^*, \mathsf{e}_1{}^\dagger\rangle$ and

$$(W_1, \mathsf{e}_1{}^*, \mathsf{e}_1{}^\dagger) \in \mathcal{V}[\![\forall\alpha.\tau]\!]_\rho$$

for some world W_1 where $W \sqsubseteq W_1$ and $\mathsf{H}_1^*, \mathsf{H}_2^* : W_1$.

Then, we can instantiate this fact with $\mathcal{V}[\![\tau']\!]_\rho$ and $\triangleright W_1$. (Note that $\mathcal{V}[\![\tau']\!]_\rho \in \mathit{Typ}$ by Lemma 2.6.) Since $W \sqsubset \triangleright W_1$ (as $W \sqsubseteq W_1$ and $W_1 \sqsubset \triangleright W_1$), we find that there exist $\mathsf{e}_\mathsf{b}^*, \mathsf{e}_\mathsf{b}^\dagger$ such that

$$\mathsf{e}_1^* = \lambda\_.\mathsf{e}_\mathsf{b}^*$$
$$\mathsf{e}_1^\dagger = \lambda\_.\mathsf{e}_\mathsf{b}^\dagger$$

and

$$(\triangleright W_1, e^*_b, e^\dagger_b) \in \mathcal{E}[\![\tau]\!]_{\rho[\alpha \to \mathcal{V}[\![\tau']\!]_\rho]}$$

Ergo, by the operational semantic, the original configuration with heap H_1 steps to $\langle \mathsf{H}^*_1, \lambda\_.\mathsf{e}^*_\mathsf{b}\ ()\rangle$ and, on the other side, the configuration with H_2 steps to $\langle \mathsf{H}^*_2, \lambda\_.\mathsf{e}^\dagger_\mathsf{b}\ ()\rangle$. Next, both of these configurations take a step to $\langle \mathsf{H}^*_1, \mathsf{e}^*_\mathsf{b}\rangle$ and $\langle \mathsf{H}^*_2, \mathsf{e}^\dagger_\mathsf{b}\rangle$, respectively. (Notice that () is not substituted anywhere because the binding in the lambda values are unused.) Next, since $\mathsf{H}^*_1, \mathsf{H}^*_2 : W_1$, by Lemma 2.5, it follows that $\mathsf{H}^*_1, \mathsf{H}^*_2 : \triangleright W_1$, so we can instantiate the above fact with $\mathsf{H}^*_1, \mathsf{H}^*_2$ to deduce that either the first configuration steps to $\mathsf{fail}\ \textsc{Conv}$, in which case the original configuration with H_1 steps to $\mathsf{fail}\ \textsc{Conv}$, or the first configuration steps to some irreducible configuration $\langle \mathsf{H}^{**}_1, \mathsf{e}^*_\mathsf{f}\rangle$, in which case the second configuration also steps to some irreducible configuration $\langle \mathsf{H}^{**}_2, \mathsf{e}^\dagger_\mathsf{f}\rangle$, and there exists some W_2 where $\triangleright W_1 \sqsubseteq W_2$, $\mathsf{H}^{**}_1, \mathsf{H}^{**}_2 : W_2$, and $(W_2, \mathsf{e}^*_\mathsf{f}, \mathsf{e}^\dagger_\mathsf{f}) \in \mathcal{V}[\![\tau]\!]_{\rho[\alpha \to \mathcal{V}[\![\tau']\!]_\rho]}$. Therefore, by Lemma 2.7, $(W_2, \mathsf{e}^*_\mathsf{f}, \mathsf{e}^\dagger_\mathsf{f}) \in \mathcal{V}[\![\tau[\tau'/\alpha]]\!]_\rho$. Ergo, $\mathsf{e}'_1 = \mathsf{e}^\dagger_\mathsf{f}$, so this suffices to show e'_1 is in the value relation at $\tau[\tau'/\alpha]$ along with the value stepped to by the configuration with H_2 on the other side. Finally, since $W \sqsubseteq W_1$, $W_1 \sqsubseteq \triangleright W_1$, and $\triangleright W_1 \sqsubseteq W_2$, we have $W \sqsubseteq W_2$ (by Lemma 2.4), which suffices to finish the proof. □

Lemma 2.29 (Compat ref).

$$\Gamma; \Omega; \Delta; \Gamma \vdash \mathtt{e} \preceq \mathtt{e} : \tau \rightsquigarrow \Gamma'; \Omega' \implies \Gamma; \Omega; \Delta; \Gamma \vdash \mathtt{ref\ e} \preceq \mathtt{ref\ e} : \mathtt{ref}\ \tau \rightsquigarrow \Gamma'; \Omega'$$

Proof. Expanding the hypotheses, we find that $\Gamma = \Gamma'$ and there exists Ω_e such that $\Omega = \Omega_\mathsf{e} \uplus \Omega'$ where $\Gamma; \Omega_\mathsf{e}; \Delta; \Gamma \vdash \mathtt{e} \preceq \mathtt{e} : \tau$. Moreover, $\Gamma; \Omega; \Delta; \Gamma \vdash \mathtt{ref\ e} : \mathtt{ref}\ \tau \rightsquigarrow \Gamma'; \Omega'$ by the ref typing rule. It thus suffices to show that $\Gamma; \Omega_\mathsf{e}; \Delta; \Gamma \vdash \mathtt{ref\ e} \preceq \mathtt{ref\ e} : \mathtt{ref}\ \tau$.

Expanding the conclusion, we must show that given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_. \wedge (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega_\mathsf{e}]\!]_.$$

then

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathtt{ref\ e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathtt{ref\ e}^+)))) \in \mathcal{E}[\![\mathtt{ref}\ \tau]\!]_\rho$$

Notice that both of the expressions have no free variables by Lemma 2.9.

We can push the compiler and substitutions through the type application to refine this to:

$$(W, \mathsf{ref}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+))), \mathsf{ref}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))) \in \mathcal{E}[\![\mathtt{ref}\ \tau]\!]_\rho$$

Expanding the expression relation definition, we find that given

$$\forall \mathsf{H}_1, \mathsf{H}_2{:}W,\ \mathsf{e}'_1,\ \mathsf{H}'_1,\ j < W.k.$$
$$\langle \mathsf{H}_1, \mathsf{ref}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+)))\rangle \xrightarrow{j} \langle \mathsf{H}'_1, \mathsf{e}'_1\rangle \not\rightarrow$$

we must show either $\mathsf{e}'_1 = \mathsf{fail}\ \textsc{Conv}$ or there exist $\mathsf{v}_2, \mathsf{H}'_2, W'$ such that:

$$\langle \mathsf{H}_2, \mathsf{ref}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))\rangle \xrightarrow{*} \langle \mathsf{H}'_2, \mathsf{v}_2\rangle$$
$$\wedge W \sqsubseteq W' \wedge \mathsf{H}'_1, \mathsf{H}'_2 : W' \wedge (W', \mathsf{e}'_1, \mathsf{v}_2) \in \mathcal{V}[\![\mathtt{ref}\ \tau]\!]_\rho$$

To proceed, we must find what e'_1 is. From the operational semantic, we know ref will run its argument using H_1 until it reaches a target value or gets stuck. From the induction hypothesis instantiated with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$, we find that:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))) \in \mathcal{E}[\![\tau]\!]_\rho$$

By instantiating this fact with $\mathsf{H}_1, \mathsf{H}_2$, we find that $\langle \mathsf{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+)))\rangle$ either reduces to $\mathsf{fail}\ \textsc{Conv}$, in which case the entire term reduced to $\mathsf{fail}\ \textsc{Conv}$, or it will reduce to some $\langle \mathsf{H}^*_1, {\mathsf{e}_1}^*\rangle$, in which case the other side with H_2 will reduce to some $\langle \mathsf{H}^*_2, {\mathsf{e}_1}^\dagger\rangle$ and $(W_1, {\mathsf{e}_1}^*, \mathsf{e}^\dagger_1) \in \mathcal{V}[\![\tau]\!]_\rho$ for some world W_1 where $W \sqsubseteq W_1$ and $\mathsf{H}^*_1, \mathsf{H}^*_2 : W_1$.

By the operational semantic, it follows that the original configuration with H_1 steps to $\langle \mathsf{H}_1^*, \mathsf{ref}\ \mathsf{e}_1^* \rangle$ and, on the other side, the configuration with H_2 steps to $\langle \mathsf{H}_2^*, \mathsf{ref}\ \mathsf{e}_1^\dagger \rangle$. Ergo, since $\mathsf{e}_1^*, \mathsf{e}_1^\dagger$ are target values, the first configuration steps to $\langle \mathsf{H}_1^*[\ell_1 \rightarrow \mathsf{e}_1^*], \ell_1 \rangle$ for some $\ell_1 \notin \mathsf{H}_1^*$ and the second configuration steps to $\langle \mathsf{H}_2^*[\ell_2 \rightarrow \mathsf{e}_1^\dagger], \ell_2 \rangle$ for some $\ell_2 \notin \mathsf{H}_2^*$. To finish the proof, we must find some world W_2 such that $W \sqsubseteq W_2$ and $\mathsf{H}_1^*[\ell_1 \rightarrow \mathsf{e}_1^*], \mathsf{H}_2^*[\ell_2 \rightarrow \mathsf{e}_1^\dagger] : W_2$ and $(W_2, \ell_1, \ell_2) \in \mathcal{V}\llbracket \texttt{ref}\ \tau \rrbracket_\rho$.

Note that, since $\mathsf{H}_1^*, \mathsf{H}_2^* : W_1$ and $\ell_1 \notin \mathsf{H}_1^*, \ell_2 \notin \mathsf{H}_2^*$, it must be that $\ell_1, \ell_2 \notin \mathrm{dom}(W_1.\Psi)$ and $\ell_1, \ell_2 \notin \mathrm{dom}(W_1.\Theta)$.

Then, let

$$W_2 = (W_1.k, \lfloor W_1.\Psi \rfloor_{W_1.k}[(\ell_1, \ell_2) \rightarrow \lfloor \mathcal{V}\llbracket \tau \rrbracket_\rho \rfloor_{W_1.k}], W_1.\Theta)$$

Notice that $W_2.k = W_1.k \leq W_1.k$. Also, for all $(\ell_1', \ell_2') \in \mathrm{dom}(W_1.\Psi)$, we have $W_2.\Psi(\ell_1', \ell_2') = \lfloor W_1.\Psi \rfloor_{W_1.k}(\ell_1', \ell_2') = \lfloor W_1.\Psi(\ell_1', \ell_2') \rfloor_{W_1.k}$. Finally, $W_2.\Theta = W_1.\Theta$, so all the affine flags in W_1 are clearly present and unchanged in W_2. Ergo, $W_1 \sqsubseteq W_2$.

Next, we would like to show $\mathsf{H}_1^*[\ell_1 \rightarrow \mathsf{e}_1^*], \mathsf{H}_2^*[\ell_2 \rightarrow \mathsf{e}_1^\dagger] : W_2$.

For any $(\ell_1', \ell_2') \rightarrow R \in W_2.\Psi$, there are two cases: **(1)** $(\ell_1', \ell_2') = (\ell_1, \ell_2)$, in which case $W_2.\Psi(\ell_1, \ell_2) = \lfloor \mathcal{V}\llbracket \tau \rrbracket_\rho \rfloor_{W_1.k}$. Then, since $(W_1, \mathsf{e}_1^*, \mathsf{e}_1^\dagger) \in \mathcal{V}\llbracket \tau \rrbracket_\rho$, it follows by Lemma 2.3 that $(W_2, \mathsf{e}_1^*, \mathsf{e}_1^\dagger) \in \mathcal{V}\llbracket \tau \rrbracket_\rho$ and thus $(\triangleright W_2, \mathsf{e}_1^*, \mathsf{e}_1^\dagger) \in \lfloor \mathcal{V}\llbracket \tau \rrbracket_\rho \rfloor_{W_2.k}$, or **(2)** $(\ell_1', \ell_2') \in \mathrm{dom}(W_1.\Psi)$, in which case $\mathsf{H}_1^*[\ell_1 \rightarrow \mathsf{e}_1^*](\ell_1') = \mathsf{H}_1^*(\ell_1')$ and $\mathsf{H}_2^*[\ell_2 \rightarrow \mathsf{e}_1^\dagger](\ell_2') = \mathsf{H}_2^*(\ell_2')$. Ergo, $(\triangleright W_1, \mathsf{H}_1^*(\ell_1'), \mathsf{H}_2^*(\ell_2')) \in W_1.\Psi(\ell_1', \ell_2')$ because $\mathsf{H}_1^*, \mathsf{H}_2^* : W_1$. Then, since $W_1 \sqsubseteq W_2$, it follows that $\triangleright W_1 \sqsubseteq \triangleright W_2$, so by Lemma 2.3, it holds that $(\triangleright W_2, \mathsf{H}_1^*(\ell_1'), \mathsf{H}_2^*(\ell_2')) \in \lfloor W_1.\Psi(\ell_1', \ell_2') \rfloor_{W_2.k} = W_2.\Psi(\ell_1', \ell_2')$.

Then, for any $(\ell_1', \ell_2') \mapsto b \in W_2.\Theta = W_1.\Theta$, we know that $\ell_1' \neq \ell_1$ and $\ell_2' \neq \ell_2$, so since $\mathsf{H}_1^*, \mathsf{H}_2^* : W_1$, we have

$$\mathsf{H}_1^*[\ell_1 \rightarrow \mathsf{e}_1^*](\ell_1') = \mathsf{H}_1^*(\ell_1') = W_1.\Theta(\ell_1', \ell_2') = W_2.\Theta(\ell_1', \ell_2')$$

and

$$\mathsf{H}_2^*[\ell_2 \rightarrow \mathsf{e}_1^\dagger](\ell_2') = \mathsf{H}_1^*(\ell_2') = W_1.\Theta(\ell_1', \ell_2') = W_2.\Theta(\ell_1', \ell_2')$$

This suffices to show that $\mathsf{H}_1^*[\ell_1 \rightarrow \mathsf{e}_1^*], \mathsf{H}_2^*[\ell_2 \rightarrow \mathsf{e}_1^\dagger] : W_2$. Then, since $W \sqsubseteq W_1$ and $W_1 \sqsubseteq W_2$, we have $W \sqsubseteq W_2$. Finally, we have

$$W_2.\Psi(\ell_1, \ell_2) = \lfloor \mathcal{V}\llbracket \tau \rrbracket_\rho \rfloor_{W_1.k} = \lfloor \mathcal{V}\llbracket \tau \rrbracket_\rho \rfloor_{W_2.k}$$

which suffices to show $(W_2, \ell_1, \ell_2) \in \mathcal{V}\llbracket \texttt{ref}\ \tau \rrbracket_\rho$. □

Lemma 2.30 (Compat !).

$$\Gamma; \Omega; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \texttt{ref}\ \tau \rightsquigarrow \Gamma'; \Omega' \implies \Gamma; \Omega; \Delta; \Gamma \vdash !\mathsf{e} \preceq !\mathsf{e} : \tau \rightsquigarrow \Gamma'; \Omega'$$

Proof. Expanding the hypotheses, we find that $\Gamma = \Gamma'$ and there exists Ω_e such that $\Omega = \Omega_\mathsf{e} \uplus \Omega'$ where $\Gamma; \Omega_\mathsf{e}; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \texttt{ref}\ \tau$. Moreover, $\Gamma; \Omega; \Delta; \Gamma \vdash !\mathsf{e} : \tau \rightsquigarrow \Gamma'; \Omega'$ by the ! typing rule. It thus suffices to show that $\Gamma; \Omega_\mathsf{e}; \Delta; \Gamma \vdash !\mathsf{e} \preceq !\mathsf{e} : \tau$.

Expanding the conclusion, we must show that given

$$\forall W. \forall \rho\ \gamma_\Gamma\ \gamma_\Gamma\ \gamma_\Omega. \rho \in \mathcal{D}\llbracket \Delta \rrbracket \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_. \wedge (W, \gamma_\Omega) \in \mathcal{G}\llbracket \Omega_\mathsf{e} \rrbracket_.$$

then

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, !\mathsf{e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, !\mathsf{e}^+)))) \in \mathcal{E}\llbracket \tau \rrbracket_\rho$$

Notice that both of the expressions have no free variables by Lemma 2.9.

We can push the compiler and substitutions through the dereference to refine this to:

$$(W, !\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+))), !\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))) \in \mathcal{E}\llbracket \tau \rrbracket_\rho$$

Expanding the expression relation definition, we find that given

$$\forall \mathsf{H}_1, \mathsf{H}_2{:}W,\ \mathsf{e}_1',\ \mathsf{H}_1',\ j < W.k.$$
$$\langle \mathsf{H}_1, !\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+)))\rangle \xrightarrow{j} \langle \mathsf{H}_1', \mathsf{e}_1'\rangle \nrightarrow$$

we must show either $\mathsf{e}_1' = \mathsf{fail}\ \textsc{Conv}$ or there exist $\mathsf{v}_2, \mathsf{H}_2', W'$ such that:

$$\langle \mathsf{H}_2, !\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))\rangle \xrightarrow{*} \langle \mathsf{H}_2', \mathsf{v}_2\rangle$$
$$\wedge W \sqsubseteq W' \wedge \mathsf{H}_1', \mathsf{H}_2' : W' \wedge (W', \mathsf{e}_1', \mathsf{v}_2) \in \mathcal{V}\llbracket \tau \rrbracket_\rho$$

To proceed, we must find what e_1' is. From the operational semantics, we know ! will run its argument using H_1 until it reaches a target value or gets stuck. From the induction hypothesis instantiated with W, γ_Γ, γ_Γ, γ_Ω, ρ, we find that:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))) \in \mathcal{E}\llbracket \mathtt{ref}\ \tau \rrbracket_\rho$$

By instantiating this fact with $\mathsf{H}_1, \mathsf{H}_2$, we find that $\langle \mathsf{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+)))\rangle$ either reduces to $\mathsf{fail}\ \textsc{Conv}$, in which case the entire term reduced to $\mathsf{fail}\ \textsc{Conv}$, or it will reduce to some $\langle \mathsf{H}_1^*, \mathsf{e}_1{}^*\rangle$, in which case the other side with H_2 will reduce to some $\langle \mathsf{H}_2^*, \mathsf{e}_1{}^\dagger\rangle$ and $(W_1, \mathsf{e}_1{}^*, \mathsf{e}_1^\dagger) \in \mathcal{V}\llbracket \mathtt{ref}\ \tau \rrbracket_\rho$ for some world W_1 where $W \sqsubseteq W_1$ and $\mathsf{H}_1^*, \mathsf{H}_2^* : W_1$.

By expanding the definition of the value relation, we then see that

$$W_1.\Psi(\ell_1, \ell_2) = \lfloor \mathcal{V}\llbracket \tau \rrbracket_\rho \rfloor_{W_1.k}$$

By the operational semantics, it follows that the original configuration with H_1 steps to $\langle \mathsf{H}_1^*, !\mathsf{e}_1^*\rangle$ and, on the other hand, the configuration with H_2 steps to $\langle \mathsf{H}_2^*, !\mathsf{e}_1^\dagger\rangle$. Since $\mathsf{H}_1^*, \mathsf{H}_2^* : W_1$, we have that $\ell_1 \in \mathrm{dom}(\mathsf{H}_1^*)$ and $\ell_2 \in \mathrm{dom}(\mathsf{H}_2^*)$. Ergo, by the operational semantics, the two configurations step to $\langle \mathsf{H}_1^*, \mathsf{H}_1^*(\ell_1)\rangle$ and $\langle \mathsf{H}_2^*, \mathsf{H}_2^*(\ell_2)\rangle$, respectively. Then, by the above fact, we have $(W_1, \mathsf{H}_1^*(\ell_1), \mathsf{H}_2^*(\ell_2)) \in \mathcal{V}\llbracket \tau \rrbracket_\rho$. Since $W \sqsubseteq W_1$, this suffices to finish the proof. □

Lemma 2.31 (Compat :=).

$$\Gamma_1; \Omega_1; \Delta; \Gamma \vdash \mathsf{e}_1 \preceq \mathsf{e}_1 : \mathtt{ref}\ \tau \rightsquigarrow \Gamma_2; \Omega_2 \wedge \Gamma_2; \Omega_2; \Delta; \Gamma \vdash \mathsf{e}_2 \preceq \mathsf{e}_2 : \tau \rightsquigarrow \Gamma_3; \Omega_3$$
$$\implies \Gamma_1; \Omega_1; \Delta; \Gamma \vdash \mathsf{e}_1 := \mathsf{e}_2 \preceq \mathsf{e}_1 := \mathsf{e}_2 : \mathtt{unit} \rightsquigarrow \Gamma_3; \Omega_3$$

Proof. Expanding the hypotheses, we find that $\Gamma_1 = \Gamma_2 = \Gamma_3$ and there exist Ω_e, Ω_e' such that $\Omega_1 = \Omega_e \uplus \Omega_2$ where $\Gamma_1; \Omega_e; \Delta; \Gamma \vdash \mathsf{e}_1 \preceq \mathsf{e}_1 : \mathtt{ref}\ \tau$ and $\Omega_2 = \Omega_e' \uplus \Omega_3$ where $\Gamma_2; \Omega_e'; \Delta; \Gamma \vdash \mathsf{e}_2 \preceq \mathsf{e}_2 : \tau$. Therefore, $\Omega_1 = (\Omega_e \uplus \Omega_e') \uplus \Omega_3$. Moreover, $\Gamma_1; \Omega_1; \Delta; \Gamma \vdash \mathsf{e}_1 := \mathsf{e}_2 : \mathtt{unit} \rightsquigarrow \Gamma_3; \Omega_3$ by the := typing rule. It thus suffices to show that $\Gamma_1; \Omega_e \uplus \Omega_e'; \Delta; \Gamma \vdash \mathsf{e}_1 := \mathsf{e}_2 \preceq \mathsf{e}_1 := \mathsf{e}_2 : \mathtt{unit}$.

Expanding the conclusion, we must show that given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}\llbracket \Delta \rrbracket \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_. \wedge (W, \gamma_\Omega) \in \mathcal{G}\llbracket \Omega_e \uplus \Omega_e' \rrbracket_.$$

then

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_1 := \mathsf{e}_2{}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}_1 := \mathsf{e}_2{}^+)))) \in \mathcal{E}\llbracket \mathtt{unit} \rrbracket_\rho$$

Notice that both of the expressions have no free variables by Lemma 2.9.

We can push the compiler and substitutions through the assignment to refine that to:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_1{}^+))) := \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_2{}^+))),$$
$$\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}_1{}^+))) := \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}_2{}^+)))) \in \mathcal{E}\llbracket \mathtt{unit} \rrbracket_\rho$$

We can expand the definition of the expression relation to get that given:

$$\forall \mathsf{H}_1, \mathsf{H}_2{:}W,\ \mathsf{e}_1',\ \mathsf{H}_1',\ j < W.k.$$
$$\langle \mathsf{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_1{}^+))) := \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_2{}^+)))\rangle \xrightarrow{j} \langle \mathsf{H}_1', \mathsf{e}_1'\rangle \nrightarrow$$

we need to show that either e_1' is $\mathsf{fail}\ \textsc{Conv}$, or there exists $\mathsf{v}_2, \mathsf{H}_2', W'$ such that:

$$\langle \mathrm{H}_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathtt{e}_1{}^+))) := \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathtt{e}_2{}^+)))\rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{v}_2\rangle$$
$$\wedge W \sqsubseteq W' \wedge \mathrm{H}_1', \mathrm{H}_2' : W' \wedge (W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![\mathtt{unit}]\!]_\rho$$

In order to proceed, first notice that, by Lemma 2.2, $\gamma_\Omega = \gamma_1 \uplus \gamma_2$ where

$$(W, \gamma_1) \in \mathcal{G}[\![\Omega_\mathrm{e}]\!].$$

and

$$(W, \gamma_2) \in \mathcal{G}[\![\Omega_\mathrm{e}']\!].$$

and, for any $i \in \{1, 2\}$

$$\mathrm{close}_i(\gamma_\Omega, \mathtt{e}_1) = \mathrm{close}_i(\gamma_1, \mathtt{e}_1)$$

and

$$\mathrm{close}_i(\gamma_\Omega, \mathtt{e}_2) = \mathrm{close}_i(\gamma_2, \mathtt{e}_2)$$

Next, we need to know what e_1' is. From the operational semantic, we know that := will first run its first component using the heap H_1 until it reaches a target value (or gets stuck). By appealing to our first induction hypothesis, instantiated it with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_1, \rho$, we get that:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathtt{e}_1{}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathtt{e}_1{}^+)))) \in \mathcal{E}[\![\mathtt{ref}\ \tau]\!]_\rho$$

And in particular, can then use this, choosing the heaps to be H_1 and H_2 (which satisfy W), to conclude that either $\langle \mathrm{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathtt{e}_1{}^+)))\rangle$ reduces to fail Conv (with any heap, as it doesn't matter), in which case the entire term will take another step to fail Conv, or it will reduce to some irreducible intermediate configuration $\langle \mathrm{H}_1^*, \mathrm{e}_1^*\rangle$, at which point the other side will reduce to a corresponding intermediate configuration $\langle \mathrm{H}_2^*, \mathrm{e}_1^\dagger\rangle$ and $(W_1, \mathrm{e}_1^*, \mathrm{e}_1^\dagger) \in \mathcal{V}[\![\tau]\!]_\rho$ for some world W_1 where $W \sqsubseteq W_1$ and $\mathrm{H}_1^*, \mathrm{H}_2^* : W_1$.

Then, since $\mathrm{e}_1^*, \mathrm{e}_1^\dagger$ are target values, the original := expression will continue reducing on the second subexpression. Then, we can appeal to the second induction hypothesis with $W_1, \gamma_\Gamma, \gamma_\Gamma, \gamma_2, \rho$, which we can do because $\mathcal{G}[\![\Gamma]\!]_\rho, \mathcal{G}[\![\Gamma_2]\!].,\mathcal{G}[\![\Omega_\mathrm{e}']\!].$ are closed under world extension by Lemma 2.3. Ergo,

$$(W_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathtt{e}_2{}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathtt{e}_2{}^+)))) \in \mathcal{E}[\![\tau]\!]_\rho$$

By instantiating this fact with $\mathrm{H}_1^*, \mathrm{H}_2^*$, we get that

$$\langle \mathrm{H}_1^*, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathtt{e}_2{}^+)))\rangle$$

either steps to fail Conv, in which case the original configuration with H_1 steps to fail Conv, or steps to an irreducible configuration $\langle \mathrm{H}_1', \mathrm{e}_2^*\rangle$, in which case the configuration on the other side steps to some irreducible configuration $\langle \mathrm{H}_2', \mathrm{e}_2^\dagger\rangle$ and there exists a world W_2 where $W_1 \sqsubseteq W_2$ and $(W_2, \mathrm{e}_2^*, \mathrm{e}_2^\dagger) \in \mathcal{V}[\![\tau]\!]_\rho$.

Thus, the original configuration with H_1 has run to $\langle \mathrm{H}_1', \mathrm{e}_1^* := \mathrm{e}_2^*\rangle$ and the original configuration with H_2 has run to $\langle \mathrm{H}_2', \mathrm{e}_1^\dagger := \mathrm{e}_2^\dagger\rangle$. Then, if we expand $(W_1, \mathrm{e}_1^*, \mathrm{e}_1^\dagger) \in \mathcal{V}[\![\mathtt{ref}\ \tau]\!]_\rho$, we find there exist locations ℓ_1, ℓ_2 such that $\mathrm{e}_1^* = \ell_1$, $\mathrm{e}_1^\dagger = \ell_2$, and

$$W_1.\Psi(\ell_1, \ell_2) = \lfloor \mathcal{V}[\![\tau]\!]_\rho \rfloor_{W_1.k}$$

Then, since $W_1 \sqsubseteq W_2$, it follows that

$$W_2.\Psi(\ell_1, \ell_2) = \lfloor \mathcal{V}[\![\tau]\!]_\rho \rfloor_{W_2.k}$$

Ergo, by the operational semantic, we find the configuration with H_1' steps to $\langle \mathrm{H}_1'[\ell_1 \to \mathrm{e}_2^*], ()\rangle$ and the configuration with H_2' steps to $\langle \mathrm{H}_2'[\ell_2 \to \mathrm{e}_2^\dagger], ()\rangle$. Since we have $(W_2, \mathrm{e}_2^*, \mathrm{e}_2^\dagger) \in \mathcal{V}[\![\tau]\!]_\rho$, it follows that

$$(\triangleright W_2, \mathrm{e}_2^*, \mathrm{e}_2^\dagger) \in \lfloor \mathcal{V}[\![\tau]\!]_\rho \rfloor_{W_2.k} = W_2.\Psi(\ell_1, \ell_2)$$

Thus, since $\mathrm{H}_1', \mathrm{H}_2' : W_2$ and the only location in the new heaps that has changed is ℓ_1, ℓ_2, and the values at those locations still satisfy the heap typing $W_2.\Psi$, we find that $\mathrm{H}_1'[\ell_1 \to \mathrm{e}_2^*], \mathrm{H}_2'[\ell_2 \to \mathrm{e}_2^\dagger] : W_2$. Moreover, we trivially have $(W_2, (), ()) \in \mathcal{V}[\![\mathtt{unit}]\!]_\rho$. Finally, since $W \sqsubseteq W_1$ and $W_1 \sqsubseteq W_2$, we have $W \sqsubseteq W_2$ (by Lemma 2.4), which suffices to finish the proof. □

Lemma 2.32 (Compat $\llparenthesis \mathrm{e} \rrparenthesis_\tau$).

$$\Omega = \Omega_\mathrm{e} \uplus \Omega' \wedge \Gamma = \Gamma' \wedge \Delta; \Gamma; \Gamma; \Omega_\mathrm{e} \vdash \mathrm{e} \preceq \mathrm{e} : \tau \rightsquigarrow \Delta; \Gamma \wedge \tau \sim \tau \implies \Gamma; \Omega; \Delta; \Gamma \vdash \llparenthesis \mathrm{e} \rrparenthesis_\tau \preceq \llparenthesis \mathrm{e} \rrparenthesis_\tau : \tau \wedge \_ : \tau \sim \tau \rightsquigarrow \Gamma'; \Omega'$$

Proof. We have $\Omega = \Omega_\mathrm{e} \uplus \Omega'$ and $\Gamma = \Gamma'$ by the first two assumptions. Moreover, $\Gamma; \Omega; \Delta; \Gamma \vdash \llparenthesis \mathrm{e} \rrparenthesis_\tau : \tau$ by the conversion typing rule. Ergo, to prove the conclusion, it suffices to show $\Gamma; \Omega_\mathrm{e}; \Delta; \Gamma \vdash \llparenthesis \mathrm{e} \rrparenthesis_\tau \preceq \llparenthesis \mathrm{e} \rrparenthesis_\tau : \tau$. Thus, we must show that given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_. \wedge (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega_\mathrm{e}]\!]_.$$

then

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \llparenthesis \mathrm{e} \rrparenthesis_\tau{}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \llparenthesis \mathrm{e} \rrparenthesis_\tau{}^+)))) \in \mathcal{E}[\![\tau]\!]_\rho$$

We can push the compiler and substitutions through to refine that to:

$$(W, C_{\tau \mapsto \tau}(\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))), C_{\tau \mapsto \tau}(\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))))) \in \mathcal{E}[\![\tau]\!]_\rho$$

Now, by instantiating our induction hypothesis with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$, we find that:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+)))) \in \mathcal{E}[\![\tau]\!]_.$$

Therefore, by Theorem 2.12, we have

$$(W, C_{\tau \mapsto \tau}(\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))), C_{\tau \mapsto \tau}(\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))))) \in \mathcal{E}[\![\tau]\!]_.$$

Finally, by Lemma 2.8, we have

$$(W, C_{\tau \mapsto \tau}(\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))), C_{\tau \mapsto \tau}(\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))))) \in \mathcal{E}[\![\tau]\!]_\rho$$

as was to be proven. □

Lemma 2.33 (Compat unit).

$$\Delta; \Gamma; \Gamma; \Omega \vdash () \preceq () : \mathrm{unit} \rightsquigarrow \Delta; \Gamma$$

Proof. Clearly, $\Delta = \Delta$ and $\Gamma = \Gamma$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash () : \mathrm{unit} \rightsquigarrow \Delta; \Gamma$ by the unit typing rule. Ergo, it suffices to show that $\Delta; \Gamma; \Gamma; \Omega \vdash () \preceq () : \mathrm{unit}$.

Expanding this definition, given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_. \wedge (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!]_.$$

we must show

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, ()^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, ()^+)))) \in \mathcal{E}[\![\mathrm{unit}]\!]_.$$

$()^+ = ()$ is a closed term, so the closings have no effect. Ergo,

$$\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, ()^+))) = \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, ()^+))) = ()$$

One can easily see $(W, (), ()) \in \mathcal{V}[\![\mathrm{unit}]\!]_.$, which suffices to show $(W, (), ()) \in \mathcal{E}[\![\mathrm{unit}]\!]_.$ by Lemma 2.1. This suffices to finish the proof. □

Lemma 2.34 (Compat true).

$$\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{true} \preceq \mathrm{true} : \mathrm{bool} \rightsquigarrow \Delta; \Gamma$$

Proof. Clearly, $\Delta = \Delta$ and $\Gamma = \Gamma$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash \mathsf{true} : \mathsf{bool} \rightsquigarrow \Delta; \Gamma$ by the true typing rule. Ergo, it suffices to show that $\Delta; \Gamma; \Gamma; \Omega \vdash \mathsf{true} \preceq \mathsf{true} : \mathsf{bool}$.

Expanding this definition, given

$$\forall W. \forall \rho\ \gamma_\Gamma\ \gamma_\Gamma\ \gamma_\Omega. \rho \in \mathcal{D}\llbracket \Delta \rrbracket \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_. \wedge (W, \gamma_\Omega) \in \mathcal{G}\llbracket \Omega \rrbracket_.$$

we must show

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{true}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{true}^+)))) \in \mathcal{E}\llbracket \mathsf{bool} \rrbracket_.$$

$\mathsf{true}^+ = 0$ is a closed term, so the closings have no effect. Ergo,

$$\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{true}^+))) = \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{true}^+))) = 0$$

One can easily see $(W, 0, 0) \in \mathcal{V}\llbracket \mathsf{bool} \rrbracket_.$, which suffices to show $(W, 0, 0) \in \mathcal{E}\llbracket \mathsf{bool} \rrbracket_.$ by Lemma 2.1. This suffices to finish the proof. □

Lemma 2.35 (Compat false).

$$\Delta; \Gamma; \Gamma; \Omega \vdash \mathsf{false} \preceq \mathsf{false} : \mathsf{bool} \rightsquigarrow \Delta; \Gamma$$

Proof. This is very similar to the proof for true, except $\mathsf{false}^+ = 1$, and since $1 \neq 0$, $(W, 1, 1) \in \mathcal{V}\llbracket \mathsf{bool} \rrbracket_.$ by the second clause. □

Lemma 2.36 (Compat int).

$$\Delta; \Gamma; \Gamma; \Omega \vdash \mathsf{n} \preceq \mathsf{n} : \mathsf{int} \rightsquigarrow \Delta; \Gamma$$

Proof. Clearly, $\Delta = \Delta$ and $\Gamma = \Gamma$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash \mathsf{n} : \mathsf{int} \rightsquigarrow \Delta; \Gamma$ by the int typing rule. Ergo, it suffices to show that $\Delta; \Gamma; \Gamma; \Omega \vdash \mathsf{n} \preceq \mathsf{n} : \mathsf{int}$.

Expanding this definition, given

$$\forall W. \forall \rho\ \gamma_\Gamma\ \gamma_\Gamma\ \gamma_\Omega. \rho \in \mathcal{D}\llbracket \Delta \rrbracket \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_. \wedge (W, \gamma_\Omega) \in \mathcal{G}\llbracket \Omega \rrbracket_.$$

we must show

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{n}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{n}^+)))) \in \mathcal{E}\llbracket \mathsf{int} \rrbracket_.$$

$\mathsf{n}^+ = \mathsf{n}$ is a closed term, so the closings have no effect. Ergo,

$$\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{n}^+))) = \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{n}^+))) = \mathsf{n}$$

Since $\mathsf{n} \in \mathbb{Z}$, one can easily see $(W, \mathsf{n}, \mathsf{n}) \in \mathcal{V}\llbracket \mathsf{int} \rrbracket_.$, which suffices to show $(W, \mathsf{n}, \mathsf{n}) \in \mathcal{E}\llbracket \mathsf{int} \rrbracket_.$ by Lemma 2.1. This suffices to finish the proof. □

Lemma 2.37 (Compat a).

$$\mathsf{a} : \tau \in \Omega \implies \Delta; \Gamma; \Gamma; \Omega \vdash \mathsf{a} \preceq \mathsf{a} : \tau \rightsquigarrow \Delta; \Gamma$$

Proof. One can easily see that $\Delta = \Delta$ and $\Gamma = \Gamma$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash \mathsf{a} : \tau \rightsquigarrow \Delta; \Gamma$ by the variable typing rule. Ergo, it suffices to show that $\Delta; \Gamma; \Gamma; \Omega \vdash \mathsf{a} \preceq \mathsf{a} : \tau$.

Expanding the conclusion, given

$$\forall W. \forall \rho\ \gamma_\Gamma\ \gamma_\Gamma\ \gamma_\Omega. \rho \in \mathcal{D}\llbracket \Delta \rrbracket \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_. \wedge (W, \gamma_\Omega) \in \mathcal{G}\llbracket \Omega \rrbracket_.$$

we must show

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{a}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{a}^+)))) \in \mathcal{E}\llbracket \tau \rrbracket_.$$

We can push the compiler and substitutions through this expression to refine this to:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{a})))\ (), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{a})))\ ()) \in \mathcal{E}\llbracket \tau \rrbracket_.$$

Since $(W, \gamma_\Omega) \in \mathcal{G}\llbracket \Omega \rrbracket_.$, there must exist $(\ell_1, \ell_2) \in W.\Theta$ and values $\mathsf{v}_1, \mathsf{v}_2$ such that

$$\mathrm{close}_1(\gamma_\Omega, \mathsf{a}) = \mathrm{guard}(\mathsf{v}_1, \ell_1) = \lambda\_.\mathrm{if}\ !\ell_1\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1 := \textsc{used}; \mathsf{v}_1\}\}$$

and

$$\mathrm{close}_2(\gamma_{\Omega}, \mathrm{a}) = \mathrm{guard}(\mathrm{v}_2, \ell_2) = \lambda\_.\mathrm{if}\ !\ell_2\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2 := \textsc{used}; \mathrm{v}_2\}\}$$

and $(W, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!]..$

Ergo, we must show

$$(W, \lambda\_.\mathrm{if}\ !\ell_1\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1 := \textsc{used}; \mathrm{v}_1\}\}\ (), \lambda\_.\mathrm{if}\ !\ell_2\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2 := \textsc{used}; \mathrm{v}_2\}\}\ ()) \in \mathcal{E}[\![\tau]\!].$$

Notice that both expressions have no free variables because v_1 and v_2 are closed, as they are in the value relation.

Expanding the definition of the expression relation, we find that given

$$\forall \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.$$
$$\langle \mathrm{H}_1, \lambda\_.\mathrm{if}\ !\ell_1\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1 := \textsc{used}; \mathrm{v}_1\}\}\ ()\rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1'\rangle \not\rightarrow$$

we need to show that either e_1' is fail Conv, or there exists $\mathrm{v}_2, \mathrm{H}_2', W'$ such that:

$$\langle \mathrm{H}_2, \lambda\_.\mathrm{if}\ !\ell_2\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2 := \textsc{used}; \mathrm{v}_2\}\}\ ()\rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{v}_2\rangle$$
$$\wedge W \sqsubseteq W' \wedge \mathrm{H}_1', \mathrm{H}_2' : W' \wedge (W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!].$$

To proceed with the proof, we must figure out what e_1' is. First, by application, we have

$$\langle \mathrm{H}_1, \lambda\_.\mathrm{if}\ !\ell_1\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1 := \textsc{used}; \mathrm{v}_1\}\}\ ()\rangle \longrightarrow \langle \mathrm{H}_1, \mathrm{if}\ !\ell_1\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1 := \textsc{used}; \mathrm{v}_1\}\}\rangle$$

and

$$\langle \mathrm{H}_2, \lambda\_.\mathrm{if}\ !\ell_2\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2 := \textsc{used}; \mathrm{v}_2\}\}\ ()\rangle \longrightarrow \langle \mathrm{H}_2, \mathrm{if}\ !\ell_2\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2 := \textsc{used}; \mathrm{v}_2\}\}\rangle$$

Next, since $\mathrm{H}_1, \mathrm{H}_2 : W$ and $(\ell_1, \ell_2) \in W.\Theta$, we have that $\mathrm{H}_1(\ell_1) = \mathrm{H}_2(\ell_2) = W.\Theta(\ell_1, \ell_2) \in \{\textsc{used}, \textsc{unused}\}$. If $W.\Theta(\ell_1, \ell_2) = \textsc{used}$, then the configuration steps to fail Conv, in which case we are done. Otherwise, if $W.\Theta(\ell_1, \ell_2) = \textsc{unused}$, then

$$\langle \mathrm{H}_1, \mathrm{if}\ !\ell_1\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1 := \textsc{used}; \mathrm{v}_1\}\}\rangle \longrightarrow \langle \mathrm{H}_1, \ell_1 := \textsc{used}; \mathrm{v}_1\rangle$$

and

$$\langle \mathrm{H}_2, \mathrm{if}\ !\ell_2\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2 := \textsc{used}; \mathrm{v}_2\}\}\rangle \longrightarrow \langle \mathrm{H}_2, \ell_2 := \textsc{used}; \mathrm{v}_2\rangle$$

Then, by the operational semantic,

$$\langle \mathrm{H}_1, \ell_1 := \textsc{used}; \mathrm{v}_1\rangle \longrightarrow \langle \mathrm{H}_1[\ell_1 \rightarrow \textsc{used}], \mathrm{v}_1\rangle$$
$$\langle \mathrm{H}_2, \ell_2 := \textsc{used}; \mathrm{v}_2\rangle \longrightarrow \langle \mathrm{H}_2[\ell_2 \rightarrow \textsc{used}], \mathrm{v}_2\rangle$$

Now, consider

$$W' = (W.k, W.\Psi, W.\Theta[(\ell_1, \ell_2) \mapsto \textsc{used}])$$

$W \sqsubseteq W'$ because W' has the same heap typing and W and W' has the same affine flags as W except that the affine flag at (ℓ_1, ℓ_2) has switched from $\textsc{unused}$ to $\textsc{used}$. Next, notice that $\mathrm{H}_1[\ell_1 \rightarrow \textsc{used}], \mathrm{H}_2[\ell_2 \rightarrow \textsc{used}] : W'$ because $\mathrm{H}_1, \mathrm{H}_2 : W$ and the only change from W to W' is that $W'.\Theta(\ell_1, \ell_2) = \textsc{used}$, which is satisfied by both $\mathrm{H}_1[\ell_1 \rightarrow \textsc{used}]$ and $\mathrm{H}_2[\ell_2 \rightarrow \textsc{used}]$. Finally, we have by assumption that $(W, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!].$, so by Lemma 2.3, we have $(W', \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!].$, which suffices to finish the proof. □

Lemma 2.38 (Compat x).

$$\mathrm{x} : \tau \in \Gamma \implies \Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{x} \preceq \mathrm{x} : \tau \rightsquigarrow \Delta; \Gamma$$

Proof. Clearly, $\Delta = \Delta$ and $\Gamma = \Gamma$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{x} : \tau \rightsquigarrow \Delta; \Gamma$ by the variable typing rule. Ergo, it suffices to show that $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{x} \preceq \mathrm{x} : \tau$.

Expanding the conclusion, given

$$\forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega.\rho \in \mathcal{D}[\![\Delta]\!] \land (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \land (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\cdot \land (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!]_\cdot$$

we must show

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{x}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{x}^+)))) \in \mathcal{E}[\![\tau]\!]_\cdot$$

Notice that $\mathrm{x}^+ = \mathrm{x}$. Then, since $\mathrm{x} \notin \Omega$ and $(W, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!]_\cdot$, we have

$$\mathrm{close}_1(\gamma_\Omega, \mathrm{x}) = \mathrm{close}_2(\gamma_\Omega, \mathrm{x}) = \mathrm{x}$$

Then, since $\mathrm{x} : \tau \in \Gamma$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\cdot$, there must exist $\mathrm{v}_1, \mathrm{v}_2$ such that

$$\gamma_\Gamma(\mathrm{x}) = (\mathrm{v}_1, \mathrm{v}_2)$$

and $(W, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!]_\cdot$. Ergo,

$$\mathrm{close}_1(\gamma_\Gamma, \mathrm{x}) = \mathrm{v}_1 \land \mathrm{close}_2(\gamma_\Gamma, \mathrm{x}) = \mathrm{v}_2$$

Since $(W, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!]_\cdot$, this suffices to show that

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{x}))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{x})))) \in \mathcal{V}[\![\tau]\!]_\cdot$$

By Lemma 2.1, $\mathcal{V}[\![\tau]\!]_\cdot \subseteq \mathcal{E}[\![\tau]\!]_\cdot$, so this suffices to finish the proof. □

Lemma 2.39 (Compat $\multimap$).

$$\Delta; \Gamma; \Gamma; \Omega, \mathrm{a} : \tau_1 \vdash \mathrm{e} \preceq \mathrm{e} : \tau_2 \rightsquigarrow \Delta'; \Gamma' \implies \Delta; \Gamma; \Gamma; \Omega \vdash \lambda \mathrm{a} : \tau_1.\mathrm{e} \preceq \lambda \mathrm{a} : \tau_1.\mathrm{e} : \tau_1 \multimap \tau_2 \rightsquigarrow \Delta'; \Gamma'$$

Proof. Expanding the hypothesis, we find $\Delta = \Delta'$ and $\Gamma = \Gamma'$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash \lambda \mathrm{a} : \tau_1.\mathrm{e} : \tau_1 \multimap \tau_2 \rightsquigarrow \Delta'; \Gamma'$ by the λ typing rule. Ergo, it suffices to show $\Delta; \Gamma; \Gamma; \Omega \vdash \lambda \mathrm{a} : \tau_1.\mathrm{e} \preceq \lambda \mathrm{a} : \tau_1.\mathrm{e} : \tau_1 \multimap \tau_2$.

Expanding the conclusion, given

$$\forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega.\rho \in \mathcal{D}[\![\Delta]\!] \land (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \land (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\cdot \land (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!]_\cdot$$

we must show

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \lambda \mathrm{a} : \tau_1.\mathrm{e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \lambda \mathrm{a} : \tau_1.\mathrm{e}^+)))) \in \mathcal{E}[\![\tau_1 \multimap \tau_2]\!]_\cdot$$

Notice that both of these expressions have no free variables by Lemma 2.10.

We can push the compiler and the substitutions to refine that to:

$$\begin{aligned}&(W, \lambda \mathrm{a}.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+))),\\ &\quad \lambda \mathrm{a}.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+)))) \in \mathcal{E}[\![\tau_1 \multimap \tau_2]\!]_\cdot\end{aligned}$$

Expanding the expression relation definition, we find that given

$$\begin{gathered}\forall \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.\\ \langle \mathrm{H}_1, \lambda \mathrm{a}.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))\rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1'\rangle \not\rightarrow\end{gathered}$$

we must show either $\mathrm{e}_1' = \mathrm{fail}\ \textsc{Conv}$ or there exist $\mathrm{v}_2, \mathrm{H}_2', W'$ such that:

$$\begin{aligned}&\langle \mathrm{H}_2, \lambda \mathrm{a}.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+)))\rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{v}_2\rangle\\ &\land W \sqsubseteq W' \land \mathrm{H}_1', \mathrm{H}_2' : W' \land (W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!]_\rho\end{aligned}$$

Clearly,

$$\langle \mathrm{H}_1, \lambda \mathrm{a}.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))\rangle \not\rightarrow$$

because this expression is a target value. Ergo, e_1' is the expression in the above configuration. Moreover, $\langle \mathrm{H}_2, \lambda \mathrm{a}.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+)))\rangle$ is also irreducible. Thus, it suffices to show

$$\begin{aligned}(W, &\lambda \mathrm{a}.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+))),\\ &\lambda \mathrm{a}.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+)))) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!]_\rho\end{aligned}$$

Expanding the value relation definition, given

$$\forall \mathrm{v}_1\ \mathrm{v}_2\ W'.W \sqsubset W' \wedge (W', \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau_1]\!].$$

we must show

$$\begin{aligned}((&W'.k, W'.\Psi, W'.\Theta \uplus (\ell_1, \ell_2) \mapsto \textsc{unused}),\\ &[\mathrm{a}{\mapsto}\mathrm{guard}(\mathrm{v}_1, \ell_1)]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))),\\ &[\mathrm{a}{\mapsto}\mathrm{guard}(\mathrm{v}_2, \ell_2)]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))))) \in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

Notice that $W'' = (W'.k, W'.\Psi, W'.\Theta \uplus (\ell_1, \ell_2) \mapsto \textsc{unused})$ is a world extension of W' because it has the same heap typing as W' and has all the affine flags as W' plus one new affine flag which is disjoint from any affine flag in W'. Ergo, since $W \sqsubseteq W'$ and $W' \sqsubseteq W''$, we have $W \sqsubseteq W''$. Next, notice that:

$$(W'', \gamma_\Omega[\mathrm{a} \mapsto (\mathrm{guard}(\mathrm{v}_1, \ell_1), \mathrm{guard}(\mathrm{v}_2, \ell_2))]) \in \mathcal{G}[\![\Omega, \mathrm{a} : \tau_1]\!].$$

because $(\ell_1, \ell_2) \in \mathrm{dom}(W''.\Theta)$, $(W'', \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau_1]\!].$ because $(W, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau_1]\!].$ and Lemma 2.3, and $(W'', \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!].$ because $(W, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!].$ and Lemma 2.3. Therefore, we can instantiate the first induction hypothesis with $W'', \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega[\mathrm{a} \mapsto (\mathrm{guard}(\mathrm{v}_1, \ell_1), \mathrm{guard}(\mathrm{v}_2, \ell_2))], \rho$ to find

$$\begin{aligned}(&W'', \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega[\mathrm{a} \mapsto (\mathrm{guard}(\mathrm{v}_1, \ell_1), \mathrm{guard}(\mathrm{v}_2, \ell_2))], \mathrm{e}^+))),\\ &\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega[\mathrm{a} \mapsto (\mathrm{guard}(\mathrm{v}_1, \ell_1), \mathrm{guard}(\mathrm{v}_2, \ell_2))], \mathrm{e}^+)))) \in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

which is equivalent to what was to be proven. □

Lemma 2.40 (Compat app).

$$\begin{aligned}&\Delta_1;\Gamma_1;\Gamma;\Omega_1 \vdash \mathrm{e}_1 \preceq \mathrm{e}_1 : \tau_1 \multimap \tau_2 \rightsquigarrow \Delta_2;\Gamma_2 \wedge \Delta_2;\Gamma_2;\Gamma;\Omega_2 \vdash \mathrm{e}_2 \preceq \mathrm{e}_2 : \tau_1 \rightsquigarrow \Delta_3;\Gamma_3\\ &\qquad\implies \Delta_1;\Gamma_1;\Gamma;\Omega_1 \uplus \Omega_2 \vdash \mathrm{e}_1\ \mathrm{e}_2 \preceq \mathrm{e}_1\ \mathrm{e}_2 : \tau_2 \rightsquigarrow \Delta_3;\Gamma_3\end{aligned}$$

Proof. Expanding the hypotheses, we find $\Delta_1 = \Delta_2 = \Delta_3$ and $\Gamma_1 = \Gamma_2 = \Gamma_3$. Moreover, $\Delta_1;\Gamma_1;\Gamma;\Omega_1 \uplus \Omega_2 \vdash \mathrm{e}_1\ \mathrm{e}_2 : \tau_2 \rightsquigarrow \Delta_3;\Gamma_3$ by the application typing rule. Ergo, it suffices to show $\Delta;\Gamma;\Gamma;\Omega \vdash \mathrm{e}_1\ \mathrm{e}_2 \preceq \mathrm{e}_1\ \mathrm{e}_2 : \tau_2$.

Expanding this definition, given

$$\forall W.\forall \rho\ \gamma_\Gamma\ \gamma_\Gamma\ \gamma_\Omega.\rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]. \wedge (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!].$$

we must show

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1\ \mathrm{e}_2{}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1\ \mathrm{e}_2{}^+)))) \in \mathcal{E}[\![\tau_2]\!].$$

Notice that both of these expressions have no free variables by Lemma 2.10.

We can push the compiler and substitutions through the application to refine this to:

$$\begin{aligned}(&W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+)))\ (\mathsf{let}\ \mathsf{x} = \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^+)))\ \mathsf{in}\ \mathsf{thunk}(\mathsf{x})),\\ &\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1{}^+)))\ (\mathsf{let}\ \mathsf{x} = \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^+)))\ \mathsf{in}\ \mathsf{thunk}(\mathsf{x}))) \in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

Expanding the expression relation definition, we find that given

$$\begin{aligned}&\forall \mathsf{H}_1, \mathsf{H}_2{:}W,\ \mathsf{e}_1',\ \mathsf{H}_1',\ j < W.k.\\ &\langle \mathsf{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+)))\\ &\quad(\mathsf{let}\ \mathsf{x} = \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^+)))\ \mathsf{in}\ \mathsf{thunk}(\mathsf{x}))\rangle \xrightarrow{j} \langle \mathsf{H}_1', \mathsf{e}_1'\rangle \nrightarrow\end{aligned}$$

we must show either $e_1' = \text{fail } \textsc{Conv}$ or there exist v_2, H_2', W' such that:

$$\begin{aligned}&\langle H_2, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Omega, e_1{}^+)))\\ &\quad(\text{let } x = \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Omega, e_2{}^+))) \text{ in thunk}(x))\rangle \xrightarrow{*} \langle H_2', v_2\rangle\\ &\quad\wedge W \sqsubseteq W' \wedge H_1', H_2' : W' \wedge (W', e_1', v_2) \in \mathcal{V}[\![\tau_2]\!].\end{aligned}$$

To proceed, we must figure out what e_1' is. First, notice that, by Lemma 2.2, $\gamma_\Omega = \gamma_1 \uplus \gamma_2$ where

$$(W, \gamma_1) \in \mathcal{G}[\![\Omega_e]\!].$$

and

$$(W, \gamma_2) \in \mathcal{G}[\![\Omega_e']\!].$$

and, for any $i \in \{1, 2\}$

$$\text{close}_i(\gamma_\Omega, e_1{}^+) = \text{close}_i(\gamma_1, e_1{}^+)$$

and

$$\text{close}_i(\gamma_\Omega, e_2{}^+) = \text{close}_i(\gamma_2, e_2{}^+)$$

Next, we need to find e_1'. From the operational semantic, the application will run the first subexpression using the heap H_1 until it reaches a target value or gets stuck. By appealing to our first induction hypothesis, instantiated with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_1, \rho$, we find that:

$$(W, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_1, e_1{}^+))), \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_1, e_1{}^+)))) \in \mathcal{E}[\![\tau_1 \multimap \tau_2]\!].$$

We can instantiate this with the heaps H_1, H_2 to find that $\langle H_1, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_1, e_1{}^+)))\rangle$ either reduces to fail $\textsc{Conv}$, in which case the original expression steps to fail $\textsc{Conv}$, or to some irreducible configuration $\langle H_1^*, e_1^*\rangle$, in which case on the other side, the configuration reduces to some irreducible configuration $\langle H_2^*, e_1^\dagger\rangle$ and there exists some W_1 where $W \sqsubseteq W_1$, $H_1^*, H_2^* : W_1$, and $(W_1, e_1^*, e_1^\dagger) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!]..$

Since terms in the value relation are target values, the original application will continue reducing on the second subexpression according to the operational semantics. Then, we can appeal to the second induction hypothesis instantiated with $W_1, \gamma_\Gamma, \gamma_\Gamma, \gamma_2, \rho$, because $W \sqsubseteq W_1$ and $\mathcal{G}[\![\Gamma]\!]_\rho, \mathcal{G}[\![\Gamma]\!]., \mathcal{G}[\![\Omega]\!].$ are closed under world extension by Lemma 2.3. Ergo,

$$(W_1, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_2, e_2{}^+))), \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_2, e_2{}^+)))) \in \mathcal{E}[\![\tau_1]\!].$$

We can instantiate this fact with H_1^*, H_2^* to find that $\langle H_1^*, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_2, e_2{}^+)))\rangle$ either reduces to fail $\textsc{Conv}$, in which case the original expression steps to fail $\textsc{Conv}$, or to some irreducible configuration $\langle H_1^{**}, e_2^*\rangle$, in which case on the other side, the configuration reduces to some irreducible configuration $\langle H_2^{**}, e_2^\dagger\rangle$ and there exists some W_2 where $W_1 \sqsubseteq W_2$, $H_1^{**}, H_2^{**} : W_2$, and $(W_2, e_2^*, e_2^\dagger) \in \mathcal{V}[\![\tau_1]\!]..$

Then, instantiate $(W_1, e_1^*, e_1^\dagger) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!].$ with $e_2^*, e_2^\dagger, \triangleright W_2$. Because $W_1 \sqsubseteq W_2$ and $W_2 \sqsubset \triangleright W_2$, it follows that $W_1 \sqsubset \triangleright W_2$. Moreover, $(\triangleright W_2, e_2^*, e_2^\dagger) \in \mathcal{V}[\![\tau_1]\!].$ (because $(W_2, e_2^*, e_2^\dagger) \in \mathcal{V}[\![\tau_1]\!].$ and $W_2 \sqsubseteq \triangleright W_2$, so we can apply Lemma 2.3). Ergo, there exist $e_b^*, e_b^\dagger$ such that

$$e_1^* = \lambda a.e_b^*$$

and

$$e_1^\dagger = \lambda a.e_b^\dagger$$

and, for any $(\ell_1, \ell_2) \notin \text{dom}(\triangleright W_2.\Psi) \cup \text{dom}(\triangleright W_2.\Theta)$,

$$((\triangleright W_2.k, \triangleright W_2.\Psi, \triangleright W_2.\Theta \uplus (\ell_1, \ell_2) \mapsto \textsc{unused}), [a \mapsto \text{guard}(e_2^*, \ell_2)]e_b^*, [a \mapsto \text{guard}(e_2^\dagger, \ell_1)]e_b^\dagger) \in \mathcal{E}[\![\tau_2]\!].$$

Thus, the original configuration in H_1 steps as follows:

$$\begin{array}{l}
\langle \mathrm{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e_1}^+)))\ (\mathrm{let\ x = close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e_2}^+)))\ \mathrm{in\ thunk(x)})\rangle \xrightarrow{*} \\
\langle \mathrm{H}_1^*, \lambda \mathrm{a.e}_\mathrm{b}^*\ (\mathrm{let\ x = close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e_2}^+)))\ \mathrm{in\ thunk(x)})\rangle \xrightarrow{*} \\
\langle \mathrm{H}_1^{**}, \lambda \mathrm{a.e}_\mathrm{b}^*\ (\mathrm{let\ x =\ e}_2^*\ \mathrm{in\ thunk(x)})\rangle \longrightarrow \\
\langle \mathrm{H}_1^{**}, \lambda \mathrm{a.e}_\mathrm{b}^*\ \mathrm{thunk(e}_2^*)\rangle \xrightarrow{0} \\
\langle \mathrm{H}_1^{**}, \lambda \mathrm{a.e}_\mathrm{b}^*\ \mathrm{let\ r_{fresh} = ref\ 1\ in\ } \lambda\_.\{\mathrm{if\ !r_{fresh}}\ \{\mathrm{fail\ \textsc{Conv}}\}\ \{\mathrm{r_{fresh}} := \textsc{used}; \mathrm{e}_2^*\}\}\rangle \longrightarrow \\
\langle \mathrm{H}_1^{**}[\ell_1 \mapsto \textsc{unused}], \lambda \mathrm{a.e}_\mathrm{b}^*\ \lambda\_.\{\mathrm{if}\ !\ell_1\ \{\mathrm{fail\ \textsc{Conv}}\}\ \{\ell_1 := \textsc{used}; \mathrm{e}_2^*\}\}\rangle \xrightarrow{0} \\
\langle \mathrm{H}_1^{**}[\ell_1 \mapsto \textsc{unused}], \lambda \mathrm{a.e}_\mathrm{b}^*\ \mathrm{guard}(\ell_1, \mathrm{e}_2^*)\rangle \longrightarrow \\
\langle \mathrm{H}_1^{**}[\ell_1 \mapsto \textsc{unused}], [\mathrm{a} \mapsto \mathrm{guard}(\ell_1, \mathrm{e}_2^*)]\mathrm{e}_\mathrm{b}^*\rangle
\end{array}$$

for some $\ell_1 \notin \mathrm{H}_1^{**}$. Similarly, the original configuration in H_2 steps to

$$\langle \mathrm{H}_1^{**}[\ell_2 \mapsto \textsc{unused}], [\mathrm{a} \mapsto \mathrm{guard}(\ell_2, \mathrm{e}_2^\dagger)]\mathrm{e}_\mathrm{b}^\dagger\rangle$$

for some $\ell_2 \notin \mathrm{H}_2^{**}$. Since $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : W_2$, this implies $(\ell_1, \ell_2) \notin \mathrm{dom}(W_2.\Psi) \cup \mathrm{dom}(W_2.\Theta)$, and thus $(\ell_1, \ell_2) \notin \mathrm{dom}(\triangleright W_2.\Psi) \cup \mathrm{dom}(\triangleright W_2.\Theta)$.

Therefore, from the fact found above by expanding the value relation for $\tau_1 \multimap \tau_2$, the two expressions in the above configurations are in $\mathcal{E}[\![\tau_2]\!]_.$ at the world $(\triangleright W_2.k, \triangleright W_2.\Psi, \triangleright W_2.\Theta \uplus (\ell_1, \ell_2) \mapsto \textsc{unused})$, which we will label as W_3. Moreover, since $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : W_2$, we also have $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : \triangleright W_2$. Therefore, the heaps above satisfy W_3, because the only difference between $\triangleright W_2$ and W_3 is that W_3 has a new affine flag $(\ell_1, \ell_2) \mapsto \textsc{unused}$, which the above heaps indeed satisfy. Ergo, we can instantiate the fact that the above expressions are in $\mathcal{E}[\![\tau_2]\!]_.$ in the world W_3 with the heaps $\mathrm{H}_1^{**}[\ell_1 \mapsto \textsc{unused}]$ and $\mathrm{H}_2^{**}[\ell_2 \mapsto \textsc{unused}]$ to find that either the first configuration steps to fail Conv, in which case the original configuration with H_1 steps to fail Conv, or the first configuration steps to some irreducible configuration $\langle \mathrm{H}_1^{***}, e_f^*\rangle$, in which case the second configuration steps to $\langle \mathrm{H}_2^{***}, e_f^\dagger\rangle$ and there exists some W_4 such that $W_3 \sqsubseteq W_4$, $\mathrm{H}_1^{***}, \mathrm{H}_2^{***} : W_4$, and $(W_4, e_f^*, e_f^\dagger) \in \mathcal{V}[\![\tau_2]\!]_.$.

This suffices to show that $\mathrm{e}_1' = \mathrm{e}^{***}$, so e_1' is indeed in the value relation at τ_2 along with the value stepped to by the original configuration on the right hand side. Ergo, since $W \sqsubseteq W_1$, $W_1 \sqsubseteq W_2$, $W_2 \sqsubseteq \triangleright W_2$, $\triangleright W_2 \sqsubseteq W_3$, and $W_3 \sqsubseteq W_4$, it follows that $W \sqsubseteq W_4$ (by Lemma 2.4), which suffices to finish the proof. □

Lemma 2.41 (Compat !).

$$\Delta; \Gamma; \Gamma; \cdot \vdash \mathrm{v} \preceq \mathrm{v} : \tau \rightsquigarrow \Delta'; \Gamma' \implies \Delta; \Gamma; \Gamma; \cdot \vdash !\mathrm{v} \preceq !\mathrm{v} : !\tau \rightsquigarrow \Delta'; \Gamma'$$

Proof. Expanding the hypotheses, we find $\Delta_1 = \Delta'$ and $\Gamma = \Gamma'$. Moreover, $\Delta; \Gamma; \Gamma; \cdot \vdash !\mathrm{v} : !\tau \rightsquigarrow \Delta'; \Gamma'$ by the ! typing rule. Ergo, it suffices to show $\Delta; \Gamma; \Gamma; \cdot \vdash !\mathrm{v} \preceq !\mathrm{v} : !\tau$.

Expanding this definition, given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_. \wedge (W, \gamma_\Omega) \in \mathcal{G}[\![\cdot]\!]_.$$

we must show

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, !\mathrm{v}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, !\mathrm{v}^+)))) \in \mathcal{E}[\![!\tau]\!]_.$$

Notice that both of these expressions have no free variables by Lemma 2.10.

Note that $!\mathrm{v}^+ = \mathrm{v}^+$. Then, by expanding the expression relation definition, we find that given

$$\forall \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.$$
$$\langle \mathrm{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{v}^+)))\rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1'\rangle \nrightarrow$$

we must show either $\mathrm{e}_1' = \mathrm{fail\ \textsc{Conv}}$ or there exist $\mathrm{v}_2, \mathrm{H}_2', W'$ such that:

$$\langle \mathrm{H}_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{v}^+)))\rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{v}_2\rangle$$
$$\wedge W \sqsubseteq W' \wedge \mathrm{H}_1', \mathrm{H}_2' : W' \wedge (W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![!\tau]\!]_\rho$$

Now, we can instantiate the first induction hypothesis with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$ to show that

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{v}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{v}^+)))) \in \mathcal{E}[\![\tau]\!].$$

By instanting this fact with $\mathrm{H}_1, \mathrm{H}_2$, since we have by assumption that $\mathrm{H}_1, \mathrm{H}_2 : W$, we find that either the first expression steps to fail CONV or there exist $W_1, \mathrm{v}_1, \mathrm{H}_1^*, \mathrm{v}_2, \mathrm{H}_2^*$ such that $W \sqsubseteq W_1$, $\mathrm{H}_1^*, \mathrm{H}_2^* : W_1$, and

$$\langle \mathrm{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{v}^+)))\rangle \xrightarrow{*} \langle \mathrm{H}_1^*, \mathrm{v}_1\rangle$$

and

$$\langle \mathrm{H}_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{v}^+)))\rangle \xrightarrow{*} \langle \mathrm{H}_2^*, \mathrm{v}_2\rangle$$

and

$$(W_1, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![\tau]\!]_\rho$$

Thus, it follows that $(W_1, \mathrm{v}_1, \mathrm{v}_2) \in \mathcal{V}[\![!\tau]\!]_\rho$, which suffices to finish the proof. □

LEMMA 2.42 (COMPAT let!).

$$\Delta_1; \Gamma_1; \Gamma; \Omega_1 \vdash \mathrm{e}_1 \preceq \mathrm{e}_1 : !\tau \rightsquigarrow \Delta_2; \Gamma_2 \wedge \Delta_2; \Gamma_2; \Gamma, \mathrm{x} : \tau; \Omega_2 \vdash \mathrm{e}_2 \preceq \mathrm{e}_2 : \tau' \rightsquigarrow \Delta_3; \Gamma_3$$
$$\implies \Delta_1; \Gamma_1; \Gamma; \Omega_1 \uplus \Omega_2 \vdash \mathrm{let}\ !\mathrm{x} = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 \preceq \mathrm{let}\ !\mathrm{x} = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 : \tau' \rightsquigarrow \Delta_3; \Gamma_3$$

PROOF. Expanding the hypotheses, we find $\Delta_1 = \Delta_2 = \Delta_3$ and $\Gamma_1 = \Gamma_2 = \Gamma_3$. Moreover, $\Delta_1; \Gamma_1; \Gamma; \Omega_1 \uplus \Omega_2 \vdash \mathrm{let}\ !\mathrm{x} = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 : \tau' \rightsquigarrow \Delta_3; \Gamma_3$ by the let! typing rule. Thus, it suffices to show $\Delta_1; \Gamma_1; \Gamma; \Omega_1 \uplus \Omega_2 \vdash \mathrm{let}\ !\mathrm{x} = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 \preceq \mathrm{let}\ !\mathrm{x} = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 : \tau'$.

Expanding the conclusion, we must show that given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]. \wedge (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega_1 \uplus \Omega_2]\!].$$

we must show

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{let}\ !\mathrm{x} = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2{}^+))),$$
$$\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{let}\ !\mathrm{x} = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2{}^+)))) \in \mathcal{E}[\![\tau']\!].$$

Notice that both of these expressions have no free variables by Lemma 2.10.

We can push the compiler and substitutions through the let expression and refine this to:

$$(W, \mathrm{let}\ \mathrm{x} = \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+)))\ \mathrm{in}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^+))),$$
$$\mathrm{let}\ \mathrm{x} = \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1{}^+)))\ \mathrm{in}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^+))) \in \mathcal{E}[\![\tau']\!].$$

Then, by Lemma 2.2, we find that $\gamma_\Omega = \gamma_1 \uplus \gamma_2$ where

$$(W, \gamma_1) \in \mathcal{G}[\![\Omega_1]\!].$$

and

$$(W, \gamma_2) \in \mathcal{G}[\![\Omega_2]\!].$$

and, for any $i \in \{1, 2\}$

$$\mathrm{close}_i(\gamma_\Omega, \mathrm{e}_1) = \mathrm{close}_i(\gamma_1, \mathrm{e}_1)$$

and

$$\mathrm{close}_i(\gamma_\Omega, \mathrm{e}_2) = \mathrm{close}_i(\gamma_2, \mathrm{e}_2)$$

Thus, we must show

$$(W, \mathrm{let}\ \mathrm{x} = \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e}_1{}^+)))\ \mathrm{in}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e}_2{}^+))),$$
$$\mathrm{let}\ \mathrm{x} = \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathrm{e}_1{}^+)))\ \mathrm{in}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e}_2{}^+))) \in \mathcal{E}[\![\tau']\!].$$

Expanding the expression relation definition, we find

$$\forall \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.$$

$$\langle \mathrm{H}_1, \mathrm{let}\ \mathrm{x} = \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, {\mathrm{e}_1}^{+}))) \ \mathrm{in}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, {\mathrm{e}_2}^{+})))\rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1'\rangle \nrightarrow$$

we must show either $\mathrm{e}_1' = \mathrm{fail}\ \textsc{Conv}$ or there exist $\mathrm{v}_2, \mathrm{H}_2', W'$ such that:

$$\langle \mathrm{H}_2, \mathrm{let}\ \mathrm{x} = \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, {\mathrm{e}_1}^{+}))) \ \mathrm{in}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, {\mathrm{e}_2}^{+})))\rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{v}_2\rangle$$
$$\wedge\, W \sqsubseteq W' \wedge \mathrm{H}_1', \mathrm{H}_2' : W' \wedge (W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![\tau_1]\!]_\rho$$

Next, we need to find e_1'. From the operational semantic, the let will run the first subexpression using the heap H_1 until it reaches a target value or gets stuck. By appealing to our first induction hypothesis, instantiated with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_1, \rho$, we find that:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, {\mathrm{e}_1}^{+}))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, {\mathrm{e}_1}^{+})))) \in \mathcal{E}[\![!\tau]\!].$$

We can instantiate this with the heaps $\mathrm{H}_1, \mathrm{H}_2$ to find that $\langle \mathrm{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, {\mathrm{e}_1}^{+})))\rangle$ either reduces to fail Conv, in which case the original expression steps to fail Conv, or to some irreducible configuration $\langle \mathrm{H}_1^*, \mathrm{e}_1^*\rangle$, in which case on the other side, the configuration reduces to some irreducible configuration $\langle \mathrm{H}_2^*, \mathrm{e}_1^\dagger\rangle$ and there exists some W_1 where $W \sqsubseteq W_1$, $\mathrm{H}_1^*, \mathrm{H}_2^* : W_1$, and $(W_1, \mathrm{e}_1^*, \mathrm{e}_1^\dagger) \in \mathcal{V}[\![!\tau]\!]..$ By expanding the value relation definition, we find $(W_1, \mathrm{e}_1^*, \mathrm{e}_1^\dagger) \in \mathcal{V}[\![\tau]\!]..$

Since terms in the value relation are target values, the original configuration with H_1 steps as follows:

$$\langle \mathrm{H}_1, \mathrm{let}\ \mathrm{x} = \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, {\mathrm{e}_1}^{+}))) \ \mathrm{in}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, {\mathrm{e}_2}^{+})))\rangle \xrightarrow{*}$$
$$\langle \mathrm{H}_1^*, \mathrm{let}\ \mathrm{x} = \ \mathrm{e}_1^* \ \mathrm{in}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, {\mathrm{e}_2}^{+})))\rangle \rightarrow$$
$$\langle \mathrm{H}_1^*, [\mathrm{x} \mapsto \mathrm{e}_1^*]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, {\mathrm{e}_2}^{+})))\rangle$$

and similarly, the original configuration with H_2 steps as follows:

$$\langle \mathrm{H}_2, \mathrm{let}\ \mathrm{x} = \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, {\mathrm{e}_1}^{+}))) \ \mathrm{in}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, {\mathrm{e}_2}^{+})))\rangle \xrightarrow{*}$$
$$\langle \mathrm{H}_2^*, \mathrm{let}\ \mathrm{x} = \ \mathrm{e}_1^\dagger \ \mathrm{in}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, {\mathrm{e}_2}^{+})))\rangle \rightarrow$$
$$\langle \mathrm{H}_2^*, [\mathrm{x} \mapsto \mathrm{e}_1^\dagger]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, {\mathrm{e}_2}^{+})))\rangle$$

Next, notice that $(W_1, \gamma_\Gamma[\mathrm{x} \mapsto (\mathrm{e}_1^*, \mathrm{e}_1^\dagger)]) \in \mathcal{G}[\![\Gamma, \mathrm{x} : \tau]\!].$ because $(W_1, \mathrm{e}_1^*, \mathrm{e}_1^\dagger) \in \mathcal{V}[\![\tau]\!].$ and $(W_1, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!].$ (which follows from Lemma 2.3 because $W \sqsubseteq W_1$ and $(W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!].$). Therefore, by instantiating the second induction hypothesis with $W_1, \gamma_\Gamma, \gamma_\Gamma[\mathrm{x} \mapsto (\mathrm{e}_1^*, \mathrm{e}_1^\dagger)], \gamma_2, \rho$, we find that

$$(W_1, [\mathrm{x} \mapsto \mathrm{e}_1^*]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, {\mathrm{e}_2}^{+}))), [\mathrm{x} \mapsto \mathrm{e}_1^\dagger]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, {\mathrm{e}_2}^{+})))) \in \mathcal{E}[\![\tau']\!].$$

Then, since $\mathrm{H}_1^*, \mathrm{H}_2^* : W_1$, we can instantiate the above fact with H_1^* and H_2^*. Ergo, the configuration above with H_1^* must either step to fail Conv, in which case the original expression steps to fail Conv, or it must step to some $\langle \mathrm{H}_1^\dagger, \mathrm{e}_1^{**}\rangle$, in which case the configuration on the other side with H_2^* must step to $\langle \mathrm{H}_2^\dagger, \mathrm{e}_1^{\dagger\dagger}\rangle$ for some heap $\mathrm{H}_2^\dagger$ and world W_2 where $W_1 \sqsubseteq W_2$, $\mathrm{H}_1^\dagger, \mathrm{H}_2^\dagger : W_2$, and $(W_2, \mathrm{e}_1^{**}, \mathrm{e}_1^{\dagger\dagger}) \in \mathcal{V}[\![\tau']\!]..$ Thus, $\mathrm{e}_1' = \mathrm{e}_1^{**}$, so e_1' is indeed in the value relation at type τ' along with $\mathrm{e}_1^{\dagger\dagger}$, which is the value which the original expression on the other side stepped to. Finally, since $W \sqsubseteq W_1$ and $W_1 \sqsubseteq W_2$, we have $W \sqsubseteq W_2$, which suffices to finish the proof. □

Lemma 2.43 (Compat &).

$$\Delta_1; \Gamma_1; \Gamma; \Omega \vdash \mathrm{e}_1 \preceq \mathrm{e}_1 : \tau_1 \rightsquigarrow \Delta_2; \Gamma_2 \wedge \Delta_2; \Gamma_2; \Gamma; \Omega \vdash \mathrm{e}_2 \preceq \mathrm{e}_2 : \tau_2 \rightsquigarrow \Delta_3; \Gamma_3$$
$$\Longrightarrow \ \Delta_1; \Gamma_1; \Gamma; \Omega \vdash \langle \mathrm{e}_1, \mathrm{e}_2\rangle \preceq \langle \mathrm{e}_1, \mathrm{e}_2\rangle : \tau_1 \& \tau_2 \rightsquigarrow \Delta_3; \Gamma_3$$

Proof. Expanding the hypotheses, we find $\Delta_1 = \Delta_2 = \Delta_3$ and $\Gamma_1 = \Gamma_2 = \Gamma_3$. Moreover, $\Delta_1; \Gamma_1; \Gamma; \Omega \vdash \langle \mathrm{e}_1, \mathrm{e}_2 \rangle : \tau_1 \& \tau_2 \rightsquigarrow \Delta_3; \Gamma_3$ by the product typing rule. Ergo, it suffices to show $\Delta_1; \Gamma_1; \Gamma; \Omega \vdash \langle \mathrm{e}_1, \mathrm{e}_2 \rangle \preceq \langle \mathrm{e}_1, \mathrm{e}_2 \rangle : \tau'$.

Expanding the conclusion, we must show that given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega . \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]. \wedge (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!].$$

we must show

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \langle \mathrm{e}_1, \mathrm{e}_2 \rangle^+))),$$
$$\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \langle \mathrm{e}_1, \mathrm{e}_2 \rangle^+)))) \in \mathcal{E}[\![\tau_1 \& \tau_2]\!].$$

Note that both of these expressions are closed by Lemma 2.10.

We can push the compiler and substitutions through the product expression and refine this to:

$$(W, (\lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+))), \lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^+)))),$$
$$(\lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1{}^+))), \lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^+))))) \in \mathcal{E}[\![\tau_1 \& \tau_2]\!].$$

Expanding the expression relation definition, we find that given

$$\forall \mathrm{H}_1, \mathrm{H}_2 {:} W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.$$
$$\langle \mathrm{H}_1, (\lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+))), \lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^+))))\rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1' \rangle \nrightarrow$$

we must show either $\mathrm{e}_1' = \mathrm{fail}\ \textsc{Conv}$ or there exist $\mathrm{v}_2, \mathrm{H}_2', W'$ such that:

$$\langle \mathrm{H}_2, (\lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1{}^+))), \lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^+))))\rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{v}_2 \rangle$$
$$\wedge W \sqsubseteq W' \wedge \mathrm{H}_1', \mathrm{H}_2' : W' \wedge (W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}[\![\tau_1 \& \tau_2]\!].$$

Clearly,

$$\langle \mathrm{H}_1, (\lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+))), \lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^+))))\rangle \nrightarrow$$

because this expression is a target value. Ergo, e_1' is the expression in the above configuration. Moreover, $\langle \mathrm{H}_2, (\lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1{}^+))), \lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^+))))\rangle$ is also irreducible. Thus, it suffices to show

$$(W, (\lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+))), \lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^+)))),$$
$$(\lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1{}^+))), \lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^+))))) \in \mathcal{V}[\![\tau_1 \& \tau_2]\!].$$

First, we can instantiate the first induction hypothesis with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$ to show that

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1{}^+)))) \in \mathcal{V}[\![\tau_1]\!].$$

and we can instantiate the second induction hypothesis with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$ to show that

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^+)))) \in \mathcal{V}[\![\tau_2]\!].$$

This suffices to show that the pairs of lambdas are in the value relation at $\tau_1 \& \tau_2$, as was to be proven. □

Lemma 2.44 (Compat .1).

$$\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{e} \preceq \mathrm{e} : \tau_1 \& \tau_2 \rightsquigarrow \Delta'; \Gamma' \implies \Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{e}.1 \preceq \mathrm{e}.1 : \tau_1 \rightsquigarrow \Delta'; \Gamma'$$

Proof. Expanding the hypotheses, we find $\Delta_1 = \Delta'$ and $\Gamma = \Gamma'$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{e}.1 : \tau_1 \rightsquigarrow \Delta'; \Gamma'$ by the .1 typing rule. Ergo, it suffices to show $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{e}.1 \preceq \mathrm{e}.1 : \tau_1$.

Expanding this definition, given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega . \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]. \wedge (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!].$$

we must show

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}.1^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}.1^+)))) \in \mathcal{E}[\![\tau_1]\!].$$

Notice that both of these expressions have no free variables by Lemma 2.10.

We can push the compiler and substitutions through the projection to refine this to:

$$(W, (\text{fst close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Omega, e^+))))\ (), (\text{fst close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Omega, e^+))))\ ()) \in \mathcal{E}\llbracket \tau_1 \rrbracket.$$

Expanding the expression relation definition, we find that given

$$\forall H_1, H_2{:}W,\ e'_1,\ H'_1,\ j < W.k.$$
$$\langle H_1, (\text{fst close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Omega, e^+))))\ ()\rangle \xrightarrow{j} \langle H'_1, e'_1\rangle \nrightarrow$$

we must show either $e'_1 = \text{fail Conv}$ or there exist v_2, H'_2, W' such that:

$$\langle H_2, (\text{fst close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Omega, e^+))))\ ()\rangle \xrightarrow{*} \langle H'_2, v_2\rangle$$
$$\wedge W \sqsubseteq W' \wedge H'_1, H'_2 : W' \wedge (W', e'_1, v_2) \in \mathcal{V}\llbracket \tau_1 \rrbracket.$$

To proceed, we must find out what e'_1 is. First, by instantiating the first induction hypothesis with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$, we find

$$(W, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Omega, e^+))), \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Omega, e^+)))) \in \mathcal{E}\llbracket \tau_1 \& \tau_2 \rrbracket.$$

Since $H_1, H_2 : W$, we find that $\langle H_1, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Omega, e^+)))\rangle$ either steps to fail Conv, in which case the original expression steps to fail Conv, or steps to some irreducible configuration $\langle H^*_1, e^*\rangle$, in which case the configuration with H_2 also steps to some irreducible configuration $\langle H^*_2, e^\dagger\rangle$ and there exists some world W_1 where $W \sqsubseteq W_1, H^*_1, H^*_2 : W_1$, and $(W_1, e^*, e^\dagger) \in \mathcal{V}\llbracket \tau_1 \& \tau_2 \rrbracket..$

Ergo, there exists some $e^*_1, e^\dagger_1, e^*_2, e^\dagger_2$ such that

$$e^* = (\lambda\_.e^*_1, \lambda\_.e^*_2)$$

and

$$e^\dagger = (\lambda\_.e^\dagger_1, \lambda\_.e^\dagger_2)$$

and

$$(W_1, e^*_1, e^\dagger_1) \in \mathcal{E}\llbracket \tau_1 \rrbracket.$$

and

$$(W_1, e^*_2, e^\dagger_2) \in \mathcal{E}\llbracket \tau_2 \rrbracket.$$

Thus, the original configuration with H_1 steps as follows:

$$\begin{aligned}
&\langle H_1, (\text{fst close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Omega, e^+))))\ ()\rangle \xrightarrow{*}\\
&\langle H^*_1, (\text{fst } (\lambda\_.e^*_1, \lambda\_.e^*_2))\ ()\rangle \rightarrow\\
&\langle H^*_1, \lambda\_.e^*_1\ ()\rangle \rightarrow\\
&\langle H^*_1, e^*_1\rangle
\end{aligned}$$

and on the other side, the original configuration with H_2 steps as follows:

$$\begin{aligned}
&\langle H_2, (\text{fst close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Omega, e^+))))\ ()\rangle \xrightarrow{*}\\
&\langle H^*_2, (\text{fst } (\lambda\_.e^\dagger_1, \lambda\_.e^\dagger_2))\ ()\rangle \rightarrow\\
&\langle H^*_2, \lambda\_.e^\dagger_1\ ()\rangle \rightarrow\\
&\langle H^*_2, e^\dagger_1\rangle
\end{aligned}$$

Then, since $H^*_1, H^*_2 : W_1$, we can instantiate $(W_1, e^*_1, e^\dagger_1) \in \mathcal{E}\llbracket \tau_1 \rrbracket.$ with H^*_1, H^*_2 to show that $\langle H^*_1, e^*_1\rangle$ either steps to fail Conv, in which case the original expression steps to fail Conv, or $\langle H^*_1, e^*_1\rangle$ steps to some irreducible $H^\dagger_1 e^*_f$, in which case $\langle H^*_2, e^\dagger_1\rangle$ steps to an irreudicble configuration $\langle H^\dagger_2, e^\dagger_f\rangle$ and there exists some W_2 such that $W_1 \sqsubseteq W_2$, $H^\dagger_1, H^\dagger_2 : W_2$, and $(W_2, e^*_f, e^\dagger_f) \in \mathcal{V}\llbracket \tau_1 \rrbracket..$ Thus, $e'_1 = e^*_f$, and e'_1 is indeed in the value relation at τ_1 with the value which the configuration on the other side steps to. Finally, since $W \sqsubseteq W_1$ and $W_1 \sqsubseteq W_2$, we have $W \sqsubseteq W_2$, which suffices to finish the proof. □

Lemma 2.45 (Compat .2).

$$\Delta;\Gamma;\Gamma;\Omega \vdash \mathrm{e} \preceq \mathrm{e} : \tau_1\&\tau_2 \rightsquigarrow \Delta';\Gamma' \implies \Delta;\Gamma;\Gamma;\Omega \vdash \mathrm{e.2} \preceq \mathrm{e.2} : \tau_2 \rightsquigarrow \Delta';\Gamma'$$

Proof. This proof is essentially identical to that of .1. □

Lemma 2.46 (Compat ⊗).

$$\begin{gathered}\Delta_1;\Gamma_1;\Gamma;\Omega_1 \vdash \mathrm{e}_1 \preceq \mathrm{e}_1 : \tau_1 \rightsquigarrow \Delta_2;\Gamma_2 \wedge \Delta_2;\Gamma_2;\Gamma;\Omega_2 \vdash \mathrm{e}_2 \preceq \mathrm{e}_2 : \tau_2 \rightsquigarrow \Delta_3;\Gamma_3 \\ \implies \Delta_1;\Gamma_1;\Gamma;\Omega_1 \uplus \Omega_2 \vdash (\mathrm{e}_1,\mathrm{e}_2) \preceq (\mathrm{e}_1,\mathrm{e}_2) : \tau_1 \otimes \tau_2 \rightsquigarrow \Delta_3;\Gamma_3\end{gathered}$$

Proof. Expanding the hypotheses, we find $\Delta_1 = \Delta_2 = \Delta_3$ and $\Gamma_1 = \Gamma_2 = \Gamma_3$. Moreover, $\Delta_1;\Gamma_1;\Gamma;\Omega_1 \uplus \Omega_2 \vdash (\mathrm{e}_1,\mathrm{e}_2) : \tau_1 \otimes \tau_2 \rightsquigarrow \Delta_3;\Gamma_3$ by the pair typing rule. Ergo, it suffices to show $\Delta_1;\Gamma_1;\Gamma;\Omega_1 \uplus \Omega_2 \vdash (\mathrm{e}_1,\mathrm{e}_2) \preceq (\mathrm{e}_1,\mathrm{e}_2) : \tau'$.

Expanding the conclusion, we must show that given

$$\forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega.\rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W,\gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W,\gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket. \wedge (W,\gamma_\Omega) \in \mathcal{G}\llbracket\Omega_1 \uplus \Omega_2\rrbracket.$$

we must show

$$\begin{gathered}(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, (\mathrm{e}_1,\mathrm{e}_2)^+))), \\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, (\mathrm{e}_1,\mathrm{e}_2)^+)))) \in \mathcal{E}\llbracket\tau_1 \otimes \tau_2\rrbracket.\end{gathered}$$

Notice that both of these expressions have no free variables by Lemma 2.10.

We can push the compiler and substitutions through the product expression and refine this to:

$$\begin{gathered}(W, (\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+))),\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^+)))), \\ (\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1{}^+))),\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^+))))) \in \mathcal{E}\llbracket\tau_1 \otimes \tau_2\rrbracket.\end{gathered}$$

Then, by Lemma 2.2, we find that $\gamma_\Omega = \gamma_1 \uplus \gamma_2$ where

$$(W,\gamma_1) \in \mathcal{G}\llbracket\Omega_1\rrbracket.$$

and

$$(W,\gamma_2) \in \mathcal{G}\llbracket\Omega_2\rrbracket.$$

and, for any $i \in \{1,2\}$

$$\mathrm{close}_i(\gamma_\Omega, \mathrm{e}_1{}^+) = \mathrm{close}_i(\gamma_1, \mathrm{e}_1{}^+)$$

and

$$\mathrm{close}_i(\gamma_\Omega, \mathrm{e}_2{}^+) = \mathrm{close}_i(\gamma_2, \mathrm{e}_2{}^+)$$

Thus, we must show

$$\begin{gathered}(W, (\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e}_1{}^+))),\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e}_2{}^+)))), \\ (\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathrm{e}_1{}^+))),\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e}_2{}^+))))) \in \mathcal{E}\llbracket\tau_1 \otimes \tau_2\rrbracket.\end{gathered}$$

Expanding the expression relation definition, we find that given

$$\forall \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.$$

$$\langle \mathrm{H}_1, (\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e}_1{}^+))),\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e}_2{}^+))))\rangle \xrightarrow{j} \langle \mathrm{H}_1', \mathrm{e}_1'\rangle \nrightarrow$$

we must show either $\mathrm{e}_1' = \mathrm{fail}\ \textsc{Conv}$ or there exist $\mathrm{v}_2, \mathrm{H}_2', W'$ such that:

$$\begin{gathered}\langle \mathrm{H}_2, (\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathrm{e}_1{}^+))),\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e}_2{}^+))))\rangle \xrightarrow{*} \langle \mathrm{H}_2', \mathrm{v}_2\rangle \\ \wedge W \sqsubseteq W' \wedge \mathrm{H}_1', \mathrm{H}_2' : W' \wedge (W', \mathrm{e}_1', \mathrm{v}_2) \in \mathcal{V}\llbracket\tau_1 \otimes \tau_2\rrbracket_\rho\end{gathered}$$

Next, we need to find e_1'. From the operational semantic, the tensor will run the first subexpression using the heap H_1 until it reaches a target value or gets stuck. By appealing to our first induction hypothesis, instantiated with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_1, \rho$, we find that:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, e_1{}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, e_1{}^+)))) \in \mathcal{E}[\![\tau_1]\!]_.$$

We can instantiate this with the heaps H_1, H_2 to find that $\langle H_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, e_1{}^+)))\rangle$ either reduces to fail Conv, in which case the original expression steps to fail Conv, or to some irreducible configuration $\langle H_1^*, e_1^*\rangle$, in which case on the other side, the configuration with H_2 reduces to some irreducible configuration $\langle H_2^*, e_1^\dagger\rangle$ and there exists some W_1 where $W \sqsubseteq W_1$, $H_1^*, H_2^* : W_1$, and $(W_1, e_1^*, e_1^\dagger) \in \mathcal{V}[\![\tau_1]\!]_.$.

Since terms in the value relation are target values, the original pair will continue reducing on the second subexpression according to the operational semantics. To figure out what happens, we can appeal to the second induction hypothesis instantiated with $W_1, \gamma_\Gamma, \gamma_\Gamma, \gamma_2, \rho$, which we can do because $\mathcal{G}[\![\Gamma]\!]_\rho, \mathcal{G}[\![\Gamma]\!]_., \mathcal{G}[\![\Omega]\!]_.$ is closed under world extension (Lemma 2.3) and choosing heaps H_1^*, H_2^*. From that, we find that $\langle H_1^*, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, e_2{}^+)))\rangle$ either reduces to fail Conv, in which case the original pair steps to fail Conv, or to some irreducible configuration $\langle H_1^\dagger, e_2^*\rangle$, in which case on the other side, the configuration with H_2^* reduces to some irreducible configuration $\langle H_2^\dagger, e_2^\dagger\rangle$ and there exists some W_2 where $W_1 \sqsubseteq W_2$, $H_1^\dagger, H_2^\dagger : W_2$ and $(W_2, e_2^*, e_2^\dagger) \in \mathcal{V}[\![\tau_2]\!]_.$.

Thus, the original pair with H_1 steps to $\langle H_1^\dagger, (e_1^*, e_2^*)\rangle$ which is a value because both e_1^* and e_2^* are values. Moreover, the original pair with H_2 steps to $\langle H_2^\dagger, (e_1^\dagger, e_2^\dagger)\rangle \nrightarrow$. Ergo, we have $(W_2, e_1^*, e_1^\dagger) \in \mathcal{V}[\![\tau_1]\!]_.$ (because $(W_1, e_1^*, e_1^\dagger) \in \mathcal{V}[\![\tau_1]\!]_.$ and $W_1 \sqsubseteq W_2$) and $(W_2, e_2^*, e_2^\dagger) \in \mathcal{V}[\![\tau_2]\!]_.$, so $(W_2, (e_1^*, e_2^*), (e_1^\dagger, e_2^\dagger)) \in \mathcal{V}[\![\tau_1 \otimes \tau_2]\!]_.$. Finally, since $W \sqsubseteq W_1$ and $W \sqsubseteq W_2$, we have $W \sqsubseteq W_2$, which suffices to finish the proof. □

Lemma 2.47 (Compat let).

$$\begin{aligned}&\Delta_1;\Gamma_1;\Gamma;\Omega_1 \vdash e_1 \preceq e_1 : \tau_1 \otimes \tau_2 \rightsquigarrow \Delta_2;\Gamma_2 \wedge \Delta_2;\Gamma_2;\Gamma;\Omega_2, a : \tau_1, a' : \tau_2 \vdash e_2 \preceq e_2 : \tau \rightsquigarrow \Delta_3;\Gamma_3\\ &\quad\Longrightarrow \Delta_1;\Gamma_1;\Gamma;\Omega_1 \uplus \Omega_2 \vdash \mathrm{let}\ (a, a') = e_1\ \mathrm{in}\ e_2 \preceq \mathrm{let}\ (a, a') = e_1\ \mathrm{in}\ e_2 : \tau \rightsquigarrow \Delta_3;\Gamma_3\end{aligned}$$

Proof. Expanding the hypotheses, we find $\Delta_1 = \Delta_2 = \Delta_3$ and $\Gamma_1 = \Gamma_2 = \Gamma_3$. Moreover, $\Delta_1;\Gamma_1;\Gamma;\Omega_1 \uplus \Omega_2 \vdash \mathrm{let}\ (a, a') = e_1\ \mathrm{in}\ e_2 : \tau \rightsquigarrow \Delta_3;\Gamma_3$ by the let typing rule. Ergo, it suffices to show $\Delta_1;\Gamma_1;\Gamma;\Omega_1 \uplus \Omega_2 \vdash \mathrm{let}\ (a, a') = e_1\ \mathrm{in}\ e_2 \preceq \mathrm{let}\ (a, a') = e_1\ \mathrm{in}\ e_2 : \tau$.

Expanding the conclusion, we must show that given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_. \wedge (W, \gamma_\Omega) \in \mathcal{G}[\![\Omega_1 \uplus \Omega_2]\!]_.$$

we must show

$$\begin{gathered}(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{let}\ (a, a') = e_1\ \mathrm{in}\ e_2{}^+))),\\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{let}\ (a, a') = e_1\ \mathrm{in}\ e_2{}^+)))) \in \mathcal{E}[\![\tau]\!]_.\end{gathered}$$

Notice that both of these expressions have no free variables by Lemma 2.10.

We can push the compiler and substitutions through the let expression and refine this to:

$$\begin{gathered}(W,\\ \mathrm{let}\ x_{\mathrm{fresh}} = \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, e_1{}^+)))\ \mathrm{in}\ \mathrm{let}\ x'_{\mathrm{fresh}} = \mathrm{fst}\ x_{\mathrm{fresh}}\ \mathrm{in}\ \mathrm{let}\ x''_{\mathrm{fresh}} = \mathrm{snd}\ x_{\mathrm{fresh}}\ \mathrm{in}\\ \mathrm{let}\ a = \mathrm{thunk}(x'_{\mathrm{fresh}})\ \mathrm{in}\ \mathrm{let}\ a' = \mathrm{thunk}(x''_{\mathrm{fresh}})\ \mathrm{in}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, e_2{}^+))),\\ \mathrm{let}\ x_{\mathrm{fresh}} = \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, e_1{}^+)))\ \mathrm{in}\ \mathrm{let}\ x'_{\mathrm{fresh}} = \mathrm{fst}\ x_{\mathrm{fresh}}\ \mathrm{in}\ \mathrm{let}\ x''_{\mathrm{fresh}} = \mathrm{snd}\ x_{\mathrm{fresh}}\ \mathrm{in}\\ \mathrm{let}\ a = \mathrm{thunk}(x'_{\mathrm{fresh}})\ \mathrm{in}\ \mathrm{let}\ a' = \mathrm{thunk}(x''_{\mathrm{fresh}})\ \mathrm{in}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, e_2{}^+))),\\ \in \mathcal{E}[\![\tau]\!]_.\end{gathered}$$

Then, by Lemma 2.2, we find that $\gamma_\Omega = \gamma_1 \uplus \gamma_2$ where

$$(W, \gamma_1) \in \mathcal{G}[\![\Omega_1]\!].$$

and

$$(W, \gamma_2) \in \mathcal{G}[\![\Omega_2]\!].$$

and, for any $i \in \{1, 2\}$

$$\text{close}_i(\gamma_\Omega, \text{e}_1{}^+) = \text{close}_i(\gamma_1, \text{e}_1{}^+)$$

and

$$\text{close}_i(\gamma_\Omega, \text{e}_2{}^+) = \text{close}_i(\gamma_2, \text{e}_2{}^+)$$

Ergo, we can refine the above statement that we must prove to

$$\begin{gathered}(W,\\ \text{let x}_{\text{fresh}} = \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_1, \text{e}_1{}^+))) \text{ in let x}'_{\text{fresh}} = \text{fst x}_{\text{fresh}} \text{ in let x}''_{\text{fresh}} = \text{snd x}_{\text{fresh}} \text{ in}\\ \text{let a} = \text{thunk}(\text{x}'_{\text{fresh}}) \text{ in let a}' = \text{thunk}(\text{x}''_{\text{fresh}}) \text{ in close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_2, \text{e}_2{}^+))),\\ \text{let x}_{\text{fresh}} = \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_1, \text{e}_1{}^+))) \text{ in let x}'_{\text{fresh}} = \text{fst x}_{\text{fresh}} \text{ in let x}''_{\text{fresh}} = \text{snd x}_{\text{fresh}} \text{ in}\\ \text{let a} = \text{thunk}(\text{x}'_{\text{fresh}}) \text{ in let a}' = \text{thunk}(\text{x}''_{\text{fresh}}) \text{ in close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_2, \text{e}_2{}^+))))\\ \in \mathcal{E}[\![\tau]\!].\end{gathered}$$

Expanding the expression relation definition, we must show that given

$$\forall \text{H}_1, \text{H}_2{:}W,\ \text{e}'_1,\ \text{H}'_1,\ j < W.k.$$

$$\begin{gathered}\langle \text{H}_1, \text{let x}_{\text{fresh}} = \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_1, \text{e}_1{}^+))) \text{ in let x}'_{\text{fresh}} = \text{fst x}_{\text{fresh}} \text{ in let x}''_{\text{fresh}} = \text{snd x}_{\text{fresh}} \text{ in}\\ \text{let a} = \text{thunk}(\text{x}'_{\text{fresh}}) \text{ in let a}' = \text{thunk}(\text{x}''_{\text{fresh}}) \text{ in close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_2, \text{e}_2{}^+)))\rangle \xrightarrow{j} \langle \text{H}'_1, \text{e}'_1\rangle \nrightarrow\end{gathered}$$

we must show either $\text{e}'_1 = \text{fail } \textsc{Conv}$ or there exist $\text{v}_2, \text{H}'_2, W'$ such that:

$$\begin{gathered}\langle \text{H}_2, \text{let x}_{\text{fresh}} = \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_1, \text{e}_1{}^+))) \text{ in let x}'_{\text{fresh}} = \text{fst x}_{\text{fresh}} \text{ in let x}''_{\text{fresh}} = \text{snd x}_{\text{fresh}} \text{ in}\\ \text{let a} = \text{thunk}(\text{x}'_{\text{fresh}}) \text{ in let a}' = \text{thunk}(\text{x}''_{\text{fresh}}) \text{ in close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_2, \text{e}_2{}^+)))\rangle \xrightarrow{*} \langle \text{H}'_2, \text{v}_2\rangle\\ \wedge W \sqsubseteq W' \wedge \text{H}'_1, \text{H}'_2 : W' \wedge (W', \text{e}'_1, \text{v}_2) \in \mathcal{V}[\![\tau_1]\!]_\rho\end{gathered}$$

Next, we need to find e'_1. From the operational semantic, the let will run the first subexpression using the heap H_1 until it reaches a target value or gets stuck. By appealing to our first induction hypothesis, instantiated with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_1, \rho$, we find that:

$$(W, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_1, \text{e}_1{}^+))), \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_1, \text{e}_1{}^+)))) \in \mathcal{E}[\![\tau_1 \otimes \tau_2]\!].$$

We can instantiate this with the heaps H_1, H_2 to find that $\langle \text{H}_1, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_1, \text{e}_1{}^+)))\rangle$ either reduces to fail $\textsc{Conv}$, in which case the original expression steps to fail $\textsc{Conv}$, or to some irreducible configuration $\langle \text{H}^*_1, \text{e}^*_1\rangle$, in which case on the other side, the configuration reduces to some irreducible configuration $\langle \text{H}^*_2, \text{e}^\dagger_1\rangle$ and there exists some W_1 where $W \sqsubseteq W_1, \text{H}^*_1, \text{H}^*_2 : W_1$, and $(W_1, \text{e}^*_1, \text{e}^\dagger_1) \in \mathcal{V}[\![\tau_1 \otimes \tau_2]\!]$..

By expanding the value relation, we find that $\text{e}^*_1 = (\text{v}^*_1, \text{v}^*_2)$ and $\text{e}^\dagger_1 = (\text{v}^\dagger_1, \text{v}^\dagger_2)$ where $(W_1, \text{v}^*_1, \text{v}^\dagger_1) \in \mathcal{V}[\![\tau_1]\!]$. and $(W_1, \text{v}^*_2, \text{v}^\dagger_2) \in \mathcal{V}[\![\tau_2]\!]$.. Thus, the original configuration with H_1 steps as follows:

$$\begin{aligned}&\langle \text{H}_1, \text{let x}_{\text{fresh}} = \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_1, \text{e}_1{}^+))) \text{ in let x}'_{\text{fresh}} = \text{fst x}_{\text{fresh}} \text{ in let x}''_{\text{fresh}} = \text{snd x}_{\text{fresh}} \text{ in}\\ &\quad \text{let a} = \text{thunk}(\text{x}'_{\text{fresh}}) \text{ in let a}' = \text{thunk}(\text{x}''_{\text{fresh}}) \text{ in close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_2, \text{e}_2{}^+)))\rangle \xrightarrow{*}\\ &\langle \text{H}_1, \text{let x}_{\text{fresh}} = (\text{v}^*_1, \text{v}^*_2) \text{ in let x}'_{\text{fresh}} = \text{fst x}_{\text{fresh}} \text{ in let x}''_{\text{fresh}} = \text{snd x}_{\text{fresh}} \text{ in}\\ &\quad \text{let a} = \text{thunk}(\text{x}'_{\text{fresh}}) \text{ in let a}' = \text{thunk}(\text{x}''_{\text{fresh}}) \text{ in close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_2, \text{e}_2{}^+)))\rangle \xrightarrow{*}\\ &\langle \text{H}_1, \text{let a} = \text{thunk}(\text{v}^*_1) \text{ in let a}' = \text{thunk}(\text{v}^*_2) \text{ in close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_2, \text{e}_2{}^+)))\rangle \xrightarrow{*}\\ &\langle \text{H}^*_1[\ell^*_1 \mapsto \textsc{unused}, \ell^*_2 \mapsto \textsc{unused}],\\ &\quad [\text{a} \mapsto \text{guard}(\text{v}^*_1, \ell^*_1), \text{a}' \mapsto \text{guard}(\text{v}^*_2, \ell^*_2)]\text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_2, \text{e}_2{}^+)))\rangle\end{aligned}$$

for some $\ell_1^*, \ell_2^* \notin \mathrm{H}_1^*$. By similar reasoning, the configuraton on the other side with H_2 steps to

$$\begin{aligned}&\langle \mathrm{H}_2^*[\ell_1^\dagger \mapsto \textsc{unused}, \ell_2^\dagger \mapsto \textsc{unused}],\\ &\quad [\mathrm{a} \mapsto \mathrm{guard}(\mathrm{v}_1^\dagger, \ell_1^\dagger), \mathrm{a}' \mapsto \mathrm{guard}(\mathrm{v}_2^\dagger, \ell_2^\dagger)]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e}_2{}^+)))\rangle\end{aligned}$$

for some $\ell_1^\dagger, \ell_2^\dagger \notin \mathrm{H}_2^*$.

Notice that, since $\ell_1^*, \ell_2^* \notin \mathrm{H}_1^*$ and $\ell_1^\dagger, \ell_2^\dagger \notin \mathrm{H}_2^*$, $(\ell_1^*, \ell_1^\dagger)$ and $(\ell_2^*, \ell_2^\dagger)$ are disjoint from $\mathrm{dom}(W_1.\Psi) \cup \mathrm{dom}(W_1.\Theta)$. Therefore, we can define the world

$$W_2 = (W_1.k, W_1.\Psi, W_1.\Theta \uplus (\ell_1^*, \ell_1^\dagger) \mapsto \textsc{unused}, (\ell_2^*, \ell_2^\dagger) \mapsto \textsc{unused})$$

One can see that $\mathrm{H}_1^*[\ell_1^* \mapsto \textsc{unused}, \ell_2^* \mapsto \textsc{unused}], \mathrm{H}_2^*[\ell_1^\dagger \mapsto \textsc{unused}, \ell_2^\dagger \mapsto \textsc{unused}] : W_2$ because $\mathrm{H}_1, \mathrm{H}_2 : W_1$, and W_2 is nothing but W_1 with some new affine flags, which are satisfied by these new heaps. Moreover, we have $W_1 \sqsubseteq W_2$, because W_2 satisfies the same heap typing as W_1 and all of the affine flags that are in W_1.

Next, notice that

$$(W_2, \gamma_2[\mathrm{a} \mapsto (\mathrm{guard}(\mathrm{v}_1^*, \ell_1^*), \mathrm{guard}(\mathrm{v}_1^\dagger, \ell_1^\dagger)), \mathrm{a}' \mapsto (\mathrm{guard}(\mathrm{v}_2^*, \ell_2^*), \mathrm{guard}(\mathrm{v}_2^\dagger, \ell_2^\dagger))]) \in \mathcal{G}\llbracket \Omega_2, \mathrm{a} : \tau_1, \mathrm{a}' : \tau_2 \rrbracket.$$

because $(\ell_1^*, \ell_1^\dagger), (\ell_2^*, \ell_2^\dagger) \in \mathrm{dom}(W_2.\Theta)$, $(W_2, \gamma_2) \in \mathcal{G}\llbracket \Omega_2 \rrbracket_.$ (since $(W, \gamma_2) \in \mathcal{G}\llbracket \Omega_2 \rrbracket_.$ and $W \sqsubseteq W_1 \sqsubseteq W_2$), $(W_2, \mathrm{v}_1^*, \mathrm{v}_1^\dagger) \in \mathcal{V}\llbracket \tau_1 \rrbracket_.$ (by $W_1 \sqsubseteq W_2$ and Lemma 2.3), and $(W_2, \mathrm{v}_2^*, \mathrm{v}_2^\dagger) \in \mathcal{V}\llbracket \tau_2 \rrbracket_.$ (again by $W_1 \sqsubseteq W_2$ and Lemma 2.3).

Therefore, we can instantiate the second induction hypothesis with

$$W_2, \gamma_\Gamma, \gamma_\Gamma, \gamma_2[\mathrm{a} \mapsto (\mathrm{guard}(\mathrm{v}_1^*, \ell_1^*), \mathrm{guard}(\mathrm{v}_1^\dagger, \ell_1^\dagger)), \mathrm{a}' \mapsto (\mathrm{guard}(\mathrm{v}_2^*, \ell_2^*), \mathrm{guard}(\mathrm{v}_2^\dagger, \ell_2^\dagger))], \rho$$

to find that

$$\begin{aligned}&(W_2, [\mathrm{a} \mapsto \mathrm{guard}(\mathrm{v}_1^*, \ell_1^*), \mathrm{a}' \mapsto \mathrm{guard}(\mathrm{v}_2^*, \ell_2^*)]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e}_2{}^+))),\\ &\quad [\mathrm{a} \mapsto \mathrm{guard}(\mathrm{v}_1^\dagger, \ell_1^\dagger), \mathrm{a}' \mapsto \mathrm{guard}(\mathrm{v}_2^\dagger, \ell_2^\dagger)]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e}_2{}^+)))) \in \mathcal{E}\llbracket \tau \rrbracket_.\end{aligned}$$

Then, consider again the following configurations:

$$\begin{aligned}&\langle \mathrm{H}_1^*[\ell_1^* \mapsto \textsc{unused}, \ell_2^* \mapsto \textsc{unused}],\\ &\quad [\mathrm{a} \mapsto \mathrm{guard}(\mathrm{v}_1^*, \ell_1^*), \mathrm{a}' \mapsto \mathrm{guard}(\mathrm{v}_2^*, \ell_2^*)]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e}_2{}^+)))\rangle\end{aligned}$$

$$\begin{aligned}&\langle \mathrm{H}_2^*[\ell_1^\dagger \mapsto \textsc{unused}, \ell_2^\dagger \mapsto \textsc{unused}],\\ &\quad [\mathrm{a} \mapsto \mathrm{guard}(\mathrm{v}_1^\dagger, \ell_1^\dagger), \mathrm{a}' \mapsto \mathrm{guard}(\mathrm{v}_2^\dagger, \ell_2^\dagger)]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e}_2{}^+)))\rangle\end{aligned}$$

Since these heaps satisfy W_2, we have that the first configuration either steps to fail Conv, in which case the original configuration with H_1 steps to fail Conv, or steps to some irreducible configuration $\langle \mathrm{H}_1^\dagger, \mathrm{e}_\mathrm{f}^* \rangle$, in which case the second configuration steps to an irreducible configuration $\langle \mathrm{H}_2^\dagger, \mathrm{e}_\mathrm{f}^\dagger \rangle$ and there exists some W_3 such that $W_2 \sqsubseteq W_3$, $\mathrm{H}_1^\dagger, \mathrm{H}_2^\dagger : W_3$, and $(W_3, \mathrm{e}_\mathrm{f}^*, \mathrm{e}_\mathrm{f}^\dagger) \in \mathcal{V}\llbracket \tau \rrbracket_.$. Finally, since $W \sqsubseteq W_1$, $W_1 \sqsubseteq W_2$, and $W_2 \sqsubseteq W_3$, we have $W \sqsubseteq W_3$, which suffices to finish the proof. □

Lemma 2.48 (Compat $\llparenthesis \mathrm{e} \rrparenthesis_\tau$).

$$\Delta = \Delta' \wedge \Gamma = \Gamma' \wedge \Gamma; \Omega; \Delta; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \tau \rightsquigarrow \Gamma; \Omega' \wedge \tau \sim \tau \implies \Delta; \Gamma; \Gamma; \Omega \vdash \llparenthesis \mathrm{e} \rrparenthesis_\tau \preceq \llparenthesis \mathrm{e} \rrparenthesis_\tau : \tau \rightsquigarrow \Delta'; \Gamma'$$

Proof. Expanding the third hypothesis, there exists some Ω_e such that $\Omega = \Omega_\mathrm{e} \uplus \Omega'$ and $\Gamma; \Omega_\mathrm{e}; \Delta; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \tau$.

We have $\Delta = \Delta'$ and $\Gamma = \Gamma'$ by the first two assumptions. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash \llparenthesis \mathrm{e} \rrparenthesis_\tau : \tau \rightsquigarrow \Delta'; \Gamma'$ by the conversion typing rule. Thus, to prove the conclusion, it suffices to show $\Delta; \Gamma; \Gamma; \Omega \vdash \llparenthesis \mathrm{e} \rrparenthesis_\tau \preceq \llparenthesis \mathrm{e} \rrparenthesis_\tau : \tau$. Expanding this conclusion, we must show that given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}\llbracket \Delta \rrbracket \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho \wedge (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_. \wedge (W, \gamma_\Omega) \in \mathcal{G}\llbracket \Omega \rrbracket_.$$

then

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, (\!|\mathsf{e}|\!)_\tau{}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, (\!|\mathsf{e}|\!)_\tau{}^+)))) \in \mathcal{E}[\![\tau]\!].$$

We can push the compiler and substitutions through the pair to refine that to:

$$(W, C_{\tau \mapsto \tau}(\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+)))), C_{\tau \mapsto \tau}(\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+))))) \in \mathcal{E}[\![\tau]\!].$$

Then, by Lemma 2.2, we find that $\gamma_\Omega = \gamma_1 \uplus \gamma_2$ where

$$(W, \gamma_1) \in \mathcal{G}[\![\Omega_{\mathsf{e}}]\!].$$

and

$$(W, \gamma_2) \in \mathcal{G}[\![\Omega']\!].$$

and, for any $i \in \{1, 2\}$

$$\mathrm{close}_i(\gamma_\Omega, \mathsf{e}) = \mathrm{close}_i(\gamma_1, \mathsf{e})$$

Now, by instantiating our induction hypothesis with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_1, \rho$, we find that:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathsf{e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathsf{e}^+)))) \in \mathcal{E}[\![\tau]\!]_\rho$$

By Lemma 2.8, it follows that:

$$(W, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathsf{e}^+))), \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathsf{e}^+)))) \in \mathcal{E}[\![\tau]\!].$$

Therefore, by Theorem 2.12, we have

$$(W, C_{\tau \mapsto \tau}(\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathsf{e}^+)))), C_{\tau \mapsto \tau}(\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathsf{e}^+))))) \in \mathcal{E}[\![\tau]\!].$$

as was to be proven. □

3 CASE STUDY: AFFINE WITH DYNAMIC SAFETY, EFFICIENTLY

In this case study, we consider the same two languages as the previous case study, but we consider how to make the resulting compilers more efficient. In particular, we want to only enforce affine types dynamically when necessary: when we statically know that they are okay, we don't want to introduce the overhead of thunks.

We do this by introducing a distinction in AFFI, between statically enforced affine arrows, written $\tau \mathrel{-\!\!\bullet} \tau$, and dynamically enforced ones, written $\tau \multimap \tau$. These come with corresponding static and dynamic affine variables.

Since, semantically, there is no difference between the two (indeed, this is only about improving efficiency), we need not present this language on the surface to users. Instead, the placement of the dynamic arrows could be inferred based on a simple taint algorithm: any arrow converted to or from `MiniML` must be a dynamic arrow, and everything else can remain static.

3.1 `MiniML` Language

$$
\begin{array}{lcl}
\text{Type } \tau & := & \mathtt{unit} \mid \mathtt{int} \mid \tau \times \tau \mid \tau + \tau \mid \tau \to \tau \mid \forall \alpha.\tau \mid \alpha \mid \mathtt{ref}\ \tau \\
\text{Expression } \mathtt{e} & := & () \mid \mathbb{Z} \mid \mathtt{x} \mid (\mathtt{e}, \mathtt{e}) \mid \mathtt{fst}\ \mathtt{e} \mid \mathtt{snd}\ \mathtt{e} \mid \mathtt{inl}\ \mathtt{e} \mid \mathtt{inr}\ \mathtt{e} \mid \mathtt{match}\ \mathtt{e}\ \mathtt{x}\{\mathtt{e}\}\ \mathtt{y}\{\mathtt{e}\} \\
 & & \mid \lambda \mathtt{x} : \tau.\mathtt{e} \mid \mathtt{e}\ \mathtt{e} \mid \Lambda \alpha.\mathtt{e} \mid \mathtt{e}[\tau] \mid \mathtt{ref}\ \mathtt{e} \mid \mathtt{!e} \mid \mathtt{e} := \mathtt{e} \mid \llparenthesis \mathrm{e} \rrparenthesis_{\tau}
\end{array}
$$

Our syntax is identical to the previous section, so is most of our static semantics, which we elide. The only typing rule which is different is the typing rule for foreign terms, which now requires that the AFFI term inside the conversion has no free static variables:

$$
\frac{\Gamma; \Omega; \Delta; \Gamma \vdash \mathrm{e} : \tau \leadsto \mathfrak{C}' \qquad \mathrm{no}_{\bullet}(\Omega) \qquad \_ : \tau \sim \tau}{\Gamma; \Omega; \Delta; \Gamma \vdash \llparenthesis \mathrm{e} \rrparenthesis_{\tau} : \tau \leadsto \mathfrak{C}'}
$$

3.2 AFFI Language

$$
\begin{array}{lcl}
\tau & ::= & \mathrm{unit} \mid \mathrm{bool} \mid \mathrm{int} \mid \tau \multimap \tau \mid \tau \mathrel{-\!\!\bullet} \tau \mid !\tau \mid \tau \& \tau \mid \tau \otimes \tau \\
\mathrm{e} & ::= & () \mid \mathrm{true} \mid \mathrm{false} \mid \mathrm{n} \mid \mathrm{x} \mid \mathrm{a}_{\circ} \mid \mathrm{a}_{\bullet} \mid \lambda \mathrm{a}_{\LEFTcircle} : \tau.\mathrm{e} \mid \mathrm{e}\ \mathrm{e} \mid \llparenthesis \mathtt{e} \rrparenthesis_{\tau} \mid !\mathrm{v} \mid \mathrm{let}\ !\mathrm{x} = \mathrm{e}\ \mathrm{in}\ \mathrm{e}' \mid \\
 & & \langle \mathrm{e}, \mathrm{e}' \rangle \mid \mathrm{e}.1 \mid \mathrm{e}.2 \mid (\mathrm{e}, \mathrm{e}) \mid \mathrm{let}\ (\mathrm{a}_{\bullet}, \mathrm{a}'_{\bullet}) = \mathrm{e}\ \mathrm{in}\ \mathrm{e}' \\
\mathrm{v} & ::= & () \mid \lambda \mathrm{a}_{\LEFTcircle} : \tau.\mathrm{e} \mid !\mathrm{v} \mid \langle \mathrm{e}, \mathrm{e}' \rangle \mid (\mathrm{v}, \mathrm{v}') \\
\LEFTcircle & ::= & \circ \mid \bullet
\end{array}
$$

Here, our rules are nearly the same, as we don't need to change anything aside from propagating the dynamic/static annotation from lambdas into our affine environment, so that variables can be compiled correctly.

$$\dfrac{a_{\circ} : \tau \in \Omega}{\mathfrak{C}; \Gamma; \Omega \vdash a_{\circ} : \tau \rightsquigarrow \mathfrak{C}} \qquad \dfrac{a_{\bullet} : \tau \in \Omega}{\mathfrak{C}; \Gamma; \Omega \vdash a_{\bullet} : \tau \rightsquigarrow \mathfrak{C}} \qquad \dfrac{x : \tau \in \Gamma}{\mathfrak{C}; \Gamma; \Omega \vdash x : \tau \rightsquigarrow \mathfrak{C}} \qquad \dfrac{}{\mathfrak{C}; \Gamma; \Omega \vdash () : \mathrm{unit} \rightsquigarrow \mathfrak{C}}$$

$$\dfrac{}{\mathfrak{C}; \Gamma; \Omega \vdash n : \mathrm{int} \rightsquigarrow \mathfrak{C}} \qquad \dfrac{}{\mathfrak{C}; \Gamma; \Omega \vdash \mathrm{true} : \mathrm{bool} \rightsquigarrow \mathfrak{C}} \qquad \dfrac{}{\mathfrak{C}; \Gamma; \Omega \vdash \mathrm{false} : \mathrm{bool} \rightsquigarrow \mathfrak{C}}$$

$$\dfrac{\mathfrak{C}; \Gamma; \Omega[a_{\circ} := \tau_1] \vdash e : \tau_2 \rightsquigarrow \mathfrak{C}' \qquad \mathrm{no}_{\bullet}(\Omega)}{\mathfrak{C}; \Gamma; \Omega \vdash \lambda a_{\circ} : \tau_1.e : \tau_1 \multimap \tau_2 \rightsquigarrow \mathfrak{C}'} \qquad \dfrac{\mathfrak{C}; \Gamma; \Omega[a_{\bullet} := \tau_1] \vdash e : \tau_2 \rightsquigarrow \mathfrak{C}'}{\mathfrak{C}; \Gamma; \Omega \vdash \lambda a_{\bullet} : \tau_1.e : \tau_1 \mathrel{-\!\!\bullet} \tau_2 \rightsquigarrow \mathfrak{C}'}$$

$$\dfrac{\Omega = \Omega_1 \uplus \Omega_2 \qquad \mathfrak{C}_1; \Gamma; \Omega_1 \vdash e_1 : \tau_1 \multimap \tau_2 \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2; \Gamma; \Omega_2 \vdash e_2 : \tau_1 \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1; \Gamma; \Omega \vdash e_1\ e_2 : \tau_2 \rightsquigarrow \mathfrak{C}_3}$$

$$\dfrac{\Omega = \Omega_1 \uplus \Omega_2 \qquad \mathfrak{C}_1; \Gamma; \Omega_1 \vdash e_1 : \tau_1 \mathrel{-\!\!\bullet} \tau_2 \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2; \Gamma; \Omega_2 \vdash e_2 : \tau_1 \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1; \Gamma; \Omega \vdash e_1\ e_2 : \tau_2 \rightsquigarrow \mathfrak{C}_3}$$

$$\dfrac{\mathfrak{C}; \Gamma; \cdot \vdash v : \tau \rightsquigarrow \mathfrak{C}'}{\mathfrak{C}; \Gamma; \cdot \vdash !v : !\tau \rightsquigarrow \mathfrak{C}'}$$

$$\dfrac{\Omega = \Omega_1 \uplus \Omega_2 \qquad \mathfrak{C}_1; \Gamma; \Omega_1 \vdash e : !\tau \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2; \Gamma[x := \tau]; \Omega_2 \vdash e' : \tau' \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1; \Gamma; \Omega \vdash \mathrm{let}\ !x = e\ \mathrm{in}\ e' \rightsquigarrow \mathfrak{C}_3}$$

$$\dfrac{\mathfrak{C}_1; \Gamma; \Omega \vdash e_1 : \tau_1 \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2; \Gamma; \Omega \vdash e_2 : \tau_2 \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1; \Gamma; \Omega \vdash \langle e_1, e_2 \rangle : \tau_1 \& \tau_2 \rightsquigarrow \mathfrak{C}_3} \qquad \dfrac{\mathfrak{C}; \Gamma; \Omega \vdash e : \tau_1 \& \tau_2 \rightsquigarrow \mathfrak{C}'}{\mathfrak{C}; \Gamma; \Omega \vdash e.1 : \tau_1 \rightsquigarrow \mathfrak{C}'}$$

$$\dfrac{\mathfrak{C}; \Gamma; \Omega \vdash e : \tau_1 \& \tau_2 \rightsquigarrow \mathfrak{C}'}{\mathfrak{C}; \Gamma; \Omega \vdash e.2 : \tau_2 \rightsquigarrow \mathfrak{C}'}$$

$$\dfrac{\Omega = \Omega_1 \uplus \Omega_2 \qquad \mathfrak{C}_1; \Gamma; \Omega_1 \vdash e_1 : \tau_1 \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2; \Gamma; \Omega_2 \vdash e_2 : \tau_2 \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1; \Gamma; \Omega \vdash (e_1, e_2) : \tau_1 \otimes \tau_2 \rightsquigarrow \mathfrak{C}_3}$$

$$\dfrac{\Omega = \Omega_1 \uplus \Omega_2 \qquad \mathfrak{C}_1; \Gamma; \Omega_1 \vdash e : \tau_1 \otimes \tau_2 \rightsquigarrow \mathfrak{C}_2 \qquad \mathfrak{C}_2; \Gamma; \Omega_2[a := \tau_1, a' := \tau_1] \vdash e' : \tau' \rightsquigarrow \mathfrak{C}_3}{\mathfrak{C}_1; \Gamma; \Omega \vdash \mathrm{let}\ (a_{\bullet}, a'_{\bullet}) = e\ \mathrm{in}\ e' : \tau' \rightsquigarrow \mathfrak{C}_3}$$

$$\dfrac{\mathfrak{C}; \Gamma; \Omega \vdash \mathsf{e} : \tau \rightsquigarrow \mathfrak{C}' \qquad \_ : \tau \sim \tau}{\mathfrak{C}; \Gamma; \Omega \vdash (\!|\mathsf{e}|\!)_{\tau} : \tau \rightsquigarrow \mathfrak{C}'}$$

3.3 Compilers

Our compiler for `MiniML` is identical to the previous section, as what we are changing is optimizations within Affi.

For Affi, the biggest difference, of course, is in the different modalities of arrows and variables. The dynamic ones are treated similarly to our previous case study, whereas for static ones, we can erase all traces of affinity, since we know statically they will only be used at most once.

$$\mathsf{thunk}(e) \triangleq \mathsf{let}\ r_{\mathsf{fresh}} = \mathsf{ref}\ 1\ \mathsf{in}\ \lambda\_.\{\mathsf{if}\ !r_{\mathsf{fresh}}\ \{\mathsf{fail}\ \textsc{Conv}\}\ \{r_{\mathsf{fresh}} := 0; e\}\}$$

$$\begin{array}{lll}
() & \leadsto & () \\
\mathrm{true} & \leadsto & 0 \\
\mathrm{false} & \leadsto & 1 \\
x & \leadsto & x \\
a_\circ & \leadsto & a\ () \\
a_\bullet & \leadsto & a_\bullet \\
\lambda a_\circ : \tau.e & \leadsto & \lambda a.\{e^+\} \\
\lambda a_\bullet : \tau.e & \leadsto & \lambda a_\bullet.\{e^+\} \\
(e_1 : \tau_1 \multimap \tau_2)\ e_2 & \leadsto & {e_1}^+\ (\mathsf{let}\ x = {e_2}^+\ \mathsf{in}\ \mathsf{thunk}(x)) \\
(e_1 : \tau_1 \multimapdot \tau_2)\ e_2 & \leadsto & {e_1}^+\ {e_2}^+ \\
!v & \leadsto & v^+ \\
\mathrm{let}\ !x = e\ \mathrm{in}\ e' & \leadsto & \mathsf{let}\ x = e^+\ \mathsf{in}\ e'^+ \\
\langle e, e' \rangle & \leadsto & (\lambda\_.\{e^+\}, \lambda\_.\{e'^+\}) \\
e.1 & \leadsto & (\mathsf{fst}\ e^+)\ () \\
e.2 & \leadsto & (\mathsf{snd}\ e^+)\ () \\
(e, e') & \leadsto & (e^+, e'^+) \\
\mathrm{let}\ (a_\bullet, a'_\bullet) = e\ \mathrm{in}\ e' & \leadsto & \mathsf{let}\ x_{\mathsf{fresh}} = e^+\ \mathsf{in}\ \mathsf{let}\ a_\bullet = \mathsf{fst}\ x_{\mathsf{fresh}}\ \mathsf{in}\ \mathsf{let}\ a'_\bullet = \mathsf{snd}\ x_{\mathsf{fresh}}\ \mathsf{in}\ e'^+ \\
(\!| \mathtt{e} : \tau |\!)_\tau & \leadsto & C_{\tau \mapsto \tau}(e^+)
\end{array}$$

3.4 Convertibility

Convertibility is similar to the previous case study, except that we translate MiniML functions to our dynamic arrows (the only one shown here – the rest are the same as before), as the semantics of enforcing affine types onto MiniML code requires we do it dynamically.

$$\frac{C_{\tau_1 \mapsto \tau_1}, C_{\tau_1 \mapsto \tau_1} : \tau_1 \sim \tau_1 \qquad C_{\tau_2 \mapsto \tau_2}, C_{\tau_2 \mapsto \tau_2} : \tau_2 \sim \tau_2}{C_{\tau_1 \multimap \tau_2 \mapsto (\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2}, C_{(\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2 \mapsto \tau_1 \multimap \tau_2} : \tau_1 \multimap \tau_2 \sim (\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2}$$

The wrapper boundaries are the same as before. Note, of course, that we cannot convert to a static arrow, as that would be unsound.

3.5 Logical Relation

For the logical relation, we define an augmented phantom operational semantics. This involves three things:

First, we add one phantom term to our LCVM language:

$$\text{Expressions } e \quad := \quad \ldots \mathrm{protect}(e, f)$$

Second, we augment all of the rules of the operational semantics to include the phantom flag set Φ in the machine configurations, threading them through.

Third, we add one rule for our new term, that uses the phantom flag set:

$$\langle \Phi \uplus \{f\}, H, \mathrm{protect}(e, f) \rangle \dashrightarrow \langle \Phi, H, e \rangle$$

Fourth, we modify two rules so that, whenever a binding annotated with $\bullet$ is substituted with a value, the value is protected by a flag.

$$\frac{f \text{ fresh}}{\langle \Phi, \mathrm{H}, \mathrm{let}\ \mathrm{a}_\bullet = \mathrm{v}\ \mathrm{in}\ \mathrm{e}\rangle \dashrightarrow \langle \Phi \uplus \{f\}, \mathrm{H}, [\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{v}, f)]\mathrm{e}\rangle}$$

$$\frac{f \text{ fresh}}{\langle \Phi, \mathrm{H}, \lambda \mathrm{a}_\bullet.\mathrm{e}\ \mathrm{v}\rangle \dashrightarrow \langle \Phi \uplus \{f\}, \mathrm{H}, [\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{v}, f)]\mathrm{e}\rangle}$$

Note that we write ⇢ for steps in our augmented phantom operational semantics, and will show later that if a term reduces in this phantom semantics, it reduces to the same thing in the normal semantics. As you can see, our phantom operational semantics exactly mirrors what we do in the true operational semantics for the dynamic case – but this is very different, as what in the dynamic case is perfectly acceptable dynamic failure corresponds to terms that are not in the relation at all (as they would get stuck when trying to run using the phantom semantics). In this way, our phantom flags are a purely logical construct to capture the same invariants that the dynamics enforce at runtime.

$$\begin{aligned} \mathit{World}_n = \{(k, \Psi, \Theta) \mid \quad & k < n \land \Psi \subset \mathit{HeapTy}_k \land \mathrm{dom}(\Psi)\#\mathrm{dom}(\Theta) \\ & \land (\forall (\ell_1, \ell_2) \mapsto (\Phi_1, \Phi_2), (\ell_1', \ell_2') \mapsto (\Phi_1', \Phi_2') \in \Theta. \\ & \quad (\ell_1, \ell_2) \neq (\ell_1', \ell_2') \implies \Phi_1 \cap \Phi_1' = \Phi_2 \cap \Phi_2' = \emptyset)\}\} \end{aligned}$$

$$\mathit{World} = \bigcup_n \mathit{World}_n$$

$$\mathit{HeapTy}_n = \{(\ell_1, \ell_2) \mapsto \mathit{Typ}_n, \ldots\}$$

Below, we write USED for 0 and UNUSED for 1.

$$\Theta = \{(\ell_1, \ell_2) \mapsto \textsc{used}\} \cup \{(\ell_1, \ell_2) \mapsto (\Phi_1, \Phi_2)\}$$

$$\Phi = \{f\}$$

For any $i \in \{1, 2\}$,

$$\mathrm{flags}(W, i) = \bigcup_{(\ell_1,\ell_2) \mapsto (\Phi_1,\Phi_2) \in W.\Theta} \Phi_i$$

$$\Phi_1, \Phi_2 : W \triangleq \forall i \in \{1, 2\}. \Phi_i \# \mathrm{flags}(W, i)$$

$$\mathit{Atom}_n = \{(W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \mid W \in \mathit{World}_n \land \Phi_1, \Phi_2 : W\}$$

$$\mathit{AtomVal}_n = \{(W, (\Phi_1, \mathrm{v}_1), (\Phi_2, \mathrm{v}_2)) \in \mathit{Atom}_n\}$$

$$\mathit{Atom} = \bigcup_n \mathit{Atom}_n$$

$$\mathit{AtomVal} = \bigcup_n \mathit{AtomVal}_n$$

$$\mathit{Typ}_n = \{R \in 2^{\mathit{AtomVal}_n} \mid \forall (W, (\Phi_1, \mathrm{v}_1), (\Phi_2, \mathrm{v}_2)) \in R. \forall W'. W \sqsubseteq_{\Phi_1,\Phi_2} W' \implies (W', (\Phi_1, \mathrm{v}_1), (\Phi_2, \mathrm{v}_2)) \in R\}$$
$$\mathit{Typ} = \{R \in 2^{\mathit{AtomVal}} \mid \forall k. \lfloor R \rfloor_k \in \mathit{Typ}_k\}$$

$$\mathit{UnrTyp} = \{R \in \mathit{Typ} \mid \forall (W, (\Phi_1, \mathrm{v}_1), (\Phi_2, \mathrm{v}_2)) \in R. \Phi_1 = \Phi_2 = \emptyset\}$$

$$
\begin{array}{lll}
(k, \Psi, \Theta) \sqsubseteq_{\Phi_1,\Phi_2} (j, \Psi', \Theta') & \triangleq & (j, \Psi', \Theta') \in World_j \\
& & \land\, j \leq k \\
& & \land\, \forall(\ell_1, \ell_2) \in \mathrm{dom}(\Psi).\lfloor \Psi(\ell_1, \ell_2) \rfloor_j = \Psi'(\ell_1, \ell_2) \\
& & \land\, \forall(\ell_1, \ell_2) \in \mathrm{dom}(\Theta).(\ell_1, \ell_2) \in \mathrm{dom}(\Theta') \land \\
& & \quad (\Theta(\ell_1, \ell_2) = \textsc{used} \implies \Theta'(\ell_1, \ell_2) = \textsc{used}) \land \\
& & \quad (\Theta(\ell_1, \ell_2) = (\Phi_1, \Phi_2) \implies \Theta'(\ell_1, \ell_2) = \textsc{used} \lor \Theta'(\ell_1, \ell_2) = (\Phi_1, \Phi_2)) \\
& & \land\, \Phi_1, \Phi_2 : (k, \Psi, \Theta) \\
& & \land\, \Phi_1, \Phi_2 : (j, \Psi', \Theta')
\end{array}
$$

$$W_1 \sqsubset_{\Phi_1,\Phi_2} W_2 \triangleq W_1.k > W_2.k \land W_1 \sqsubseteq_{\Phi_1,\Phi_2} W_2$$

$$\mathsf{H} = \{\ell \mapsto v\}$$

$$
\begin{gathered}
\mathsf{H}_1, \mathsf{H}_2 : W \triangleq \\
(\forall(\ell_1, \ell_2) \mapsto R \in W.\Psi.\ (\triangleright W, \mathsf{H}_1(\ell_1), \mathsf{H}_2(\ell_2)) \in R) \\
\land\ (\forall(\ell_1, \ell_2) \mapsto \textsc{used} \in W.\Theta.\forall i \in \{1, 2\}.\ \mathsf{H}_i(\ell_i) = \textsc{used}) \\
\land\ (\forall(\ell_1, \ell_2) \mapsto (\Phi_1, \Phi_2) \in W.\Theta.\forall i \in \{1, 2\}.\ \mathsf{H}_i(\ell_i) = \textsc{unused})
\end{gathered}
$$

$$
\begin{array}{l}
\mathcal{E}[\![\tau]\!]_\rho = \{(W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \mid \mathrm{freevars}(\mathrm{e}_1) = \mathrm{freevars}(\mathrm{e}_2) = \emptyset \land \\
\qquad \forall \Phi_{r1}, \Phi_{r2}, \mathsf{H}_1, \mathsf{H}_2{:}W,\ \mathrm{e}_1',\ \mathsf{H}_1',\ j < W.k. \\
\qquad \Phi_{r1} \# \Phi_1 \land \Phi_{r2} \# \Phi_2 \land \Phi_{r1} \uplus \Phi_1, \Phi_{r2} \uplus \Phi_2 : W \land \\
\qquad \langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathsf{H}_1, \mathrm{e}_1 \rangle \overset{j}{\dashrightarrow} \langle \Phi_1', \mathsf{H}_1', \mathrm{e}_1' \rangle \nrightarrow \\
\qquad \implies \mathrm{e}_1' = \mathrm{fail}\ \textsc{Conv} \lor (\exists \Phi_{f1}\ \Phi_{g1}\ \Phi_{f2}\ \Phi_{g2}\ \mathrm{v}_2 \mathsf{H}_2' W'. \\
\qquad\qquad \langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathsf{H}_2, \mathrm{e}_2 \rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathsf{H}_2', \mathrm{v}_2 \rangle \nrightarrow \\
\qquad\qquad \land\, \Phi_1' = \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \land \\
\qquad\qquad \land\, W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W' \land\ \mathsf{H}_1', \mathsf{H}_2' : W' \\
\qquad\qquad \land\, (W', (\Phi_{f1}, \mathrm{e}_1'), (\Phi_{f2}, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho)\}
\end{array}
$$

$$\mathrm{guard}(\mathrm{e}, \ell) \triangleq \lambda\_.\{\mathrm{if}\ !\ell\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell := \textsc{used}; \mathrm{e}\}\}$$

$$
\begin{aligned}
\mathcal{V}\llbracket \mathtt{unit} \rrbracket_{\rho} &= \{(W, (\emptyset, ()), (\emptyset, ()))\} \\
\mathcal{V}\llbracket \mathtt{int} \rrbracket_{\rho} &= \{(W, (\emptyset, \mathsf{n}), (\emptyset, \mathsf{n})) \mid \mathsf{n} \in \mathbb{Z}\} \\
\mathcal{V}\llbracket \tau_1 \times \tau_2 \rrbracket_{\rho} &= \{(W, (\emptyset, (\mathsf{v}_{1a}, \mathsf{v}_{2a})), (\emptyset, (\mathsf{v}_{1b}, \mathsf{v}_{2b}))) \\
&\quad \mid (W, (\emptyset, \mathsf{v}_{1a}), (\emptyset, \mathsf{v}_{1b})) \in \mathcal{V}\llbracket \tau_1 \rrbracket_{\rho} \land (W, (\emptyset, \mathsf{v}_{2a}), (\emptyset, \mathsf{v}_{2b})) \in \mathcal{V}\llbracket \tau_2 \rrbracket_{\rho}\} \\
\mathcal{V}\llbracket \tau_1 + \tau_2 \rrbracket_{\rho} &= \{(W, (\emptyset, \mathsf{inl}\ \mathsf{v}_1), (\emptyset, \mathsf{inl}\ \mathsf{v}_2)) \mid (W, (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}\llbracket \tau_1 \rrbracket_{\rho}\} \\
&\quad \cup \{(W, (\emptyset, \mathsf{inr}\ \mathsf{v}_1), (\emptyset, \mathsf{inr}\ \mathsf{v}_2)) \mid (W, (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}\llbracket \tau_2 \rrbracket_{\rho}\} \\
\mathcal{V}\llbracket \tau_1 \rightarrow \tau_2 \rrbracket_{\rho} &= \{(W, (\emptyset, \lambda \mathsf{x}.\{\mathsf{e}_1\}), (\emptyset, \lambda \mathsf{x}.\{\mathsf{e}_2\})) \mid \forall \mathsf{v}_1\ \mathsf{v}_2\ W'.W \sqsubset_{\emptyset,\emptyset} W' \\
&\land (W', (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}\llbracket \tau_1 \rrbracket_{\rho} \implies (W', (\emptyset, [x\mapsto \mathsf{v}_1]\mathsf{e}_1), (\emptyset, [x\mapsto \mathsf{v}_2]\mathsf{e}_2)) \in \mathcal{E}\llbracket \tau_2 \rrbracket_{\rho}\} \\
\mathcal{V}\llbracket \mathtt{ref}\ \tau \rrbracket_{\rho} &= \{(W, (\emptyset, \ell_1), (\emptyset, \ell_2)) \mid W.\Psi(\ell_1, \ell_2) = \lfloor \mathcal{V}\llbracket \tau \rrbracket_{\rho} \rfloor_{W.k}\} \\
\mathcal{V}\llbracket \forall \alpha.\tau \rrbracket_{\rho} &= \{(W, (\emptyset, \lambda\_.\mathsf{e}_1), (\emptyset, \lambda\_.\mathsf{e}_2)) \mid \forall R \in \mathit{UnrTyp},\ W'.W \sqsubset_{\emptyset,\emptyset} W' \\
&\implies (W', (\emptyset, \mathsf{e}_1), (\emptyset, \mathsf{e}_2)) \in \mathcal{E}\llbracket \tau \rrbracket_{\rho[\alpha\mapsto R]}\} \\
\mathcal{V}\llbracket \alpha \rrbracket_{\rho} &= \rho(\alpha)
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{V}\llbracket \mathrm{unit} \rrbracket_{.} &= \{(W, (\emptyset, ()), (\emptyset, ()))\} \\
\mathcal{V}\llbracket \mathrm{bool} \rrbracket_{\rho} &= \{(W, (\emptyset, 0), (\emptyset, 0))\} \cup \{(W, (\emptyset, \mathsf{n}_1), (\emptyset, \mathsf{n}_2)) \mid n_1 \neq 0 \land n_2 \neq 0\} \\
\mathcal{V}\llbracket \mathrm{int} \rrbracket_{.} &= \{(W, (\emptyset, \mathsf{n}), (\emptyset, \mathsf{n})) \mid \mathsf{n} \in \mathbb{Z}\} \\
\mathcal{V}\llbracket \tau_1 \multimap \tau_2 \rrbracket_{.} &= \{(W, (\emptyset, \lambda\, \mathsf{x}\{\mathsf{e}_1\}), (\emptyset, \lambda\, \mathsf{x}\{\mathsf{e}_2\})) \mid \\
&\forall \Phi_1\ \mathsf{v}_1\ \Phi_2\ \mathsf{v}_2\ W'.W \sqsubset_{\emptyset,\emptyset} W' \land (W', (\Phi_1, \mathsf{v}_1), (\Phi_2, \mathsf{v}_2)) \in \mathcal{V}\llbracket \tau_1 \rrbracket_{.} \\
&\implies ((W'.k, W'.\Psi, W'.\Theta \uplus (\ell_1, \ell_2) \mapsto (\Phi_1, \Phi_2)), \\
&\quad (\emptyset, [x\mapsto \mathrm{guard}(\mathsf{v}_1, \ell_1)]\mathsf{e}_1), (\emptyset, [x\mapsto \mathrm{guard}(\mathsf{v}_2, \ell_2)]\mathsf{e}_2)) \in \mathcal{E}\llbracket \tau_2 \rrbracket_{.}\} \\
\mathcal{V}\llbracket \tau_1 \multimapdot \tau_2 \rrbracket_{.} &= \{(W, (\Phi_1, \lambda\, \mathsf{a}_{\bullet}.\{\mathsf{e}_1\}), (\Phi_2, \lambda\, \mathsf{a}_{\bullet}.\{\mathsf{e}_2\})) \mid \forall \Phi_1'\ \Phi_2'\ f_1\ f_2\ \mathsf{v}_1\ \mathsf{v}_2\ W'.W \sqsubset_{\Phi_1,\Phi_2} W' \\
&\quad \land (W', (\Phi_1', \mathsf{v}_1), (\Phi_2', \mathsf{v}_2)) \in \mathcal{V}\llbracket \tau_1 \rrbracket_{.} \land \Phi_1 \cap \Phi_1' = \Phi_2 \cap \Phi_2' = \emptyset \\
&\quad \land f_1 \notin \Phi_1 \uplus \Phi_1' \uplus \mathrm{flags}(W', 1) \land f_2 \notin \Phi_2 \uplus \Phi_2' \uplus \mathrm{flags}(W', 2) \\
&\implies (W', (\Phi_1 \uplus \Phi_1' \uplus \{f_1\}, [\mathsf{a}_{\bullet}\mapsto \mathrm{protect}(\mathsf{v}_1, f_1)]\mathsf{e}_1), \\
&\quad (\Phi_2 \uplus \Phi_2' \uplus \{f_2\}, [\mathsf{a}_{\bullet}\mapsto \mathrm{protect}(\mathsf{v}_2, f_2)]\mathsf{e}_2)) \in \mathcal{E}\llbracket \tau_2 \rrbracket_{.}\} \\
\mathcal{V}\llbracket !\tau \rrbracket_{.} &= \{(W, (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \mid (W, (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_{.}\} \\
\mathcal{V}\llbracket \tau_1 \otimes \tau_2 \rrbracket_{.} &= \{(W, (\Phi_1 \uplus \Phi_1', (\mathsf{v}_{1a}, \mathsf{v}_{2a})), (\Phi_2 \uplus \Phi_2', (\mathsf{v}_{1b}, \mathsf{v}_{2b}))) \\
&\quad \mid (W, (\Phi_1, \mathsf{v}_{1a}), (\Phi_2, \mathsf{v}_{1b})) \in \mathcal{V}\llbracket \tau_1 \rrbracket_{.} \land (W, (\Phi_1', \mathsf{v}_{2a}), (\Phi_2', \mathsf{v}_{2b})) \in \mathcal{V}\llbracket \tau_2 \rrbracket_{.}\} \\
\mathcal{V}\llbracket \tau_1 \& \tau_2 \rrbracket_{.} &= \{(W, (\Phi_1, (\lambda\_.\{\mathsf{e}_{1a}\}, \lambda\_.\{\mathsf{e}_{2a}\})), (\Phi_2, (\lambda\_.\{\mathsf{e}_{1b}\}, \lambda\_.\{\mathsf{e}_{2b}\}))) \\
&\quad \mid (W, (\Phi_1, \mathsf{e}_{1a}), (\Phi_2, \mathsf{e}_{1b})) \in \mathcal{E}\llbracket \tau_1 \rrbracket_{.} \land (W, (\Phi_1, \mathsf{e}_{2a}), (\Phi_2, \mathsf{e}_{2b})) \in \mathcal{E}\llbracket \tau_2 \rrbracket_{.}\}
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{D}\llbracket \cdot \rrbracket &= \{\cdot\} \\
\mathcal{D}\llbracket \Delta, \alpha \rrbracket &= \{\rho[\alpha \mapsto R] \mid R \in \mathit{UnrTyp} \land \rho \in \mathcal{D}\llbracket \Delta \rrbracket\}
\end{aligned}
$$

$$\begin{array}{lcl}
\mathcal{G}\llbracket \cdot \rrbracket_\rho & = & \{(W, \emptyset, \emptyset, \cdot)\} \\[1em]
\mathcal{G}\llbracket \Gamma, x : \tau \rrbracket_\rho & = & \{(W, \emptyset, \emptyset, \gamma; x {\mapsto} (\mathrm{v}_1, \mathrm{v}_2)) \mid (W, (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_\rho \land (W, \emptyset, \emptyset, \gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho\} \\[1em]
\mathcal{G}\llbracket \Gamma, \mathrm{x} : \tau \rrbracket_\rho & = & \{(W, \emptyset, \emptyset, \gamma; x {\mapsto} (\mathrm{v}_1, \mathrm{v}_2)) \mid (W, (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_\rho \land (W, \emptyset, \emptyset, \gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho\} \\[1em]
\mathcal{G}\llbracket \Omega, \mathrm{a}_\circ : \tau \rrbracket_\rho & = & \{(W, \Phi_1, \Phi_2, \gamma; a_\circ {\mapsto} (\mathrm{guard}(\mathrm{v}_1, \ell_1), \mathrm{guard}(\mathrm{v}_2, \ell_2))) \mid \\
& & \quad (W.\Theta = \Theta' \uplus (\ell_1, \ell_2) \mapsto \textsc{used}) \lor (\exists \Theta'\ \Phi_1'\ \Phi_2'. W.\Theta = \Theta' \uplus (\ell_1, \ell_2) \mapsto (\Phi_1', \Phi_2') \\
& & \quad \land ((W.k, W.\Psi, \Theta'), (\Phi_1', \mathrm{v}_1), (\Phi_2', \mathrm{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_\rho \land (W, \Phi_1, \Phi_2, \gamma) \in \mathcal{G}\llbracket \Omega \rrbracket_\rho)\} \\[1em]
\mathcal{G}\llbracket \Omega, \mathrm{a}_\bullet : \tau \rrbracket_\rho & = & \{(W, \Phi_1 \uplus \Phi_1' \uplus \{f_1\}, \Phi_2 \uplus \Phi_2' \uplus \{f_2\}, \gamma; a_\bullet {\mapsto} (\mathrm{protect}(\mathrm{v}_1, f_1), \mathrm{protect}(\mathrm{v}_2, f_2))) \mid \\
& & \quad (W, (\Phi_1', \mathrm{v}_1), (\Phi_2', \mathrm{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_\rho \\
& & \quad \land (W, \Phi_1, \Phi_2, \gamma) \in \mathcal{G}\llbracket \Omega \rrbracket_\rho \\
& & \quad \land \Phi_1 \cap \Phi_1' = \emptyset \land \Phi_2 \cap \Phi_2' = \emptyset\} \\
& & \quad \land f_1 \notin \Phi_1 \uplus \Phi_1' \land f_2 \notin \Phi_2 \uplus \Phi_2'\}
\end{array}$$

$$\begin{array}{l}
\Gamma; \Omega; \Delta; \Gamma \vdash \mathrm{e}_1 \preceq \mathrm{e}_2 : \tau \equiv \forall W. \forall \rho\ \gamma_\Gamma\ \gamma_\Gamma\ \gamma_\Omega \\
\quad \rho \in \mathcal{D}\llbracket \Delta \rrbracket \land (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho \land (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket. \land (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}\llbracket \Omega \rrbracket. \\
\quad \Longrightarrow \ (W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+)))), \\
\qquad\quad (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^+))))) \in \mathcal{E}\llbracket \tau \rrbracket_\rho
\end{array}$$

$$\begin{array}{l}
\Gamma; \Omega; \Delta; \Gamma \vdash \mathrm{e}_1 \preceq \mathrm{e}_2 : \tau \equiv \forall W. \forall \rho\ \gamma_\Gamma\ \gamma_\Gamma\ \gamma_\Omega \\
\quad \rho \in \mathcal{D}\llbracket \Delta \rrbracket \land (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho \land (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket. \land (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}\llbracket \Omega \rrbracket. \\
\quad \Longrightarrow \ (W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+)))), \\
\qquad\quad (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^+))))) \in \mathcal{E}\llbracket \tau \rrbracket_\rho
\end{array}$$

Finally, for any environment Ω, let $\Omega_\circ$ be the set of dynamic variables in Ω. This notation will be used in the supporting lemmas and some proofs of compatibility lemmas below.

3.6 Logical Relation Soundness

Lemma 3.1 (Expression Relation Contains Value Relation).

$$\mathcal{V}\llbracket \tau \rrbracket_\rho \subseteq \mathcal{E}\llbracket \tau \rrbracket_\rho$$

Proof. All terms in the value relation are irreducible, and thus are trivially in the expression relation. □

Lemma 3.2 (Values With No Flags Are In Expression Relation). *For all $\tau, \rho, W, \Phi_1, \mathrm{v}_1, \Phi_2, \mathrm{v}_2$, if $(W, (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_\rho$, then $(W, (\Phi_1, \mathrm{v}_1), (\Phi_2, \mathrm{v}_2)) \in \mathcal{E}\llbracket \tau \rrbracket_\rho$.*

Proof. Expanding the definition of the expression relation, given:

$$\begin{gathered}
\forall \Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k. \\
\Phi_{r1} \# \Phi_1 \land \Phi_{r2} \# \Phi_2 \land \Phi_{r1} \uplus \Phi_1, \Phi_{r2} \uplus \Phi_2 : W \land \\
\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, \mathrm{v}_1 \rangle \overset{j}{\dashrightarrow} \langle \Phi_1', \mathrm{H}_1', \mathrm{e}_1' \rangle \nrightarrow
\end{gathered}$$

we must show that either e_1' is fail Conv or there exist $\Phi_{f1}, \Phi_{g1}, \Phi_{f2}, \Phi_{g2}, \mathrm{v}_2^*, \mathrm{H}_2', W'$ such that:

$$\begin{aligned}
&\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, \mathrm{v}_2\rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathrm{H}_2', \mathrm{v}_2^*\rangle \nrightarrow\\
&\land\ \Phi_1' = \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \land\\
&\land\ W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W' \land\ \mathrm{H}_1', \mathrm{H}_2' : W'\\
&\land\ (W', (\Phi_{f1}, \mathrm{e}_1'), (\Phi_{f2}, \mathrm{v}_2^*)) \in \mathcal{V}[\![\tau]\!]_\rho)
\end{aligned}$$

Since $\mathrm{v}_1, \mathrm{v}_2$ are in the value relation, they are target values, so the configurations

$$\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, \mathrm{v}_1\rangle$$

and

$$\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, \mathrm{v}_2\rangle$$

are irreducible. Thus, Φ_1' is simply equal to the set of static flags in the initial configuration, so $\Phi_1' = \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1$. Then, we can take $\Phi_{f1} = \emptyset$, $\Phi_{g1} = \Phi_1$, $\Phi_{f2} = \emptyset$, $\Phi_{g2} = \Phi_2$, $\mathrm{v}_2^* = \mathrm{v}_2$, $\mathrm{H}_2' = \mathrm{H}_2$, and $W' = W$.

Since $\Phi_{r1}, \Phi_{r2} : W$ by assumption, we have $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W$. Everything else in the expression relation is trivial by assumption, so this suffices to finish the proof. □

Lemma 3.3 (Expressions With No Flags Are In Expression Relation). *For all $\tau, \rho, W, \Phi_1, \mathrm{e}_1, \Phi_2, \mathrm{e}_2$, if $(W, (\emptyset, \mathrm{e}_1), (\emptyset, \mathrm{e}_2)) \in \mathcal{E}[\![\tau]\!]_\rho$, then $(W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}[\![\tau]\!]_\rho$.*

Proof. Expanding the definition of the expression relation, given:

$$\begin{gathered}
\forall \Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.\\
\Phi_{r1} \# \Phi_1 \land \Phi_{r2} \# \Phi_2 \land \Phi_{r1} \uplus \Phi_1, \Phi_{r2} \uplus \Phi_2 : W \land\\
\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, \mathrm{e}_1\rangle \overset{j}{\dashrightarrow} \langle \Phi_1', \mathrm{H}_1', \mathrm{e}_1'\rangle \nrightarrow
\end{gathered}$$

we must show that either e_1' is fail Conv or there exist $\Phi_{f1}, \Phi_{g1}, \Phi_{f2}, \Phi_{g2}, \mathrm{v}_2, \mathrm{H}_2', W'$ such that:

$$\begin{aligned}
&\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, \mathrm{e}_2\rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathrm{H}_2', \mathrm{v}_2\rangle \nrightarrow\\
&\land\ \Phi_1' = \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \land\\
&\land\ W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W' \land\ \mathrm{H}_1', \mathrm{H}_2' : W'\\
&\land\ (W', (\Phi_{f1}, \mathrm{e}_1'), (\Phi_{f2}, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho)
\end{aligned}$$

Now, by expanding the expression relation in the assumption, we have that, if

$$\begin{gathered}
\forall \Phi_{r1}^*, \Phi_{r2}^*, \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.\\
\Phi_{r1}^* \# \emptyset \land \Phi_{r2}^* \# \emptyset \land \Phi_{r1}^* \uplus \emptyset, \Phi_{r2}^* \uplus \emptyset : W \land\\
\langle \Phi_{r1}^* \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, \mathrm{e}_1\rangle \overset{j}{\dashrightarrow} \langle \Phi_1', \mathrm{H}_1', \mathrm{e}_1'\rangle \nrightarrow
\end{gathered}$$

then either e_1' is fail Conv or there exist $\Phi_{f1}^*, \Phi_{g1}^*, \Phi_{f2}^*, \Phi_{g2}^*, \mathrm{v}_2, \mathrm{H}_2', W'$ such that:

$$\begin{aligned}
&\langle \Phi_{r2}^* \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, \mathrm{e}_2\rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2}^* \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2}^* \uplus \Phi_{g2}^*, \mathrm{H}_2', \mathrm{v}_2\rangle \nrightarrow\\
&\land\ \Phi_1' = \Phi_{r1}^* \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1}^* \uplus \Phi_{g1}^* \land\\
&\land\ W \sqsubseteq_{\Phi_{r1}^*, \Phi_{r2}^*} W' \land\ \mathrm{H}_1', \mathrm{H}_2' : W'\\
&\land\ (W', (\Phi_{f1}^*, \mathrm{e}_1'), (\Phi_{f2}^*, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho)
\end{aligned}$$

Then, we can instantiate this fact with $\Phi_{r1}^* = \Phi_{r1} \uplus \Phi_1, \Phi_{r2}^* = \Phi_{r2} \uplus \Phi_2$. We then find that:

$$\begin{aligned}
&\langle \Phi_{r2} \uplus \Phi_2 \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, \mathrm{e}_2\rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \Phi_2 \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2}^* \uplus \Phi_{g2}^*, \mathrm{H}_2', \mathrm{v}_2\rangle \nrightarrow\\
&\land\ \Phi_1' = \Phi_{r1} \uplus \Phi_1 \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1}^* \uplus \Phi_{g1}^* \land\\
&\land\ W \sqsubseteq_{\Phi_{r1}^*, \Phi_{r2}^*} W' \land\ \mathrm{H}_1', \mathrm{H}_2' : W'\\
&\land\ (W', (\Phi_{f1}^*, \mathrm{e}_1'), (\Phi_{f2}^*, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho)
\end{aligned}$$

Then, we can take $\Phi_{f1} = \Phi^*_{f1}, \Phi_{g1} = \Phi^*_{g1} \uplus \Phi_1, \Phi_{f2} = \Phi^*_{f2}, \Phi_{g2} = \Phi^*_{g2} \uplus \Phi_2$. Then, everything in the expression relation we have to prove trivially follows from the above, so the proof is finished. □

Lemma 3.4 (**Affi** Values Compile to Target Values).

Proof. By induction over the syntax: $()$ compiles to $()$, $\lambda \mathrm{a}_{◐} : \tau.\mathrm{e}$ compiles to a target function, $\langle \mathrm{e}, \mathrm{e}' \rangle$ compiles to a pair of target functions, $!\mathrm{v}$ compiles to v^+ (which is a target value by the induction hypothesis), and $(\mathrm{v}, \mathrm{v}')$ compiles to $(\mathrm{v}^+, \mathrm{v}'^+)$ (where both v^+ and v'^+ are target values by the induction hypothesis). □

Lemma 3.5 (Split Substitutions). *For any world W, flagsets Φ_1, Φ_2, and substitution γ such that*

$$(W, \Phi_1, \Phi_2, \gamma) \in \mathcal{G}[\![\Omega_1 \uplus \Omega_2]\!]_\rho$$

there exist flagsets $\Phi_{1l}, \Phi_{1r}, \Phi_{2l}, \Phi_{2r}$ such that $\Phi_1 = \Phi_{1l} \uplus \Phi_{1r}$, $\Phi_2 = \Phi_{2l} \uplus \Phi_{2r}$, and substitutions γ_1, γ_2 such that $\gamma = \gamma_1 \uplus \gamma_2$ and

$$(W, \Phi_{1l}, \Phi_{2l}, \gamma_1) \in \mathcal{G}[\![\Omega_1]\!]_\rho$$

and

$$(W, \Phi_{1r}, \Phi_{2r}, \gamma_2) \in \mathcal{G}[\![\Omega_2]\!]_\rho$$

Moreover, for any $i, j \in \{1, 2\}$, for any $\Gamma; \Omega_\mathrm{j}; \Delta; \Gamma \vdash \mathrm{e} : \tau \rightsquigarrow \Gamma'; \Omega'$,

$$close_i(\gamma, \mathrm{e}^+) = close_i(\gamma_j, \mathrm{e}^+)$$

and for any $\Gamma; \Omega_\mathrm{j}; \Delta; \Gamma \vdash \mathrm{e} : \tau \rightsquigarrow \Delta'; \Gamma'$,

$$close_i(\gamma, \mathrm{e}^+) = close_i(\gamma_j, \mathrm{e}^+)$$

Proof. First, we need to show that there exist substitutions γ_1 and γ_2. This follows from the inductive structure of $\mathcal{G}[\![\Omega]\!]_\rho$, where we can separate the parts that came from $\mathcal{G}[\![\Omega_1]\!]_\rho$ and $\mathcal{G}[\![\Omega_2]\!]_\rho$. The second follows from the fact that the statics means that the rest of the substitution must not occur in the term, and thus $\mathrm{close}_i(\gamma, \mathrm{e}^+) = \mathrm{close}_i(\gamma_1, \mathrm{close}_i(\gamma_2, \mathrm{e}^+)) = \mathrm{close}_i(\gamma_1, \mathrm{e}^+)$ (for example). □

Lemma 3.6 (No Static Variables in `MiniML` Terms). *For any world W, flagsets Φ_1, Φ_2, and substitution γ such that*

$$(W, \Phi_1, \Phi_2, \gamma) \in \mathcal{G}[\![\Omega]\!]_\rho$$

then there exists a substitution γ' such that

$$(W, \emptyset, \emptyset, \gamma') \in \mathcal{G}[\![\Omega_\circ]\!]_\rho$$

and, for all $\Gamma; \Omega; \Delta; \Gamma \vdash \mathrm{e} : \tau \rightsquigarrow \Gamma'; \Omega'$ and for all $i \in \{1, 2\}$,

$$close_i(\gamma, \mathrm{e}^+) = close_i(\gamma', \mathrm{e}^+)$$

Proof. Let $\Omega_\bullet$ be the set of all static variables in Ω. Since Ω only contains dynamic or static variables, $\Omega = \Omega_\circ \uplus \Omega_\bullet$, so by Lemma 3.5, there exist flagsets $f_{1l}, f_{1r}, f_{2l}, f_{2r}$ and substitutions γ_1, γ_2 such that $f_1 = f_{1l} \uplus f_{1r}$, $f_2 = f_{2l} \uplus f_{2r}$, $\gamma = \gamma_1 \uplus \gamma_2$, $(W, f_{1l}, f_{2l}, \gamma_1) \in \mathcal{G}[\![\Omega_\circ]\!]_\rho$ and $(W, f_{1r}, f_{2r}, \gamma_2) \in \mathcal{G}[\![\Omega_\bullet]\!]_\rho$. Since $\Omega_\circ$ only contains dynamic variables, $f_{1l} = f_{2l} = \emptyset$. Thus, we can take $\gamma' = \gamma_1$.

Now, we must prove, for any $\Gamma; \Omega; \Delta; \Gamma \vdash \mathrm{e} : \tau \rightsquigarrow \Gamma'; \Omega'$ and for any $i \in \{1, 2\}$, it holds that $\mathrm{close}_i(\gamma, \mathrm{e}^+) = \mathrm{close}_i(\gamma_1, \mathrm{e}^+)$. Since $\gamma = \gamma_1 \uplus \gamma_2$, we have

$$\mathrm{close}_i(\gamma, \mathrm{e}^+) = \mathrm{close}_i(\gamma_1, \mathrm{close}_i(\gamma_2, \mathrm{e}^+))$$

Notice that γ_2 only contains variables annotated with $\bullet$. However, e^+ contains no free variables annotated with $\bullet$ because, if it did, then there would need to be a free static variable would under a $(\!|\cdot|\!)_\tau$ boundary, as only static variables in **Affi** get compiled to variables annotated with $\bullet$ in the target. However, the typing rule for $(\!|\cdot|\!)_\tau$ does not allow for free static variables, so this is impossible and thus e^+ contains no free variables annotated with $\bullet$. Ergo, closing e^+ with γ_2 has no impact, so

$$\mathrm{close}_i(\gamma, \mathrm{e}^+) = \mathrm{close}_i(\gamma_1, \mathrm{close}_i(\gamma_2, \mathrm{e}^+)) = \mathrm{close}_i(\gamma_1, \mathrm{e}^+)$$

as was to be proven. □

Lemma 3.7 (Strengthening Logical Relation for MiniML). *For all* $\Gamma; \Omega; \Delta; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \tau$, *if there exists some* $(W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}\llbracket\Omega\rrbracket.$, *it holds that:*

$$\begin{aligned}
&\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega \\
&\quad \rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket. \wedge (W, \emptyset, \emptyset, \gamma_{\Omega_\circ}) \in \mathcal{G}\llbracket\Omega_\circ\rrbracket. \\
&\quad \Longrightarrow (W, (\emptyset, \mathit{close}_1(\gamma_\Gamma, \mathit{close}_1(\gamma_\Gamma, \mathit{close}_1(\gamma_{\Omega_\circ}, \mathrm{e}^+)))), \\
&\qquad\quad (\emptyset, \mathit{close}_2(\gamma_\Gamma, \mathit{close}_2(\gamma_\Gamma, \mathit{close}_2(\gamma_{\Omega_\circ}, \mathrm{e}^+))))) \in \mathcal{E}\llbracket\tau\rrbracket_\rho
\end{aligned}$$

Proof. Since Ω only contains dynamic or static variables, $\Omega = \Omega_\circ \uplus \Omega_\bullet$, so by Lemma 3.5, there exist flagsets $f_{1l}, f_{1r}, f_{2l}, f_{2r}$ and substitutions γ_1, γ_2 such that $f_1 = f_{1l} \uplus f_{1r}$, $f_2 = f_{2l} \uplus f_{2r}$, $\gamma = \gamma_1 \uplus \gamma_2$, $(W, f_{1l}, f_{2l}, \gamma_1) \in \mathcal{G}\llbracket\Omega_\circ\rrbracket_\rho$ and $(W, f_{1r}, f_{2r}, \gamma_2) \in \mathcal{G}\llbracket\Omega_\bullet\rrbracket_\rho$.

Now, consider the given hypothesis. Given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket. \wedge (W, \emptyset, \emptyset, \gamma_{\Omega_\circ}) \in \mathcal{G}\llbracket\Omega_\circ\rrbracket.$$

we must show:

$$\begin{gathered}
(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))), \\
(\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))))) \in \mathcal{E}\llbracket\tau\rrbracket_\rho
\end{gathered}$$

Since $(W, f_{1r}, f_{2r}, \gamma_2) \in \mathcal{G}\llbracket\Omega_\bullet\rrbracket_\rho$, $(W, \emptyset, \emptyset, \gamma_{\Omega_\circ}) \in \mathcal{G}\llbracket\Omega_\circ\rrbracket.$, and $\Omega = \Omega_\bullet \uplus \Omega_\circ$, it holds that $(W, f_{1r}, f_{2r}, \gamma_2 \uplus \gamma_{\Omega_\circ}) \in \mathcal{G}\llbracket\Omega\rrbracket..$ Thus, by applying $\Gamma; \Omega; \Delta; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \tau$, we find

$$\begin{gathered}
(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2 \uplus \gamma_{\Omega_\circ}, \mathrm{e}^+)))), \\
(\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2 \uplus \gamma_{\Omega_\circ}, \mathrm{e}^+))))) \in \mathcal{E}\llbracket\tau\rrbracket_\rho
\end{gathered}$$

As explained in the proof for Lemma 3.6, e^+ has no free variables annotated with $\bullet$, so closing e^+ over with γ_2 has no impact. Ergo,

$$\begin{gathered}
(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_{\Omega_\circ}, \mathrm{e}^+)))), \\
(\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_{\Omega_\circ}, \mathrm{e}^+))))) \in \mathcal{E}\llbracket\tau\rrbracket_\rho
\end{gathered}$$

which suffices to finish the proof. □

Lemma 3.8 (World Extension).

(1) *If* $(W_1, (\Phi_1, \mathrm{v}_1), (\Phi_2, \mathrm{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho$ *and* $W_1 \sqsubseteq_{\Phi_1, \Phi_2} W_2$, *then* $(W_2, (\Phi_1, \mathrm{v}_1), (\Phi_2, \mathrm{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho$
(2) *If* $(W_1, \Phi_1, \Phi_2, \gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho$ *and* $W_1 \sqsubseteq_{\Phi_1, \Phi_2} W_2$, *then* $(W_2, \Phi_1, \Phi_2, \gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho$

Proof. We note that world extension allows three things: the step index to decrease, the heap typing to add bindings (holding all existing bindings at same relation, module decreasing step index), and add flag references (ensuring existing flag references can go from pairs of sets of static flags to used, but not the other way). In all cases, this is straightforward based on the definition (relying on Lemma 2.4 in some cases). □

Lemma 3.9 (World Extension Transitive). *If* $W_1 \sqsubseteq_{\Phi_1, \Phi_2} W_2$ *and* $W_2 \sqsubseteq_{\Phi'_1, \Phi'_2} W_3$ *then* $W_1 \sqsubseteq_{\Phi_1 \cap \Phi'_1, \Phi_2 \cap \Phi'_2} W_3$.

Proof. This holds trivially for step indices, the heap typing, and the monotonicity of marking affine flags as used. What remains is the side condition that the world satisfies Φ_1, Φ_2. Since that is defined as being disjoint from the set of flags in W and W', the set of flags that is disjoint from both W_1 and W_3 is the intersection. □

LEMMA 3.10 (HEAPS IN LATER WORLD). *For any $W \in World$ and $\mathsf{H}_1, \mathsf{H}_2 : W$, it holds that $\mathsf{H}_1, \mathsf{H}_2 : \triangleright W$.*

PROOF. For $\mathsf{H}_1, \mathsf{H}_2 : \triangleright W$, we need three things.

The first is that for any mapping $(\ell_1, \ell_2) \mapsto R$ in $\triangleright W.\Psi$, $(\triangleright\triangleright W, \mathsf{H}_1(\ell_1), \mathsf{H}_2(\ell_2)) \in R$. Since R is drawn from Typ, we know it is closed under world extension and thus the fact that $(\triangleright W, \mathsf{H}_1(\ell_1), \mathsf{H}_2(\ell_2)) \in R$ means this holds.

The other two conditions, which relate to $W.\Theta$, are unaffected by the shift of step index, and so hold trivially in $\triangleright W$. □

LEMMA 3.11 (HEAPS IN LATER WORLD). *For any $W \in World$ and $\mathsf{H}_1, \mathsf{H}_2 : W$, it holds that $\mathsf{H}_1, \mathsf{H}_2 : \triangleright W$.*

PROOF. Since heap typings map to relations that are by definition closed under world extension, and world extension cannot remove locations, only restrict them to future step indices, this holds by definition. □

LEMMA 3.12 (LOGICAL RELATIONS FOR `MiniML` IN *UnrTyp*). *For any Δ, $\rho \in \mathcal{D}[\![\Delta]\!]$, and τ, if $\Delta \vdash \tau$, then $\mathcal{V}[\![\tau]\!]_\rho \in UnrTyp$.*

PROOF. First, we show $\mathcal{V}[\![\tau]\!]_\rho \in Typ$. By the definition of Typ, it suffices to show, for all natural numbers n, $\lfloor \mathcal{V}[\![\tau]\!]_\rho \rfloor_n \in Typ_n$, for which we must show two facts: first, that it is in $2^{AtomVal_n}$, and second that it is closed under world extension. The latter holds by Lemma 3.8. For the former, we note that we are required to show that the worlds are in $World_n$, which holds by definition, and that for any $(W, (\Phi_1, \mathsf{v}_1), (\Phi_2, \mathsf{v}_2))$ in the relation, $\Phi_1, \Phi_2 : W$. For the latter, note that $\Phi_1 = \Phi_2 = \emptyset$ as shown earlier, and $\emptyset$ is trivially disjoint from $\mathrm{flags}(W, 1)$ and $\mathrm{flags}(W, 2)$.

Second, we show that for any $(W, (\Phi_1, \mathsf{v}_1), (\Phi_2, \mathsf{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho$, $\Phi_1 = \Phi_2 = \emptyset$. This is trivial by the definition of $\mathcal{V}[\![\tau]\!]_\rho$, aside from the case for α, where it holds because the relation is drawn from *UnrTyp*. □

LEMMA 3.13 (COMPOSITIONALITY).

$$(W, (\Phi_1, \mathsf{v}_1), (\Phi_2, \mathsf{v}_2)) \in \mathcal{V}[\![\tau]\!]_{\rho[\alpha \mapsto \mathcal{V}[\![\tau']\!]_\rho]} \iff (W, (\Phi_1, \mathsf{v}_1), (\Phi_2, \mathsf{v}_2)) \in \mathcal{V}[\![\tau[\tau'/\alpha]]\!]_\rho$$

PROOF. The proof for compositionality in this case study is essentially verbatim the proof for compositionality in the last case study. □

LEMMA 3.14 (EXPRESSION RELATION FOR CLOSED TYPES). *For any `MiniML` type τ where $\cdot \vdash \tau$ and any ρ,*

$$\mathcal{E}[\![\tau]\!]_\rho = \mathcal{E}[\![\tau]\!]_\cdot$$

PROOF. Since $\mathcal{E}[\![\tau]\!]_\rho$ is defined in terms of $\mathcal{V}[\![\tau]\!]_\rho$, this proof is analogous to Lemma 3.13, though since what we are substituting is not used, the interpretation can be arbitrary. □

LEMMA 3.15 (CLOSING `MiniML` TERMS). *For any `MiniML` term e where $\Gamma; \Omega; \Delta; \Gamma \vdash \mathsf{e} : \tau \rightsquigarrow \Gamma'; \Omega'$, for any $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$ where $\rho \in \mathcal{D}[\![\Delta]\!]$, $(W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho$, $(W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\cdot$, and $(W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!]_\cdot$, it holds that*

$$close_1(\gamma_\Gamma, close_1(\gamma_\Gamma, close_1(\gamma_\Omega, \mathsf{e}^+)))$$

and

$$close_2(\gamma_\Gamma, close_2(\gamma_\Gamma, close_2(\gamma_\Omega, \mathsf{e}^+)))$$

are closed terms.

PROOF. Since free variables are compiled to free variables, and no other free variables are introduced via compilation, this follows trivially from the structure of $\mathcal{G}[\![\Gamma]\!]_\rho$. □

Lemma 3.16 (Closing **Affi** Terms). *For any* **Affi** *term* e *where* $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{e} : \tau \rightsquigarrow \Delta'; \Gamma'$, *for any* $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$ *where* $\rho \in \mathcal{D}[\![\Delta]\!]$, $(W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho$, $(W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!].$, *and* $(W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!].$, *it holds that*

$$close_1(\gamma_\Gamma, close_1(\gamma_\Gamma, close_1(\gamma_\Omega, \mathrm{e}^+)))$$

and

$$close_2(\gamma_\Gamma, close_2(\gamma_\Gamma, close_2(\gamma_\Omega, \mathrm{e}^+)))$$

are closed terms.

Proof. Since free variables are compiled to free variables, and no other free variables are introduced via compilation, this follows trivially from the structure of $\mathcal{G}[\![\Gamma]\!]_\rho$. □

Lemma 3.17 ($\texttt{MiniML}$ Values Contain No Flags). *If* $\Delta \vdash \tau, \rho \in \mathcal{D}[\![\Delta]\!]$, *and* $(W, (\Phi_1, \mathrm{v}_1), (\Phi_2, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho$, *then* $\Phi_1 = \Phi_2 = \emptyset$.

Proof. If τ is not a type variable, then the theorem is trivially true because all non-type variable interpretations of $\texttt{MiniML}$ types are defined to only contain tuples where the sets of static flags are $\emptyset$.

If τ is some type variable α, then, since $\Delta \vdash \tau$, $\alpha \in \Delta$. Thus, since $\rho \in \mathcal{D}[\![\Delta]\!]$, it must be that $\rho(\alpha) \in UnrTyp$. Then, for any $(W, (\Phi_1, \mathrm{v}_1), (\Phi_2, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho = \rho(\alpha)$, it must be that $\Phi_1 = \Phi_2 = \emptyset$ by the definition of *UnrTyp*. □

Theorem 3.18 (Convertibility Soundness). *If* $\tau_A \sim \tau_B$ *then*
$\forall\, (W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}[\![\tau_A]\!].\implies (W, (\Phi_1, C_{\tau_A \mapsto \tau_B}(\mathrm{e}_1)), (\Phi_2, C_{\tau_A \mapsto \tau_B}(\mathrm{e}_2))) \in \mathcal{E}[\![\tau_B]\!].$
$\wedge\ \forall\, (W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}[\![\tau_B]\!].\implies (W, (\Phi_1, C_{\tau_B \mapsto \tau_A}(\mathrm{e}_1)), (\Phi_2, C_{\tau_B \mapsto \tau_A}(\mathrm{e}_2))) \in \mathcal{E}[\![\tau_A]\!]..$

Proof. We prove this by simultaneous induction on the structure of the convertibility relation.

$\boxed{\texttt{unit} \sim \mathrm{unit}}$ There are two directions to this proof:

$\forall\, (W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}[\![\texttt{unit}]\!].\implies (W, (\Phi_1, C_{\texttt{unit} \mapsto \mathrm{unit}}(\mathrm{e}_1)), (\Phi_2, C_{\texttt{unit} \mapsto \mathrm{unit}}(\mathrm{e}_2))) \in \mathcal{E}[\![\mathrm{unit}]\!].$

and:

$\forall\, (W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}[\![\mathrm{unit}]\!].\implies (W, (\Phi_1, C_{\mathrm{unit} \mapsto \texttt{unit}}(\mathrm{e}_1)), (\Phi_2, C_{\mathrm{unit} \mapsto \texttt{unit}}(\mathrm{e}_2))) \in \mathcal{E}[\![\texttt{unit}]\!].$

Both directions are trivially similar to each other, so we will only prove the first direction. Expanding the definition of the convertibility boundaries, we refine this to:

$$\forall\, (W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}[\![\texttt{unit}]\!].\implies (W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}[\![\mathrm{unit}]\!].$$

From the expression relation, we first need to show $\mathrm{e}_1, \mathrm{e}_2$ are closed. This follows directly from the fact the assumption that $(W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}[\![\texttt{unit}]\!].$, and all terms in the expression relation are closed. Next, we need to show that given:

$$\begin{aligned}&\forall \Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.\\ &\quad \Phi_{r1}, \Phi_{r2} : W \wedge\\ &\quad \langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, \mathrm{e}_1\rangle \overset{j}{\dashrightarrow} \langle \Phi_1', \mathrm{H}_1', \mathrm{e}_1'\rangle \not\twoheadrightarrow\end{aligned}$$

Then it holds that:

$$\begin{aligned} &\mathrm{e}'_1 = \text{fail } \textsc{Conv} \lor (\exists \Phi_{f1}\ \Phi_{g1}\ \Phi_{f2}\ \Phi_{g2}\ \mathrm{v}_2 \mathrm{H}'_2\, W'.\\ &\qquad \langle \Phi_{r2} \uplus \text{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, \mathrm{e}_2\rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \text{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathrm{H}'_2, \mathrm{v}_2\rangle \not\rightarrow\\ &\qquad \land\ \Phi'_1 = \Phi_{r1} \uplus \text{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \land\\ &\qquad \land\ W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W' \land\ \mathrm{H}'_1, \mathrm{H}'_2 : W'\\ &\qquad \land\ (W', (\Phi_{f1}, \mathrm{e}'_1), (\Phi_{f2}, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!].)\} \end{aligned}$$

By instantiating the assumption $(W, (\Phi_1, \mathrm{e}_1), (\Phi_1, \mathrm{e}_2)) \in \mathcal{E}[\![\texttt{unit}]\!].$ with $\Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2$, etc, we find that

$$\begin{aligned} &\mathrm{e}'_1 = \text{fail } \textsc{Conv} \lor (\exists \Phi_{f1}\ \Phi_{g1}\ \Phi_{f2}\ \Phi_{g2}\ \mathrm{v}_2 \mathrm{H}'_2\, W'.\\ &\qquad \langle \Phi_{r2} \uplus \text{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, \mathrm{e}_2\rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \text{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathrm{H}'_2, \mathrm{v}_2\rangle \not\rightarrow\\ &\qquad \land\ \Phi'_1 = \Phi_{r1} \uplus \text{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \land\\ &\qquad \land\ W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W' \land\ \mathrm{H}'_1, \mathrm{H}'_2 : W'\\ &\qquad \land\ (W', (\Phi_{f1}, \mathrm{e}'_1), (\Phi_{f2}, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!].)\} \end{aligned}$$

Ergo, it suffices to show that if $(W', (\Phi_{f1}, \mathrm{e}'_1), (\Phi_{f2}, \mathrm{v}_2)) \in \mathcal{V}[\![\texttt{unit}]\!].$, then $(W', (\Phi_{f1}, \mathrm{e}'_1), (\Phi_{f2}, \mathrm{v}_2)) \in \mathcal{V}[\![\text{unit}]\!]..$ However, this is trivial because $\mathcal{V}[\![\texttt{unit}]\!]. = \mathcal{V}[\![\text{unit}]\!]. = \{(W, (\emptyset, ()), (\emptyset, ()))\}$.

$\boxed{\texttt{int} \sim \text{bool}}$ There are two directions to this proof:

$$\forall\, (W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}[\![\texttt{int}]\!]. \implies (W, (\Phi_1, C_{\texttt{int}\mapsto\text{bool}}(\mathrm{e}_1)), (\Phi_2, C_{\texttt{int}\mapsto\text{bool}}(\mathrm{e}_2))) \in \mathcal{E}[\![\text{bool}]\!].$$

and:

$$\forall\, (W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}[\![\text{int}]\!]. \implies (W, (\Phi_1, C_{\text{bool}\mapsto\texttt{int}}(\mathrm{e}_1)), (\Phi_2, C_{\text{bool}\mapsto\texttt{int}}(\mathrm{e}_2))) \in \mathcal{E}[\![\texttt{int}]\!].$$

First, consider the first direction.

Expanding the definition of the convertibility boundaries, we refine this to:

$$\forall\, (W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}[\![\texttt{int}]\!]. \implies (W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}[\![\text{bool}]\!].$$

From the expression relation, we first need to show $\mathrm{e}_1, \mathrm{e}_2$ are closed. This follows directly from the fact the assumption that $(W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}[\![\texttt{int}]\!].$, and all terms in the expression relation are closed. Next, we need to show that given:

$$\begin{aligned} &\forall \Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}'_1,\ \mathrm{H}'_1,\ j < W.k.\\ &\qquad \Phi_{r1}, \Phi_{r2} : W \land\\ &\qquad \langle \Phi_{r1} \uplus \text{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, \mathrm{e}_1\rangle \overset{j}{\dashrightarrow} \langle \Phi'_1, \mathrm{H}'_1, \mathrm{e}'_1\rangle \not\rightarrow \end{aligned}$$

Then it holds that:

$$\begin{aligned} &\mathrm{e}'_1 = \text{fail } \textsc{Conv} \lor (\exists \Phi_{f1}\ \Phi_{g1}\ \Phi_{f2}\ \Phi_{g2}\ \mathrm{v}_2 \mathrm{H}'_2\, W'.\\ &\qquad \langle \Phi_{r2} \uplus \text{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, \mathrm{e}_2\rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \text{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathrm{H}'_2, \mathrm{v}_2\rangle \not\rightarrow\\ &\qquad \land\ \Phi'_1 = \Phi_{r1} \uplus \text{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \land\\ &\qquad \land\ W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W' \land\ \mathrm{H}'_1, \mathrm{H}'_2 : W'\\ &\qquad \land\ (W', (\Phi_{f1}, \mathrm{e}'_1), (\Phi_{f2}, \mathrm{v}_2)) \in \mathcal{V}[\![\text{bool}]\!].)\} \end{aligned}$$

By instantiating the assumption $(W, (\Phi_1, \mathrm{e}_1), (\Phi_1, \mathrm{e}_2)) \in \mathcal{E}[\![\texttt{int}]\!].$ with $\Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2$, etc, we find that

$$\begin{aligned}
&\mathsf{e}_1' = \mathsf{fail}\ \textsc{Conv} \vee (\exists \Phi_{f1}\ \Phi_{g1}\ \Phi_{f2}\ \Phi_{g2}\ \mathsf{v}_2 \mathsf{H}_2' W'.\\
&\qquad \langle \Phi_{r2} \uplus \mathsf{flags}(W, 2) \uplus \Phi_2, \mathsf{H}_2, \mathsf{e}_2 \rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathsf{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathsf{H}_2', \mathsf{v}_2 \rangle \nrightarrow\\
&\qquad \wedge \Phi_1' = \Phi_{r1} \uplus \mathsf{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge\\
&\qquad \wedge\ W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W' \wedge\ \mathsf{H}_1', \mathsf{H}_2' : W'\\
&\qquad \wedge (W', (\Phi_{f1}, \mathsf{e}_1'), (\Phi_{f2}, \mathsf{v}_2)) \in \mathcal{V}\llbracket \texttt{int} \rrbracket_{.})\}
\end{aligned}$$

Ergo, it suffices to show that if $(W', (\Phi_{f1}, \mathsf{e}_1'), (\Phi_{f2}, \mathsf{v}_2)) \in \mathcal{V}\llbracket \texttt{int} \rrbracket_{.}$, then $(W', (\Phi_{f1}, \mathsf{e}_1'), (\Phi_{f2}, \mathsf{v}_2)) \in \mathcal{V}\llbracket \mathsf{bool} \rrbracket_{.}$. However, this is trivial because $\mathcal{V}\llbracket \texttt{int} \rrbracket_{.} \subseteq \mathcal{V}\llbracket \mathsf{bool} \rrbracket_{.}$.

Next, consider the first direction.

Expanding the definition of the convertibility boundaries, we refine this to:

$$\forall\ (W, (\Phi_1, \mathsf{e}_1), (\Phi_2, \mathsf{e}_2)) \in \mathcal{E}\llbracket \mathsf{bool} \rrbracket_{.} \implies (W, (\Phi_1, \mathsf{if}\ \mathsf{e}_1\ 0\ 1), (\Phi_2, \mathsf{if}\ \mathsf{e}_2\ 0\ 1)) \in \mathcal{E}\llbracket \texttt{int} \rrbracket_{.}$$

Expanding the expression relation, we must show that given

$$\begin{gathered}
\forall \Phi_{r1}, \Phi_{r2}, \mathsf{H}_1, \mathsf{H}_2{:}W,\ \mathsf{e}_1',\ \mathsf{H}_1',\ j < W.k.\\
\Phi_{r1} \# \Phi_1 \wedge \Phi_{r2} \# \Phi_2 \wedge \Phi_{r1} \uplus \Phi_1, \Phi_{r2} \uplus \Phi_2 : W \wedge\\
\langle \Phi_{r1} \uplus \mathsf{flags}(W, 1) \uplus \Phi_1, \mathsf{H}_1, \mathsf{if}\ \mathsf{e}_1\ 0\ 1 \rangle \overset{j}{\dashrightarrow} \langle \Phi_1', \mathsf{H}_1', \mathsf{e}_1' \rangle \nrightarrow
\end{gathered}$$

it holds that:

$$\begin{aligned}
&\mathsf{e}_1' = \mathsf{fail}\ \textsc{Conv} \vee (\exists \Phi_{f1}\ \Phi_{g1}\ \Phi_{f2}\ \Phi_{g2}\ \mathsf{v}_2 \mathsf{H}_2' W'.\\
&\qquad \langle \Phi_{r2} \uplus \mathsf{flags}(W, 2) \uplus \Phi_2, \mathsf{H}_2, \mathsf{if}\ \mathsf{e}_2\ 0\ 1 \rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathsf{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathsf{H}_2', \mathsf{v}_2 \rangle \nrightarrow\\
&\qquad \wedge \Phi_1' = \Phi_{r1} \uplus \mathsf{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge\\
&\qquad \wedge\ W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W' \wedge\ \mathsf{H}_1', \mathsf{H}_2' : W'\\
&\qquad \wedge (W', (\Phi_{f1}, \mathsf{e}_1'), (\Phi_{f2}, \mathsf{v}_2)) \in \mathcal{V}\llbracket \texttt{int} \rrbracket_{\rho})
\end{aligned}$$

By applying $(W, (\Phi_1, \mathsf{e}_1), (\Phi_2, \mathsf{e}_2)) \in \mathcal{E}\llbracket \texttt{int} \rrbracket_{.}$, we find that $\langle \Phi_{r1} \uplus \mathsf{flags}(W, 1) \uplus \Phi_1, \mathsf{H}_1, \mathsf{e}_1 \rangle$ either steps to fail Conv, in which case the original configuration with $\mathsf{if}\ \mathsf{e}_1\ 0\ 1$ takes another step to fail Conv, or steps to an irreducible configuration

$$\langle \Phi_{r1} \uplus \mathsf{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1}, \mathsf{H}_1^*, \mathsf{e}_1^* \rangle$$

in which case $\langle \Phi_{r2} \uplus \mathsf{flags}(W, 2) \uplus \Phi_2, \mathsf{H}_2, \mathsf{e}_2 \rangle$ steps to an irreducible configuration

$$\langle \Phi_{r2} \uplus \mathsf{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathsf{H}_2^*, \mathsf{e}_2^* \rangle$$

and there exists some world W' such that $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W', \mathsf{H}_1^*, \mathsf{H}_2^* : W'$, and $(W', (\Phi_{f1}, \mathsf{e}_1^*), (\Phi_{f2}, \mathsf{e}_2^*)) \in \mathcal{V}\llbracket \mathsf{bool} \rrbracket_{\rho}$. By expanding the value relation, we find $\Phi_{f1} = \Phi_{f2} = \emptyset$ and there are two cases:

(1) $\mathsf{e}_1^* = \mathsf{e}_2^* = 0$. In this scenario, we have

$$\begin{aligned}
&\langle \Phi_{r1} \uplus \mathsf{flags}(W, 1) \uplus \Phi_1, \mathsf{H}_1, \mathsf{if}\ \mathsf{e}_1\ 0\ 1 \rangle \overset{*}{\dashrightarrow}\\
&\langle \Phi_{r1} \uplus \mathsf{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1}, \mathsf{H}_1^*, \mathsf{if}\ 0\ 0\ 1 \rangle \dashrightarrow\\
&\langle \Phi_{r1} \uplus \mathsf{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1}, \mathsf{H}_1^*, 0 \rangle
\end{aligned}$$

and

$$\begin{aligned}
&\langle \Phi_{r2} \uplus \mathsf{flags}(W, 2) \uplus \Phi_2, \mathsf{H}_2, \mathsf{if}\ \mathsf{e}_2\ 0\ 1 \rangle \overset{*}{\dashrightarrow}\\
&\langle \Phi_{r2} \uplus \mathsf{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathsf{H}_2^*, \mathsf{if}\ 0\ 0\ 1 \rangle \dashrightarrow\\
&\langle \Phi_{r2} \uplus \mathsf{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathsf{H}_2^*, 0 \rangle
\end{aligned}$$

Then, we have from before that $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W'$ and $\mathsf{H}_1^*, \mathsf{H}_2^* : W'$, and one can easily see that $(W', (\emptyset, 0), (\emptyset, 0)) \in \mathcal{V}\llbracket \texttt{int} \rrbracket_{.}$, which suffices to finish the proof.

(2) $e_1^* = n_1$ and $e_2^* = n_2$ with $n_1, n_2 \neq 0$. In this scenario, we have

$$\begin{aligned}&\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, H_1, \mathrm{if}\ e_1\ 0\ 1\rangle \overset{*}{\dashrightarrow}\\ &\langle \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1}, H_1^*, \mathrm{if}\ n_1\ 0\ 1\rangle \dashrightarrow\\ &\langle \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1}, H_1^*, 1\rangle\end{aligned}$$

and

$$\begin{aligned}&\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, H_2, \mathrm{if}\ e_2\ 0\ 1\rangle \overset{*}{\dashrightarrow}\\ &\langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, H_2^*, \mathrm{if}\ n_2\ 0\ 1\rangle \dashrightarrow\\ &\langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, H_2^*, 1\rangle\end{aligned}$$

Then, we have from before that $W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W'$ and $H_1^*, H_2^* : W'$, and one can easily see that $(W', (\emptyset, 1), (\emptyset, 1)) \in \mathcal{V}\llbracket \mathtt{int} \rrbracket$., which suffices to finish the proof.

$\boxed{\tau_1 \otimes \tau_2 \sim \tau_1 \times \tau_2}$ There are two directions to this proof:

$$\forall\, (W, (\Phi_1, e_1), (\Phi_2, e_2)) \in \mathcal{E}\llbracket \tau_1 \otimes \tau_2 \rrbracket.\ \implies\ (W, (\Phi_1, C_{\tau_1 \otimes \tau_2 \mapsto \tau_1 \times \tau_2}(e_1)), (\Phi_2, C_{\tau_1 \otimes \tau_2 \mapsto \tau_1 \times \tau_2}(e_2))) \in \mathcal{E}\llbracket \tau_1 \times \tau$$

and:

$$\forall\, (W, (\Phi_1, e_1), (\Phi_2, e_2)) \in \mathcal{E}\llbracket \tau_1 \times \tau_2 \rrbracket.\ \implies\ (W, (\Phi_1, C_{\tau_1 \times \tau_2 \mapsto \tau_1 \otimes \tau_2}(e_1)), (\Phi_2, C_{\tau_1 \times \tau_2 \mapsto \tau_1 \otimes \tau_2}(e_2))) \in \mathcal{E}\llbracket \tau_1 \otimes \tau$$

Both directions are trivially similar to each other, so we will only prove the first direction. Expanding the definition of the convertibility boundaries, we refine this to:

$$\begin{aligned}&\forall\, (W, (\Phi_1, e_1), (\Phi_1, e_2)) \in \mathcal{E}\llbracket \tau_1 \otimes \tau_2 \rrbracket.\ \implies\\ &\quad (W,\\ &\quad (\Phi_1, \mathrm{let}\ x = e_1\ \mathrm{in}\ (C_{\tau_1 \mapsto \tau_1}(\mathrm{fst}\ x), C_{\tau_2 \mapsto \tau_2}(\mathrm{snd}\ x))),\\ &\quad (\Phi_2, \mathrm{let}\ x = e_2\ \mathrm{in}\ (C_{\tau_1 \mapsto \tau_1}(\mathrm{fst}\ x), C_{\tau_2 \mapsto \tau_2}(\mathrm{snd}\ x)))) \in \mathcal{E}\llbracket \tau_1 \times \tau_2 \rrbracket.\end{aligned}$$

From the expression relation, we first need to show the two expressions in the conclusion are closed. This follows from the fact that e_1, e_2 are closed, by the assumption that $(W, (\Phi_1, e_1), (\Phi_2, e_2)) \in \mathcal{E}\llbracket \tau_1 \otimes \tau_2 \rrbracket$., and that the new expressions do not introduce any new free variables. Next, we need to show that given:

$$\begin{aligned}&\forall \Phi_{r1}, \Phi_{r2}, H_1, H_2{:}W,\ e_1',\ H_1',\ j < W.k.\\ &\quad \Phi_{r1}, \Phi_{r2} : W \wedge\\ &\quad \langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, H_1, \mathrm{let}\ x = e_1\ \mathrm{in}\ (C_{\tau_1 \mapsto \tau_1}(\mathrm{fst}\ x), C_{\tau_2 \mapsto \tau_2}(\mathrm{snd}\ x))\rangle \overset{j}{\dashrightarrow} \langle \Phi_1', H_1', e_1'\rangle \nrightarrow\end{aligned}$$

Then it holds that:

$$\begin{aligned}&e_1' = \mathrm{fail}\ \textsc{Conv} \vee (\exists \Phi_{f1}\ \Phi_{g1}\ \Phi_{f2}\ \Phi_{g2}\ v_2 H_2' W'.\\ &\qquad \langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, H_2, \mathrm{let}\ x = e_2\ \mathrm{in}\ (C_{\tau_1 \mapsto \tau_1}(\mathrm{fst}\ x), C_{\tau_2 \mapsto \tau_2}(\mathrm{snd}\ x))\rangle\\ &\qquad\quad \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, H_2', v_2\rangle \nrightarrow\\ &\qquad \wedge\ \Phi_1' = \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge\\ &\qquad \wedge\ W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W' \wedge\ H_1', H_2' : W'\\ &\qquad \wedge\ (W', (\Phi_{f1}, e_1'), (\Phi_{f2}, v_2)) \in \mathcal{V}\llbracket \tau_1 \times \tau_2 \rrbracket)\}\end{aligned}$$

First, since the let expression in the first configuration terminates to an irreducible configuration, by inspection on the operational semantic, it must be the case that $\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, H_1, e_1\rangle$ terminates to some irreducible configuration $\langle \Phi_1^*, H_1^*, e_1^*\rangle$. Then, by assumption, it follows that either $e_1^* = \mathrm{fail}\ \textsc{Conv}$, in which case the whole let expression steps to fail Conv, or that e_1^* is a value, in which case $\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, H_2, e_2\rangle$ also steps to some irreducible configuration $\langle \Phi_2^*, H_2^*, e_2^*\rangle$ and there exists some world W_1 where $\Phi_i^* = \Phi_{ri} \uplus \mathrm{flags}(W_1, i) \uplus \Phi_i^\dagger$, $W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W_1$, $H_1^*, H_2^* : W_1$, and

$(W_1, (\Phi_1^\dagger, \mathrm{e}_1^*), (\Phi_2^\dagger, \mathrm{e}_2^*)) \in \mathcal{V}[\![\tau_1 \otimes \tau_2]\!]_{.}$. By expanding the value relation definition, we find that $\mathrm{e}_1^* = (\mathrm{v}_1^*, \mathrm{v}_2^*)$ and $\mathrm{e}_2^* = (\mathrm{v}_1^\dagger, \mathrm{v}_2^\dagger)$ where $(W_1, (\Phi_{1a}, \mathrm{v}_1^*), (\Phi_{2a}, \mathrm{v}_1^\dagger)) \in \mathcal{V}[\![\tau_1]\!]_{.}$ and $(W_1, (\Phi_{1b}, \mathrm{v}_2^*), (\Phi_{2b}, \mathrm{v}_2^\dagger)) \in \mathcal{V}[\![\tau_2]\!]_{.}$, where $\Phi_1^\dagger = \Phi_{1a} \uplus \Phi_{1b}$ and $\Phi_2^\dagger = \Phi_{2a} \uplus \Phi_{2b}$.

Thus, the first configuration steps as follows:

$$\begin{aligned}
&\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, \mathrm{let\ x = e_1\ in\ } (\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{fst\ x}), \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{snd\ x}))\rangle \xrightarrow{*}\\
&\langle \Phi_{r1} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_1^\dagger, \mathrm{H}_1^*, \mathrm{let\ x} = (\mathrm{v}_1^*, \mathrm{v}_2^*)\ \mathrm{in\ } (\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{fst\ x}), \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{snd\ x}))\rangle \longrightarrow\\
&\langle \Phi_{r1} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_1^\dagger, \mathrm{H}_1^*, (\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{fst\ }(\mathrm{v}_1^*, \mathrm{v}_2^*)), \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{snd\ }(\mathrm{v}_1^*, \mathrm{v}_2^*)))\rangle \longrightarrow\\
&\langle \Phi_{r1} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_1^\dagger, \mathrm{H}_1^*, (\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{v}_1^*), \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{v}_2^*))\rangle
\end{aligned}$$

By a similar argument, the configuration on the other side with H_2 steps to

$$\langle \Phi_{r2} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_2^\dagger, \mathrm{H}_2^*, (\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{v}_1^\dagger), \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{v}_2^\dagger))\rangle$$

Since $(W_1, (\Phi_{1a}, \mathrm{v}_1^*), (\Phi_{2a}, \mathrm{v}_1^\dagger)) \in \mathcal{V}[\![\tau_1]\!]_{.} \subseteq \mathcal{E}[\![\tau_1]\!]_{.}$ and $(W_1, (\Phi_{1b}, \mathrm{v}_2^*), (\Phi_{2b}, \mathrm{v}_2^\dagger)) \in \mathcal{V}[\![\tau_2]\!]_{.} \subseteq \mathcal{E}[\![\tau_2]\!]_{.}$, by the induction hypothesis, we have that

$$(W_1, (\Phi_{1a}, \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{v}_1^*)), (\Phi_{2a}, \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{v}_1^\dagger))) \in \mathcal{E}[\![\tau_1]\!].$$

and

$$(W_1, (\Phi_{1b}, \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{v}_2^*)), (\Phi_{2b}, \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{v}_2^\dagger))) \in \mathcal{E}[\![\tau_2]\!].$$

By the first fact, either $\langle \Phi_{r1} \uplus \Phi_{1b} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{1a}, \mathrm{H}_1^*, \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{v}_1^*)\rangle$ steps to fail Conv (note our choice of "rest" of flags includes those owned by the other half of the pair), in which case the original configuration with H_1 steps to fail Conv, or it steps to an irreducible configuration

$$\langle \Phi_{r1} \uplus \Phi_{1b} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{1a}^f, \mathrm{H}_1^\dagger, \mathrm{v}_1^{**}\rangle$$

in which case $\langle \Phi_{r2} \uplus \Phi_{2b} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{2a}, \mathrm{H}_2^*, \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{v}_1^\dagger)\rangle$ also steps to an irreducible configuration

$$\langle \Phi_{r2} \uplus \Phi_{2b} \uplus \mathrm{flags}(W_2, 2) \uplus \Phi_{2a}^f, \mathrm{H}_2^\dagger, \mathrm{v}_1^{\dagger\dagger}\rangle$$

and there exists some world W_2 where $W_1 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{1b}, \Phi_{r2} \uplus \Phi_{2b}} W_2, \mathrm{H}_1^\dagger, \mathrm{H}_2^\dagger : W_2$, and $(W_2, (\Phi_{1a}^f, \mathrm{v}_1^{**}), (\Phi_{2a}^f, \mathrm{v}_1^{\dagger\dagger})) \in \mathcal{V}[\![\tau_1]\!]_{.}$.

Once the first component of the pair in the configurations above have stepped to values v_1^{**} and $\mathrm{v}_1^{\dagger\dagger}$, the pair will continue reducing on the second component. Then, by Lemma 3.8, since $W_1 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{1b}, \Phi_{r2} \uplus \Phi_{2b}} W_2$ (which includes Φ_{1b} and Φ_{2b}),

$$(W_2, (\Phi_{1b}, \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{v}_2^*)), (\Phi_{2b}, \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{v}_2^\dagger))) \in \mathcal{E}[\![\tau_2]\!].$$

Thus, either $\langle \Phi_{r1} \uplus \Phi_{1a}^f \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{1b}, \mathrm{H}_1^\dagger, \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{v}_2^*)\rangle$ steps to fail Conv, in which case the original configuration also takes a step to fail Conv, or it steps to an irreducible configuration

$$\langle \Phi_{r1} \uplus \Phi_{1a}^f \uplus \mathrm{flags}(W_3, 1) \uplus \Phi_{1b}^f, \mathrm{H}_1^f, \mathrm{v}_2^{**}\rangle$$

in which case $\langle \Phi_{r2} \uplus \Phi_{2a}^f \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{2b}, \mathrm{H}_2^\dagger, \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{v}_2^\dagger)\rangle$ also steps to an irreducible configuration $\langle \Phi_{r2} \uplus \Phi_{2a}^f \uplus \mathrm{flags}(W_3, 1) \uplus \Phi_{2b}^f, \mathrm{H}_2^f, \mathrm{v}_2^{\dagger\dagger}\rangle$ and there exists some world W_3 where $W_2 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{1a}^f, \Phi_{r2} \uplus \Phi_{2a}^f} W_3, \mathrm{H}_1^f, \mathrm{H}_2^f : W_3$, and $(W_3, (\Phi_{1b}^f, \mathrm{v}_2^{**}), (\Phi_{2b}^f, \mathrm{v}_2^{\dagger\dagger})) \in \mathcal{V}[\![\tau_2]\!]_{.}$.

Thus, the original configuration with H_1 and $\Phi_1 \uplus \Phi_2$ steps to $\langle \Phi_r \uplus \mathrm{flags}(W_3, 1) \uplus \Phi_{1a}^f \uplus \Phi_{1b}^f, \mathrm{H}_1^f, (\mathrm{v}_1^{**}, \mathrm{v}_2^{**})\rangle$ and the original configuration with H_2 steps to $\langle \Phi_r \uplus \mathrm{flags}(W_3, 2) \uplus \Phi_{2a}^f \uplus \Phi_{2b}^f, \mathrm{H}_2^f, (\mathrm{v}_1^{\dagger\dagger}, \mathrm{v}_2^{\dagger\dagger})\rangle$. We have $\mathrm{H}_1^f, \mathrm{H}_2^f : W_3$ and, since $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_1$, $W_1 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{1b}^\dagger, \Phi_{r2} \uplus \Phi_{2b}^\dagger} W_2$, and $W_2 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{1a}^f, \Phi_{r2} \uplus \Phi_{2a}^f} W_3$, it follows from Lemma 3.9 that $W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W_3$. Moreover, since $W_2 \sqsubseteq_{\Phi_{r1}\uplus\Phi^f_{1a},\Phi_{r2}\uplus\Phi^f_{2a}} W_3$ and $(W_2, (\Phi^f_{1a}, \mathrm{v}^{**}_1), (\Phi^f_{2a}, \mathrm{v}^{\dagger\dagger}_1)) \in \mathcal{V}\llbracket\tau_1\rrbracket$., we have $(W_3, (\Phi^f_{1a}, \mathrm{v}^{**}_1), (\Phi^f_{2a}, \mathrm{v}^{\dagger\dagger}_1)) \in \mathcal{V}\llbracket\tau_1\rrbracket$.. Finally, we also have $(W_3, (\Phi^f_{1b}, \mathrm{v}^{**}_2), (\Phi^f_{2b}, \mathrm{v}^{\dagger\dagger}_2)) \in \mathcal{V}\llbracket\tau_2\rrbracket$.. Ergo,

$$(W_3, (\Phi^f_{1a} \uplus \Phi^f_{1b}, (\mathrm{v}^{**}_1, \mathrm{v}^{**}_2)), (\Phi^f_{2a} \uplus \Phi^f_{2b}, (\mathrm{v}^{\dagger\dagger}_1, \mathrm{v}^{\dagger\dagger}_2))) \in \mathcal{V}\llbracket\tau_1 \times \tau_2\rrbracket.$$

which suffices to finish the proof.

$\boxed{\tau_1 \multimap \tau_2 \sim (\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2}$

There are two directions, we first prove the former implication, that is, that:

$$\begin{array}{l}\forall\, (W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}\llbracket\tau_1 \multimap \tau_2\rrbracket.\implies \\ (W, (\Phi_1, C_{\tau_1 \multimap \tau_2 \mapsto (\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2}(\mathrm{e}_1)), (\Phi_2, C_{\tau_1 \multimap \tau_2 \mapsto (\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2}(\mathrm{e}_2))) \in \mathcal{E}\llbracket(\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2\rrbracket.\end{array}$$

Expanding the definition of the convertibility boundaries, we refine our goal to:

$$\begin{array}{l}(W, (\Phi_1, \mathrm{let\ x} = \mathrm{e}_1 \mathrm{\ in\ } \lambda \mathrm{x_{thnk}}.\mathrm{let\ x_{conv}} = \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}}\ ()) \\ \qquad\qquad \mathrm{in\ let\ x_{access}} = \mathrm{thunk}(\mathrm{x_{conv}}) \mathrm{\ in\ C}_{\tau_2 \mapsto \tau_2}(\mathrm{x\ x_{access}})), \\ \quad (\Phi_2, \mathrm{let\ x} = \mathrm{e}_2 \mathrm{\ in\ } \lambda \mathrm{x_{thnk}}.\mathrm{let\ x_{conv}} = \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}}\ ()) \\ \qquad\qquad \mathrm{in\ let\ x_{access}} = \mathrm{thunk}(\mathrm{x_{conv}}) \mathrm{\ in\ C}_{\tau_2 \mapsto \tau_2}(\mathrm{x\ x_{access}}))) \\ \quad \in \mathcal{E}\llbracket(\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2\rrbracket.\end{array}$$

From the expression relation, we must show first that the terms are closed, which follows from out hypothesis given we did not introduce any new free variables. Then, we need to show that given:

$$\begin{array}{l}\forall \Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}'_1,\ \mathrm{H}'_1,\ j < W.k. \\ \quad \Phi_{r1}, \Phi_{r2} : W \wedge \\ \quad \left\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1,\ \begin{array}{l}\mathrm{let\ x} = \mathrm{e}_1 \mathrm{\ in\ } \lambda \mathrm{x_{thnk}}.\mathrm{let\ x_{conv}} = \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}}\ ()) \mathrm{\ in} \\ \mathrm{let\ x_{access}} = \mathrm{thunk}(\mathrm{x_{conv}}) \mathrm{\ in\ C}_{\tau_2 \mapsto \tau_2}(\mathrm{x\ x_{access}})\end{array} \right\rangle \overset{j}{\dashrightarrow} \langle \Phi'_1, \mathrm{H}'_1, \mathrm{e}'_1 \rangle \nrightarrow\end{array}$$

Then it holds that:

$$\begin{array}{l}\mathrm{e}'_1 = \mathrm{fail}\ \textsc{Conv} \vee (\exists \Phi_{f1}\ \Phi_{g1}\ \Phi_{f2}\ \Phi_{g2}\ \mathrm{v}_2 \mathrm{H}'_2 W'. \\ \qquad \left\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2,\ \begin{array}{l}\mathrm{let\ x} = \mathrm{e}_2 \mathrm{\ in\ } \lambda \mathrm{x_{thnk}}.\mathrm{let\ x_{conv}} = \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}}\ ()) \mathrm{\ in} \\ \mathrm{let\ x_{access}} = \mathrm{thunk}(\mathrm{x_{conv}}) \mathrm{\ in\ C}_{\tau_2 \mapsto \tau_2}(\mathrm{x\ x_{access}})\end{array} \right\rangle \\ \qquad\quad \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathrm{H}'_2, \mathrm{v}_2 \rangle \nrightarrow \\ \qquad \wedge\ \Phi'_1 = \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge \\ \qquad \wedge\ W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W' \wedge\ \mathrm{H}'_1, \mathrm{H}'_2 : W' \\ \qquad \wedge\ (W', (\Phi_{f1}, \mathrm{e}'_1), (\Phi_{f2}, \mathrm{v}_2)) \in \mathcal{V}\llbracket(\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2\rrbracket)\}\end{array}$$

To figure out what e'_1 is, we know from the operational semantics that first we will evaluate e_1 until it is a value and then will substitute. From our hypothesis, which we can instantiate with $\Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2$, etc, we know that either e_1 will run forever, in which case the entire term will and we are done (trivially). Otherwise, we have that:

$$\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, \mathrm{e}_1 \rangle \overset{j}{\dashrightarrow} \langle \overline{\Phi_1}, \mathrm{H}^{\dagger}_1, \mathrm{e}^{\dagger}_1 \rangle \nrightarrow$$

And that:

$$\begin{aligned}\mathrm{e}_1^\dagger = \mathrm{fail}\ \textsc{Conv} \vee (\exists \Phi_{f1}\ \Phi_{g1}\ \Phi_{f2}\ \Phi_{g2}\ \mathrm{v}_2 \mathrm{H}_2' W'.\\ &\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, \mathrm{e}_2\rangle\\ &\quad \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W^\dagger, 2) \uplus \Phi_2^\dagger \uplus \Phi_{g2}, \mathrm{H}_2^\dagger, \mathrm{e}_2^\dagger\rangle \not\twoheadrightarrow\\ &\wedge \overline{\Phi_1} = \Phi_{r1} \uplus \mathrm{flags}(W^\dagger, 1) \uplus \Phi_1^\dagger \uplus \Phi_{g1} \wedge\\ &\wedge\ W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W^\dagger \wedge\ \mathrm{H}_1^\dagger, \mathrm{H}_2^\dagger : W^\dagger\\ &\wedge (W^\dagger, (\Phi_1^\dagger, \mathrm{e}_1^\dagger), (\Phi_2^\dagger, \mathrm{e}_2^\dagger)) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!])\}\end{aligned}$$

Where if $\mathrm{e}_1{}^\dagger$ is fail Conv then the operational semantics will lift that to the entire term and we will be done. Note also that from the definition of $\mathcal{V}[\![\tau_1 \multimap \tau_2]\!]$., we know $\Phi_i^\dagger = \emptyset$.

Now, returning to our original reduction, we will take another step and substitute $\mathrm{e}_1{}^\dagger$ for x, which results in the following term:

$$\lambda \mathrm{x}_{\mathrm{thnk}}.\mathrm{let}\ \mathrm{x}_{\mathrm{conv}} = \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x}_{\mathrm{thnk}}\ ())\ \mathrm{in}\ \mathrm{let}\ \mathrm{x}_{\mathrm{access}} = \mathrm{thunk}(\mathrm{x}_{\mathrm{conv}})\ \mathrm{in}\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{e}_1^\dagger\ \mathrm{x}_{\mathrm{access}})$$

This is clearly irreducible (it is a value), so we now need to show that the other side similarly reduces to a value, which follows in the same way from our hypothesis, and thus what remains to show is that these two values are related at $W^\dagger$ in $\mathcal{V}[\![(\mathtt{unit} \to \tau_1) \to \tau_2]\!]$. (we choose $W^\dagger$ because no changes to heap or flags happened in the substitution).

The definition of $\mathcal{V}[\![(\mathtt{unit} \to \tau_1) \to \tau_2]\!]$. says that we need to take any world W', where $W^\dagger \sqsubseteq_{\emptyset,\emptyset} W'$, $(W', (\emptyset, \mathrm{v}_1'), (\emptyset, \mathrm{v}_2')) \in \mathcal{V}[\![\mathtt{unit} \to \tau_1]\!]$. and show that

$$\begin{aligned}(W', (\emptyset, [\mathrm{x}_{\mathrm{thnk}} \mapsto \mathrm{v}_1']\mathrm{let}\ \mathrm{x}_{\mathrm{conv}} = \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x}_{\mathrm{thnk}}\ ())\ \mathrm{in}\ \mathrm{let}\ \mathrm{x}_{\mathrm{access}} = \mathrm{thunk}(\mathrm{x}_{\mathrm{conv}})\ \mathrm{in}\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{e}_1^\dagger\ \mathrm{x}_{\mathrm{access}})),\\ (\emptyset, [\mathrm{x}_{\mathrm{thnk}} \mapsto \mathrm{v}_2']\mathrm{let}\ \mathrm{x}_{\mathrm{conv}} = \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x}_{\mathrm{thnk}}\ ())\ \mathrm{in}\ \mathrm{let}\ \mathrm{x}_{\mathrm{access}} = \mathrm{thunk}(\mathrm{x}_{\mathrm{conv}})\ \mathrm{in}\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{e}_2^\dagger\ \mathrm{x}_{\mathrm{access}}))) \in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

Where if we substitute, we get:

$$\begin{aligned}(W', (\emptyset, \mathrm{let}\ \mathrm{x}_{\mathrm{conv}} = \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{v}_1'\ ())\ \mathrm{in}\ \mathrm{let}\ \mathrm{x}_{\mathrm{access}} = \mathrm{thunk}(\mathrm{x}_{\mathrm{conv}})\ \mathrm{in}\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{e}_1^\dagger\ \mathrm{x}_{\mathrm{access}})),\\ (\emptyset, \mathrm{let}\ \mathrm{x}_{\mathrm{conv}} = \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{v}_2'\ ())\ \mathrm{in}\ \mathrm{let}\ \mathrm{x}_{\mathrm{access}} = \mathrm{thunk}(\mathrm{x}_{\mathrm{conv}})\ \mathrm{in}\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{e}_2^\dagger\ \mathrm{x}_{\mathrm{access}}))) \in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

Now we can expand the definition of thunk(·), to get:

$$\begin{aligned}&(W', (\emptyset, \mathrm{let}\ \mathrm{x}_{\mathrm{conv}} = \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{v}_1'\ ())\ \mathrm{in}\ \mathrm{let}\ \mathrm{x}_{\mathrm{access}} =\\ &\qquad (\mathrm{let}\ \mathrm{r}_{\mathrm{fresh}} = \mathrm{ref}\ 1\ \mathrm{in}\ \lambda\_.\{\mathrm{if}\ !\mathrm{r}_{\mathrm{fresh}}\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\mathrm{r}_{\mathrm{fresh}} := 0; \mathrm{x}_{\mathrm{conv}}\}\})\ \mathrm{in}\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{e}_1^\dagger\ \mathrm{x}_{\mathrm{access}})),\\ &\quad (\emptyset, \mathrm{let}\ \mathrm{x}_{\mathrm{conv}} = \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{v}_2'\ ())\ \mathrm{in}\ \mathrm{let}\ \mathrm{x}_{\mathrm{access}} =\\ &\qquad (\mathrm{let}\ \mathrm{r}_{\mathrm{fresh}} = \mathrm{ref}\ 1\ \mathrm{in}\ \lambda\_.\{\mathrm{if}\ !\mathrm{r}_{\mathrm{fresh}}\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\mathrm{r}_{\mathrm{fresh}} := 0; \mathrm{x}_{\mathrm{conv}}\}\})\ \mathrm{in}\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{e}_2^\dagger\ \mathrm{x}_{\mathrm{access}})))\\ &\quad \in \mathcal{E}[\![\tau_2]\!].\end{aligned}$$

From our induction hypothesis, instantiated with $\triangleright W'$ we know $(\triangleright W', (\emptyset, \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{v}_1'\ ())), (\emptyset, \mathrm{C}_{\tau_1 \mapsto \tau_1}(v_2'\ ())))$ will be in $\mathcal{E}[\![\tau_1]\!]$. if $(\triangleright W', (\emptyset, \mathrm{v}_1'\ ()), (\emptyset, \mathrm{v}_2'\ ()))$ is in $\mathcal{E}[\![\tau_1]\!]$. But, since $(W', (\emptyset, \mathrm{v}_1'), (\emptyset, \mathrm{v}_2')) \in \mathcal{V}[\![\mathtt{unit} \to \tau_1]\!]$., by definition the latter holds, since the only values in $\mathcal{V}[\![\mathtt{unit}]\!]$. are ().

This means we can unfold the definition of $\mathcal{E}[\![\tau_1]\!]$. and know that for any $\Phi_{r1}, \Phi_{r2} : \triangleright W'$, $\mathrm{H}_1, \mathrm{H}_2 : \triangleright W'$:

$$\langle \Phi_{r1} \uplus \mathrm{flags}(\triangleright W', 1) \uplus \emptyset, \mathrm{H}_1, \mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{v}_1'\ ())\rangle \overset{j}{\dashrightarrow} \langle \overline{\Phi_1}, \mathrm{H}_{c1}, \mathrm{v}_{c1}\rangle \not\twoheadrightarrow$$

Assuming v_{c1} is not fail Conv:

$$\begin{aligned}
&\exists \Phi_{c1}\ \Phi_{g1}\ \Phi_{c2}\ \Phi_{g2}\ \mathsf{v}_{c2}\mathsf{H}_{c2}\, W''.\\
&\quad \langle \Phi_{r2} \uplus \text{flags}(\triangleright W', 2) \uplus \emptyset, \mathsf{H}_2, \mathsf{C}_{\tau_1 \mapsto \tau_1}(v_2'\ ()))\rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \text{flags}(W^c, 2) \uplus \Phi_{c2} \uplus \Phi_{g2}, \mathsf{H}_{c2}, \mathsf{v}_{c2}\rangle \nrightarrow\\
&\qquad \wedge\ \overline{\Phi_1} = \Phi_{r1} \uplus \text{flags}(W'', 1) \uplus \Phi_{c1} \uplus \Phi_{g1} \wedge\\
&\qquad \wedge\ \triangleright W' \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W'' \wedge\ \mathsf{H}_{c1}, \mathsf{H}_{c2} : W''\\
&\qquad \wedge\ (W'', (\Phi_{c1}, \mathsf{v}_{c1}), (\Phi_{c2}, \mathsf{v}_{c2})) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!])\}
\end{aligned}$$

If we return to our original obligation, we need to show that for some $\Phi_{r1}', \Phi_{r2}', \mathsf{H}_1', \mathsf{H}_2' : W'$ that if:

$$\begin{aligned}
&\left\langle \Phi_{r1}' \uplus \text{flags}(W', 1) \uplus \emptyset, \mathsf{H}_1,\
\begin{array}{l}
\mathsf{let}\ \mathsf{x}_{\mathsf{conv}} = \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{v}_1'\ ())\ \mathsf{in}\ \mathsf{let}\ \mathsf{x}_{\mathsf{access}} =\\
(\mathsf{let}\ \mathsf{r}_{\mathsf{fresh}} = \mathsf{ref}\ 1\ \mathsf{in}\ \lambda\_.\{\mathsf{if}\ !\mathsf{r}_{\mathsf{fresh}}\ \{\mathsf{fail}\ \textsc{Conv}\}\ \{\mathsf{r}_{\mathsf{fresh}} := 0; \mathsf{x}_{\mathsf{conv}}\}\})\ \mathsf{in}\\
\mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{e}_1^{\dagger}\ \mathsf{x}_{\mathsf{access}})
\end{array}\right\rangle\\
&\quad \overset{j}{\dashrightarrow} \langle \overline{\Phi_1}, \mathsf{H}_1'', \mathsf{e}_1' \rangle \nrightarrow
\end{aligned}$$

Then:

$$\begin{aligned}
&\exists \Phi_1''\ \Phi_{g1}\ \Phi_2''\ \Phi_{g2}\ \mathsf{e}_2'\mathsf{H}_2''\, W'''.\\
&\quad \left\langle \Phi_{r2} \uplus \text{flags}(W', 2) \uplus \emptyset, \mathsf{H}_2,\
\begin{array}{l}
\mathsf{let}\ \mathsf{x}_{\mathsf{conv}} = \mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{v}_2'\ ())\ \mathsf{in}\\
\mathsf{let}\ \mathsf{x}_{\mathsf{access}} = (\mathsf{let}\ \mathsf{r}_{\mathsf{fresh}} = \mathsf{ref}\ 1\ \mathsf{in}\\
\quad \lambda\_.\{\mathsf{if}\ !\mathsf{r}_{\mathsf{fresh}}\ \{\mathsf{fail}\ \textsc{Conv}\}\ \{\mathsf{r}_{\mathsf{fresh}} := 0; \mathsf{x}_{\mathsf{conv}}\}\})\\
\mathsf{in}\ \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_2\ \mathsf{x}_{\mathsf{access}})
\end{array}\right\rangle\\
&\qquad \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \text{flags}(W^c, 2) \uplus \Phi_{c2} \uplus \Phi_{g2}, \mathsf{H}_{c2}, \mathsf{v}_{c2}\rangle \nrightarrow\\
&\qquad \wedge\ \overline{\Phi_1} = \Phi_{r1} \uplus \text{flags}(W'', 1) \uplus \Phi_{c1} \uplus \Phi_{g1} \wedge\\
&\qquad \wedge\ \triangleright W' \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W'' \wedge\ \mathsf{H}_{c1}, \mathsf{H}_{c2} : W''\\
&\qquad \wedge\ (W'', (\Phi_{c1}, \mathsf{v}_{c1}), (\Phi_{c2}, \mathsf{v}_{c2})) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!])\}
\end{aligned}$$

If we choose Φ_{ri}' to be that chosen above, we know $\mathsf{C}_{\tau_1 \mapsto \tau_1}(\mathsf{v}_1'\ ())$ reduces to v_{c2} with Φ_{c1}, and thus the entire term takes a step to:

$$\left\langle \Phi_{r1} \uplus \text{flags}(W'', 1) \uplus \Phi_{c1}, \mathsf{H}_{c1},\
\begin{array}{l}
\mathsf{let}\ \mathsf{x}_{\mathsf{conv}} = \mathsf{v}_{c1}\ \mathsf{in}\ \mathsf{let}\ \mathsf{x}_{\mathsf{access}} =\\
(\mathsf{let}\ \mathsf{r}_{\mathsf{fresh}} = \mathsf{ref}\ 1\ \mathsf{in}\ \lambda\_.\{\mathsf{if}\ !\mathsf{r}_{\mathsf{fresh}}\ \{\mathsf{fail}\ \textsc{Conv}\}\ \{\mathsf{r}_{\mathsf{fresh}} := 0; \mathsf{x}_{\mathsf{conv}}\}\})\ \mathsf{in}\\
\mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{e}_1^{\dagger}\ \mathsf{x}_{\mathsf{access}})
\end{array}\right\rangle$$

Which then takes two more steps to:

$$\left\langle \Phi_{r1} \uplus \text{flags}(W'', 1) \uplus \Phi_{c1}, \mathsf{H}_{c1},\
\begin{array}{l}
\mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{e}_1^{\dagger}\\
(\mathsf{let}\ \mathsf{r}_{\mathsf{fresh}} = \mathsf{ref}\ 1\ \mathsf{in}\ \lambda\_.\{\mathsf{if}\ !\mathsf{r}_{\mathsf{fresh}}\ \{\mathsf{fail}\ \textsc{Conv}\}\ \{\mathsf{r}_{\mathsf{fresh}} := 0; \mathsf{v}_{c1}\}\}))
\end{array}\right\rangle$$

To figure out where that steps next, we need to appeal to our induction hypothesis. In particular, we instantiate it with W'', which then tells us that:

$$\begin{aligned}
&(W'', (\Phi_{c1}, \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{e}_1^{\dagger}\ (\mathsf{let}\ \mathsf{r}_{\mathsf{fresh}} = \mathsf{ref}\ 1\ \mathsf{in}\ \lambda\_.\{\mathsf{if}\ !\mathsf{r}_{\mathsf{fresh}}\ \{\mathsf{fail}\ \textsc{Conv}\}\ \{\mathsf{r}_{\mathsf{fresh}} := 0; \mathsf{v}_{c1}\}\}))),\\
&\quad (\Phi_{c2}, \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{e}_2^{\dagger}\ (\mathsf{let}\ \mathsf{r}_{\mathsf{fresh}} = \mathsf{ref}\ 1\ \mathsf{in}\ \lambda\_.\{\mathsf{if}\ !\mathsf{r}_{\mathsf{fresh}}\ \{\mathsf{fail}\ \textsc{Conv}\}\ \{\mathsf{r}_{\mathsf{fresh}} := 0; \mathsf{v}_{c2}\}\})))) \in \mathcal{E}[\![\tau_2]\!].
\end{aligned}$$

If we can show:

$$\begin{aligned}
&(W'', (\Phi_{c1}, (\mathsf{e}_1^{\dagger}\ (\mathsf{let}\ \mathsf{r}_{\mathsf{fresh}} = \mathsf{ref}\ 1\ \mathsf{in}\ \lambda\_.\{\mathsf{if}\ !\mathsf{r}_{\mathsf{fresh}}\ \{\mathsf{fail}\ \textsc{Conv}\}\ \{\mathsf{r}_{\mathsf{fresh}} := 0; \mathsf{v}_{c1}\}\}))),\\
&\quad (\Phi_{c2}, (\mathsf{e}_2^{\dagger}\ (\mathsf{let}\ \mathsf{r}_{\mathsf{fresh}} = \mathsf{ref}\ 1\ \mathsf{in}\ \lambda\_.\{\mathsf{if}\ !\mathsf{r}_{\mathsf{fresh}}\ \{\mathsf{fail}\ \textsc{Conv}\}\ \{\mathsf{r}_{\mathsf{fresh}} := 0; \mathsf{v}_{c2}\}\})))) \in \mathcal{E}[\![\tau_2]\!].
\end{aligned}$$

To show the latter, recall that $(W^{\dagger}, (\emptyset, \mathrm{e}_1^{\dagger}), (\emptyset, \mathrm{e}_2^{\dagger})) \in \mathcal{V}\llbracket \tau_1 \multimap \tau_1 \rrbracket$.. We know that $W^{\dagger} \sqsubseteq_{\emptyset,\emptyset} W'$, $W' \sqsubseteq_{\emptyset,\emptyset} \triangleright W'$, and $\triangleright W' \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W''$, so via Lemma 3.9, $W^{\dagger} \sqsubseteq_{\emptyset,\emptyset} W''$ and thus via Lemma 3.8, $(W'', (\emptyset, \mathrm{e}_1^{\dagger}), (\emptyset, \mathrm{e}_2^{\dagger})) \in \mathcal{V}\llbracket \tau_1 \multimap \tau_1 \rrbracket$.. In particular, we know that each have the form $\lambda \mathrm{x}.\mathrm{e}_i^{*}$.

That means, if we can show, for some Φ_{c1}, Φ_{c2} and some world W''' where $W'' \sqsubseteq_{\emptyset,\emptyset} W'''$, that $(W''', (\Phi_{c1}, v_{c1}), (\Phi_{c2}, v_{c2})) \in \mathcal{V}\llbracket \tau_2 \rrbracket$. (which we have from before) then

$$(W^A, (\emptyset, [x \mapsto \mathrm{guard}(v_{c1}, \ell_1)] e_1^{*}), (\emptyset, [x \mapsto \mathrm{guard}(v_{c2}, \ell_2)] e_2^{*})) \in \mathcal{E}\llbracket \tau_1 \rrbracket.$$

Where $W^A = (W'''.k, W'''.\Psi, W'''.\Theta \uplus (\ell_1, \ell_2) \mapsto (\Phi_{c1}, \Phi_{c2}))$.

In particular, we let $W''' = W''$.

To connect these two together, we first unfold the former: the definition means that for any $\Phi''_{r1}, \Phi''_{r1} : W''$ and $\mathrm{H}''_1, \mathrm{H}''_2 : W''$, we need to show:

$$\begin{array}{l}\langle \Phi''_{r1} \uplus \mathrm{flags}(W'', 1) \uplus \Phi_{c1}, \mathrm{H}''_1, (\lambda \mathrm{x}.\mathrm{e}_1^{*})\ (\mathrm{let}\ \mathrm{r_{fresh}} = \mathrm{ref}\ 1\ \mathrm{in}\ \lambda\_.\{\mathrm{if}\ !\mathrm{r_{fresh}}\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\mathrm{r_{fresh}} := 0; \mathrm{v_{c1}}\}\})\rangle \\ \overset{j}{\dashrightarrow} \langle \overline{\Phi'''_1}, \mathrm{H}''''_1, \mathrm{e}''''_1 \rangle \not\twoheadrightarrow\end{array}$$

The latter will give us the reduction, for $\Phi^A_{r1}, \Phi^A_{r2} : W^A$ and $\mathrm{H}^A_1, \mathrm{H}^A_2 : W^A$:

$$\langle \Phi^A_{r1} \uplus \mathrm{flags}(W^A, 1) \uplus \emptyset, \mathrm{H}^A_1, [x \mapsto \mathrm{guard}(v_{c1}, \ell_1)] e_1^{*} \rangle \overset{j}{\dashrightarrow} \langle \overline{\Phi^A_1}, \mathrm{H}^B_1, \mathrm{e}^{\mathrm{B}}_1 \rangle \not\twoheadrightarrow$$

In particular, since W^A is identical to W'' aside from gaining Φ_{c1}, Φ_{c2}, we can use Φ''_{ri} as Φ^A_{ri} and $\mathrm{flags}(W'') \uplus \Phi_{c1} = \mathrm{flags}(W^A) \uplus \emptyset$.

Thus, the former takes one step to the latter, and the rest of what we need follows.

We now return to our original goal, that is, showing how this reduces:

$$\left\langle \Phi_{r1} \uplus \mathrm{flags}(W'', 1) \uplus \Phi_{c1}, \mathrm{H}_{c1}, \begin{array}{l} \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{e}_1^{\dagger} \\ (\mathrm{let}\ \mathrm{r_{fresh}} = \mathrm{ref}\ 1\ \mathrm{in}\ \lambda\_.\{\mathrm{if}\ !\mathrm{r_{fresh}}\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\mathrm{r_{fresh}} := 0; \mathrm{v_{c1}}\}\})) \end{array} \right\rangle$$

Since we now know:

$$\begin{array}{l}(W'', (\Phi_{c1}, \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{e}_1^{\dagger}\ (\mathrm{let}\ \mathrm{r_{fresh}} = \mathrm{ref}\ 1\ \mathrm{in}\ \lambda\_.\{\mathrm{if}\ !\mathrm{r_{fresh}}\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\mathrm{r_{fresh}} := 0; \mathrm{v_{c1}}\}\}))), \\ \quad (\Phi_{c2}, \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{e}_2^{\dagger}\ (\mathrm{let}\ \mathrm{r_{fresh}} = \mathrm{ref}\ 1\ \mathrm{in}\ \lambda\_.\{\mathrm{if}\ !\mathrm{r_{fresh}}\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\mathrm{r_{fresh}} := 0; \mathrm{v_{c2}}\}\})))) \in \mathcal{E}\llbracket \tau_2 \rrbracket.\end{array}$$

We can unfold the definition and get exactly what we need, as what we were originally showing was that the term in question was in $\mathcal{E}\llbracket \tau_2 \rrbracket$..

Thus, we are done with the first direction.

Now we have to prove the other direction, that is, that:

$$\begin{array}{l}\forall\ (W, (\Phi_1, \mathrm{e}_1), (\Phi_2, \mathrm{e}_2)) \in \mathcal{E}\llbracket (\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2 \rrbracket. \implies \\ (W, (\Phi_1, C_{(\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2 \mapsto \tau_1 \multimap \tau_2}(\mathrm{e}_1)), (\Phi_2, C_{(\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2 \mapsto \tau_1 \multimap \tau_2}(\mathrm{e}_2))) \in \mathcal{E}\llbracket \tau_1 \multimap \tau_2 \rrbracket.\end{array}$$

Expanding the definition of the convertibility boundaries, we refine our goal to:

$$\begin{array}{l}(W, (\Phi_1, \mathrm{let}\ \mathrm{x}\ =\ \mathrm{e}_1\ \mathrm{in}\ \lambda \mathrm{x_{thnk}}.\mathrm{let}\ \mathrm{x_{access}}\ =\ \mathrm{thunk}(\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}}\ ()))\ \mathrm{in}\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{x}\ \mathrm{x_{access}})), \\ \quad (\Phi_2, \mathrm{let}\ \mathrm{x}\ =\ \mathrm{e}_2\ \mathrm{in}\ \lambda \mathrm{x_{thnk}}.\mathrm{let}\ \mathrm{x_{access}}\ =\ \mathrm{thunk}(\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}}\ ()))\ \mathrm{in}\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{x}\ \mathrm{x_{access}}))) \\ \quad \in \mathcal{E}\llbracket \tau_1 \multimap \tau_2 \rrbracket.\end{array}$$

From the expression relation, we must show first that the terms are closed, which follows from out hypothesis given we did not introduce any new free variables. Then, we need to show that given:

$$\begin{array}{l}
\forall \Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}'_1,\ \mathrm{H}'_1,\ j < W.k. \\
\quad \Phi_{r1}, \Phi_{r2} : W \wedge \\
\quad \langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, \begin{array}{l} \mathrm{let\ x\ =\ e_1\ in\ } \lambda \mathrm{x_{thnk}.let\ x_{access}\ =\ thunk}(\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}\ ()}))\ \mathrm{in} \\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{x\ x_{access}}) \end{array} \rangle \\
\quad \overset{j}{\dashrightarrow} \langle \Phi'_1, \mathrm{H}'_1, \mathrm{e}'_1 \rangle \nrightarrow
\end{array}$$

Then it holds that:

$$\begin{array}{l}
\mathrm{e}'_1 = \mathrm{fail\ }\textsc{Conv} \vee (\exists \Phi_{f1}\ \Phi_{g1}\ \Phi_{f2}\ \Phi_{g2}\ \mathrm{v}_2 \mathrm{H}'_2\, W'. \\
\qquad \langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, \begin{array}{l} \mathrm{let\ x\ =\ e_2\ in\ } \lambda \mathrm{x_{thnk}.let\ x_{access}\ =\ thunk}(\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}\ ()}))\ \mathrm{in} \\ \mathrm{C}_{\tau_2 \mapsto \tau_2}(\mathrm{x\ x_{access}}) \end{array} \rangle \\
\qquad \quad \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathrm{H}'_2, \mathrm{v}_2 \rangle \nrightarrow \\
\qquad \wedge\ \Phi'_1 = \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge \\
\qquad \wedge\ W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W' \wedge\ \mathrm{H}'_1, \mathrm{H}'_2 : W' \\
\qquad \wedge\ (W', (\Phi_{f1}, \mathrm{e}'_1), (\Phi_{f2}, \mathrm{v}_2)) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!])\}
\end{array}$$

To figure out what e'_1 is, we know from the operational semantics that first we will evaluate e_1 until it is a value and then will substitute. From our hypothesis, which we can instantiate with $\Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2$, etc, we know that e_1 will run with either fail $\textsc{Conv}$ (in which case this will lift into the entire term running to fail $\textsc{Conv}$) or will run to a value v_1 related in $\mathcal{V}[\![(\mathtt{unit} \rightarrow \tau_1) \rightarrow \tau_2]\!]$. at a future world $W^\dagger$ where $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W^\dagger$ to another value v_2 that e_2 will run to, where the heaps have evolved to $\mathrm{H}^\dagger_1, \mathrm{H}^\dagger_2 : W^\dagger$, and empty flag stores.

Now, our original term will take another step and substitute v_1 for x (note that the operational semantics lifts steps on the subterm to steps on the whole term), which results in the following term:

$$\lambda \mathrm{x_{thnk}.let\ x_{access}\ =\ thunk}(\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}\ ()}))\ \mathrm{in\ C}_{\tau_2 \mapsto \tau_2}(\mathrm{v_1\ x_{access}})$$

This is clearly irreducible (it is a value), so we now need to show that the other side similarly reduces to a value v_2, which follows in the same way from our hypothesis, and thus what remains to show is that:

$$\begin{array}{l}
(W^\dagger, (\emptyset, \lambda \mathrm{x_{thnk}.let\ x_{access}\ =\ thunk}(\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}\ ()}))\ \mathrm{in\ C}_{\tau_2 \mapsto \tau_2}(\mathrm{v_1\ x_{access}})), \\
\quad (\emptyset, \lambda \mathrm{x_{thnk}.let\ x_{access}\ =\ thunk}(\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}\ ()}))\ \mathrm{in\ C}_{\tau_2 \mapsto \tau_2}(\mathrm{v_2\ x_{access}}))) \\
\quad \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!].
\end{array}$$

The definition of $\mathcal{V}[\![\tau_1 \multimap \tau_2]\!]$. says that we need to take any $W^\dagger \sqsubset W'$, v'_1, v'_2, ℓ_1, ℓ_2 where $(W^\dagger, (\Phi'_1, \mathrm{v}'_1), (\Phi'_2, \mathrm{v}'_2))$ are in $\mathcal{V}[\![\tau_1]\!]$. and (ℓ_1, ℓ_2) are not in either $W'.\Psi$ or $W'.\Theta$ and show that

$$\begin{array}{l}
((W'.k, W'.\Psi, W'.\Theta \uplus (\ell_1, \ell_2) {\mapsto} (\Phi'_1, \Phi'_2)), \\
\quad (\emptyset, [\mathrm{x_{thnk}} {\mapsto} \mathrm{guard}(\mathrm{v}'_1, \ell_1)]\mathrm{let\ x_{access}\ =\ thunk}(\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}\ ()}))\ \mathrm{in\ C}_{\tau_2 \mapsto \tau_2}(\mathrm{v_1\ x_{access}})), \\
\quad (\emptyset, [\mathrm{x_{thnk}} {\mapsto} \mathrm{guard}(\mathrm{v}'_2, \ell_2)]\mathrm{let\ x_{access}\ =\ thunk}(\mathrm{C}_{\tau_1 \mapsto \tau_1}(\mathrm{x_{thnk}\ ()}))\ \mathrm{in\ C}_{\tau_2 \mapsto \tau_2}(\mathrm{v_2\ x_{access}}))) \\
\quad \in \mathcal{E}[\![\tau_2]\!].
\end{array}$$

Where if we substitute (letting $W^* = (W'.k, W'.\Psi, W'.\Theta \uplus (\ell_1, \ell_2) {\mapsto} (\Phi'_1, \Phi'_2))$), we get:

$$\begin{array}{l}
(W^*, (\emptyset, \text{let } \mathsf{x}_{\text{access}} \;=\; \text{thunk}(\mathsf{C}_{\tau_1 \mapsto \tau_1}(\text{guard}(\mathsf{v}'_1, \ell_1)\ ()))\ \text{in } \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_1\ \mathsf{x}_{\text{access}})), \\
\qquad (\emptyset, \text{let } \mathsf{x}_{\text{access}} \;=\; \text{thunk}(\mathsf{C}_{\tau_1 \mapsto \tau_1}(\text{guard}(\mathsf{v}'_2, \ell_2)\ ()))\ \text{in } \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_2\ \mathsf{x}_{\text{access}}))) \\
\qquad \in \mathcal{E}\llbracket \tau_2 \rrbracket.
\end{array}$$

First, let's expand the definition of thunk$(\cdot)$:

$$\begin{array}{l}
(W^*,\ \ (\emptyset, \text{let } \mathsf{x}_{\text{access}} \;=\; \text{let } \mathsf{r}_{\text{fresh}} = \text{ref } \textsc{unused} \text{ in} \\
\qquad\quad \lambda\_.\{\text{if } !\mathsf{r}_{\text{fresh}}\ \{\text{fail } \textsc{Conv}\}\ \{\mathsf{r}_{\text{fresh}} := \textsc{used}; \mathsf{C}_{\tau_1 \mapsto \tau_1}(\text{guard}(\mathsf{v}'_1, \ell_1)\ ())\}) \text{ in } \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_1\ \mathsf{x}_{\text{access}})) \quad , \\
\qquad (\emptyset, \text{let } \mathsf{x}_{\text{access}} \;=\; \text{let } \mathsf{r}_{\text{fresh}} = \text{ref } \textsc{unused} \text{ in} \qquad\qquad\qquad\qquad\qquad) \\
\qquad\quad \lambda\_.\{\text{if } !\mathsf{r}_{\text{fresh}}\ \{\text{fail } \textsc{Conv}\}\ \{\mathsf{r}_{\text{fresh}} := \textsc{used}; \mathsf{C}_{\tau_1 \mapsto \tau_1}(\text{guard}(\mathsf{v}'_2, \ell_2)\ ()))\} \text{ in } \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_2\ \mathsf{x}_{\text{access}})) \\
\quad \in \mathcal{E}\llbracket \tau_2 \rrbracket.
\end{array}$$

To understand what happens, consider the operational reductions: allocating a new reference (ℓ'_i), substituting it for $\mathsf{r}_{\text{fresh}}$, and then substituting all of $\mathsf{x}_{\text{access}}$, and thus suffices to show that:

$$\begin{array}{l}
(W^\dagger, (\emptyset, \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_1\ (\lambda\_.\{\text{if } !\ell'_1\ \{\text{fail } \textsc{Conv}\}\ \{\ell'_1 := \textsc{used}; \mathsf{C}_{\tau_1 \mapsto \tau_1}(\text{guard}(\mathsf{v}'_1, \ell_1)\ ())\}))), \\
\qquad (\emptyset, \mathsf{C}_{\tau_2 \mapsto \tau_2}(\mathsf{v}_2\ (\lambda\_.\{\text{if } !\ell'_2\ \{\text{fail } \textsc{Conv}\}\ \{\ell'_2 := \textsc{used}; \mathsf{C}_{\tau_1 \mapsto \tau_1}(\text{guard}(\mathsf{v}'_2, \ell_2)\ ())\}))) \\
\qquad \in \mathcal{E}\llbracket \tau_2 \rrbracket.
\end{array}$$

Where $W^\dagger$ has a new pair of references in $W^\dagger.\Theta$ (set to $(\emptyset, \emptyset)$) but otherwise is identical to W^*. For this, we can appeal to our induction hypothesis, which requires us to show that:

$$\begin{array}{l}
(W^\dagger, (\emptyset, \mathsf{v}_1\ (\lambda\_.\{\text{if } !\ell'_1\ \{\text{fail } \textsc{Conv}\}\ \{\ell'_1 := \textsc{used}; \mathsf{C}_{\tau_1 \mapsto \tau_1}(\text{guard}(\mathsf{v}'_1, \ell_1)\ ())\})), \\
\qquad (\emptyset, \mathsf{v}_2\ (\lambda\_.\{\text{if } !\ell'_2\ \{\text{fail } \textsc{Conv}\}\ \{\ell'_2 := \textsc{used}; \mathsf{C}_{\tau_1 \mapsto \tau_1}(\text{guard}(\mathsf{v}'_2, \ell_2)\ ())\}))) \\
\qquad \in \mathcal{E}\llbracket \tau_2 \rrbracket.
\end{array}$$

Recalling that v_1 and v_2 came from $\mathcal{V}\llbracket (\texttt{unit} \to \tau_1) \to \tau_2 \rrbracket$., we can proceed by appealing to the definition of that relation, which tells us that for any arguments in $\mathcal{V}\llbracket \texttt{unit} \to \tau_1 \rrbracket$., the result of substituting will be in $\mathcal{E}\llbracket \tau_2 \rrbracket$.. It thus remains to show that:

$$\begin{array}{l}
(W^*, (\emptyset, \lambda\_.\{\text{if } !\ell'_1\ \{\text{fail } \textsc{Conv}\}\ \{\ell'_1 := \textsc{used}; \mathsf{C}_{\tau_1 \mapsto \tau_1}(\text{guard}(\mathsf{v}'_1, \ell_1)\ ())\}), \\
\qquad (\emptyset, \lambda\_.\{\text{if } !\ell'_2\ \{\text{fail } \textsc{Conv}\}\ \{\ell'_2 := \textsc{used}; \mathsf{C}_{\tau_1 \mapsto \tau_1}(\text{guard}(\mathsf{v}'_2, \ell_2)\ ())\})) \\
\qquad \in \mathcal{V}\llbracket \texttt{unit} \to \tau_1 \rrbracket.
\end{array}$$

Where W^* is some future world of $W^\dagger$. From the definition of $\mathcal{V}\llbracket \texttt{unit} \to \tau_1 \rrbracket$., we have to show that substituting () for the unused argument results in terms in $\mathcal{E}\llbracket \tau_1 \rrbracket$., at some arbitrary future world W^{**}.

We proceed first by case analysis on whether the affine flags (ℓ'_1, ℓ'_2) have been set to USED, which they can be in a future world. If they have been, we can expand the definition of the expression relation, choose Φ_{r1} and heaps $\mathsf{H}_1^{**}, \mathsf{H}_2^{**} : W^{**}$, and show that

$$\begin{array}{l}
\langle \Phi_{r1} \uplus \text{flags}(W^{**}, 1), \mathsf{H}_1, \text{if } !\ell'_1\ \{\text{fail } \textsc{Conv}\}\ \{\ell'_1 := \textsc{used}; \mathsf{C}_{\tau_1 \mapsto \tau_1}(\text{guard}(\mathsf{v}'_1, \ell_1)\ ())\rangle \overset{2}{\dashrightarrow} \\
\langle \Phi_{r1} \uplus \text{flags}(W^{**}, 1), \mathsf{H}_1, \text{fail } \textsc{Conv}\rangle
\end{array}$$

At which point we are done.

Thus, we now consider if (ℓ'_1, ℓ'_2) are still set to a pair of flag sets (Φ_a, Φ'_a). If that's the case, we instead take three steps to move into the else branches and update the affine flags to USED. That means we reduce our task to showing that in a world W^{***}, which now has those locations marked used in Θ, we need to show:

$$(W^{***}, (\emptyset, \mathsf{C}_{\tau_1 \mapsto \tau_1}(\text{guard}(\mathsf{v}'_1, \ell_1)\ ())), (\emptyset, \mathsf{C}_{\tau_1 \mapsto \tau_1}(\text{guard}(\mathsf{v}'_2, \ell_2)\ ()))) \in \mathcal{E}\llbracket \tau_1 \rrbracket.$$

We now again appeal to our induction hypothesis, expanding the definition of guard$(\cdot)$ at the same time to yield the following obligation:

$$\begin{gathered}(W^{***}, (\emptyset, (\lambda\_.\{\text{if } !\ell_1 \ \{\text{fail } \textsc{Conv}\} \ \{\ell_1 := \textsc{used}; \mathsf{v}_1'\}\}) \ ()), \\ (\emptyset, (\lambda\_.\{\text{if } !\ell_2 \ \{\text{fail } \textsc{Conv}\} \ \{\ell_2 := \textsc{used}; \mathsf{v}_2'\}\}) \ ())) \in \mathcal{E}[\![\tau_1]\!].\end{gathered}$$

We can then take one step, eliminating the pointless beta-reduction (for simplicity, we use the same name for the world, even though it is a future world):

$$(W^{***}, (\emptyset, \text{if } !\ell_1 \ \{\text{fail } \textsc{Conv}\} \ \{\ell_1 := \textsc{used}; \mathsf{v}_1'\}\}), (\emptyset, \text{if } !\ell_2 \ \{\text{fail } \textsc{Conv}\} \ \{\ell_2 := \textsc{used}; \mathsf{v}_2'\})) \in \mathcal{E}[\![\tau_1]\!].$$

Now we again do case analysis on whether (ℓ_1, ℓ_2) is USED in $W^{***}.\Theta$. If it is, then, as before, we trivially reduce the left side to failure and are done. If it is not, then we update those affine flags and reduce both sides to the values v_1' and v_2', at a future world W^{final}. Now we knew, originally, that those values were in $\mathcal{V}[\![\tau_1]\!]$. at world $W^{\dagger}$, but since, through many applications of Lemma 3.9 and Lemma 3.8, that also means that they are related at W^{final}, we are done.

□

Lemma 3.19 (Phantom Steps Translate to Actual Steps). *For any expression* e *in the phantom* LCVM *language, let* $Z(\mathsf{e})$ *be an expression in the original* LCVM *language where every subexpression of the form protect*(e', f) *is replaced with* e'.

For any heap H *in the phantom* LCVM *language, let* $Z_H(\mathsf{H}) = \{\ell \mapsto Z(\mathsf{v}) \mid \ell \mapsto \mathsf{v} \in \mathsf{H}\}$.

For any sets of flags Φ, Φ', *heaps* H, H', *and expressions* e, e', *if*

$$\langle \Phi, \mathsf{H}, \mathsf{e}\rangle \overset{m}{\dashrightarrow} \langle \Phi', \mathsf{H}', \mathsf{e}'\rangle$$

then

$$\langle Z_H(\mathsf{H}), Z(\mathsf{e})\rangle \xrightarrow{n} \langle Z_H(\mathsf{H}'), Z(\mathsf{e}')\rangle$$

where n is the number of steps in the first reduction sequence which are not invoked by the following reduction rule

$$\langle \Phi \uplus \{f\}, \mathsf{H}, \mathit{protect}(\mathsf{e}, f)\rangle \dashrightarrow \langle \Phi, \mathsf{H}, \mathsf{e}\rangle \tag{24}$$

Proof. There exists some natural number j such that $\langle \Phi, \mathsf{H}, \mathsf{e}\rangle \overset{j}{\dashrightarrow} \langle \Phi', \mathsf{H}', \mathsf{e}'\rangle$. We will prove the theorem by induction on j.

If $j = 0$, then $\Phi = \Phi'$, $\mathsf{H} = \mathsf{H}'$, and $\mathsf{e} = \mathsf{e}'$. It is then trivial to show that $\langle Z_H(\mathsf{H}), Z(\mathsf{e})\rangle \xrightarrow{0} \langle Z_H(\mathsf{H}), Z(\mathsf{e})\rangle$, which finishes the proof for this case.

If $j > 0$, then there exist $\Phi_j, \mathsf{H}_j, \mathsf{e_j}$ such that

$$\langle \Phi, \mathsf{H}, \mathsf{e}\rangle \overset{j-1}{\dashrightarrow} \langle \Phi_j, \mathsf{H}_j, \mathsf{e_j}\rangle$$

and

$$\langle \Phi_j, \mathsf{H}_j, \mathsf{e_j}\rangle \dashrightarrow \langle \Phi', \mathsf{H}', \mathsf{e}'\rangle$$

By the induction hypothesis, we have

$$\langle Z_H(\mathsf{H}), Z(\mathsf{e})\rangle \xrightarrow{n_j} \langle Z_H(\mathsf{H}_j), Z(\mathsf{e_j})\rangle$$

where n_j is the number of steps in the sequence $\langle \Phi, \mathsf{H}, \mathsf{e}\rangle \overset{j-1}{\dashrightarrow} \langle \Phi_j, \mathsf{H}_j, \mathsf{e_j}\rangle$ not invoked by (24).

Thus, by transitivity of $\xrightarrow{*}$, it suffices to show

$$\langle Z_H(\mathsf{H}_j), Z(\mathsf{e_j})\rangle \xrightarrow{k} \langle Z_H(\mathsf{H}'), Z(\mathsf{e}')\rangle$$

where $k = 0$ if $\langle \Phi_j, \mathsf{H}_j, \mathsf{e_j}\rangle \dashrightarrow \langle \Phi', \mathsf{H}', \mathsf{e}'\rangle$ is invoked by (24), and $k = 1$ otherwise.

We will prove the above by induction over the derivation of $\langle \Phi_j, \mathsf{H}_j, \mathsf{e_j} \rangle \dashrightarrow \langle \Phi', \mathsf{H}', \mathsf{e}' \rangle$. Most cases of this proof by induction are trivial because most reduction rules in $\dashrightarrow$ come from the original $\longrightarrow$. Thus, we prove the three non-trivial cases where the reduction rule is not derived from $\longrightarrow$ and then show three of the trivial cases which comes from $\longrightarrow$.

(1) Consider the reduction rule

$$\langle \Phi \uplus \{f\}, \mathsf{H}, \mathrm{protect}(\mathsf{e}, f) \rangle \dashrightarrow \langle \Phi, \mathsf{H}, \mathsf{e} \rangle$$

Then, we must show

$$\langle Z_H(\mathsf{H}), Z(\mathrm{protect}(\mathsf{e}, f)) \rangle \xrightarrow{0} \langle Z_H(\mathsf{H}), Z(\mathsf{e}) \rangle$$

However, notice that $Z(\mathrm{protect}(\mathsf{e}, f)) = Z(\mathsf{e})$. Then, we trivially have

$$\langle Z_H(\mathsf{H}), Z(\mathsf{e}) \rangle \xrightarrow{0} \langle Z_H(\mathsf{H}), Z(\mathsf{e}) \rangle$$

which finishes the proof for this case.

(2) Consider the reduction rule

$$\frac{f \text{ fresh}}{\langle \Phi, \mathsf{H}, \mathsf{let}\ \mathsf{a}_\bullet = \mathsf{v}\ \mathsf{in}\ \mathsf{e} \rangle \dashrightarrow \langle \Phi \uplus \{f\}, \mathsf{H}, [\mathsf{a}_\bullet \mapsto \mathrm{protect}(\mathsf{v}, f)]\mathsf{e} \rangle}$$

Then, we must show

$$\langle Z_H(\mathsf{H}), Z(\mathsf{let}\ \mathsf{a}_\bullet = \mathsf{v}\ \mathsf{in}\ \mathsf{e}) \rangle \xrightarrow{1} \langle Z_H(\mathsf{H}), Z([\mathsf{a}_\bullet \mapsto \mathrm{protect}(\mathsf{v}, f)]\mathsf{e}) \rangle$$

Factor the Z function through the expressions:

$$\langle Z_H(\mathsf{H}), \mathsf{let}\ \mathsf{a}_\bullet = Z(\mathsf{v})\ \mathsf{in}\ Z(\mathsf{e}) \rangle \xrightarrow{1} \langle Z_H(\mathsf{H}), [\mathsf{a}_\bullet \mapsto Z(\mathsf{v})]Z(\mathsf{e}) \rangle$$

Since $Z(\mathsf{v})$ is still a target value, the above reduction follows from the normal reduction rule on let.

(3) Consider the reduction rule

$$\frac{f \text{ fresh}}{\langle \Phi, \mathsf{H}, \lambda \mathsf{a}_\bullet.\mathsf{e}\ \mathsf{v} \rangle \dashrightarrow \langle \Phi \uplus \{f\}, \mathsf{H}, [\mathsf{a}_\bullet \mapsto \mathrm{protect}(\mathsf{v}, f)]\mathsf{e} \rangle}$$

Then, we must show

$$\langle Z_H(\mathsf{H}), Z(\lambda \mathsf{a}_\bullet.\mathsf{e}\ \mathsf{v}) \rangle \xrightarrow{1} \langle Z_H(\mathsf{H}), Z([\mathsf{a}_\bullet \mapsto \mathrm{protect}(\mathsf{v}, f)]\mathsf{e}) \rangle$$

Factor the Z function through the expressions:

$$\langle Z_H(\mathsf{H}), \lambda \mathsf{a}_\bullet.Z(\mathsf{e})\ Z(\mathsf{v}) \rangle \xrightarrow{1} \langle Z_H(\mathsf{H}), [\mathsf{a}_\bullet \mapsto Z(\mathsf{v})]Z(\mathsf{e}) \rangle$$

Since $Z(\mathsf{v})$ is still a target value, the above reduction follows from the normal reduction rule on λ.

(4) Consider the reduction rule

$$\frac{\text{fresh } \ell}{\langle \Phi, \mathsf{H}, \mathsf{ref}\ \mathsf{v} \rangle \dashrightarrow \langle \Phi, \mathsf{H}[\ell \mapsto \mathsf{v}], \ell \rangle}$$

Thus, we must show

$$\langle Z_H(\mathsf{H}), Z(\mathsf{ref}\ \mathsf{v}) \rangle \xrightarrow{1} \langle Z_H(\mathsf{H}[\ell \mapsto \mathsf{v}]), Z(\ell) \rangle$$

Factor through Z_H and Z:

$$\langle Z_H(\mathsf{H}), \mathsf{ref}\ Z(\mathsf{v}) \rangle \xrightarrow{1} \langle Z_H(\mathsf{H})[\ell \mapsto Z(\mathsf{v})], \ell \rangle$$

Since $Z(\mathsf{v})$ is a target value, the above reduction follows directly from the normal ref reduction rule.

(5) Consider the reduction rule

$$\frac{\mathsf{H}[\ell] = \mathsf{v}}{\langle \Phi, \mathsf{H}, !\ell \rangle \dashrightarrow \langle \Phi, \mathsf{H}, \mathsf{v} \rangle}$$

Thus, we must show

$$\langle Z_H(\mathsf{H}), Z(!\ell) \rangle \xrightarrow{1} \langle Z_H(\mathsf{H}), Z(\mathsf{v}) \rangle$$

Factor through Z on the left side:

$$\langle Z_H(\mathsf{H}), !\ell \rangle \xrightarrow{1} \langle Z_H(\mathsf{H}), Z(\mathsf{v}) \rangle$$

By the definition of Z_H, if $\mathsf{H}[\ell] = \mathsf{v}$, then $Z_H(\mathsf{H})[\ell] = Z(\mathsf{v})$. Thus, the above follows directly from the normal ! reduction rule.

(6) Consider the reduction rule

$$\frac{\langle \Phi, \mathsf{H}, \mathsf{e} \rangle \dashrightarrow \langle \Phi, \mathsf{H}', \mathsf{e}' \rangle}{\langle \Phi, \mathsf{H}, \mathsf{K}[\mathsf{e}] \rangle \dashrightarrow \langle \Phi, \mathsf{H}', \mathsf{K}[\mathsf{e}'] \rangle}$$

By the induction hypothesis, we have $\langle Z_H(\mathsf{H}), Z(\mathsf{e}) \rangle \xrightarrow{k} \langle Z_H(\mathsf{H}'), Z(\mathsf{e}') \rangle$, where $k = 0$ if $\langle \Phi, \mathsf{H}, \mathsf{e} \rangle \dashrightarrow \langle \Phi, \mathsf{H}', \mathsf{e}' \rangle$ was invoked by (24) and $k = 1$ otherwise. Then, we must show

$$\langle Z_H(\mathsf{H}), Z(\mathsf{K}[\mathsf{e}]) \rangle \xrightarrow{k} \langle Z_H(\mathsf{H}'), Z(\mathsf{K}[\mathsf{e}']) \rangle$$

Factor Z through K:

$$\langle Z_H(\mathsf{H}), \mathrm{Z}(\mathsf{K})[\mathrm{Z}(\mathsf{e})] \rangle \xrightarrow{k} \langle Z_H(\mathsf{H}'), \mathrm{Z}(\mathsf{K})[\mathrm{Z}(\mathsf{e}')] \rangle$$

If $k = 0$, then by $\langle Z_H(\mathsf{H}), Z(\mathsf{e}) \rangle \xrightarrow{k} \langle Z_H(\mathsf{H}'), Z(\mathsf{e}') \rangle$, we must have $Z_H(\mathsf{H}) = Z_H(\mathsf{H}')$ and $Z(\mathsf{e}) = Z(\mathsf{e}')$, in which case the above is trivial. Otherwise, if $k = 1$, the above follows directly from the evaluation context reduction rule in the target.

□

Lemma 3.20 (Phantom Steps Bounded). *If*

$$\langle \mathsf{H}, \mathsf{e}^+ \rangle \xrightarrow{n} \langle \mathsf{H}', \mathsf{e}' \rangle \not\rightarrow$$

then for any set of static flags Φ_{r1}, there exists some set of static flags Φ'_1, $m \leq 2n$, and expression e'_1 such that

$$\langle \Phi_{r1}, \mathsf{H}, \mathsf{e}^+ \rangle \overset{m}{\dashrightarrow} \langle \Phi'_1, \mathsf{H}'_1, \mathsf{e}'_1 \rangle \not\rightarrow$$

where, if e'_1 is a value, then $\mathsf{H}' = Z(\mathsf{H}'_1)$ and $\mathsf{e}' = Z(\mathsf{e}'_1)$

where, as defined in the previous Lemma, let $Z(\mathsf{e})$ be an expression in the original LCVM *language where every subexpression of the form protect(e', f) is replaced with e'*

and, for any heap H, let $Z_H(\mathsf{H}) = \{\ell \mapsto Z(\mathsf{v}) \mid \ell \mapsto \mathsf{v} \in \mathsf{H}\}$.

Note that we write e^+ to indicate that we are proving this with respect to compiled terms. The only constraint we actually need is that H and e^+ is a valid heap and expression, respectively, in the original LCVM *language and thus does not include any subexpressions of the form protect($\cdot$), as it is not intended to be written by programmers (or compilers), but rather arise through reduction in the phantom operational semantics.*

Proof. Suppose that $\langle \Phi_{r1}, \mathsf{H}, \mathsf{e}^{+} \rangle \overset{m}{\dashrightarrow} \langle \Phi'_1, \mathsf{H}'_1, \mathsf{e}'_1 \rangle$ for some m. Then, by Lemma 3.19,

$$\langle Z_H(\mathsf{H}), Z(\mathsf{e}^{+}) \rangle = \langle \mathsf{H}, \mathsf{e}^{+} \rangle \xrightarrow{n'} \langle Z_H(\mathsf{H}'_1), Z(\mathsf{e}'_1) \rangle$$

where n' is the number of steps in the original reduction sequence not invoked by $\mathsf{protect}(\cdot)$. Since $\langle \mathsf{H}, \mathsf{e}^{+} \rangle$ terminates in n steps by assumption, $n' \leq n$.

Consider that, since $\mathsf{protect}(\cdot)$ does not occur in H or e^{+}, $\mathsf{protect}(\cdot)$ instructions are only introduced by let and λ, and they are substituted for variable occurrences. Further, note that, for the reduction to have succeeded in the phantom semantics, out of each set of variable uses (that share a flag), only one $\mathsf{protect}(\cdot)$ term could have been evaluated. This means that each reduction of $\mathsf{protect}(\cdot)$ corresponds to a reduction of the let or λ that introduced it, so the number of reductions of $\mathsf{protect}(\cdot)$ is at most the number of reductions not of $\mathsf{protect}(\cdot)$, which means $m - n' \leq n'$. Ergo, $m \leq 2n' \leq 2n$.

This suffices to show that $\langle \Phi_{r1}, \mathsf{H}, \mathsf{e}^{+} \rangle$ can not take more than $2n$ steps, so there is some $m \leq 2n$ such that $\langle \Phi_{r1}, \mathsf{H}, \mathsf{e}^{+} \rangle \overset{m}{\dashrightarrow} \langle \Phi'_1, \mathsf{H}'_1, \mathsf{e}'_1 \rangle \nrightarrow$.

To finish the proof, suppose that e'_1 is a value. Then, as shown above, $\langle \mathsf{H}, \mathsf{e}^{+} \rangle \xrightarrow{n'} \langle Z_H(\mathsf{H}'_1), Z(\mathsf{e}'_1) \rangle$. If e'_1 is a value, then $Z(\mathsf{e}'_1)$ is also a value, so $\langle Z_H(\mathsf{H}'_1), Z(\mathsf{e}'_1) \rangle$ is irreducible. Ergo, since $\langle \mathsf{H}, \mathsf{e}^{+} \rangle \xrightarrow{n} \langle \mathsf{H}', \mathsf{e}' \rangle \nrightarrow$ and $\langle \mathsf{H}, \mathsf{e}^{+} \rangle$ can only possibly step to one irreducible configuration, $\mathsf{H}' = Z_H(\mathsf{H}'_1)$ and $\mathsf{e}' = Z(\mathsf{e}'_1)$. □

Theorem 3.21 (Fundamental Property). *If* $\Gamma; \Omega; \Delta; \Gamma \vdash \mathsf{e} : \tau \rightsquigarrow \Gamma'; \Omega'$ *then* $\Gamma; \Omega; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau \rightsquigarrow \Gamma'; \Omega'$ *and if* $\Delta; \Gamma; \Gamma; \Omega \vdash \mathsf{e} : \tau \rightsquigarrow \Delta'; \Gamma'$ *then* $\Delta; \Gamma; \Gamma; \Omega \vdash \mathsf{e} \preceq \mathsf{e} : \tau \rightsquigarrow \Delta'; \Gamma'$.

Proof. By induction on typing derivation, relying on the following compatibility lemmas, which have to exist for every typing rule in both source languages. □

Theorem 3.22 (Type Safety for MiniML). *For any* MiniML *term* e *where* $\cdot; \cdot; \cdot; \cdot \vdash \mathsf{e} : \tau \rightsquigarrow \cdot; \cdot$ *and for any heap* H, *if* $\langle \mathsf{H}, \mathsf{e}^{+} \rangle \xrightarrow{*} \langle \mathsf{H}', \mathsf{e}' \rangle$, *then either* $\mathsf{e}' = \mathsf{fail}\ \textsc{Conv}$, e' *is a value, or there exist* $\mathsf{H}'', \mathsf{e}''$ *such that* $\langle \mathsf{H}', \mathsf{e}' \rangle \longrightarrow \langle \mathsf{H}'', \mathsf{e}'' \rangle$.

Proof. Suppose $\langle \mathsf{H}, \mathsf{e}^{+} \rangle \xrightarrow{n} \langle \mathsf{H}', \mathsf{e}' \rangle$ for some natural number n. Either $\langle \mathsf{H}', \mathsf{e}' \rangle \longrightarrow \langle \mathsf{H}'', \mathsf{e}'' \rangle$, in which case we are done, or $\langle \mathsf{H}', \mathsf{e}' \rangle$ is irreducible.

Consider a trivial world W that has an arbitrary $k > 2n$, an empty heap typing and an empty affine store. Then, since the term is closed, by the Fundamental Property, $(W, (\emptyset, \mathsf{e}^{+}), (\emptyset, \mathsf{e}^{+})) \in \mathcal{E}[\![\tau]\!]_{\cdot,\cdot}$. Now by Lemma 3.20, we know that for any Φ_{r1}, Φ_{r2}, $\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1), \mathsf{H}_1, \mathsf{e}_1{}^{+} \rangle \overset{j}{\dashrightarrow} \langle \Phi'_1, \mathsf{H}'_1, \mathsf{e}'_1 \rangle \nrightarrow$ where $j \leq 2n$ and if e'_1 is a value, then $Z(\mathsf{e}'_1) = \mathsf{e}'$.

Then, by applying $(W, (\emptyset, \mathsf{e}^{+}), (\emptyset, \mathsf{e}^{+})) \in \mathcal{E}[\![\tau]\!]_{\cdot,\cdot}$, we find that either $\mathsf{e}'_1 = \mathsf{fail}\ \textsc{Conv}$ or there exist $\Phi'', \mathsf{H}''_2, \mathsf{v}_2$ such that $\langle \Phi'_2 \uplus \mathrm{flags}(W, 2), \mathsf{H}'_2, \mathsf{e}'_2 \rangle \overset{*}{\dashrightarrow} \langle \Phi'', \mathsf{H}''_2, \mathsf{v}_2 \rangle$ and e'_1 and v_2 are in the value relation with some world and sets of static flags. Ergo, since expressions in the value relation are values, e'_1 is a value. Finally, since e'_1 being a value implies $\mathsf{e}' = Z(\mathsf{e}'_1)$, we find that e' is a value. □

Theorem 3.23 (Type Safety for Affi). *For any* Affi *term* e *where* $\cdot; \cdot; \cdot; \cdot \vdash \mathsf{e} : \tau \rightsquigarrow \cdot; \cdot$ *and for any heap* H, *if* $\langle \mathsf{H}, \mathsf{e}^{+} \rangle \xrightarrow{*} \langle \mathsf{H}', \mathsf{e}' \rangle$, *then either* $\mathsf{e}' = \mathsf{fail}\ \textsc{Conv}$, e' *is a value, or there exist* $\mathsf{H}'', \mathsf{e}''$ *such that* $\langle \mathsf{H}', \mathsf{e}' \rangle \longrightarrow \langle \mathsf{H}'', \mathsf{e}'' \rangle$.

Proof. This proof is identical to that of MiniML. □

Note that we omit many of the MiniML compatibility lemmas because the differences between the proofs from the MiniML compatibility lemmas from the last case study and the corresponding compatibility lemmas in this case study are relatively straightforward, as demonstrated by the compatibility lemmas proven below.

Lemma 3.24 (Compat $\rightarrow$).

$$\Gamma; \Omega; \Delta; \Gamma[\mathrm{x} : \tau_1] \vdash \mathrm{e} \preceq \mathrm{e} : \tau_2 \rightsquigarrow \Gamma'; \Omega' \implies \Gamma; \Omega; \Delta; \Gamma \vdash \lambda \mathrm{x} : \tau_1.\mathrm{e} \preceq \lambda \mathrm{x} : \tau_1.\mathrm{e} : \tau_1 \rightarrow \tau_2 \rightsquigarrow \Gamma'; \Omega'$$

Proof. Expanding the hypotheses, we find that $\Gamma = \Gamma'$ and there exists Ω_e such that $\Omega = \Omega_e \uplus \Omega'$ where $\Gamma; \Omega_e; \Delta; \Gamma[\mathrm{x} : \tau_1] \vdash \mathrm{e} \preceq \mathrm{e} : \tau_2$. Moreover, $\Gamma; \Omega; \Delta; \Gamma \vdash \lambda \mathrm{x} : \tau_1.\mathrm{e} : \tau_1 \rightarrow \tau_2 \rightsquigarrow \Gamma'; \Omega'$ by the λ typing rule. It thus suffices to show that $\Gamma; \Omega_e; \Delta; \Gamma \vdash \lambda \mathrm{x} : \tau_1.\mathrm{e} \preceq \lambda \mathrm{x} : \tau_1.\mathrm{e} : \tau_1 \rightarrow \tau_2$.

Expanding the conclusion, given

$$\forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega.\rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_. \wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!].$$

we must show

$$\begin{gathered}(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \lambda \mathrm{x} : \tau_1.\mathrm{e}^+)))),\\ (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \lambda \mathrm{x} : \tau_1.\mathrm{e}^+))))) \in \mathcal{E}[\![\tau_1 \rightarrow \tau_2]\!].\end{gathered}$$

Notice that both of the expressions have no free variables by Lemma 3.15.

We can push the compiler and substitutions through the lambda to refine that to:

$$\begin{gathered}(W, (\emptyset, \lambda \mathrm{x}.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))),\\ (\emptyset, \lambda \mathrm{x}.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))))) \in \mathcal{E}[\![\tau_1 \rightarrow \tau_2]\!]_\rho\end{gathered}$$

Then, by Lemma 3.6, there exists a γ' such that $(W, \emptyset, \emptyset, \gamma') \in \mathcal{G}[\![\Omega_\circ]\!]_.$ and closing over e^+ with γ' is the same as closing with γ_Ω. Thus, we refine the above to:

$$\begin{gathered}(W, (\emptyset, \lambda \mathrm{x}.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma', \mathrm{e}^+)))),\\ (\emptyset, \lambda \mathrm{x}.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma', \mathrm{e}^+))))) \in \mathcal{E}[\![\tau_1 \rightarrow \tau_2]\!]_\rho\end{gathered}$$

Since $\mathcal{V}[\![\tau_1 \rightarrow \tau_2]\!]_\rho \subseteq \mathcal{E}[\![\tau_1 \rightarrow \tau_2]\!]_\rho$ by Lemma 3.1, it suffices to show that:

$$\begin{gathered}(W, (\emptyset, \lambda \mathrm{x}.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma', \mathrm{e}^+)))),\\ (\emptyset, \lambda \mathrm{x}.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma', \mathrm{e}^+))))) \in \mathcal{V}[\![\tau_1 \rightarrow \tau_2]\!]_\rho\end{gathered}$$

Expanding the value relation, given

$$\forall \mathrm{v}_1\ \mathrm{v}_2\ W'.W \sqsubset_{\emptyset,\emptyset} W' \ \wedge\ (W', (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}[\![\tau_1]\!]_\rho$$

we must prove:

$$\begin{gathered}(W', (\emptyset, [\mathrm{x} {\mapsto} \mathrm{v}_1]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma', \mathrm{e}^+)))),\\ (\emptyset, [\mathrm{x} {\mapsto} \mathrm{v}_2]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma', \mathrm{e}^+))))) \in \mathcal{E}[\![\tau_2]\!]_\rho\end{gathered}$$

By $W \sqsubseteq_{\emptyset,\emptyset} W'$ and Lemma 3.8, we have

$$(W', \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho$$

$$(W', \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho$$

$$(W', \emptyset, \emptyset, \gamma') \in \mathcal{G}[\![\Omega_\circ]\!]_\rho$$

Notice that

$$(W', \emptyset, \emptyset, \gamma_\Gamma[\mathrm{x} \rightarrow (\mathrm{v}_1, \mathrm{v}_2)]) \in \mathcal{G}[\![\Gamma[\mathrm{x} : \tau_1]]\!]_\rho$$

because $(W', \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho$ and $(W', (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}[\![\tau_1]\!]_\rho$. Then, we can instantiate Lemma 3.7 with the first induction hypothesis and $W', \gamma_\Gamma[\mathrm{x} \rightarrow (\mathrm{v}_1, \mathrm{v}_2)], \gamma_\Gamma, \gamma', \rho$. Therefore,

$$\begin{gathered}(W', (\emptyset, \mathrm{close}_1(\gamma_\Gamma[\mathrm{x} \rightarrow (\mathrm{v}_1, \mathrm{v}_2)], \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma', \mathrm{e}^+)))),\\ (\emptyset, \mathrm{close}_2(\gamma_\Gamma[\mathrm{x} \rightarrow (\mathrm{v}_1, \mathrm{v}_2)], \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma', \mathrm{e}^+))))) \in \mathcal{E}[\![\tau_2]\!]_\rho\end{gathered}$$

We can simplify the above statement by bringing $\mathrm{x} \rightarrow \mathrm{v}_1$ out of the close_1 on the left side and bringing $\mathrm{x} \rightarrow \mathrm{v}_2$ out of the close_2 on the right side. This suffices to finish the proof. □

Lemma 3.25 (Compat app).

$$\Gamma_1;\Omega_1;\Delta;\Gamma \vdash \mathsf{e}_1 \preceq \mathsf{e}_1 : \tau_1 \to \tau_2 \rightsquigarrow \Gamma_2;\Omega_2 \wedge \Gamma_2;\Omega_2;\Delta;\Gamma \vdash \mathsf{e}_2 \preceq \mathsf{e}_2 : \tau_1 \rightsquigarrow \Gamma_3;\Omega_3 \implies \Gamma_1;\Omega_1;\Delta;\Gamma \vdash \mathsf{e}_1\ \mathsf{e}_2 \preceq \mathsf{e}_1\ \mathsf{e}_2 : \tau_2 \rightsquigarrow \Gamma_3;\Omega_3$$

Proof. Expanding the hypotheses, we find that $\Gamma_1 = \Gamma_2 = \Gamma_3$ and there exist Ω_e, Ω_e' such that $\Omega_1 = \Omega_e \uplus \Omega_2$ where $\Gamma_1;\Omega_e;\Delta;\Gamma \vdash \mathsf{e}_1 \preceq \mathsf{e}_1 : \tau_1 \to \tau_2$ and $\Omega_2 = \Omega_e' \uplus \Omega_3$ where $\Gamma_2;\Omega_e';\Delta;\Gamma \vdash \mathsf{e}_2 \preceq \mathsf{e}_2 : \tau_1$. Therefore, $\Omega_1 = (\Omega_e \uplus \Omega_e') \uplus \Omega_3$. Moreover, $\Gamma_1;\Omega_1;\Delta;\Gamma \vdash \mathsf{e}_1\ \mathsf{e}_2 \preceq \mathsf{e}_1\ \mathsf{e}_2 : \tau_2 \rightsquigarrow \Gamma_3;\Omega_3$ by the application typing rule. It thus suffices to show that $\Gamma_1;\Omega_e \uplus \Omega_e';\Delta;\Gamma \vdash \mathsf{e}_1\ \mathsf{e}_2 \preceq \mathsf{e}_1\ \mathsf{e}_2 : \tau_2$.

Expanding the conclusion, given

$$\forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega.\rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket. \wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}\llbracket\Omega\rrbracket.$$

we must show

$$(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_1\ \mathsf{e}_2{}^+)))), (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}_1\ \mathsf{e}_2{}^+))))) \in \mathcal{E}\llbracket\tau_2\rrbracket.$$

Notice that both of the expressions have no free variables by Lemma 3.15.

We can push the compiler and substitutions through the application to refine that to:

$$(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_1{}^+)))\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_2{}^+)))), \\ (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}_1{}^+)))\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}_2{}^+))))) \in \mathcal{E}\llbracket\tau_2\rrbracket_\rho$$

Next, by Lemma 3.5, we have that $\gamma_\Omega = \gamma_1 \uplus \gamma_2$, $\Phi_1 = \Phi_{1l} \uplus \Phi_{1r}$, and $\Phi_2 = \Phi_{2l} \uplus \Phi_{2r}$ where

$$(W, \Phi_{1l}, \Phi_{2l}, \gamma_1) \in \mathcal{G}\llbracket\Omega_1\rrbracket.$$

and

$$(W, \Phi_{1r}, \Phi_{2r}, \gamma_2) \in \mathcal{G}\llbracket\Omega_2\rrbracket.$$

and for all $i \in \{1, 2\}$,

$$\mathrm{close}_i(\gamma_\Omega, \mathsf{e}_1{}^+) = \mathrm{close}_i(\gamma_1, \mathsf{e}_1{}^+)$$

and

$$\mathrm{close}_i(\gamma_\Omega, \mathsf{e}_2{}^+) = \mathrm{close}_i(\gamma_1, \mathsf{e}_2{}^+)$$

Thus, we refine the statement we need to prove to:

$$(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathsf{e}_1{}^+)))\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathsf{e}_2{}^+)))), \\ (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathsf{e}_1{}^+)))\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathsf{e}_2{}^+))))) \in \mathcal{E}\llbracket\tau_2\rrbracket_\rho$$

Let e_1 and e_2 be the first and second expressions, respectively, in the above tuple. Expanding the definition of the expression relation, given:

$$\forall \Phi_{r1}, \Phi_{r2}, \mathsf{H}_1, \mathsf{H}_2{:}W,\ \mathrm{e}_1',\ \mathsf{H}_1',\ j < W.k. \\ \Phi_{r1}\#\emptyset \wedge \Phi_{r2}\#\emptyset \wedge \Phi_{r1} \uplus \emptyset, \Phi_{r2} \uplus \emptyset : W \wedge \\ \langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \emptyset, \mathsf{H}_1, \mathrm{e}_1\rangle \overset{j}{\dashrightarrow} \langle \Phi_1', \mathsf{H}_1', \mathrm{e}_1'\rangle \nrightarrow$$

we must show that either e_1' is fail Conv or there exist $\Phi_{f1}, \Phi_{g1}, \Phi_{f2}, \Phi_{g2}, \mathsf{v}_2, \mathsf{H}_2', W'$ such that:

$$\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \emptyset, \mathsf{H}_2, \mathrm{e}_2\rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathsf{H}_2', \mathsf{v}_2\rangle \nrightarrow \\ \wedge\ \Phi_1' = \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge \\ \wedge\ W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W' \wedge\ \mathsf{H}_1', \mathsf{H}_2' : W' \\ \wedge\ (W', (\Phi_{f1}, \mathrm{e}_1'), (\Phi_{f2}, \mathsf{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho)$$

Next, we need to know what e_1' is. From the operational semantic, the application will run the first subexpression using the heap H_1 until it reaches a target value or gets stuck. By appealing to our first induction hypothesis, instantiated with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_1, \rho$, we get that:

$$(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathsf{e}_1{}^+)))), (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathsf{e}_1{}^+))))) \in \mathcal{E}\llbracket\tau_1\rrbracket_\rho$$

Therefore, the configuration

$$\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1), \mathrm{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathsf{e}_1{}^{+})))\rangle$$

either steps to fail Conv, in which case the whole application expression steps to fail Conv, or steps to some irreducible configuration $\langle \Phi_{r1} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{f1l} \uplus \Phi_{g1l}, \mathrm{H}_1^*, \mathrm{e}_1^*\rangle$, in which case the configuration

$$\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2), \mathrm{H}_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathsf{e}_1{}^{+})))\rangle$$

steps to some irreducible configuration $\langle \Phi_{r2} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{f2l} \uplus \Phi_{g2l}, \mathrm{H}_2^*, \mathrm{e}_1^\dagger\rangle$ and there exists some world W_1 such that $W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W_1$, $\mathrm{H}_1^*, \mathrm{H}_2^* : W_1$, and $(W_1, (\Phi_{f1l}, \mathrm{e}_1^*), (\Phi_{f2l}, \mathrm{e}_1^\dagger))$. By Lemma 3.17, $\Phi_{f1l} = \Phi_{f2l} = \emptyset$.

Since terms in the value relation are target values, the original application will continue reducing on the second subexpression according to the operational semantics. Then, we can appeal to the second induction hypothesis instantiated with $W_1, \gamma_\Gamma, \gamma_\Gamma, \gamma_2, \rho$, because $W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W_1$ and $\mathcal{G}[\![\Gamma]\!]_\rho, \mathcal{G}[\![\Gamma]\!]_\cdot, \mathcal{G}[\![\Omega]\!]_\cdot$ are closed under world extension by Lemma 3.8. Thus,

$$(W_1, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathsf{e}_2{}^{+})))), (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathsf{e}_2{}^{+}))))) \in \mathcal{E}[\![\tau_2]\!]_\rho$$

Therefore, the configuration:

$$\langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \mathrm{flags}(W_1, 1), \mathrm{H}_1^*, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathsf{e}_2{}^{+})))\rangle$$

either reduces to fail Conv, in which case the whole expression steps to fail Conv, or to some irreducible configuration $\langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{f1r} \uplus \Phi_{g1r}, \mathrm{H}_1^{**}, \mathrm{e}_2^*\rangle$, in which case on the other side, the configuration

$$\langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \mathrm{flags}(W_1, 2), \mathrm{H}_2^*, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathsf{e}_2{}^{+})))\rangle$$

reduces to some irreducible configuration $\langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \mathrm{flags}(W_2, 2) \uplus \Phi_{f2r} \uplus \Phi_{g2r}, \mathrm{H}_2^{**}, \mathrm{e}_2^\dagger\rangle$, and there exists some W_2 such that $W_1 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{g1l}, \Phi_{r2} \uplus \Phi_{g2l}} W_2$, $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : W_2$, and $(W_2, (\Phi_{f1r}, \mathrm{e}_2^*), (\Phi_{f2r}, \mathrm{e}_2^\dagger)) \in \mathcal{V}[\![\tau_1]\!]_\rho$. By Lemma 3.17, $\Phi_{f1r} = \Phi_{f2r} = \emptyset$.

Then, instantiate $(W_1, (\emptyset, \mathrm{e}_1^*), (\emptyset, \mathrm{e}_1^\dagger)) \in \mathcal{V}[\![\tau_1 \rightarrow \tau_2]\!]_\rho$ with $\mathrm{e}_2^*, \mathrm{e}_2^\dagger, \triangleright W_2$. Because $W_1 \sqsubseteq_{\emptyset,\emptyset} W_2$ and $W_2 \sqsubset_{\emptyset,\emptyset} \triangleright W_2$, it follows that $W_1 \sqsubset_{\emptyset,\emptyset} \triangleright W_2$. Moreover, $(\triangleright W_2, (\emptyset, \mathrm{e}_2^*), (\emptyset, \mathrm{e}_2^\dagger)) \in \mathcal{V}[\![\tau_1]\!]_\rho$ (because $(W_2, (\emptyset, \mathrm{e}_2^*), (\emptyset, \mathrm{e}_2^\dagger)) \in \mathcal{V}[\![\tau_1]\!]_\rho$ and $W_2 \sqsubseteq_{\emptyset,\emptyset} \triangleright W_2$), so we find that there exist $\mathrm{e}_\mathrm{b}^*, \mathrm{e}_\mathrm{b}^\dagger$ such that

$$\mathrm{e}_1^* = \lambda \mathrm{x}.\mathrm{e}_\mathrm{b}^*$$

and

$$\mathrm{e}_1^\dagger = \lambda \mathrm{x}.\mathrm{e}_\mathrm{b}^\dagger$$

and

$$(\triangleright W_2, (\emptyset, [\mathrm{x} \mapsto \mathrm{e}_2^*]\mathrm{e}_\mathrm{b}^*), (\emptyset, [\mathrm{x} \rightarrow \mathrm{e}_2^\dagger]\mathrm{e}_\mathrm{b}^\dagger)) \in \mathcal{E}[\![\tau_2]\!]_\rho$$

Now, by the operational semantic, the original configuration with heap H_1 steps to

$$\begin{gathered}\langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \Phi_{g1r} \uplus \mathrm{flags}(W_2, 1), \mathrm{H}_1^{**}, \lambda \mathrm{x}.\mathrm{e}_\mathrm{b}^*\ \mathrm{e}_2^*\rangle \dashrightarrow \\ \langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \Phi_{g1r} \uplus \mathrm{flags}(W_2, 1), \mathrm{H}_1^{**}, [\mathrm{x} \mapsto \mathrm{e}_2^*]\mathrm{e}_\mathrm{b}^*\rangle\end{gathered}$$

and, on the other side, the original configuration with H_2 steps to

$$\begin{gathered}\langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \Phi_{g2r} \uplus \mathrm{flags}(W_2, 2), \mathrm{H}_2^{**}, \lambda \mathrm{x}.\mathrm{e}_\mathrm{b}^\dagger\ \mathrm{e}_2^\dagger\rangle \dashrightarrow \\ \langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \Phi_{g2r} \uplus \mathrm{flags}(W_2, 2), \mathrm{H}_2^{**}, [\mathrm{x} \mapsto \mathrm{e}_2^\dagger]\mathrm{e}_\mathrm{b}^\dagger\rangle\end{gathered}$$

Then, since $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : W_2$, by Lemma 3.11, it follows that $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : \triangleright W_2$. We also have $\mathrm{flags}(W_2, 1) = \mathrm{flags}(\triangleright W_2, 1)$ and $\mathrm{flags}(W_2, 2) = \mathrm{flags}(\triangleright W_2, 2)$, since $\triangleright$ does not change the dynamic flags in the world. Thus, we can instantiate the above fact to deduce that either the first configuration steps to fail Conv, in which case the original configuration with H_1 steps to fail Conv, or the first configuration steps to some irreducible configuration

$$\langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \Phi_{g1r} \uplus \mathrm{flags}(W_3, 1) \uplus \Phi_{f1f} \uplus \Phi_{g1f}, \mathrm{H}_1^f, \mathrm{e}_\mathrm{f}^* \rangle$$

in which case the second configuration steps to some irreducible configuration

$$\langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \Phi_{g2r} \uplus \mathrm{flags}(W_3, 2) \uplus \Phi_{f2f} \uplus \Phi_{g2f}, \mathrm{H}_2^f, \mathrm{e}_\mathrm{f}^\dagger \rangle$$

and there exists some W_3 such that $\triangleright W_2 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{g1l} \uplus \Phi_{g1r}, \Phi_{r2} \uplus \Phi_{g2l} \uplus \Phi_{g2r}} W_3$, $\mathrm{H}_1^f, \mathrm{H}_2^f : W_3$, and

$$(W_3, (\Phi_{f1f}, \mathrm{e}_\mathrm{f}^*), (\Phi_{f2f}, \mathrm{e}_\mathrm{f}^\dagger)) \in \mathcal{V}[\![\tau_2]\!]_\rho$$

Then, since $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_1$, $W_1 \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_2$, $W_2 \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} \triangleright W_2$, $\triangleright W_2 \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_3$, we have $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_3$, which suffices to finish the proof. □

Lemma 3.26 (Compat $\forall$).

$$\Gamma; \Omega; \Delta, \alpha; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \tau \rightsquigarrow \Gamma'; \Omega' \implies \Gamma; \Omega; \Delta; \Gamma \vdash \Lambda\alpha.e \preceq \Lambda\alpha.e : \forall\alpha.\tau \rightsquigarrow \Gamma'; \Omega'$$

Proof. Expanding the hypotheses, we find that $\Gamma = \Gamma'$ and there exists Ω_e such that $\Omega = \Omega_\mathrm{e} \uplus \Omega'$ where $\Gamma; \Omega_\mathrm{e}; \Delta, \alpha; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \tau$. Moreover, $\Gamma; \Omega; \Delta; \Gamma \vdash \Lambda\alpha.e : \forall\alpha.\tau \rightsquigarrow \Gamma'; \Omega'$ by the type abstraction typing rule. It thus suffices to show that $\Gamma; \Omega_\mathrm{e}; \Delta; \Gamma \vdash \Lambda\alpha.e \preceq \Lambda\alpha.e : \forall\alpha.\tau$.

Expanding the conclusion, given

$$\forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega.\rho \in \mathcal{D}[\![\Delta]\!] \land (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \land (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_{.} \land (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!]_{.}$$

we must show

$$(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \Lambda\alpha.e^+)))), (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \Lambda\alpha.e^+))))) \in \mathcal{E}[\![\forall\alpha.\tau]\!].$$

Notice that both of the expressions have no free variables by Lemma 3.15.

We can push the compiler and substitutions through the pair to refine that to:

$$(W, (\emptyset, \lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))), (\emptyset, \lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))))) \in \mathcal{E}[\![\forall\alpha.\tau]\!]_\rho$$

Then, by Lemma 3.6, there exists a γ' such that $(W, \emptyset, \emptyset, \gamma') \in \mathcal{G}[\![\Omega_\circ]\!]_{.}$ and closing over e^+ with γ' is the same as closing with γ_Ω. Thus, we refine the above to:

$$\begin{gathered}(W, (\emptyset, \lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma', \mathrm{e}^+)))),\\ (\emptyset, \lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma', \mathrm{e}^+))))) \in \mathcal{E}[\![\forall\alpha.\tau]\!]_\rho\end{gathered}$$

Then, since $\mathcal{V}[\![\forall\alpha.\tau]\!]_\rho \subseteq \mathcal{E}[\![\forall\alpha.\tau]\!]_\rho$, it suffices to prove:

$$(W, (\emptyset, \lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma', \mathrm{e}^+)))), (\emptyset, \lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma', \mathrm{e}^+))))) \in \mathcal{V}[\![\forall\alpha.\tau]\!]_\rho$$

Consider some arbitrary $R \in \mathit{UnrTyp}$ and W' such that $W \sqsubset_{\emptyset,\emptyset} W'$. We must prove that

$$(W', (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma', \mathrm{e}^+)))), (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma', \mathrm{e}^+))))) \in \mathcal{E}[\![\tau]\!]_{\rho[\alpha \mapsto R]}$$

Since $R \in \mathit{UnrTyp}$ and $\rho \in \mathcal{D}[\![\Delta]\!]$, it follows that $\rho[\alpha \mapsto R] \in \mathcal{D}[\![\Delta, \alpha]\!]$. Thus, we can instantiate Lemma 3.7 with the first induction hypothesis and $W', \gamma_\Gamma, \gamma_\Gamma, \gamma', \rho[\alpha \mapsto R]$, because $W \sqsubseteq_{\emptyset,\emptyset} W'$ and thus by Lemma 3.8, the substitutions are still in the interpretation of $\mathcal{G}[\![\Gamma]\!]_\rho, \mathcal{G}[\![\Gamma]\!]_{.}, \mathcal{G}[\![\Omega]\!]_{.}$, respectively, with the world W'. This suffices to prove the above fact. □

Lemma 3.27 (Compat $[\tau/\alpha]$).

$$\Delta \vdash \tau' \land \Gamma; \Omega; \Delta; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \forall\alpha.\tau \rightsquigarrow \Gamma'; \Omega' \implies \Gamma; \Omega; \Delta; \Gamma \vdash \mathrm{e}[\tau'] \preceq \mathrm{e}[\tau'] : \tau[\tau'/\alpha] \rightsquigarrow \Gamma'; \Omega'$$

Proof. Expanding the hypotheses, we find that $\Gamma = \Gamma'$ and there exists Ω_e such that $\Omega = \Omega_e \uplus \Omega'$ where $\Gamma; \Omega_e; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau$. Moreover, $\Gamma; \Omega; \Delta; \Gamma \vdash \mathsf{e}[\tau'] : \tau[\tau'/\alpha] \rightsquigarrow \Gamma'; \Omega'$ by the type application typing rule. It thus suffices to show that $\Gamma; \Omega_e; \Delta; \Gamma \vdash \mathsf{e}[\tau'] \preceq \mathsf{e}[\tau'] : \tau[\tau'/\alpha]$.

Expanding the conclusion, given

$$\forall W. \forall \rho\; \gamma_\Gamma\; \gamma_\Gamma\; \gamma_\Omega . \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]. \wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!].$$

we must show

$$(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}[\tau']^+)))), (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}[\tau']^+))))) \in \mathcal{E}[\![\tau[\tau'/\alpha]]\!].$$

Notice that both of the expressions have no free variables by Lemma 3.15.

We can push the compiler and substitutions through the type application to refine this to:

$$(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+)))\;()), (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+)))\;())) \in \mathcal{E}[\![\tau[\tau'/\alpha]]\!]_\rho$$

Let e_1 and e_2 be the first and second expressions, respectively, in the above tuple. Expanding the definition of the expression relation, given:

$$\begin{gathered} \forall \Phi_{r1}, \Phi_{r2}, \mathsf{H}_1, \mathsf{H}_2 {:} W,\; \mathsf{e}_1',\; \mathsf{H}_1',\; j < W.k. \\ \Phi_{r1} \# \emptyset \wedge \Phi_{r2} \# \emptyset \wedge \Phi_{r1} \uplus \emptyset, \Phi_{r2} \uplus \emptyset : W \wedge \\ \langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \emptyset, \mathsf{H}_1, \mathsf{e}_1 \rangle \overset{j}{\dashrightarrow} \langle \Phi_1', \mathsf{H}_1', \mathsf{e}_1' \rangle \not\rightarrow \end{gathered}$$

we must show that either e_1' is fail Conv or there exist $\Phi_{f1}, \Phi_{g1}, \Phi_{f2}, \Phi_{g2}, \mathsf{v}_2, \mathsf{H}_2', W'$ such that:

$$\begin{aligned} &\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \emptyset, \mathsf{H}_2, \mathsf{e}_2 \rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathsf{H}_2', \mathsf{v}_2 \rangle \not\rightarrow \\ &\wedge \Phi_1' = \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge \\ &\wedge W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W' \wedge \mathsf{H}_1', \mathsf{H}_2' : W' \\ &\wedge (W', (\Phi_{f1}, \mathsf{e}_1'), (\Phi_{f2}, \mathsf{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho) \end{aligned}$$

To proceed, we must find what e_1' is. From the operational semantic, we know the application will run its subexpression using H_1 until it reaches a target value or gets stuck. From the induction hypothesis instantiated with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$, we find that:

$$(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+)))), (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+))))) \in \mathcal{E}[\![\forall \alpha . \tau]\!]_\rho$$

Thus, the configuration

$$\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1), \mathsf{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}^+))) \rangle$$

either reduces to fail Conv, in which case the entire term reduced to fail Conv, or it will reduce to some $\langle \Phi_{r1} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{f1l} \uplus \Phi_{g1l}, \mathsf{H}_1^*, {\mathsf{e}_1}^* \rangle$, in which case the configuration

$$\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2), \mathsf{H}_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}^+))) \rangle$$

will reduce to some $\langle \Phi_{r2} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{f2l} \uplus \Phi_{g2l}, \mathsf{H}_2^*, {\mathsf{e}_1}^\dagger \rangle$ and there exists some world W_1 where $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_1$, $\mathsf{H}_1^*, \mathsf{H}_2^* : W_1$, and

$$(W_1, (\Phi_{f1l}, {\mathsf{e}_1}^*), (\Phi_{f2l}, {\mathsf{e}_1}^\dagger)) \in \mathcal{V}[\![\forall \alpha . \tau]\!]_\rho$$

By expanding the value relation, we find $\Phi_{f1l} = \Phi_{f2l} = \emptyset$.

Then, we can instantiate the above fact with $\mathcal{V}[\![\tau']\!]_\rho$ and $\triangleright W_1$. (Note that $\mathcal{V}[\![\tau']\!]_\rho \in \mathit{UnrTyp}$ by Lemma 3.12.) Since $W \sqsubset \triangleright W_1$ (as $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_1$ and $W_1 \sqsubset_{\Phi_{r1}, \Phi_{r2}} \triangleright W_1$ since W_1 and $\triangleright W_1$ have the same dynamic flags), we find that there exist $\mathsf{e}_\mathsf{b}^*, \mathsf{e}_\mathsf{b}^\dagger$ such that

$$\mathsf{e}_1^* = \lambda\_.\mathsf{e}_\mathsf{b}^*$$

$$\mathsf{e}_1^\dagger = \lambda\_.\mathsf{e}_\mathsf{b}^\dagger$$

and

$$(\triangleright W_1, (\emptyset, \mathrm{e}_\mathrm{b}^*), (\emptyset, \mathrm{e}_\mathrm{b}^\dagger)) \in \mathcal{E}[\![\tau]\!]_{\rho[\alpha \to \mathcal{V}[\![\tau']\!]_\rho]}$$

Notice that $\mathrm{flags}(W_1, 1) = \mathrm{flags}(\triangleright W_1, 1)$ and $\mathrm{flags}(W_1, 2) = \mathrm{flags}(\triangleright W_1, 2)$ because $\triangleright$ does not change the dynamic flags in the world.

Ergo, by the operational semantic, the original configuration with heap H_1 steps to

$$\begin{array}{l}\langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \mathrm{flags}(\triangleright W_1, 1), \mathrm{H}_1^*, \lambda\_.\mathrm{e}_\mathrm{b}^*\ ()\rangle \dashrightarrow \\ \langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \mathrm{flags}(\triangleright W_1, 1), \mathrm{H}_1^*, \mathrm{e}_\mathrm{b}^*\rangle\end{array}$$

and, on the other side, the configuration with H_2 steps to

$$\begin{array}{l}\langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \mathrm{flags}(\triangleright W_1, 2), \mathrm{H}_2^*, \lambda\_.\mathrm{e}_\mathrm{b}^\dagger\ ()\rangle \dashrightarrow \\ \langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \mathrm{flags}(\triangleright W_1, 2), \mathrm{H}_2^*, \mathrm{e}_\mathrm{b}^\dagger\rangle\end{array}$$

Next, since $\mathrm{H}_1^*, \mathrm{H}_2^* : W_1$, by Lemma 3.11, it follows that $\mathrm{H}_1^*, \mathrm{H}_2^* : \triangleright W_1$, so we can instantiate the above fact with $\mathrm{H}_1^*, \mathrm{H}_2^*$ to deduce that either the first configuration steps to fail CONV, in which case the original configuration with H_1 steps to fail CONV, or the first configuration steps to some irreducible configuration $\langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{f1f} \uplus \Phi_{g1f}, \mathrm{H}_1^{**}, \mathrm{e}_\mathrm{f}^*\rangle$, in which case the second configuration also steps to some irreducible configuration $\langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \mathrm{flags}(W_2, 2) \uplus \Phi_{f2f} \uplus \Phi_{g2f}, \mathrm{H}_2^{**}, \mathrm{e}_\mathrm{f}^\dagger\rangle$, and there exists some W_2 where $\triangleright W_1 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{g1l}, \Phi_{r2} \uplus \Phi_{g2l}} W_2, \mathrm{H}_1^{**}, \mathrm{H}_2^{**} : W_2$, and $(W_2, (\Phi_{f1f}, \mathrm{e}_\mathrm{f}^*), (\Phi_{f2f}, \mathrm{e}_\mathrm{f}^\dagger)) \in \mathcal{V}[\![\tau]\!]_{\rho[\alpha \to \mathcal{V}[\![\tau']\!]_\rho]}$. Therefore, by Lemma 3.13, $(W_2, (\Phi_{f1f}, \mathrm{e}_\mathrm{f}^*), (\Phi_{f2f}, \mathrm{e}_\mathrm{f}^\dagger)) \in \mathcal{V}[\![\tau[\tau'/\alpha]]\!]_\rho$. Finally, since $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_1$, $W_1 \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} \triangleright W_1$, and $\triangleright W_1 \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_2$, we have $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_2$, which suffices to finish the proof. □

LEMMA 3.28 (COMPAT $(\!|\mathrm{e}|\!)_\tau$).

$$\begin{array}{l}\Omega = \Omega_\mathrm{e} \uplus \Omega' \land \Gamma = \Gamma' \land \Delta; \Gamma; \Gamma; \Omega_\mathrm{e} \vdash \mathrm{e} \preceq \mathrm{e} : \tau \rightsquigarrow \Delta; \Gamma \land no_\bullet(\Omega) \land \_ : \tau \sim \tau \\ \qquad \Longrightarrow \ \Gamma; \Omega; \Delta; \Gamma \vdash (\!|\mathrm{e}|\!)_\tau \preceq (\!|\mathrm{e}|\!)_\tau : \tau \land \_ : \tau \sim \tau \rightsquigarrow \Gamma'; \Omega'\end{array}$$

PROOF. We have $\Omega = \Omega_\mathrm{e} \uplus \Omega'$ and $\Gamma = \Gamma'$ by the first two assumptions. Moreover, $\Gamma; \Omega; \Delta; \Gamma \vdash (\!|\mathrm{e}|\!)_\tau : \tau$ by the conversion typing rule. Ergo, to prove the conclusion, it suffices to show $\Gamma; \Omega_\mathrm{e}; \Delta; \Gamma \vdash (\!|\mathrm{e}|\!)_\tau \preceq (\!|\mathrm{e}|\!)_\tau : \tau$. Thus, we must show that given

$$\forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega.\rho \in \mathcal{D}[\![\Delta]\!] \land (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \land (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!].\land (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\Omega_\mathrm{e}]\!].$$

we must show

$$(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, (\!|\mathrm{e}|\!)_\tau{}^+)))), (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, (\!|\mathrm{e}|\!)_\tau{}^+))))) \in \mathcal{E}[\![\tau]\!]_\rho$$

We can push the compiler and substitutions through the pair to refine that to:

$$\begin{array}{l}(W, (\emptyset, C_{\tau \mapsto \tau}(\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+))))), \\ (\emptyset, C_{\tau \mapsto \tau}(\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+)))))) \in \mathcal{E}[\![\tau]\!]_\rho\end{array}$$

Now, by instantiating our induction hypothesis with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$, we find that:

$$(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))), (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))))) \in \mathcal{E}[\![\tau]\!].$$

However, since $\mathrm{no}_\bullet(\Omega)$, there are no static affine variables in Ω_e, because $\Omega_\mathrm{e} \subseteq \Omega$. Ergo, since $(W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\Omega_\mathrm{e}]\!]$., it must be the case that $\Phi_1 = \Phi_2 = \emptyset$.

Therefore, by Theorem 3.18, we have

$$\begin{array}{l}(W, (\emptyset, C_{\tau \mapsto \tau}(\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+))))), \\ (\emptyset, C_{\tau \mapsto \tau}(\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+)))))) \in \mathcal{E}[\![\tau]\!].\end{array}$$

Finally, by Lemma 3.14, we have

$$\begin{array}{l}(W, (\emptyset, C_{\tau \mapsto \tau}(\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+))))), \\ (\emptyset, C_{\tau \mapsto \tau}(\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+)))))) \in \mathcal{E}[\![\tau]\!]_\rho\end{array}$$

as was to be proven. □

Lemma 3.29 (Compat unit).

$$\Delta; \Gamma; \Gamma; \Omega \vdash () \preceq () : \mathrm{unit} \rightsquigarrow \Delta; \Gamma$$

Proof. Clearly, $\Delta = \Delta$ and $\Gamma = \Gamma$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash () : \mathrm{unit} \rightsquigarrow \Delta; \Gamma$ by the unit typing rule. Ergo, it suffices to show that $\Delta; \Gamma; \Gamma; \Omega \vdash () \preceq () : \mathrm{unit}$.

Expanding the conclusion, given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket. \wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}\llbracket\Omega\rrbracket.$$

we must show

$$(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, ()^+)))), (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, ()^+))))) \in \mathcal{E}\llbracket\mathrm{unit}\rrbracket.$$

$()^+ = ()$ is a closed term, so the closings have no effect. Ergo, we must show:

$$(W, (\Phi_1, ()), (\Phi_2, ()) \in \mathcal{E}\llbracket\tau\rrbracket.$$

This trivially follows from $(W, (\emptyset, ()), (\emptyset, ()) \in \mathcal{V}\llbracket\mathrm{unit}\rrbracket_\rho$ and Lemma 3.2. □

Lemma 3.30 (Compat true).

$$\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{true} \preceq \mathrm{true} : \mathrm{bool} \rightsquigarrow \Delta; \Gamma$$

Proof. Clearly, $\Delta = \Delta$ and $\Gamma = \Gamma$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{true} : \mathrm{bool} \rightsquigarrow \Delta; \Gamma$ by the true typing rule. Ergo, it suffices to show that $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{true} \preceq \mathrm{true} : \mathrm{bool}$.

Expanding the conclusion, given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket. \wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}\llbracket\Omega\rrbracket.$$

we must show

$$(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{true}^+)))), (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{true}^+))))) \in \mathcal{E}\llbracket\mathrm{bool}\rrbracket.$$

$\mathrm{true}^+ = 0$ is a closed term, so the closings have no effect. Ergo, we must show:

$$(W, (\Phi_1, 0), (\Phi_2, 0)) \in \mathcal{E}\llbracket\mathrm{bool}\rrbracket.$$

This trivially follows from $(W, (\emptyset, 0), (\emptyset, 0) \in \mathcal{V}\llbracket\mathrm{bool}\rrbracket_\rho$ and Lemma 3.2. □

Lemma 3.31 (Compat false).

$$\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{false} \preceq \mathrm{false} : \mathrm{bool} \rightsquigarrow \Delta; \Gamma$$

Proof. This case is trivially similar to true, since $\mathrm{false}^+ = 1$ and $(W, (\emptyset, 1), (\emptyset, 1) \in \mathcal{V}\llbracket\mathrm{bool}\rrbracket_\rho$. □

Lemma 3.32 (Compat int).

$$\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{n} \preceq \mathrm{n} : \mathrm{int} \rightsquigarrow \Delta; \Gamma$$

Proof. Clearly, $\Delta = \Delta$ and $\Gamma = \Gamma$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{n} : \mathrm{int} \rightsquigarrow \Delta; \Gamma$ by the int typing rule. Ergo, it suffices to show that $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{n} \preceq \mathrm{n} : \mathrm{int}$.

Expanding the conclusion, given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket. \wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}\llbracket\Omega\rrbracket.$$

we must show

$$(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{n}^+)))), (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{n}^+))))) \in \mathcal{E}\llbracket\mathrm{int}\rrbracket.$$

$\mathrm{n}^+ = \mathrm{n}$ is a closed term, so the closings have no effect. Ergo, we must show:

$$(W, (\Phi_1, \mathrm{n}), (\Phi_2, \mathrm{n})) \in \mathcal{E}\llbracket\tau\rrbracket.$$

This trivially follows from $(W, (\emptyset, \mathrm{n}), (\emptyset, \mathrm{n}) \in \mathcal{V}\llbracket\mathrm{int}\rrbracket_\rho$ and Lemma 3.2. □

Lemma 3.33 (Compat x).

$$\mathrm{x} : \tau \in \Gamma \implies \Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{x} \preceq \mathrm{x} : \tau \rightsquigarrow \Delta; \Gamma$$

Proof. Clearly, $\Delta = \Delta$ and $\Gamma = \Gamma$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{x} : \tau \rightsquigarrow \Delta; \Gamma$ by the variable typing rule. Ergo, it suffices to show that $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{x} \preceq \mathrm{x} : \tau$.

Expanding the conclusion, given

$\forall W.\forall \rho\ \gamma_\Gamma\ \gamma_\Gamma\ \gamma_\Omega.\rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket. \wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}\llbracket\Omega\rrbracket.$

we must show

$(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{x}^+)))), (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{x}^+))))) \in \mathcal{E}\llbracket\tau\rrbracket.$

Notice that $\mathrm{x}^+ = \mathrm{x}$. Then, since $\mathrm{x} : \tau \in \Gamma$ and $(W, \emptyset, \emptyset, \gamma_\Gamma))$, we have

$$\gamma_\Gamma(\mathrm{x}) = (\mathrm{v}_1, \mathrm{v}_2)$$

where $(W, (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket..$

Thus,

$$\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{x}^+))) = \mathrm{v}_1$$

and

$$\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{x}^+))) = \mathrm{v}_2$$

Ergo, we must show

$$(W, (\Phi_1, \mathrm{v}_1), (\Phi_2, \mathrm{v}_2)) \in \mathcal{E}\llbracket\tau\rrbracket.$$

This trivially follows from $(W, (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket.$ and Lemma 3.2. □

Lemma 3.34 (Compat $\mathrm{a}_\circ$).

$$\mathrm{a}_\circ : \tau \in \Omega \implies \Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{a}_\circ \preceq \mathrm{a}_\circ : \tau \rightsquigarrow \Delta; \Gamma$$

Proof. One can easily see that $\Delta = \Delta$ and $\Gamma = \Gamma$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{a}_\circ : \tau \rightsquigarrow \Delta; \Gamma$ by the dynamic variable typing rule. Ergo, it suffices to show $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{a}_\circ \preceq \mathrm{a}_\circ : \tau$.

Expanding the conclusion, given

$\forall W.\forall \rho\ \gamma_\Gamma\ \gamma_\Gamma\ \gamma_\Omega.\rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket. \wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}\llbracket\Omega\rrbracket.$

we must show:

$(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{a}_\circ{}^+)))), (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{a}_\circ{}^+))))) \in \mathcal{E}\llbracket\tau\rrbracket.$

We can push the compiler and the substitutions through this expression to refine this to:

$(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{a})))\ ()), (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{a})))\ ())) \in \mathcal{E}\llbracket\tau\rrbracket.$

Since $(W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}\llbracket\Omega\rrbracket.$, there must exist $(\ell_1, \ell_2) \in W.\Theta$ and values $\mathrm{v}_1, \mathrm{v}_2$ such that:

$$\gamma_\Omega(\mathrm{a}) = (\mathrm{guard}(\mathrm{v}_1, \ell_1), \mathrm{guard}(\mathrm{v}_2, \ell_2))$$

where either $W.\Theta(\ell_1, \ell_2) = \textsc{used}$ or $W.\Theta = \Theta' \uplus (\ell_1, \ell_2) \mapsto (\Phi_1^*, \Phi_2^*)$ and

$$((W.k, W.\Psi, \Theta'), (\Phi_1^*, \mathrm{v}_1), (\Phi_2^*, \mathrm{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket.$$

Ergo, we must show:

$$(W, (\Phi_1, \mathrm{guard}(\mathrm{v}_1, \ell_1)\ ()), (\Phi_2, \mathrm{guard}(\mathrm{v}_2, \ell_2)\ ())) \in \mathcal{E}\llbracket\tau\rrbracket.$$

which we can expand to:

$(W, (\Phi_1, (\lambda\_.\mathrm{if}\ !\ell_1\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1 := \textsc{used}; \mathrm{v}_1\})\ ()), (\Phi_2, (\lambda\_.\mathrm{if}\ !\ell_2\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2 := \textsc{used}; \mathrm{v}_2\})\ ())) \in \mathcal{E}\llbracket\tau\rrbracket.$

Notice that both expressions have no free variables because v_1 and v_2 are closed, as they are in the value relation.

Let e_1 and e_2 be the first and second expressions, respectively, in the above tuple. Expanding the definition of the expression relation, given:

$$\begin{gathered}\forall \Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2 {:} W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k. \\ \Phi_{r1} \# \Phi_1 \wedge \Phi_{r2} \# \Phi_2 \wedge \Phi_{r1} \uplus \Phi_1, \Phi_{r2} \uplus \Phi_2 : W \wedge \\ \langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, \mathrm{e}_1 \rangle \overset{j}{\dashrightarrow} \langle \Phi_1', \mathrm{H}_1', \mathrm{e}_1' \rangle \not\twoheadrightarrow\end{gathered}$$

we must show that either e_1' is $\mathrm{fail}\ \textsc{Conv}$ or there exist $\Phi_{f1}, \Phi_{g1}, \Phi_{f2}, \Phi_{g2}, \mathrm{v}_2, \mathrm{H}_2', W'$ such that:

$$\begin{aligned}&\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, \mathrm{e}_2 \rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathrm{H}_2', \mathrm{v}_2 \rangle \not\twoheadrightarrow \\ &\wedge \Phi_1' = \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge \\ &\wedge W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W' \wedge \mathrm{H}_1', \mathrm{H}_2' : W' \\ &\wedge (W', (\Phi_{f1}, \mathrm{e}_1'), (\Phi_{f2}, \mathrm{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_\rho)\end{aligned}$$

Then, by application, we have

$$\begin{aligned}&\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, (\lambda\_.\mathrm{if}\ !\ell_1\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1 := \textsc{used}; \mathrm{v}_1\})\ ()\rangle \dashrightarrow \\ &\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, \mathrm{if}\ !\ell_1\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1 := \textsc{used}; \mathrm{v}_1\}\rangle\end{aligned}$$

and

$$\begin{aligned}&\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, (\lambda\_.\mathrm{if}\ !\ell_2\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2 := \textsc{used}; \mathrm{v}_2\})\ ()\rangle \dashrightarrow \\ &\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, \mathrm{if}\ !\ell_2\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2 := \textsc{used}; \mathrm{v}_2\}\rangle\end{aligned}$$

Then, as mentioned before, we have two cases: either $W.\Theta(\ell_1, \ell_2) = \textsc{used}$ or $W.\Theta(\ell_1, \ell_2) = (\Phi_1^*, \Phi_2^*)$.

If $W.\Theta(\ell_1, \ell_2) = \textsc{used}$, then since $\mathrm{H}_1, \mathrm{H}_2 : W$, it follows that $\mathrm{H}_1(\ell_1) = \mathrm{H}_2(\ell_2) = \textsc{used}$. In this case, the configuration steps to $\mathrm{fail}\ \textsc{Conv}$, so we are done.

If $W.\Theta(\ell_1, \ell_2) = (\Phi_1^*, \Phi_2^*)$, then since $\mathrm{H}_1, \mathrm{H}_2 : W$, it follows that $\mathrm{H}_1(\ell_1) = \mathrm{H}_2(\ell_2) = \textsc{unused}$.

$$\begin{aligned}&\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, \mathrm{if}\ !\ell_1\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_1 := \textsc{used}; \mathrm{v}_1\}\rangle \\ \dashrightarrow\ &\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, \ell_1 := \textsc{used}; \mathrm{v}_1\rangle \\ \dashrightarrow\ &\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1[\ell_1 \mapsto \textsc{used}], \mathrm{v}_1\rangle\end{aligned}$$

and

$$\begin{aligned}&\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, \mathrm{if}\ !\ell_2\ \{\mathrm{fail}\ \textsc{Conv}\}\ \{\ell_2 := \textsc{used}; \mathrm{v}_2\}\rangle \\ \dashrightarrow\ &\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2, \ell_2 := \textsc{used}; \mathrm{v}_2\rangle \\ \dashrightarrow\ &\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, \mathrm{H}_2[\ell_2 \mapsto \textsc{used}], \mathrm{v}_2\rangle\end{aligned}$$

Now, consider

$$W' = (W.k, W.\Psi, W.\Theta[(\ell_1, \ell_2) \mapsto \textsc{used}])$$

Notice that for all $i \in \{1, 2\}$, $\mathrm{flags}(W, i) = \mathrm{flags}(W', i) \uplus \Phi_i^*$. This is because the dynamic flags in W' are the exact same as W, except (ℓ_1, ℓ_2) has been switched to $\textsc{used}$, meaning Φ_1^* has been removed from the left side and Φ_2^* has been removed from the right side. Ergo, since $\Phi_{r1}, \Phi_{r2} \subseteq W$ and $\mathrm{flags}(W', i) \subseteq \mathrm{flags}(W, i)$ for all $i \in \{1, 2\}$, it follows that $\Phi_{r1}, \Phi_{r2} : W'$. Since W and W' also have the same heap typing, we can then conclude that $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W'$.

Next, notice that $\mathrm{H}_1[\ell_1 \rightarrow \textsc{used}], \mathrm{H}_2[\ell_2 \rightarrow \textsc{used}] : W'$ because $\mathrm{H}_1, \mathrm{H}_2 : W$ and the only change from W to W' is that $W'.\Theta(\ell_1, \ell_2) = \textsc{used}$, which is satisfied by both of these new heaps.

Moreover, let $W_b = (W.k, W.\Psi, \Theta')$. The only difference between W_b and W' is that the dynamic flag store in W_b does not contain the locations (ℓ_1, ℓ_2) whereas $W'.\Theta$ contains $(\ell_1, \ell_2) \mapsto \textsc{used}$. Furthermore, since for all $i \in \{1, 2\}$, $\mathrm{flags}(W, i) = \mathrm{flags}(W', i) \uplus \Phi_i^*$, we find that $\mathrm{flags}(W', i) \# \Phi_i^*$ and thus $\Phi_1^*, \Phi_2^* : W'$. Ergo, $W_b \sqsubseteq_{\Phi_1^*, \Phi_2^*} W'$.

Finally, for all $i \in \{1, 2\}$, let $\Phi_{fi} = \Phi_i^*$ and let $\Phi_{gi} = \Phi_i$. We have by assumption that $(W_b, (\Phi_1^*, \mathrm{v}_1), (\Phi_2^*, \mathrm{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_{\cdot}$, so since $W_b \sqsubseteq_{\Phi_1^*, \Phi_2^*} W'$, by Lemma 3.8, we have $(W', (\Phi_1^*, \mathrm{v}_1), (\Phi_2^*, \mathrm{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_{\cdot}$, which suffices to finish the proof. □

Lemma 3.35 (Compat $a_\bullet$).

$$a_\bullet : \tau \in \Omega \implies \Delta; \Gamma; \Gamma; \Omega \vdash a_\bullet \preceq a_\bullet : \tau \rightsquigarrow \Delta; \Gamma$$

Proof. One can easily see that $\Delta = \Delta$ and $\Gamma = \Gamma$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash a_\bullet : \tau \rightsquigarrow \Delta; \Gamma$ by the static affine variable typing rule. Ergo, it suffices to show $\Delta; \Gamma; \Gamma; \Omega \vdash a_\bullet \preceq a_\bullet : \tau$.

Expanding the conclusion, given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]. \wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!].$$

we must show

$$(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, {a_\bullet}^+)))), (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, {a_\bullet}^+))))) \in \mathcal{E}[\![\tau]\!].$$

Notice that ${a_\bullet}^+ = a_\bullet$. Then, since $a_\bullet : \tau \in \Omega$ and $(W, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!].$, then there exist $\Phi'_1, \Phi'_2, v_1, v_2, f_1, f_2$ such that

$$\gamma_\Omega(a_\bullet) = (\mathrm{protect}(v_1, f_1), \mathrm{protect}(v_2, f_2))$$

where $(W, (\Phi'_1, v_1), (\Phi'_2, v_2)) \in \mathcal{V}[\![\tau]\!].$, $\Phi'_1 \cup \{f_1\} \subseteq \Phi_1$, $\Phi'_2 \cup \{f_2\} \subseteq \Phi_2$, $f_1 \notin \Phi'_1$, and $f_2 \notin \Phi'_2$. Thus, we must show

$$(W, (\Phi_1, \mathrm{protect}(v_1, f_1)), (\Phi_2, \mathrm{protect}(v_2, f_2))) \in \mathcal{E}[\![\tau]\!].$$

Let $e_1 = \mathrm{protect}(v_1, f_1)$ and $e_2 = \mathrm{protect}(v_2, f_2)$. Expanding the definition of the expression relation, given:

$$\forall \Phi_{r1}, \Phi_{r2}, H_1, H_2{:}W,\ e'_1,\ H'_1,\ j < W.k.$$
$$\Phi_{r1} \# \Phi_1 \wedge \Phi_{r2} \# \Phi_2 \wedge \Phi_{r1} \uplus \Phi_1, \Phi_{r2} \uplus \Phi_2 : W \wedge$$
$$\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, H_1, e_1 \rangle \overset{j}{\dashrightarrow} \langle \Phi'_1, H'_1, e'_1 \rangle \nrightarrow$$

we must show that either e'_1 is fail Conv or there exist $\Phi_{f1}, \Phi_{g1}, \Phi_{f2}, \Phi_{g2}, v_2, H'_2, W'$ such that:

$$\begin{aligned}
&\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, H_2, e_2 \rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, H'_2, v_2 \rangle \nrightarrow \\
&\wedge \Phi'_1 = \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge \\
&\wedge\ W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W' \wedge\ H'_1, H'_2 : W' \\
&\wedge (W', (\Phi_{f1}, e'_1), (\Phi_{f2}, v_2)) \in \mathcal{V}[\![\tau]\!]_\rho)
\end{aligned}$$

Since $f_1 \in \Phi_1$,

$$\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, H_1, \mathrm{protect}(v_1, f_1) \rangle \dashrightarrow \langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1 \setminus \{f_1\}, H_1, v_1 \rangle$$

and since $f_2 \in \Phi_2$,

$$\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2, H_2, \mathrm{protect}(v_2, f_2) \rangle \dashrightarrow \langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2 \setminus \{f_2\}, H_2, v_2 \rangle$$

Then, since $\Phi'_1 \subseteq \Phi_1$ and $f_1 \notin \Phi'_1$, we have $\Phi'_1 \subseteq \Phi_1 \setminus \{f_1\}$. Similarly, $\Phi'_2 \subseteq \Phi_2 \setminus \{f_2\}$. Ergo, for all $i \in \{1, 2\}$, let $\Phi_{fi} = \Phi'_i$ and let $\Phi_{gi} = \Phi_i \setminus \{f_i\} \setminus \Phi'_i$. Then, we can reexpress the above configurations as

$$\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1 \setminus \{f_1\}, H_1, v_1 \rangle = \langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_{f1} \uplus \Phi_{g1}, H_1, v_1 \rangle$$

and

$$\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_2 \setminus \{f_2\}, H_2, v_2 \rangle = \langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, H_2, v_2 \rangle$$

Finally, we have $(W, (\Phi_{f1}, v_1), (\Phi_{f2}, v_2)) \in \mathcal{V}[\![\tau]\!].$ because $\Phi_{fi} = \Phi'_i$ for all $i \in \{1, 2\}$, which suffices to finish the proof. □

Lemma 3.36 (Compat $\multimap$).

$$\begin{aligned}
&\Delta; \Gamma; \Gamma; \Omega, a_\circ : \tau_1 \vdash e \preceq e : \tau_2 \rightsquigarrow \Delta'; \Gamma' \wedge no_\bullet(\Omega) \\
\implies\ &\Delta; \Gamma; \Gamma; \Omega\ \vdash \lambda a_\circ : \tau_1.e \preceq \lambda a_\circ : \tau_1.e : \tau_1 \multimap \tau_2 \rightsquigarrow \Delta'; \Gamma'
\end{aligned}$$

Proof. Expanding the hypothesis, we find $\Delta = \Delta'$ and $\Gamma = \Gamma'$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash \lambda \mathrm{a}_{\circ} : \tau_1.\mathrm{e} : \tau_1 \multimap \tau_2 \rightsquigarrow \Delta'; \Gamma'$ by the λ typing rule. Ergo, it suffices to show $\Delta; \Gamma; \Gamma; \Omega \vdash \lambda \mathrm{a}_{\circ} : \tau_1.\mathrm{e} \preceq \lambda \mathrm{a}_{\circ} : \tau_1.\mathrm{e} : \tau_1 \multimap \tau_2$.

Expanding the conclusion, given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega. \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_. \wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!]_.$$

we must show

$$\begin{gathered}(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \lambda \mathrm{a}_{\circ} : \tau_1.\mathrm{e}^+)))),\\ (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \lambda \mathrm{a}_{\circ} : \tau_1.\mathrm{e}^+))))) \in \mathcal{E}[\![\tau]\!]_.\end{gathered}$$

Notice that both of these expressions have no free variables by Lemma 3.16. Moreover, notice that since $\mathrm{no}_{\bullet}(\Omega)$, $\Phi_1 = \Phi_2 = \emptyset$.

We can push the compiler and the substitutions to refine the above to:

$$\begin{gathered}(W, (\emptyset, \lambda \mathrm{a}.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))),\\ (\emptyset, \lambda \mathrm{a}.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))))) \in \mathcal{E}[\![\tau_1 \multimap \tau_2]\!]_.\end{gathered}$$

Since $\mathcal{V}[\![\tau_1 \multimap \tau_2]\!]_. \subseteq \mathcal{E}[\![\tau_1 \multimap \tau_2]\!]_.$, it suffices to show:

$$\begin{gathered}(W, (\emptyset, \lambda \mathrm{a}.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))),\\ (\emptyset, \lambda \mathrm{a}.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))))) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!]_.\end{gathered}$$

Expanding the value relation, given:

$$\forall \Phi_1'\ \mathrm{v}_1\ \Phi_2'\ \mathrm{v}_2\ W'. W \sqsubset_{\emptyset,\emptyset} W' \wedge (W', (\Phi_1', \mathrm{v}_1), (\Phi_2', \mathrm{v}_2)) \in \mathcal{V}[\![\tau_1]\!]_.$$

we must show that:

$$\begin{gathered}((W'.k, W'.\Psi, W'.\Theta \uplus (\ell_1, \ell_2) \mapsto (\Phi_1', \Phi_2')),\\ (\emptyset, [\mathrm{a} {\mapsto} \mathrm{guard}(\mathrm{v}_1, \ell_1)]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))),\\ (\emptyset, [\mathrm{a} {\mapsto} \mathrm{guard}(\mathrm{v}_2, \ell_2)\}]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))))) \in \mathcal{E}[\![\tau_2]\!]_.\end{gathered}$$

Notice that $W'' = (W'.k, W'.\Psi, W'.\Theta \uplus (\ell_1, \ell_2) \mapsto (\Phi_1', \Phi_2'))$ is a world extension of W' because it has the same heap typing as W' and has all the affine flags as W' plus one new affine flag which is disjoint from any affine flag in W'. Ergo, since $W \sqsubseteq_{\emptyset,\emptyset} W'$ and $W' \sqsubseteq_{\emptyset,\emptyset} W''$, we have $W \sqsubseteq W''$. Next, notice that:

$$(W'', \emptyset, \emptyset, \gamma_\Omega[\mathrm{a} \mapsto (\mathrm{guard}(\mathrm{v}_1, \ell_1), \mathrm{guard}(\mathrm{v}_2, \ell_2))]) \in \mathcal{G}[\![\Omega, \mathrm{a} : \tau_1]\!]_.$$

because $(\ell_1, \ell_2) \in \mathrm{dom}(W''.\Theta)$, $(W'', (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}[\![\tau_1]\!]_.$ (by Lemma 3.8 and $(W, (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}[\![\tau_1]\!]_.$), and $(W'', \emptyset, \emptyset, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!]_.$ (by Lemma 3.8 and $(W, \emptyset, \emptyset, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!]_.$). Therefore, we can instantiate the first induction hypothesis with

$$W'', \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega[\mathrm{a} \mapsto (\mathrm{guard}(\mathrm{v}_1, \ell_1), \mathrm{guard}(\mathrm{v}_2, \ell_2))], \rho$$

to find

$$\begin{gathered}(W'', (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega[\mathrm{a} \mapsto \mathrm{guard}(\mathrm{v}_1, \ell_1)], \mathrm{e}^+)))),\\ (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega[\mathrm{a} \mapsto \mathrm{guard}(\mathrm{v}_2, \ell_2))], \mathrm{e}^+)))) \in \mathcal{E}[\![\tau_2]\!]_.\end{gathered}$$

which is equivalent to what was to be proven. □

Lemma 3.37 (Compat $\mathrel{-\!\!\bullet}$).

$$\Delta; \Gamma; \Gamma; \Omega, \mathrm{a}_{\bullet} : \tau_1 \vdash \mathrm{e} \preceq \mathrm{e} : \tau_2 \rightsquigarrow \Delta'; \Gamma' \implies \Delta; \Gamma; \Gamma; \Omega \vdash \lambda \mathrm{a}_{\bullet} : \tau_1.\mathrm{e} \preceq \lambda \mathrm{a}_{\bullet} : \tau_1.\mathrm{e} : \tau_1 \mathrel{-\!\!\bullet} \tau_2 \rightsquigarrow \Delta'; \Gamma'$$

Proof. Expanding the hypothesis, we find that $\Delta = \Delta'$ and $\Gamma = \Gamma'$. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash \lambda \mathrm{a}_{\bullet} : \tau_1.\mathrm{e} : \tau_1 \mathrel{-\!\!\bullet} \tau_2 \rightsquigarrow \Delta'; \Gamma'$ by the $\lambda \mathrm{a}_{\bullet}$ typing rule. Ergo, it suffices to show $\Delta; \Gamma; \Gamma; \Omega \vdash \lambda \mathrm{a}_{\bullet} : \tau_1.\mathrm{e} \preceq \lambda \mathrm{a}_{\bullet} : \tau_1.\mathrm{e} : \tau_1 \mathrel{-\!\!\bullet} \tau_2$.

Expanding the conclusion, given

$$\forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega.\rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket. \wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}\llbracket\Omega\rrbracket.$$

we must show

$$\begin{gathered}(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \lambda \mathrm{a}_\bullet : {\tau_1}^+)))),\\ (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \lambda \mathrm{a}_\bullet : {\tau_1}^+))))) \in \mathcal{E}\llbracket\tau_1 \multimap\!\!\bullet\ \tau_2\rrbracket.\end{gathered}$$

By pushing the compiler and substitutions through the lambda expression, we can refine this to:

$$\begin{gathered}(W, (\Phi_1, \lambda \mathrm{a}_\bullet.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))),\\ (\Phi_2, \lambda \mathrm{a}_\bullet.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))))) \in \mathcal{E}\llbracket\tau_1 \multimap\!\!\bullet\ \tau_2\rrbracket.\end{gathered}$$

Since $\mathcal{V}\llbracket\tau_1 \multimap\!\!\bullet\ \tau_2\rrbracket. \subseteq \mathcal{E}\llbracket\tau_1 \multimap\!\!\bullet\ \tau_2\rrbracket.$ by Lemma 3.1, it suffices to show:

$$\begin{gathered}(W, (\Phi_1, \lambda \mathrm{a}_\bullet.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+)))),\\ (\Phi_2, \lambda \mathrm{a}_\bullet.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))))) \in \mathcal{V}\llbracket\tau_1 \multimap\!\!\bullet\ \tau_2\rrbracket.\end{gathered}$$

Expanding the value relation definition, we find that we need to show that given:

$$\begin{aligned}&\forall \Phi_1'\ \Phi_2'\ f_1\ f_2\ \mathrm{v}_1\ \mathrm{v}_2\ W'.W \sqsubset_{\Phi_1,\Phi_2} W'\\ &\quad \wedge (W', (\Phi_1', \mathrm{v}_1), (\Phi_2', \mathrm{v}_2)) \in \mathcal{V}\llbracket\tau_1\rrbracket. \wedge \Phi_1 \cap \Phi_1' = \Phi_2 \cap \Phi_2' = \emptyset\\ &\quad \wedge f_1 \notin \Phi_1 \uplus \Phi_1' \uplus \mathrm{flags}(W', 1) \wedge f_2 \notin \Phi_2 \uplus \Phi_2' \uplus \mathrm{flags}(W', 2)\end{aligned}$$

it holds that:

$$\begin{gathered}(W', (\Phi_1 \uplus \Phi_1' \uplus \{f_1\}, [\mathrm{a}_\bullet {\mapsto} \mathrm{protect}(\mathrm{v}_1, f_1)]\mathrm{e}_1),\\ (\Phi_2 \uplus \Phi_2' \uplus \{f_2\}, [\mathrm{a}_\bullet {\mapsto} \mathrm{protect}(\mathrm{v}_2, f_2)]\mathrm{e}_2)) \in \mathcal{E}\llbracket\tau_2\rrbracket.\end{gathered}$$

By Lemma 3.8, since $W \sqsubseteq_{\Phi_1,\Phi_2} W'$, we have $(W', \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}\llbracket\Omega\rrbracket..$ Moreover, we have $(W', (\Phi_1', \mathrm{v}_1), (\Phi_2', \mathrm{v}_2)) \in \mathcal{V}\llbracket\tau_1\rrbracket.$, $\Phi_1 \cap \Phi_1' = \Phi_2 \cap \Phi_2' = \emptyset$, $f_1 \notin \Phi_1 \uplus \Phi_1'$, and $f_2 \notin \Phi_2 \uplus \Phi_2'$. Therefore,

$$(W', \Phi_1 \uplus \Phi_1' \uplus \{f_1\}, \Phi_2 \uplus \Phi_2' \uplus \{f_2\}, \gamma_\Omega[\mathrm{a}_\bullet \mapsto (\mathrm{protect}(\mathrm{v}_1, f_1), \mathrm{protect}(\mathrm{v}_2, f_2))]) \in \mathcal{G}\llbracket\Omega, \mathrm{a}_\bullet : \tau_1\rrbracket.$$

Then, we can instantiate the first induction hypothesis with

$$W', \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega[\mathrm{a}_\bullet \mapsto (\mathrm{protect}(\mathrm{v}_1, f_1), \mathrm{protect}(\mathrm{v}_2, f_2))], \rho$$

to find that:

$$\begin{gathered}(W', (\Phi_1 \uplus \Phi_1' \uplus \{f_1\}, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega[\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{v}_1, f_1)], \mathrm{e}^+)))),\\ (\Phi_2 \uplus \Phi_2' \uplus \{f_2\}, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega[\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{v}_2, f_2)], \mathrm{e}^+))))) \in \mathcal{E}\llbracket\tau_2\rrbracket.\end{gathered}$$

We can simplify this by bringing the $[\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{v}_1, f_1)]$ and $[\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{v}_2, f_2)]$ outside of the closings, which suffices to finish the proof. □

Lemma 3.38 (Compat app $:\!\multimap$).

$$\begin{gathered}\Delta_1; \Gamma_1; \Gamma; \Omega_1 \vdash \mathrm{e}_1 \preceq \mathrm{e}_1 : \tau_1 \multimap\!\!\bullet\ \tau_2 \rightsquigarrow \Delta_2; \Gamma_2 \wedge \Delta_2; \Gamma_2; \Gamma; \Omega_2 \vdash \mathrm{e}_2 \preceq \mathrm{e}_2 : \tau_1 \rightsquigarrow \Delta_3; \Gamma_3\\ \Longrightarrow \Delta_1; \Gamma_1; \Gamma; \Omega_1 \uplus \Omega_2 \vdash \mathrm{e}_1\ \mathrm{e}_2 \preceq \mathrm{e}_1\ \mathrm{e}_2 : \tau_2 \rightsquigarrow \Delta_3; \Gamma_3\end{gathered}$$

Proof. Expanding the hypotheses, we find $\Delta_1 = \Delta_2 = \Delta_3$ and $\Gamma_1 = \Gamma_2 = \Gamma_3$. Moreover, $\Delta_1; \Gamma_1; \Gamma; \Omega_1 \uplus \Omega_2 \vdash \mathrm{e}_1\ \mathrm{e}_2 : \tau_2 \rightsquigarrow \Delta_3; \Gamma_3$ by the application typing rule. Ergo, it suffices to show $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{e}_1\ \mathrm{e}_2 \preceq \mathrm{e}_1\ \mathrm{e}_2 : \tau_2$.

Expanding the conclusion, given

$$\forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega.\rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket. \wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}\llbracket\Omega_1 \uplus \Omega_2\rrbracket.$$

we must show

$$(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1\ {\mathrm{e}_2}^+)))), (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1\ {\mathrm{e}_2}^+))))) \in \mathcal{E}\llbracket\tau_2\rrbracket.$$

Notice that both of these expressions have no free variables by Lemma 3.16.

We can push the compiler and substitutions through the application to refine this to:

$$\begin{gathered}(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+)))\ (\mathtt{let\ x = }\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^+)))\mathtt{\ in\ thunk(x)})),\\ (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1{}^+)))\ (\mathtt{let\ x = }\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^+)))\mathtt{\ in\ thunk(x)})))\\ \in \mathcal{E}[\![\tau_2]\!].\end{gathered}$$

Next, by Lemma 3.5, we have that $\gamma_\Omega = \gamma_1 \uplus \gamma_2$, $\Phi_1 = \Phi_{1l} \uplus \Phi_{1r}$, and $\Phi_2 = \Phi_{2l} \uplus \Phi_{2r}$ where

$$(W, \Phi_{1l}, \Phi_{2l}, \gamma_1) \in \mathcal{G}[\![\Omega_1]\!].$$

and

$$(W, \Phi_{1r}, \Phi_{2r}, \gamma_2) \in \mathcal{G}[\![\Omega_2]\!].$$

and for all $i \in \{1, 2\}$,

$$\mathrm{close}_i(\gamma_\Omega, \mathrm{e}_1{}^+) = \mathrm{close}_i(\gamma_1, \mathrm{e}_1{}^+)$$

and

$$\mathrm{close}_i(\gamma_\Omega, \mathrm{e}_2{}^+) = \mathrm{close}_i(\gamma_1, \mathrm{e}_2{}^+)$$

Thus, we refine the statement we need to prove to:

$$\begin{gathered}(W,\\ (\Phi_{1l} \uplus \Phi_{1r},\\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e}_1{}^+)))\ (\mathtt{let\ x = }\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e}_2{}^+)))\mathtt{\ in\ thunk(x)})),\\ (\Phi_{2l} \uplus \Phi_{2r},\\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathrm{e}_1{}^+)))\ (\mathtt{let\ x = }\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e}_2{}^+)))\mathtt{\ in\ thunk(x)})))\\ \in \mathcal{E}[\![\tau_2]\!].\end{gathered}$$

Let e_1 and e_2 be the first and second expressions, respectively, in the above tuple. Expanding the definition of the expression relation, given:

$$\begin{gathered}\forall \Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2 {:} W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.\\ \Phi_{r1} \# \Phi_{1l} \uplus \Phi_{1r} \wedge \Phi_{r2} \# \Phi_{2l} \uplus \Phi_{2r} \wedge \Phi_{r1} \uplus \Phi_{1l} \uplus \Phi_{1r}, \Phi_{r2} \uplus \Phi_{2l} \uplus \Phi_{2r} : W \wedge\\ \langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_{1l} \uplus \Phi_{1r}, \mathrm{H}_1, \mathrm{e}_1 \rangle \overset{j}{\dashrightarrow} \langle \Phi_1', \mathrm{H}_1', \mathrm{e}_1' \rangle \not\twoheadrightarrow\end{gathered}$$

we must show that either e_1' is fail Conv or there exist $\Phi_{f1}, \Phi_{g1}, \Phi_{f2}, \Phi_{g2}, \mathrm{v}_2, \mathrm{H}_2', W'$ such that:

$$\begin{aligned}&\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_{2l} \uplus \Phi_{2r}, \mathrm{H}_2, \mathrm{e}_2 \rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathrm{H}_2', \mathrm{v}_2 \rangle \not\twoheadrightarrow\\ &\wedge \Phi_1' = \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge\\ &\wedge\ W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W' \wedge\ \mathrm{H}_1', \mathrm{H}_2' : W'\\ &\wedge\ (W', (\Phi_{f1}, \mathrm{e}_1'), (\Phi_{f2}, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho)\end{aligned}$$

Next, we need to find e_1'. From the operational semantic, the application will run the first subexpression using the heap H_1 until it reaches a target value or gets stuck. By appealing to our first induction hypothesis, instantiated with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_1, \rho$, we find that:

$$\begin{gathered}(W,\\ (\Phi_{1l}, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e}_1{}^+)))),\\ (\Phi_{2l}, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathrm{e}_1{}^+))))) \in \mathcal{E}[\![\tau_1 \multimap \tau_2]\!].\end{gathered}$$

Therefore,

$$\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_{1r} \uplus \Phi_{1l}, \mathrm{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e}_1{}^+))) \rangle$$

either reduces to fail Conv, in which case the original expression steps to fail Conv, or to some irreducible configuration $\langle \Phi_{r1} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{1r} \uplus \Phi_{f1l} \uplus \Phi_{g1l}, \mathrm{H}_1^*, \mathrm{e}_1^* \rangle$, in which case on the other side, the configuration

$$\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_{2r} \uplus \Phi_{2l}, \mathrm{H}_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathrm{e}_1{}^+))) \rangle$$

reduces to some irreducible configuration $\langle \Phi_{r2} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{2r} \uplus \Phi_{f2l} \uplus \Phi_{g2l}, \mathrm{H}_2^*, \mathrm{e}_1^\dagger \rangle$ and there exists some W_1 where $W \sqsubseteq_{\Phi_{r1} \uplus \Phi_{1r}, \Phi_{r2} \uplus \Phi_{2r}} W_1$, $\mathrm{H}_1^*, \mathrm{H}_2^* : W_1$, and $(W_1, (\Phi_{f1l}, \mathrm{e}_1^*), (\Phi_{f2l}, \mathrm{e}_1^\dagger)) \in \mathcal{V}\llbracket \tau_1 \multimap \tau_2 \rrbracket$.. By expanding the value relation, we find that $\Phi_{f1l} = \Phi_{f2l} = \emptyset$.

Since terms in the value relation are target values, the original application will continue reducing on the second subexpression according to the operational semantics. Then, we can appeal to the second induction hypothesis instantiated with $W_1, \gamma_\Gamma, \gamma_\Gamma, \gamma_2, \rho$, by Lemma 3.8 because $W \sqsubseteq_{\Phi_{1r}, \Phi_{2r}} W_1$. Ergo,

$$(W_1, (\Phi_{1r}, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e_2}^+)))),\\ (\Phi_{2r}, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e_2}^+))))) \in \mathcal{E}\llbracket \tau_1 \rrbracket.$$

Therefore,

$$\langle \Phi_{r1} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{g1l} \uplus \Phi_{1r}, \mathrm{H}_1^*, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e_2}^+))) \rangle$$

either reduces to fail Conv, in which case the original expression steps to fail Conv, or to some irreducible configuration $\langle \Phi_{r1} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{g1l} \uplus \Phi_{f1r} \uplus \Phi_{g1r}, \mathrm{H}_1^{**}, \mathrm{e}_2^* \rangle$, in which case on the other side, the configuration

$$\langle \Phi_{r2} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{g2l} \uplus \Phi_{2r}, \mathrm{H}_1^*, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e_2}^+))) \rangle$$

reduces to some irreducible configuration $\langle \Phi_{r2} \uplus \mathrm{flags}(W_2, 2) \uplus \Phi_{g2l} \uplus \Phi_{f2r} \uplus \Phi_{g2r}, \mathrm{H}_2^{**}, \mathrm{e}_2^\dagger \rangle$ and there exists some W_2 where $W_1 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{g1l}, \Phi_{r2} \uplus \Phi_{g2l}} W_2$, $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : W_2$, and $(W_2, (\Phi_{f1r}, \mathrm{e}_2^*), (\Phi_{f2r}, \mathrm{e}_2^\dagger)) \in \mathcal{V}\llbracket \tau_1 \rrbracket$..

Then, instantiate $(W_1, \mathrm{e}_1^*, \mathrm{e}_1^\dagger) \in \mathcal{V}\llbracket \tau_1 \multimap \tau_2 \rrbracket$. with $\Phi_{f1r}, \mathrm{e}_2^*, \Phi_{f2r}, \mathrm{e}_2^\dagger, \rhd W_2$. Because $W_1 \sqsubseteq_{\emptyset,\emptyset} W_2$ and $W_2 \sqsubset_{\emptyset,\emptyset} \rhd W_2$, it follows that $W_1 \sqsubset_{\emptyset,\emptyset} \rhd W_2$. Moreover, $(\rhd W_2, (\Phi_{f1r}, \mathrm{e}_2^*), (\Phi_{f2r}, \mathrm{e}_2^\dagger)) \in \mathcal{V}\llbracket \tau_1 \rrbracket$., because $\Phi_{f1r}, \Phi_{f2r} : W_2$ by Lemma 3.8, which implies $\Phi_{f1r}, \Phi_{f2r} : W_2$ and thus $W_2 \sqsubseteq_{\Phi_{f1r}, \Phi_{f2r}} \rhd W_2$. Ergo, there exist $\mathrm{e}_b^*, \mathrm{e}_b^\dagger$ such that

$$\mathrm{e}_1^* = \lambda \mathrm{a}.\mathrm{e}_b^*$$

and

$$\mathrm{e}_1^\dagger = \lambda \mathrm{a}.\mathrm{e}_b^\dagger$$

and, for any $(\ell_1, \ell_2) \notin \mathrm{dom}(\rhd W_2.\Psi) \cup \mathrm{dom}(\rhd W_2.\Theta)$,

$$((\rhd W_2.k, \rhd W_2.\Psi, \rhd W_2.\Theta \uplus (\ell_1, \ell_2) \mapsto (\Phi_{f1r}, \Phi_{f2r})),\\ (\emptyset, [\mathrm{a} \mapsto \mathrm{guard}(\mathrm{e}_2^*, \ell_2)]\mathrm{e}_b^*), (\emptyset, [\mathrm{a} \mapsto \mathrm{guard}(\mathrm{e}_2^\dagger, \ell_1)]\mathrm{e}_b^\dagger)) \in \mathcal{E}\llbracket \tau_2 \rrbracket.$$

Let $W_3 = (\rhd W_2.k, \rhd W_2.\Psi, \rhd W_2.\Theta \uplus (\ell_1, \ell_2) \mapsto (\Phi_{f1r}, \Phi_{f2r}))$.

Thus, the original configuration in H_1 steps as follows:

$$\begin{array}{l}
\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_{1l} \uplus \Phi_{1r} \mathrm{H}_1,\\
\quad \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e_1}^+)))\ (\mathrm{let\ x} = \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e_2}^+)))\ \mathrm{in\ thunk(x)}) \rangle \overset{*}{\dashrightarrow}\\
\langle \Phi_{r1} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{1r} \uplus \Phi_{g1l}, \mathrm{H}_1^*,\\
\quad \lambda \mathrm{a}.\mathrm{e}_b^*\ (\mathrm{let\ x} = \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e_2}^+)))\ \mathrm{in\ thunk(x)}) \rangle \overset{*}{\dashrightarrow}\\
\langle \Phi_{r1} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{g1l} \uplus \Phi_{f1r} \uplus \Phi_{g1r}, \mathrm{H}_1^{**}, \lambda \mathrm{a}.\mathrm{e}_b^*\ (\mathrm{let\ x} =\ \mathrm{e}_2^*\ \mathrm{in\ thunk(x)}) \rangle \dashrightarrow\\
\langle \Phi_{r1} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{g1l} \uplus \Phi_{f1r} \uplus \Phi_{g1r}, \mathrm{H}_1^{**}, \lambda \mathrm{a}.\mathrm{e}_b^*\ \mathrm{thunk}(\mathrm{e}_2^*) \rangle \overset{0}{\dashrightarrow}\\
\langle \Phi_{r1} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{g1l} \uplus \Phi_{f1r} \uplus \Phi_{g1r}, \mathrm{H}_1^{**},\\
\quad \lambda \mathrm{a}.\mathrm{e}_b^*\ \mathrm{let\ r_{fresh}} = \mathrm{ref\ 1\ in}\ \lambda\_.\{\mathrm{if}\ !\mathrm{r_{fresh}}\ \{\mathrm{fail\ C{\scriptsize ONV}}\}\ \{\mathrm{r_{fresh}} := \mathrm{{\scriptsize USED}}; \mathrm{e}_2^*\}\} \dashrightarrow\\
\langle \Phi_{r1} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{g1l} \uplus \Phi_{f1r} \uplus \Phi_{g1r}, \mathrm{H}_1^{**}[\ell_1 \rightarrow \mathrm{{\scriptsize UNUSED}}], \lambda \mathrm{a}.\mathrm{e}_b^*\ \lambda\_.\{\mathrm{if}\ !\ell_1\ \{\mathrm{fail\ C{\scriptsize ONV}}\}\ \{\ell_1 := \mathrm{{\scriptsize USED}}; \mathrm{e}_2^*\}\} \rangle\ \text{-}\\
\langle \Phi_{r1} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{g1l} \uplus \Phi_{f1r} \uplus \Phi_{g1r}, \mathrm{H}_1^{**}[\ell_1 \rightarrow \mathrm{{\scriptsize UNUSED}}], \lambda \mathrm{a}.\mathrm{e}_b^*\ \mathrm{guard}(\ell_1, \mathrm{e}_2^*) \rangle \dashrightarrow\\
\langle \Phi_{r1} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{g1l} \uplus \Phi_{f1r} \uplus \Phi_{g1r}, \mathrm{H}_1^{**}[\ell_1 \rightarrow \mathrm{{\scriptsize UNUSED}}], [\mathrm{a} \mapsto \mathrm{guard}(\ell_1, \mathrm{e}_2^*)]\mathrm{e}_b^* \rangle
\end{array}$$

for some $\ell_1 \notin \mathrm{H}_1^{**}$. Similarly, the original configuration in H_2 steps to

$$\langle \Phi_{r2} \uplus \Phi(W_2, 1) \uplus \Phi_{g2l} \uplus \Phi_{f2r} \uplus \Phi_{g2r}, \mathrm{H}_2^{**}[\ell_2 \longrightarrow 1], [\mathrm{a} \mapsto \mathrm{guard}(\ell_2, \mathrm{e}_2^{\dagger})]\mathrm{e}_\mathrm{b}^{\dagger}\rangle$$

for some $\ell_2 \notin \mathrm{H}_2^{**}$. Since $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : W_2$, this implies $(\ell_1, \ell_2) \notin \mathrm{dom}(W_2.\Psi) \cup \mathrm{dom}(W_2.\Theta)$, and thus $(\ell_1, \ell_2) \notin \mathrm{dom}(\triangleright W_2.\Psi) \cup \mathrm{dom}(\triangleright W_2.\Theta)$.

Therefore, by expanding the value relation for $\tau_1 \multimap \tau_2$, we find:

$$(W_3, (\emptyset, [\mathrm{a} \mapsto \mathrm{guard}(\ell_1, \mathrm{e}_2^{*})]\mathrm{e}_\mathrm{b}^{*}), (\emptyset, [\mathrm{a} \mapsto \mathrm{guard}(\ell_2, \mathrm{e}_2^{\dagger})]\mathrm{e}_\mathrm{b}^{\dagger})) \in \mathcal{E}[\![\tau_2]\!].$$

Moreover, since $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : W_2$, we also have $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : \triangleright W_2$. Therefore, $\mathrm{H}_1^{**}[\ell_1 \mapsto \textsc{unused}], \mathrm{H}_2^{**}[\ell_2 \mapsto \textsc{unused}] : W_3$, because the only difference between $\triangleright W_2$ and W_3 is that W_3 has a new affine flag $(\ell_1, \ell_2) \longrightarrow (\Phi_{f1l}, \Phi_{f1r})$, and both of the above heaps indeed have ℓ_1 and ℓ_2, respectively, set to UNUSED.

Finally, notice that, for all $i \in \{1, 2\}$, $\mathrm{flags}(W_3, i) = \mathrm{flags}(W_2, i) \uplus \Phi_{fir}$, because W_3 has the exact same dynamic flags as W_2, except for $(\ell_1, \ell_2) \mapsto (\Phi_{f1r}, \Phi_{f2r})$, which has the affect of adding Φ_{f1r} on the left side and Φ_{f2r} on ther right side. Thus, we can rewrite the above configurations as

$$\langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \Phi_{g1r} \uplus \mathrm{flags}(W_3, 1), \mathrm{H}_1^{**}[\ell_1 \longrightarrow \textsc{unused}], [\mathrm{a} \mapsto \mathrm{guard}(\ell_1, \mathrm{e}_2^{*})]\mathrm{e}_\mathrm{b}^{*}\rangle$$

$$\langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \Phi_{g2r} \uplus \mathrm{flags}(W_3, 1), \mathrm{H}_2^{**}[\ell_2 \longrightarrow \textsc{unused}], [\mathrm{a} \mapsto \mathrm{guard}(\ell_2, \mathrm{e}_2^{\dagger})]\mathrm{e}_\mathrm{b}^{\dagger}\rangle$$

Ergo, we can instantiate the fact that the above expressions are in $\mathcal{E}[\![\tau_2]\!]$. in the world W_3 to find that either the first configuration steps to fail CONV, in which case the original configuration with H_1 steps to fail CONV, or the first configuration steps to some irreducible configuration

$$\langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \Phi_{g1r} \uplus \mathrm{flags}(W_4, 1) \uplus \Phi_{f1n} \uplus \Phi_{g1n}, \mathrm{H}_1^{***}, \mathrm{e}_\mathrm{f}^{*}\rangle$$

in which case the second configuration steps to

$$\langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \Phi_{g2r} \uplus \mathrm{flags}(W_4, 2) \uplus \Phi_{f2n} \uplus \Phi_{g2n}, \mathrm{H}_2^{***}, \mathrm{e}_\mathrm{f}^{\dagger}\rangle$$

and there exists some W_4 such that $W_3 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{g1l} \uplus \Phi_{g1r}, \Phi_{r2} \uplus \Phi_{g2l} \uplus \Phi_{g2r}} W_4$, $\mathrm{H}_1^{***}, \mathrm{H}_2^{***} : W_4$, and $(W_4, (\Phi_{f1n}, \mathrm{e}_\mathrm{f}^{*}), (\Phi_{f2n}, \mathrm{e}_\mathrm{f}^{\dagger})) \in \mathcal{V}[\![\tau_2]\!]..$

This suffices to show that $\mathrm{e}_1' = \mathrm{e}^{***}$, so e_1' is indeed in the value relation at τ_2 along with the value stepped to by the original configuration on the right hand side. Ergo, since $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_1$, $W_1 \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_2$, $W_2 \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} \triangleright W_2$, $\triangleright W_2 \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_3$, and $W_3 \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_4$ (note that these are weaker statements of what we learned above, but hold – and in particular, via transitivity, will be what hold), it follows that $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_4$, which suffices to finish the proof. □

LEMMA 3.39 (COMPAT app $:\!-\!\!\bullet$).

$$\begin{gathered}\Delta_1; \Gamma_1; \Gamma; \Omega_1 \vdash \mathrm{e}_1 \preceq \mathrm{e}_1 : \tau_1 -\!\!\bullet\, \tau_2 \rightsquigarrow \Delta_2; \Gamma_2 \wedge \Delta_2; \Gamma_2; \Gamma; \Omega_2 \vdash \mathrm{e}_2 \preceq \mathrm{e}_2 : \tau_1 \rightsquigarrow \Delta_3; \Gamma_3 \\ \Longrightarrow \Delta_1; \Gamma_1; \Gamma; \Omega_1 \uplus \Omega_2 \vdash \mathrm{e}_1\ \mathrm{e}_2 \preceq \mathrm{e}_1\ \mathrm{e}_2 : \tau_2 \rightsquigarrow \Delta_3; \Gamma_3\end{gathered}$$

PROOF. Expanding the hypotheses, it is clear that $\Delta_1 = \Delta_2 = \Delta_3$ and $\Gamma_1 = \Gamma_2 = \Gamma_3$. Let $\Delta = \Delta_1$ and $\Gamma = \Gamma_1$.

Moreover, $\Delta_1; \Gamma_1; \Gamma; \Omega \vdash \mathrm{e}_1\ \mathrm{e}_2 : \tau_2 \rightsquigarrow \Delta_3; \Gamma_3$ by the application typing rule. Ergo, it suffices to show $\Delta; \Gamma; \Gamma; \Omega \vdash \mathrm{e}_1\ \mathrm{e}_2 \preceq \mathrm{e}_1\ \mathrm{e}_2 : \tau_2$.

Expanding the conclusion, given

$$\forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega.\rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!].\wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\Omega_1 \uplus \Omega_2]\!].$$

we must show

$$(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1\ \mathrm{e}_2{}^{+})))), (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1 \mathrm{e}_2{}^{+}))))) \in \mathcal{E}[\![\tau_2]\!].$$

By pushing the compiler and substitutions through the application, we can refine this to:

$$\begin{gathered}(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e_1}^+)))\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e_2}^+)))),\\ (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e_1}^+)))\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e_2}^+))))) \in \mathcal{E}[\![\tau_2]\!].\end{gathered}$$

Next, by Lemma 3.5, we have that $\gamma_\Omega = \gamma_1 \uplus \gamma_2$, $\Phi_1 = \Phi_{1l} \uplus \Phi_{1r}$, and $\Phi_2 = \Phi_{2l} \uplus \Phi_{2r}$ where

$$(W, \Phi_{1l}, \Phi_{2l}, \gamma_1) \in \mathcal{G}[\![\Omega]\!].$$

and

$$(W, \Phi_{1r}, \Phi_{2r}, \gamma_2) \in \mathcal{G}[\![\Omega]\!].$$

and for all $i \in \{1, 2\}$,

$$\mathrm{close}_i(\gamma_\Omega, \mathrm{e_1}^+) = \mathrm{close}_i(\gamma_1, \mathrm{e_1}^+)$$

and

$$\mathrm{close}_i(\gamma_\Omega, \mathrm{e_2}^+) = \mathrm{close}_i(\gamma_1, \mathrm{e_2}^+)$$

Thus, we can refine the statement we need to prove as:

$$\begin{gathered}(W, (\Phi_{1l} \uplus \Phi_{1r}, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e_1}^+)))\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e_2}^+)))),\\ (\Phi_{2l} \uplus \Phi_{2r}, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathrm{e_1}^+)))\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e_2}^+))))) \in \mathcal{E}[\![\tau_2]\!].\end{gathered}$$

Let $\mathrm{e_1}$ and $\mathrm{e_2}$ be the first and second expressions, respectively, in the tuple above. Expanding the definition of the expression relation, given:

$$\begin{gathered}\forall \Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}'_1,\ \mathrm{H}'_1,\ j < W.k.\\ \Phi_{r1}\#\Phi_{1l} \uplus \Phi_{1r} \wedge \Phi_{r2}\#\Phi_{2l} \uplus \Phi_{2r} \wedge \Phi_{r1} \uplus \Phi_{1l} \uplus \Phi_{1r}, \Phi_{r2} \uplus \Phi_{2l} \uplus \Phi_{2r} : W \wedge\\ \langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_{1l} \uplus \Phi_{1r}, \mathrm{H}_1, \mathrm{e}_1 \rangle \overset{j}{\dashrightarrow} \langle \Phi'_1, \mathrm{H}'_1, \mathrm{e}'_1 \rangle \not\twoheadrightarrow\end{gathered}$$

we must show that either e'_1 is fail Conv or there exist $\Phi_{f1}, \Phi_{g1}, \Phi_{f2}, \Phi_{g2}, \mathrm{v}_2, \mathrm{H}'_2, W'$ such that:

$$\begin{aligned}&\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_{2l} \uplus \Phi_{2r}, \mathrm{H}_2, \mathrm{e}_2 \rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathrm{H}'_2, \mathrm{v}_2 \rangle \not\twoheadrightarrow\\ &\wedge\ \Phi'_1 = \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge\\ &\wedge\ W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W' \wedge\ \mathrm{H}'_1, \mathrm{H}'_2 : W'\\ &\wedge\ (W', (\Phi_{f1}, \mathrm{e}'_1), (\Phi_{f2}, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho)\end{aligned}$$

By instantiating the first induction hypothesis with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_1, \rho$, we find that:

$$(W, (\Phi_{1l}, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e_1}^+)))), (\Phi_{1r}, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathrm{e_1}^+))))) \in \mathcal{E}[\![\tau_1 \multimap \tau_2]\!].$$

Thus,

$$\langle \Phi_{r1} \uplus \Phi_{1r} \uplus \mathrm{flags}(W, 1) \uplus \Phi_{1l}, \mathrm{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e_1}^+))) \rangle$$

either steps to fail Conv, in which case the whole expression steps to fail Conv, or steps to an irreducible configuration $\langle \Phi_{r1} \uplus \Phi_{1r} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{f1l} \uplus \Phi_{g1l}, \mathrm{H}^*_1, \mathrm{e}^*_1 \rangle$, in which case

$$\langle \Phi_{r1} \uplus \Phi_{2r} \uplus \mathrm{flags}(W, 2) \uplus \Phi_{2l}, \mathrm{H}_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathrm{e_1}^+))) \rangle$$

also steps to an irreducible configuration $\langle \Phi_{r1} \uplus \Phi_{2r} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{f2l} \uplus \Phi_{g2l}, \mathrm{H}^*_2, \mathrm{e}^*_2 \rangle$ and there exists some world W_1 where $W \sqsubseteq_{\Phi_{r1} \uplus \Phi_{1r}, \Phi_{r2} \uplus \Phi_{2r}} W_1$, $\mathrm{H}^*_1, \mathrm{H}^*_2 : W_1$, and $(W_1, (\Phi_{f1l}, \mathrm{e}^*_1), (\Phi_{f2l}, \mathrm{e}^*_2)) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!]$.. By expanding the value relation, there exist expressions $\mathrm{e}^*_{\mathrm{b1}}, \mathrm{e}^*_{\mathrm{b2}}$ such that $\mathrm{e}^*_1 = \lambda \mathrm{a}_\bullet.\mathrm{e}^*_{\mathrm{b1}}$ and $\mathrm{e}^*_2 = \lambda \mathrm{a}_\bullet.\mathrm{e}^*_{\mathrm{b2}}$.

Then, by the operational semantic, the original application expression continues reducing on the second subexpression. By instantiating the second induction hypothesis with $W_1, \gamma_\Gamma, \gamma_\Gamma, \gamma_2, \rho$, we find that:

$$(W_1, (\Phi_{2l}, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e_2}^+)))), (\Phi_{2r}, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e_2}^+))))) \in \mathcal{E}[\![\tau_1]\!].$$

Thus,

$$\langle \Phi_{r1} \uplus \Phi_{f1l} \uplus \Phi_{g1l} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{1r}, \mathrm{H}_1^*, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e_2}^+)))\rangle$$

either steps to fail Conv, in which case the whole expression steps to fail Conv, or steps to an irreducible configuration $\langle \Phi_{r1} \uplus \Phi_{f1l} \uplus \Phi_{g1l} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{f1r} \uplus \Phi_{g1r}, \mathrm{H}_1^\dagger, \mathrm{e}_1^\dagger\rangle$, in which case

$$\langle \Phi_{r2} \uplus \Phi_{f2l} \uplus \Phi_{g2l} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{2r}, \mathrm{H}_2^*, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e_2}^+)))\rangle$$

also steps to an irreducible configuration $\langle \Phi_{r2} \uplus \Phi_{f2l} \uplus \Phi_{g2l} \uplus \mathrm{flags}(W_2, 2) \uplus \Phi_{f2r} \uplus \Phi_{g2r}, \mathrm{H}_2^\dagger, \mathrm{e}_2^\dagger\rangle$ and there exists some world W_2 where $W_1 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{f1l} \uplus \Phi_{g1l}, \Phi_{r2} \uplus \Phi_{f2l}, \Phi_{g2l}} W_2$, $\mathrm{H}_1^\dagger, \mathrm{H}_2^\dagger : W_2$, and

$$(W_2, (\Phi_{f1r}, \mathrm{e}_1^\dagger), (\Phi_{f2r}, \mathrm{e}_2^\dagger)) \in \mathcal{V}[\![\tau_1]\!].$$

Thus, the original configuration with H_1 steps to

$$\langle \Phi_{r1} \uplus \Phi_{f1l} \uplus \Phi_{g1l} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{f1r} \uplus \Phi_{g1r}, \mathrm{H}_1^\dagger, \lambda \mathrm{a}_\bullet.\mathrm{e}_{\mathrm{b}1}^*\ \mathrm{e}_1^\dagger\rangle$$

which steps to

$$\langle \Phi_{r1} \uplus \Phi_{f1l} \uplus \Phi_{g1l} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{f1r} \uplus \Phi_{g1r} \uplus \{f_1\}, \mathrm{H}_1^\dagger, [\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{e}_1^\dagger, f_1)]\mathrm{e}_{\mathrm{b}1}^*\rangle$$

for some $f_1 \notin \Phi_{r1} \uplus \Phi_{f1l} \uplus \Phi_{g1l} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{f1r} \uplus \Phi_{g1r}$.

Similarly, the original configuration with H_2 steps to

$$\langle \Phi_{r2} \uplus \Phi_{f2l} \uplus \Phi_{g2l} \uplus \mathrm{flags}(W_2, 2) \uplus \Phi_{f2r} \uplus \Phi_{g2r} \uplus \{f_2\}, \mathrm{H}_2^\dagger, [\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{e}_2^\dagger, f_2)]\mathrm{e}_{\mathrm{b}2}^*\rangle$$

for some $f_2 \notin \Phi_{r2} \uplus \Phi_{f2l} \uplus \Phi_{g2l} \uplus \mathrm{flags}(W_2, 2) \uplus \Phi_{f2r} \uplus \Phi_{g2r}$.

We can instantiate the fact that $(W_1, (\Phi_{f1l}, \lambda \mathrm{a}_\bullet.\mathrm{e}_{\mathrm{b}1}^*), (\Phi_{f2l}, \lambda \mathrm{a}_\bullet.\mathrm{e}_{\mathrm{b}2}^*)) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!]$. with Φ_{f1r}, Φ_{f2r}, f_1, f_2, $\mathrm{e}_1^\dagger$, $\mathrm{e}_2^\dagger$, W_2 to find that:

$$(W_2, (\Phi_{f1l} \uplus \Phi_{f1r} \uplus \{f_1\}, [\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{e}_1^\dagger, f_1)]\mathrm{e}_{\mathrm{b}1}^*),$$
$$(\Phi_{f2l} \uplus \Phi_{f2r} \uplus \{f_2\}, [\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{e}_2^\dagger, f_2)]\mathrm{e}_{\mathrm{b}2}^*)) \in \mathcal{E}[\![\tau_2]\!].$$

Given $\mathrm{H}_1^\dagger, \mathrm{H}_2^\dagger : W_2$, it follows that

$$\langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \Phi_{g1r} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{f1l} \uplus \Phi_{f1r} \uplus \{f_1\}, \mathrm{H}_1^\dagger, [\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{e}_1^\dagger, f_1)]\mathrm{e}_{\mathrm{b}1}^*\rangle$$

either steps to fail Conv, in which case the original configuration with H_1 steps to fail Conv, or steps to an irreducible configuration

$$\langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \Phi_{g1r} \uplus \mathrm{flags}(W_3, 1) \uplus \Phi_{f1f} \uplus \Phi_{g1f}, \mathrm{H}_1^{**}, \mathrm{e}_1^{**}\rangle$$

in which case the configuration

$$\langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \Phi_{g2r} \uplus \mathrm{flags}(W_2, 2) \uplus \Phi_{f2l} \uplus \Phi_{f2r} \uplus \{f_2\}, \mathrm{H}_2^\dagger, [\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{e}_2^\dagger, f_2)]\mathrm{e}_{\mathrm{b}2}^*\rangle$$

also steps to an irreducible configuration

$$\langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \Phi_{g2r} \uplus \mathrm{flags}(W_3, 2) \uplus \Phi_{f2f} \uplus \Phi_{g2f}, \mathrm{H}_2^{**}, \mathrm{e}_2^{**}\rangle$$

and there exists a world W_3 such that $W_2 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{g1l} \uplus \Phi_{g1r}, \Phi_{r2} \uplus \Phi_{g2l} \uplus \Phi_{g2r}} W_3$, $\mathrm{H}_1^{**}, \mathrm{H}_2^{**} : W_3$, and $(W_3, (\Phi_{f1f}, \mathrm{e}_1^{**}), (\Phi_{f2f}, \mathrm{e}_2^{**})) \in \mathcal{V}[\![\tau_2]\!]$.. Finally, since $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_1$, $W_1 \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_2$, and $W_2 \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_3$, it follows that $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_3$, which suffices to finish the proof. □

Lemma 3.40 (Compat !).

$$\Delta; \Gamma; \Gamma; \cdot \vdash \mathrm{v} : \tau \rightsquigarrow \Delta'; \Gamma' \implies \Delta; \Gamma; \Gamma; \cdot \vdash !\mathrm{v} : !\tau \rightsquigarrow \Delta'; \Gamma'$$

Proof. Expanding the hypotheses, we find $\Delta_1 = \Delta'$ and $\Gamma = \Gamma'$. Moreover, $\Delta; \Gamma; \Gamma; \cdot \vdash \mathtt{!v} : \mathtt{!}\tau \rightsquigarrow \Delta'; \Gamma'$ by the $\mathtt{!}$ typing rule. Ergo, it suffices to show $\Delta; \Gamma; \Gamma; \cdot \vdash \mathtt{!v} \preceq \mathtt{!v} : \mathtt{!}\tau$.

Expanding the conclusion, given

$$\forall W. \forall \rho\ \gamma_\Gamma\ \gamma_\Gamma\ \gamma_\Omega. \rho \in \mathcal{D}[\![\Delta]\!] \land (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \land (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\cdot \land (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\cdot]\!]_\cdot$$

we must show

$$(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathtt{!v}^+)))), (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathtt{!v}^+))))) \in \mathcal{E}[\![\mathtt{!}\tau]\!]_\cdot$$

Notice that both of these expressions have no free variables by Lemma 3.16. Moreover, since $(W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\cdot]\!]_\cdot$, we have $\Phi_1 = \Phi_2 = \emptyset$ and $\gamma_\Omega = \cdot$. Furthermore, $\mathtt{!v}^+ = \mathtt{v}^+$. Thus, we can refine the above to:

$$(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathtt{v}^+))), (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathtt{v}^+)))) \in \mathcal{E}[\![\mathtt{!}\tau]\!]_\cdot$$

Let $\mathtt{e}_1$ and $\mathtt{e}_2$ be the first and second expressions, respectively, in the above tuple. Expanding the definition of the expression relation, given:

$$\begin{gathered}\forall \Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathtt{e}_1',\ \mathrm{H}_1',\ j < W.k. \\ \Phi_{r1} \# \emptyset \land \Phi_{r2} \# \emptyset \land \Phi_{r1} \uplus \emptyset, \Phi_{r2} \uplus \emptyset : W \land \\ \langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \emptyset, \mathrm{H}_1, \mathtt{e}_1 \rangle \overset{j}{\dashrightarrow} \langle \Phi_1', \mathrm{H}_1', \mathtt{e}_1' \rangle \nrightarrow\end{gathered}$$

we must show that either $\mathtt{e}_1'$ is fail Conv or there exist $\Phi_{f1}, \Phi_{g1}, \Phi_{f2}, \Phi_{g2}, \mathtt{v}_2, \mathrm{H}_2', W'$ such that:

$$\begin{aligned}&\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \emptyset, \mathrm{H}_2, \mathtt{e}_2 \rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathrm{H}_2', \mathtt{v}_2 \rangle \nrightarrow \\ &\land \Phi_1' = \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \land \\ &\land W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W' \land \mathrm{H}_1', \mathrm{H}_2' : W' \\ &\land (W', (\Phi_{f1}, \mathtt{e}_1'), (\Phi_{f2}, \mathtt{v}_2)) \in \mathcal{V}[\![\mathtt{!}\tau]\!]_\rho)\end{aligned}$$

Next, consider $W_1 = (W.k, W.\Psi, \Theta')$, where $\mathrm{dom}(\Theta') = \mathrm{dom}(W.\Theta)$ and for all $(\ell_1, \ell_2) \in \mathrm{dom}(W.\Theta)$, $\Theta'(\ell_1, \ell_2) = \textsc{used}$. Thus, since all dynamic flags in W_1 have been used $\mathrm{flags}(W_1, 1) = \mathrm{flags}(W_1, 2) = \emptyset$, so we trivially have $\Phi_{r1}, \Phi_{r2} : W_1$. It then follows that $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_1$ because W and W_1 have the exact same heap typing and all of the locations in W have been switched to $\textsc{used}$ in W_1.

Thus, by Lemma 3.8, we have $(W_1, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho$ and $(W_1, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\cdot$. We also trivially have $(W_1, \emptyset, \emptyset, \cdot) \in \mathcal{G}[\![\cdot]\!]_\cdot$. Thus, by instantiating the first induction hypothesis with $W_1, \gamma_\Gamma, \gamma_\Gamma, \cdot, \rho$, we find:

$$(W_1, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathtt{v}^+))), (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathtt{v}^+)))) \in \mathcal{E}[\![\tau]\!]_\cdot$$

Thus, since $\mathrm{flags}(W_1, 1) = \mathrm{flags}(W_1, 2) = \emptyset$, the configuration

$$\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \emptyset \uplus \emptyset, \mathrm{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathtt{v}^+)) \rangle$$

must either step to fail Conv, in which case the proof is done, or steps to some irreducible configuration $\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \emptyset \uplus \Phi_{f1} \uplus \Phi_{g1}, \mathrm{H}_1^*, \mathtt{e}_1^* \rangle$, in which case the configuration

$$\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \emptyset \uplus \emptyset, \mathrm{H}_2, (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathtt{v}^+))) \rangle$$

steps to an irreducible configuration $\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \emptyset \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathrm{H}_1^*, \mathtt{e}_2^* \rangle$, and there exists some world W_2 such that $W_1 \sqsubseteq_{\Phi_{r1} \uplus \mathrm{flags}(W,1), \Phi_{r2} \uplus \mathrm{flags}(W,2)} W_2, \mathrm{H}_1^*, \mathrm{H}_2^* : W_2$, and $(W_2, (\Phi_{f1}, \mathtt{e}_1^*), (\Phi_{f2}, \mathtt{e}_2^*)) \in \mathcal{V}[\![\tau]\!]_\cdot$.

However, from Lemma 3.4, we know both the original configurations above are indeed irreducible and do not step. This means the set of static flags in the original configurations equal that in the final configurations. Thus,

$$\Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \emptyset \uplus \emptyset = \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \emptyset \uplus \Phi_{f1} \uplus \Phi_{g1}$$

and

$$\Phi_{r2} \uplus \text{flags}(W, 2) \uplus \emptyset \uplus \emptyset = \Phi_{r2} \uplus \text{flags}(W, 2) \uplus \emptyset \uplus \Phi_{f2} \uplus \Phi_{g2}$$

This implies $\Phi_{f1} = \Phi_{g1} = \emptyset$ and $\Phi_{f2} = \Phi_{g2} = \emptyset$. Ergo, $(W_2, (\emptyset, e_1^*), (\emptyset, e_2^*)) \in \mathcal{V}[\![\tau]\!]$., from which it follows that $(W_2, (\emptyset, e_1^*), (\emptyset, e_2^*)) \in \mathcal{V}[\![!\tau]\!]$..

Finally, since $W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W_1$ and $W_1 \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W_2$, we have $W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W_2$, which suffices to finish the proof. □

Lemma 3.41 (Compat let!).

$$\begin{aligned} &\Delta_1;\Gamma_1;\Gamma;\Omega_1 \vdash e_1 \preceq e_1 : !\tau \rightsquigarrow \Delta_2;\Gamma_2 \wedge \Delta_2;\Gamma_2;\Gamma, x : \tau;\Omega_2 \vdash e_2 \preceq e_2 : \tau' \rightsquigarrow \Delta_3;\Gamma_3 \\ &\implies \Delta_1;\Gamma_1;\Gamma;\Omega_1 \uplus \Omega_2 \vdash \text{let } !x = e_1 \text{ in } e_2 \preceq \text{let } !x = e_1 \text{ in } e_2 : \tau' \rightsquigarrow \Delta_3;\Gamma_3 \end{aligned}$$

Proof. Expanding the hypotheses, we find $\Delta_1 = \Delta_2 = \Delta_3$ and $\Gamma_1 = \Gamma_2 = \Gamma_3$. Moreover, $\Delta_1;\Gamma_1;\Gamma;\Omega_1 \uplus \Omega_2 \vdash \text{let } !x = e_1 \text{ in } e_2 : \tau' \rightsquigarrow \Delta_3;\Gamma_3$ by the let! typing rule. Thus, it suffices to show $\Delta_1;\Gamma_1;\Gamma;\Omega_1 \uplus \Omega_2 \vdash \text{let } !x = e_1 \text{ in } e_2 \preceq \text{let } !x = e_1 \text{ in } e_2 : \tau'$.

Expanding the conclusion, given

$$\forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega.\rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!].\wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\Omega_1 \uplus \Omega_2]\!].$$

we must show

$$\begin{gathered} (W, (\Phi_1, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Omega, \text{let } !x = e_1 \text{ in } {e_2}^{+})))), \\ (\Phi_2, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Omega, \text{let } !x = e_1 \text{ in } {e_2}^{+}))))) \in \mathcal{E}[\![\tau']\!]. \end{gathered}$$

Notice that both of these expressions have no free variables by Lemma 3.16.

We can push the compiler and substitutions through the let expression and refine this to:

$$\begin{gathered} (W, (\Phi_1, \text{let } x = \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Omega, {e_1}^{+}))) \text{ in } \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Omega, {e_2}^{+})))), \\ (\Phi_2, \text{let } x = \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Omega, {e_1}^{+}))) \text{ in } \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Omega, {e_2}^{+}))))) \in \mathcal{E}[\![\tau']\!]. \end{gathered}$$

Next, by Lemma 3.5, we have that $\gamma_\Omega = \gamma_1 \uplus \gamma_2$, $\Phi_1 = \Phi_{1l} \uplus \Phi_{1r}$, and $\Phi_2 = \Phi_{2l} \uplus \Phi_{2r}$ where

$$(W, \Phi_{1l}, \Phi_{2l}, \gamma_1) \in \mathcal{G}[\![\Omega_1]\!].$$

and

$$(W, \Phi_{1r}, \Phi_{2r}, \gamma_2) \in \mathcal{G}[\![\Omega_2]\!].$$

and for all $i \in \{1, 2\}$,

$$\text{close}_i(\gamma_\Omega, {e_1}^{+}) = \text{close}_i(\gamma_1, {e_1}^{+})$$

and

$$\text{close}_i(\gamma_\Omega, {e_2}^{+}) = \text{close}_i(\gamma_1, {e_2}^{+})$$

Thus, we must show

$$\begin{gathered} (W, (\Phi_{1l} \uplus \Phi_{1r}, \text{let } x = \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_1, {e_1}^{+}))) \text{ in } \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_2, {e_2}^{+})))), \\ (\Phi_{2l} \uplus \Phi_{2r}, \text{let } x = \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_1, {e_1}^{+}))) \text{ in } \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_2, {e_2}^{+}))))) \in \mathcal{E}[\![\tau']\!]. \end{gathered}$$

Let e_1 and e_2 be the first and second expressions, respectively, in the above tuple. Expanding the definition of the expression relation, given:

$$\begin{gathered} \forall \Phi_{r1}, \Phi_{r2}, H_1, H_2{:}W,\ e_1',\ H_1',\ j < W.k. \\ \Phi_{r1} \# \Phi_{1l} \uplus \Phi_{1r} \wedge \Phi_{r2} \# \Phi_{2l} \uplus \Phi_{2r} \wedge \Phi_{r1} \uplus \Phi_{1l} \uplus \Phi_{1r}, \Phi_{r2} \uplus \Phi_{2l} \uplus \Phi_{2r} : W \wedge \\ \langle \Phi_{r1} \uplus \text{flags}(W, 1) \uplus \Phi_{1l} \uplus \Phi_{1r}, H_1, e_1 \rangle \overset{j}{\dashrightarrow} \langle \Phi_1', H_1', e_1' \rangle \nrightarrow \end{gathered}$$

we must show that either e_1' is fail Conv or there exist $\Phi_{f1}, \Phi_{g1}, \Phi_{f2}, \Phi_{g2}, v_2, H_2', W'$ such that:

$$\begin{aligned} &\langle \Phi_{r2} \uplus \text{flags}(W, 2) \uplus \Phi_{2l} \uplus \Phi_{2r}, H_2, e_2 \rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \text{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, H_2', v_2 \rangle \nrightarrow \\ &\wedge \Phi_1' = \Phi_{r1} \uplus \text{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge \\ &\wedge\ W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W' \wedge\ H_1', H_2' : W' \\ &\wedge (W', (\Phi_{f1}, e_1'), (\Phi_{f2}, v_2)) \in \mathcal{V}[\![\tau]\!]_\rho) \end{aligned}$$

Next, we need to find e'_1. From the operational semantic, the application will run the first subexpression using the heap H_1 until it reaches a target value or gets stuck. By appealing to our first induction hypothesis, instantiated with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_1, \rho$, we find that:

$(W, (\Phi_{1l}, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, e_1{}^+)))), (\Phi_{1r}, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, e_1{}^+))))) \in \mathcal{E}\llbracket !\tau \rrbracket$.

Therefore, the configuration

$$\langle \Phi_{r1} \uplus \Phi_{1r} \uplus \mathrm{flags}(W, 1) \uplus \Phi_{1l}, H_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, e_1{}^+))) \rangle$$

either reduces to fail Conv, in which case the original expression steps to fail Conv, or to some irreducible configuration $\langle \Phi_{r1} \uplus \Phi_{1r} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{f1l} \uplus \Phi_{g1l}, H_1^*, e_1^* \rangle$, in which case the configuration

$$\langle \Phi_{r2} \uplus \Phi_{2r} \uplus \mathrm{flags}(W, 2) \uplus \Phi_{2l}, H_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, e_1{}^+))) \rangle$$

also reduces to some irreducible configuration $\langle \Phi_{r2} \uplus \Phi_{2r} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{f2l} \uplus \Phi_{g2l}, H_2^*, e_1^\dagger \rangle$ and there exists some W_1 where $W \sqsubseteq_{\Phi_{r1} \uplus \Phi_{1r}, \Phi_{r2} \uplus \Phi_{2r}} W_1$, $H_1^*, H_2^* : W_1$, and $(W_1, (\Phi_{f1l}, e_1^*), (\Phi_{f1r}, e_1^\dagger)) \in \mathcal{V}\llbracket !\tau \rrbracket$.. By expanding the value relation definition, we find $\Phi_{f1l} = \Phi_{f1r} = \emptyset$ and $(W_1, (\emptyset, e_1^*), (\emptyset, e_1^\dagger)) \in \mathcal{V}\llbracket \tau \rrbracket$..

Since terms in the value relation are target values, the original configuration with H_1 steps as follows:

$$\begin{aligned}
&\left\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_{1l} \uplus \Phi_{1r}, H_1, \begin{array}{l} \mathrm{let}\ x = \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, e_1{}^+)))\ \mathrm{in} \\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, e_2{}^+))) \end{array} \right\rangle \xrightarrow{*} \\
&\langle \Phi_{r1} \uplus \Phi_{1r} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{g1l}, H_1^*, \mathrm{let}\ x = \ e_1^*\ \mathrm{in}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, e_2{}^+))) \rangle \longrightarrow \\
&\langle \Phi_{r1} \uplus \Phi_{1r} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{g1l}, H_1^*, [x \mapsto e_1^*]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, e_2{}^+))) \rangle
\end{aligned}$$

and similarly, the original configuration with H_2 steps to:

$$\langle \Phi_{r2} \uplus \Phi_{2r} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{g2l}, H_2^*, [x \mapsto e_1^\dagger]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, e_2{}^+))) \rangle$$

Next, notice that $(W_1, \emptyset, \emptyset, \gamma_\Gamma[x \mapsto (e_1^*, e_1^\dagger)]) \in \mathcal{G}\llbracket \Gamma, x : \tau \rrbracket$. because $(W_1, (\emptyset, e_1^*), (\emptyset, e_1^\dagger)) \in \mathcal{V}\llbracket \tau \rrbracket$. and $(W_1, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket$. (which follows from Lemma 3.8 because $W \sqsubseteq_{\emptyset,\emptyset} W_1$ and $(W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket$.). Therefore, by instantiating the second induction hypothesis with $W_1, \gamma_\Gamma, \gamma_\Gamma[x \mapsto (e_1^*, e_1^\dagger)], \gamma_2, \rho$, we find that

$$\begin{gathered}
(W_1, (\Phi_{1r}, [x \mapsto e_1^*]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, e_2{}^+)))), \\
(\Phi_{2r}, [x \mapsto e_1^\dagger]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, e_2{}^+))))) \in \mathcal{E}\llbracket \tau' \rrbracket.
\end{gathered}$$

Then, since $H_1^*, H_2^* : W_1$, we can instantiate the above fact with H_1^* and H_2^*. Ergo, the configuration

$$\langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{1r}, H_1^*, [x \mapsto e_1^*]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, e_2{}^+))) \rangle$$

must either step to fail Conv, in which case the original expression steps to fail Conv, or it must step to some $\langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{f1r} \uplus \Phi_{g1r}, H_1^\dagger, e_1^{**} \rangle$, in which case the configuration on the other side

$$\langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{2r}, H_2^*, [x \mapsto e_1^\dagger]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, e_2{}^+)))\rangle)$$

must step to $\langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \mathrm{flags}(W_2, 2) \uplus \Phi_{f2r} \uplus \Phi_{g2r}, H_2^\dagger, e_1^{\dagger\dagger} \rangle$ for some heap $H_2^\dagger$ and world W_2 where $W_1 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{g1l}, \Phi_{r2} \uplus \Phi_{g2l}} W_2$, $H_1^\dagger, H_2^\dagger : W_2$, and $(W_2, (\Phi_{f2r}, e_1^{**}), (\Phi_{f2r}, e_1^{\dagger\dagger})) \in \mathcal{V}\llbracket \tau' \rrbracket$.. Finally, since $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_1$ and $W_1 \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_2$, we have $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_2$, which suffices to finish the proof. □

Lemma 3.42 (Compat &).

$$\begin{gathered}
\Delta_1; \Gamma_1; \Gamma; \Omega \vdash e_1 \preceq e_1 : \tau_1 \rightsquigarrow \Delta_2; \Gamma_2 \wedge \Delta_2; \Gamma_2; \Gamma; \Omega \vdash e_2 \preceq e_2 : \tau_2 \rightsquigarrow \Delta_3; \Gamma_3 \\
\implies \Delta_1; \Gamma_1; \Gamma; \Omega \vdash \langle e_1, e_2 \rangle \preceq \langle e_1, e_2 \rangle : \tau_1 \& \tau_2 \rightsquigarrow \Delta_3; \Gamma_3
\end{gathered}$$

Proof. Expanding the hypotheses, we find $\Delta_1 = \Delta_2 = \Delta_3$ and $\Gamma_1 = \Gamma_2 = \Gamma_3$. Moreover, $\Delta_1;\Gamma_1;\Gamma;\Omega \vdash \langle \mathrm{e}_1, \mathrm{e}_2\rangle : \tau_1 \& \tau_2 \rightsquigarrow \Delta_3;\Gamma_3$ by the product typing rule. Ergo, it suffices to show $\Delta_1;\Gamma_1;\Gamma;\Omega \vdash \langle \mathrm{e}_1, \mathrm{e}_2\rangle \preceq \langle \mathrm{e}_1, \mathrm{e}_2\rangle : \tau'$.

Expanding the conclusion, given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega . \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_{.} \wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!]_{.}$$

we must show

$$\begin{gathered}(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \langle \mathrm{e}_1, \mathrm{e}_2\rangle^+)))),\\ (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \langle \mathrm{e}_1, \mathrm{e}_2\rangle^+))))) \in \mathcal{E}[\![\tau_1 \& \tau_2]\!]_{.}\end{gathered}$$

Note that both of these expressions are closed by Lemma 3.16.

We can push the compiler and substitutions through the product expression and refine this to:

$$\begin{gathered}(W, (\Phi_1, (\lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+))), \lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^+))))),\\ (\Phi_2, (\lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1{}^+))), \lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^+)))))) \in \mathcal{E}[\![\tau_1 \& \tau_2]\!]_{.}\end{gathered}$$

Since $\mathcal{V}[\![\tau_1 \& \tau_2]\!]_{.} \subseteq \mathcal{E}[\![\tau_1 \& \tau_2]\!]_{.}$ by Lemma 3.1, it suffices to show

$$\begin{gathered}(W, (\Phi_1, (\lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+))), \lambda\_.\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^+))))),\\ (\Phi_2, (\lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1{}^+))), \lambda\_.\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^+)))))) \in \mathcal{V}[\![\tau_1 \& \tau_2]\!]_{.}\end{gathered}$$

First, we can instantiate the first induction hypothesis with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$ to show that

$$(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_1{}^+)))), (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_1{}^+))))) \in \mathcal{V}[\![\tau_1]\!]_{.}$$

and we can instantiate the second induction hypothesis with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$ to show that

$$(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}_2{}^+)))), (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}_2{}^+))))) \in \mathcal{V}[\![\tau_2]\!]_{.}$$

This suffices to show that the pairs of lambdas are in the value relation at $\tau_1 \& \tau_2$, as was to be proven. □

Lemma 3.43 (Compat .1).

$$\Delta;\Gamma;\Gamma;\Omega \vdash \mathrm{e} \preceq \mathrm{e} : \tau_1 \& \tau_2 \rightsquigarrow \Delta';\Gamma' \implies \Delta;\Gamma;\Gamma;\Omega \vdash \mathrm{e}.1 \preceq \mathrm{e}.1 : \tau_1 \rightsquigarrow \Delta';\Gamma'$$

Proof. Expanding the hypotheses, we find $\Delta_1 = \Delta'$ and $\Gamma = \Gamma'$. Moreover, $\Delta;\Gamma;\Gamma;\Omega \vdash \mathrm{e}.1 : \tau_1 \rightsquigarrow \Delta';\Gamma'$ by the .1 typing rule. Ergo, it suffices to show $\Delta;\Gamma;\Gamma;\Omega \vdash \mathrm{e}.1 \preceq \mathrm{e}.1 : \tau_1$.

Expanding the conclusion, given

$$\forall W. \forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega . \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_{.} \wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\Omega]\!]_{.}$$

we must show

$$(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}.1^+)))), (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}.1^+))))) \in \mathcal{E}[\![\tau_1]\!]_{.}$$

Notice that both of these expressions have no free variables by Lemma 3.16.

We can push the compiler and substitutions through the projection to refine this to:

$$\begin{gathered}(W, (\Phi_1, (\mathrm{fst}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathrm{e}^+))))\ ()),\\ (\Phi_2, (\mathrm{fst}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathrm{e}^+))))\ ())) \in \mathcal{E}[\![\tau_1]\!]_{.}\end{gathered}$$

Expanding the definition of the expression relation, given:

$$\begin{gathered}\forall \Phi_{r1}, \Phi_{r2}, \mathrm{H}_1, \mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k.\\ \Phi_{r1} \# \Phi_1 \wedge \Phi_{r2} \# \Phi_2 \wedge \Phi_{r1} \uplus \Phi_1, \Phi_{r2} \uplus \Phi_2 : W \wedge\\ \langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_1, \mathrm{H}_1, \mathrm{e}_1\rangle \overset{j}{\dashrightarrow} \langle \Phi_1', \mathrm{H}_1', \mathrm{e}_1'\rangle \nrightarrow\end{gathered}$$

we must show that either e_1' is fail Conv or there exist $\Phi_{f1}, \Phi_{g1}, \Phi_{f2}, \Phi_{g2}, v_2, H_2', W'$ such that:

$$\begin{array}{l} \langle \Phi_{r2} \uplus \text{flags}(W,2) \uplus \Phi_2, H_2, e_2\rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \text{flags}(W',2) \uplus \Phi_{f2} \uplus \Phi_{g2}, H_2', v_2\rangle \not\twoheadrightarrow \\ \wedge\ \Phi_1' = \Phi_{r1} \uplus \text{flags}(W',1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge \\ \wedge\ W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W' \wedge\ H_1', H_2' : W' \\ \wedge\ (W', (\Phi_{f1}, e_1'), (\Phi_{f2}, v_2)) \in \mathcal{V}[\![\tau]\!]_\rho) \end{array}$$

To proceed, we must find out what e_1' is. First, by instantiating the first induction hypothesis with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_\Omega, \rho$, we find $(W, (\Phi_1, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Omega, e^+)))), (\Phi_2, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Omega, e^+))))) \in \mathcal{E}[\![\tau_1 \& \tau_2]\!]$. Therefore, the configuration

$$\langle \Phi_{r1} \uplus \text{flags}(W,1) \uplus \Phi_1, H_1, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Omega, e^+)))\rangle$$

either steps to fail Conv, in which case the original expression steps to fail Conv, or steps to some irreducible configuration $\langle \Phi_{r1} \uplus \text{flags}(W_1,1) \uplus \Phi_{f1} \uplus \Phi_{g1}, H_1^*, e^*\rangle$, in which case the configuration

$$\langle \Phi_{r2} \uplus \text{flags}(W,2) \uplus \Phi_2, H_2, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Gamma, \text{close}_2(\gamma_\Omega, e^+)))\rangle$$

also steps to some irreducible configuration $\langle \Phi_{r2} \uplus \text{flags}(W_1,2) \uplus \Phi_{f2} \uplus \Phi_{g2}, H_2^*, e^\dagger\rangle$ and there exists some world W_1 where $W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W_1$, $H_1^*, H_2^* : W_1$, and $(W_1, (\Phi_{f1}, e^*), (\Phi_{f2}, e^\dagger)) \in \mathcal{V}[\![\tau_1 \& \tau_2]\!]$..

Ergo, there exists some $e_1^*, e_1^\dagger, e_2^*, e_2^\dagger$ such that

$$e^* = (\lambda\_.e_1^*, \lambda\_.e_2^*)$$

and

$$e^\dagger = (\lambda\_.e_1^\dagger, \lambda\_.e_2^\dagger)$$

and

$$(W_1, (\Phi_{f1}, e_1^*), (\Phi_{f2}, e_1^\dagger)) \in \mathcal{E}[\![\tau_1]\!].$$

and

$$(W_1, (\Phi_{f1}, e_2^*), (\Phi_{f2}, e_2^\dagger)) \in \mathcal{E}[\![\tau_2]\!].$$

Thus, the original configuration with H_1 steps as follows:

$$\begin{array}{l} \langle \Phi_{r1} \uplus \text{flags}(W,1) \uplus \Phi_1, H_1, (\text{fst close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Gamma, \text{close}_1(\gamma_\Omega, e^+))))\ ()\rangle \xrightarrow{*} \\ \langle \Phi_{r1} \uplus \text{flags}(W_1,1) \uplus \Phi_{f1} \uplus \Phi_{g1}, H_1^*, (\text{fst } (\lambda\_.e_1^*, \lambda\_.e_2^*))\ ()\rangle \rightarrow \\ \langle \Phi_{r1} \uplus \text{flags}(W_1,1) \uplus \Phi_{f1} \uplus \Phi_{g1}, H_1^*, \lambda\_.e_1^*\ ()\rangle \rightarrow \\ \langle \Phi_{r1} \uplus \text{flags}(W_1,1) \uplus \Phi_{f1} \uplus \Phi_{g1}, H_1^*, e_1^*\rangle \end{array}$$

and on the other side, the original configuration with H_2 steps to:

$$\langle \Phi_{r2} \uplus \text{flags}(W_1,2) \uplus \Phi_{f2} \uplus \Phi_{g2}, H_2^*, e_1^\dagger\rangle$$

Then, since $(W_1, (\Phi_{f1}, e_1^*), (\Phi_{f2}, e_1^\dagger)) \in \mathcal{E}[\![\tau_1]\!]$., we find that the first configuration either steps to fail Conv, in which case the original expression steps to fail Conv, or steps to some irreducible

$$\langle \Phi_{r1} \uplus \Phi_{g1} \uplus \text{flags}(W_2,1) \uplus \Phi_{f1}' \uplus \Phi_{g1}', H_1^\dagger, e_1^{**}\rangle$$

in which case the second configuration also steps to an irreducible

$$\langle \Phi_{r2} \uplus \Phi_{g2} \uplus \text{flags}(W_2,2) \uplus \Phi_{f2}' \uplus \Phi_{g2}', H_2^\dagger, e_1^{\dagger\dagger}\rangle$$

and there exists some world W_2 where $W_1 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{g1}, \Phi_{r2} \uplus \Phi_{g2}} W_2$, $H_1^\dagger, H_2^\dagger : W_2$, and $(W_1, (\Phi_{f1}, e_1^{**}), (\Phi_{f2}, e_1^{\dagger\dagger})) \in \mathcal{V}[\![\tau_1]\!]$.. Fianlly, since $W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W_1$ and $W_1 \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W_2$, it follows that $W_1 \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W_2$, which suffices to finish the proof. □

Lemma 3.44 (Compat .2).

$$\Delta;\Gamma;\Gamma;\Omega \vdash \mathrm{e} \preceq \mathrm{e} : \tau_1 \& \tau_2 \rightsquigarrow \Delta';\Gamma' \implies \Delta;\Gamma;\Gamma;\Omega \vdash \mathrm{e}.2 \preceq \mathrm{e}.2 : \tau_2 \rightsquigarrow \Delta';\Gamma'$$

Proof. This proof is essentially identical to that of .1. □

Lemma 3.45 (Compat ⊗).

$$\begin{gathered}\Delta_1;\Gamma_1;\Gamma;\Omega_1 \vdash \mathrm{e}_1 \preceq \mathrm{e}_1 : \tau_1 \rightsquigarrow \Delta_2;\Gamma_2 \wedge \Delta_2;\Gamma_2;\Gamma;\Omega_2 \vdash \mathrm{e}_2 \preceq \mathrm{e}_2 : \tau_2 \rightsquigarrow \Delta_3;\Gamma_3 \\ \implies \Delta_1;\Gamma_1;\Gamma;\Omega_1 \uplus \Omega_2 \vdash (\mathrm{e}_1,\mathrm{e}_2) \preceq (\mathrm{e}_1,\mathrm{e}_2) : \tau_1 \otimes \tau_2 \rightsquigarrow \Delta_3;\Gamma_3\end{gathered}$$

Proof. Expanding the hypotheses, we find $\Delta_1 = \Delta_2 = \Delta_3$ and $\Gamma_1 = \Gamma_2 = \Gamma_3$. Moreover, $\Delta_1;\Gamma_1;\Gamma;\Omega_1 \uplus \Omega_2 \vdash (\mathrm{e}_1,\mathrm{e}_2) : \tau_1 \otimes \tau_2 \rightsquigarrow \Delta_3;\Gamma_3$ by the pair typing rule. Ergo, it suffices to show $\Delta_1;\Gamma_1;\Gamma;\Omega_1 \uplus \Omega_2 \vdash (\mathrm{e}_1,\mathrm{e}_2) \preceq (\mathrm{e}_1,\mathrm{e}_2) : \tau_1 \otimes \tau_2$.

Expanding the conclusion, given

$$\forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega.\rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W,\emptyset,\emptyset,\gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W,\emptyset,\emptyset,\gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket.\wedge(W,\Phi_1,\Phi_2,\gamma_\Omega) \in \mathcal{G}\llbracket\Omega_1 \uplus \Omega_2\rrbracket.$$

we must show

$$\begin{gathered}(W,(\Phi_1,\mathrm{close}_1(\gamma_\Gamma,\mathrm{close}_1(\gamma_\Gamma,\mathrm{close}_1(\gamma_\Omega,(\mathrm{e}_1,\mathrm{e}_2)^+)))), \\ (\Phi_2,\mathrm{close}_2(\gamma_\Gamma,\mathrm{close}_2(\gamma_\Gamma,\mathrm{close}_2(\gamma_\Omega,(\mathrm{e}_1,\mathrm{e}_2)^+))))) \in \mathcal{E}\llbracket\tau_1 \otimes \tau_2\rrbracket.\end{gathered}$$

Notice that both of these expressions have no free variables by Lemma 3.16.

We can push the compiler and substitutions through the product expression and refine this to:

$$\begin{gathered}(W,(\Phi_1,(\mathrm{close}_1(\gamma_\Gamma,\mathrm{close}_1(\gamma_\Gamma,\mathrm{close}_1(\gamma_\Omega,\mathrm{e}_1{}^+))),\mathrm{close}_1(\gamma_\Gamma,\mathrm{close}_1(\gamma_\Gamma,\mathrm{close}_1(\gamma_\Omega,\mathrm{e}_2{}^+))))), \\ (\Phi_2,(\mathrm{close}_2(\gamma_\Gamma,\mathrm{close}_2(\gamma_\Gamma,\mathrm{close}_2(\gamma_\Omega,\mathrm{e}_1{}^+))),\mathrm{close}_2(\gamma_\Gamma,\mathrm{close}_2(\gamma_\Gamma,\mathrm{close}_2(\gamma_\Omega,\mathrm{e}_2{}^+)))))) \in \mathcal{E}\llbracket\tau_1 \otimes \tau_2\rrbracket.\end{gathered}$$

Next, by Lemma 3.5, we have that $\gamma_\Omega = \gamma_1 \uplus \gamma_2$, $\Phi_1 = \Phi_{1l} \uplus \Phi_{1r}$, and $\Phi_2 = \Phi_{2l} \uplus \Phi_{2r}$ where

$$(W,\Phi_{1l},\Phi_{2l},\gamma_1) \in \mathcal{G}\llbracket\Omega_1\rrbracket.$$

and

$$(W,\Phi_{1r},\Phi_{2r},\gamma_2) \in \mathcal{G}\llbracket\Omega_2\rrbracket.$$

and for all $i \in \{1,2\}$,

$$\mathrm{close}_i(\gamma_\Omega,\mathrm{e}_1{}^+) = \mathrm{close}_i(\gamma_1,\mathrm{e}_1{}^+)$$

and

$$\mathrm{close}_i(\gamma_\Omega,\mathrm{e}_2{}^+) = \mathrm{close}_i(\gamma_1,\mathrm{e}_2{}^+)$$

Thus, we must show

$$\begin{gathered}(W,(\Phi_{1l} \uplus \Phi_{1r},(\mathrm{close}_1(\gamma_\Gamma,\mathrm{close}_1(\gamma_\Gamma,\mathrm{close}_1(\gamma_1,\mathrm{e}_1{}^+))),\mathrm{close}_1(\gamma_\Gamma,\mathrm{close}_1(\gamma_\Gamma,\mathrm{close}_1(\gamma_2,\mathrm{e}_2{}^+))))), \\ (\Phi_{2l} \uplus \Phi_{2r},(\mathrm{close}_2(\gamma_\Gamma,\mathrm{close}_2(\gamma_\Gamma,\mathrm{close}_2(\gamma_1,\mathrm{e}_1{}^+))),\mathrm{close}_2(\gamma_\Gamma,\mathrm{close}_2(\gamma_\Gamma,\mathrm{close}_2(\gamma_2,\mathrm{e}_2{}^+)))))) \in \mathcal{E}\llbracket\tau_1 \otimes \tau_2\rrbracket.\end{gathered}$$

Let e_1 and e_2 be the first and second expressions, respectively, in the above tuple. Expanding the definition of the expression relation, given:

$$\begin{gathered}\forall \Phi_{r1},\Phi_{r2},\mathrm{H}_1,\mathrm{H}_2{:}W,\ \mathrm{e}_1',\ \mathrm{H}_1',\ j < W.k. \\ \Phi_{r1}\#\Phi_{1l} \uplus \Phi_{1r} \wedge \Phi_{r2}\#\Phi_{2l} \uplus \Phi_{2r} \wedge \Phi_{r1} \uplus \Phi_{1l} \uplus \Phi_{1r},\Phi_{r2} \uplus \Phi_{2l} \uplus \Phi_{2r} : W \wedge \\ \langle \Phi_{r1} \uplus \mathrm{flags}(W,1) \uplus \Phi_{1l} \uplus \Phi_{1r},\mathrm{H}_1,\mathrm{e}_1\rangle \overset{j}{\dashrightarrow} \langle \Phi_1',\mathrm{H}_1',\mathrm{e}_1'\rangle \nrightarrow\end{gathered}$$

we must show that either e_1' is fail Conv or there exist $\Phi_{f1},\Phi_{g1},\Phi_{f2},\Phi_{g2},\mathrm{v}_2,\mathrm{H}_2',W'$ such that:

$$\begin{aligned}&\langle \Phi_{r2} \uplus \mathrm{flags}(W,2) \uplus \Phi_{2l} \uplus \Phi_{2r},\mathrm{H}_2,\mathrm{e}_2\rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W',2) \uplus \Phi_{f2} \uplus \Phi_{g2},\mathrm{H}_2',\mathrm{v}_2\rangle \nrightarrow \\ &\wedge\ \Phi_1' = \Phi_{r1} \uplus \mathrm{flags}(W',1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge \\ &\wedge\ W \sqsubseteq_{\Phi_{r1},\Phi_{r2}} W' \wedge\ \mathrm{H}_1',\mathrm{H}_2' : W' \\ &\wedge\ (W',(\Phi_{f1},\mathrm{e}_1'),(\Phi_{f2},\mathrm{v}_2)) \in \mathcal{V}\llbracket\tau_1 \otimes \tau_2\rrbracket_\rho)\end{aligned}$$

Next, we need to find e_1'. From the operational semantic, the tensor will run the first subexpression using the heap H_1 until it reaches a target value or gets stuck. By appealing to our first induction hypothesis, instantiated with $W, \gamma_\Gamma, \gamma_\Gamma, \gamma_1, \rho$, we find that:

$$(W, (\Phi_{1l}, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e_1}^+)))), (\Phi_{2l}, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathrm{e_1}^+))))) \in \mathcal{E}[\![\tau_1]\!]_{.}$$

Thus, the configuration

$$\langle \Phi_{r1} \uplus \Phi_{1r} \uplus \mathrm{flags}(W, 1) \uplus \Phi_{1l}, \mathrm{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e_1}^+)))\rangle$$

either reduces to fail Conv, in which case the original expression steps to fail Conv, or to some irreducible configuration $\langle \Phi_{r1} \uplus \Phi_{1r} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{f1l} \uplus \Phi_{g1l}, \mathrm{H}_1^*, \mathrm{e}_1^*\rangle$, in which case on the other side, the configuration

$$\langle \Phi_{r2} \uplus \Phi_{2r} \uplus \mathrm{flags}(W, 2) \uplus \Phi_{2l}, \mathrm{H}_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathrm{e_1}^+)))\rangle$$

reduces to some irreducible configuration $\langle \Phi_{r2} \uplus \Phi_{2r} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{f2l} \uplus \Phi_{g2l}, \mathrm{H}_2^*, \mathrm{e}_1^\dagger\rangle$ and there exists some W_1 where $W \sqsubseteq_{\Phi_{r1} \uplus \Phi_{1r}, \Phi_{r2} \uplus \Phi_{2r}} W_1, \mathrm{H}_1^*, \mathrm{H}_2^* : W_1$, and $(W_1, (\Phi_{f1l}, \mathrm{e}_1^*), (\Phi_{f2l}, \mathrm{e}_1^\dagger)) \in \mathcal{V}[\![\tau_1]\!]_{.}$.

Since terms in the value relation are target values, the original pair will continue reducing on the second subexpression according to the operational semantics. Next, we can instantiate the second induction hypothesis with $W_1, \gamma_\Gamma, \gamma_\Gamma, \gamma_2, \rho$, which we can do because $\mathcal{G}[\![\Gamma]\!]_\rho, \mathcal{G}[\![\Gamma]\!]_{.}, \mathcal{G}[\![\Omega]\!]_{.}$ are closed under world extension (Lemma 3.8). Thus:

$$(W, (\Phi_{1r}, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e_2}^+)))), (\Phi_{2r}, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e_2}^+))))) \in \mathcal{E}[\![\tau_2]\!]_{.}$$

Ergo, the configuration

$$\langle \Phi_{r1} \uplus \Phi_{f1l} \uplus \Phi_{g1l} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{1r}, \mathrm{H}_1^*, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e_2}^+)))\rangle$$

either reduces to fail Conv, in which case the original pair steps to fail Conv, or to some irreducible configuration $\langle \Phi_{r1} \uplus \Phi_{f1l} \uplus \Phi_{g1l} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{f1r} \uplus \Phi_{g1r}, \mathrm{H}_1^\dagger, \mathrm{e}_2^*\rangle$, in which case on the other side, the configuration

$$\langle \Phi_{r2} \uplus \Phi_{f2l} \uplus \Phi_{g2l} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{2r}, \mathrm{H}_2^*, \mathrm{e}_1^\dagger\rangle$$

reduces to some irreducible configuration $\langle \Phi_{r2} \uplus \Phi_{f2l} \uplus \Phi_{g2l} \uplus \mathrm{flags}(W_2, 2) \uplus \Phi_{f2r} \uplus \Phi_{g2r}, \mathrm{H}_2^\dagger, \mathrm{e}_2^\dagger\rangle$ and there exists some W_2 where $W_1 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{f1l} \uplus \Phi_{g1l}, \Phi_{r2} \uplus \Phi_{f2l} \uplus \Phi_{g2l}} W_2, \mathrm{H}_1^\dagger, \mathrm{H}_2^\dagger : W_2$ and

$$(W_2, (\Phi_{f1r}, \mathrm{e}_2^*), (\Phi_{f2r}, \mathrm{e}_2^\dagger)) \in \mathcal{V}[\![\tau_2]\!]_{.}$$

Thus, the original pair with H_1 steps to $\langle \Phi_{r1} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{f1l} \uplus \Phi_{f1r} \uplus \Phi_{g1l} \uplus \Phi_{g1r}, \mathrm{H}_1^\dagger, (\mathrm{e}_1^*, \mathrm{e}_2^*)\rangle$ which is a value and thus an irreducible configuration because both e_1^* and e_2^* are values. Similarly, the original pair with H_2 steps to $\langle \Phi_{r2} \uplus \mathrm{flags}(W_2, 2) \uplus \Phi_{f2l} \uplus \Phi_{f2r} \uplus \Phi_{g2l} \uplus \Phi_{g2r}, \mathrm{H}_2^\dagger, (\mathrm{e}_1^\dagger, \mathrm{e}_2^\dagger)\rangle \not\twoheadrightarrow$. Ergo, since $(W_2, (\Phi_{f1l}, \mathrm{e}_1^*), (\Phi_{f1r}, \mathrm{e}_1^\dagger)) \in \mathcal{V}[\![\tau_1]\!]_{.}$ (because $(W_1, (\Phi_{f1l}, \mathrm{e}_1^*), (\Phi_{f2l}, \mathrm{e}_1^\dagger)) \in \mathcal{V}[\![\tau_1]\!]_{.}$ and $W_1 \sqsubseteq_{\Phi_{f1l}, \Phi_{f2l}} W_2$) and $(W_2, (\Phi_{f1r}, \mathrm{e}_2^*), (\Phi_{f2r}, \mathrm{e}_2^\dagger)) \in \mathcal{V}[\![\tau_2]\!]_{.}$, so $(W_2, (\Phi_{f1l} \uplus \Phi_{f1r}, (\mathrm{e}_1^*, \mathrm{e}_2^*)), (\Phi_{f2l} \uplus \Phi_{f2r}, (\mathrm{e}_1^\dagger, \mathrm{e}_2^\dagger)) \in \mathcal{V}[\![\tau_1 \otimes \tau_2]\!]_{.}$. Finally, since $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_1$ and $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_2$, we have $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_2$, which suffices to finish the proof. □

Lemma 3.46 (Compat let).

$$\begin{aligned} &\Delta_1; \Gamma_1; \Gamma; \Omega_1 \vdash \mathrm{e}_1 \preceq \mathrm{e}_1 : \tau_1 \otimes \tau_2 \leadsto \Delta_2; \Gamma_2 \wedge \Delta_2; \Gamma_2; \Gamma; \Omega_2, \mathrm{a}_\bullet : \tau_1, \mathrm{a}_\bullet' : \tau_2 \vdash \mathrm{e}_2 \preceq \mathrm{e}_2 : \tau \leadsto \Delta_3; \Gamma_3 \\ &\implies \Delta_1; \Gamma_1; \Gamma; \Omega_1 \uplus \Omega_2 \vdash \mathrm{let}\ (\mathrm{a}_\bullet, \mathrm{a}_\bullet') = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 \preceq \mathrm{let}\ (\mathrm{a}_\bullet, \mathrm{a}_\bullet') = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 : \tau \leadsto \Delta_3; \Gamma_3 \end{aligned}$$

Proof. Expanding the hypotheses, it is clear that $\Delta_1 = \Delta_2 = \Delta_3$ and $\Gamma_1 = \Gamma_2 = \Gamma_3$. Let $\Delta = \Delta_1$ and $\Gamma = \Gamma_1$.

Moreover, $\Delta_1; \Gamma_1; \Gamma; \Omega_1 \uplus \Omega_2 \vdash \mathrm{let}\ (\mathrm{a}_\bullet, \mathrm{a}_\bullet') = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 : \tau \leadsto \Delta_3; \Gamma_3$ by the let typing rule. Ergo, it suffices to show $\Delta; \Gamma; \Gamma; \Omega_1 \uplus \Omega_2 \vdash \mathrm{let}\ (\mathrm{a}_\bullet, \mathrm{a}_\bullet') = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 \preceq \mathrm{let}\ (\mathrm{a}_\bullet, \mathrm{a}_\bullet') = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 : \tau$.

Expanding the conclusion, given

$$\forall W.\forall \rho\, \gamma_\Gamma\, \gamma_\Gamma\, \gamma_\Omega.\rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \emptyset, \emptyset, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!].\wedge (W, \Phi_1, \Phi_2, \gamma_\Omega) \in \mathcal{G}[\![\Omega_1 \uplus \Omega_2]\!].$$

we must show

$$\begin{gathered}(W, (\Phi_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{let}\ (\mathsf{a}_\bullet, \mathsf{a}'_\bullet) = \mathsf{e}_1\ \mathsf{in}\ \mathsf{e}_2{}^+)))),\\ (\Phi_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{let}\ (\mathsf{a}_\bullet, \mathsf{a}'_\bullet) = \mathsf{e}_1\ \mathsf{in}\ \mathsf{e}_2{}^+))))) \in \mathcal{E}[\![\tau]\!].\end{gathered}$$

By pushing the compilers and substitutions through the let, we can refine this to:

$$\begin{gathered}(W, (\Phi_1, \mathsf{let}\ \mathsf{x}_{\mathsf{fresh}} = \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_1{}^+)))\ \mathsf{in}\\ \mathsf{let}\ \mathsf{a}_\bullet = \mathsf{fst}\ \mathsf{x}_{\mathsf{fresh}}\ \mathsf{in}\ \mathsf{let}\ \mathsf{a}'_\bullet = \mathsf{snd}\ \mathsf{x}_{\mathsf{fresh}}\ \mathsf{in}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Omega, \mathsf{e}_2{}^+)))),\\ (\Phi_2, \mathsf{let}\ \mathsf{x}_{\mathsf{fresh}} = \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}_1{}^+)))\ \mathsf{in}\\ \mathsf{let}\ \mathsf{a}_\bullet = \mathsf{fst}\ \mathsf{x}_{\mathsf{fresh}}\ \mathsf{in}\ \mathsf{let}\ \mathsf{a}'_\bullet = \mathsf{snd}\ \mathsf{x}_{\mathsf{fresh}}\ \mathsf{in}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Omega, \mathsf{e}_2{}^+))))) \in \mathcal{E}[\![\tau]\!].\end{gathered}$$

Next, by Lemma 3.5, we have that $\gamma_\Omega = \gamma_1 \uplus \gamma_2$, $\Phi_1 = \Phi_{1l} \uplus \Phi_{1r}$, and $\Phi_2 = \Phi_{2l} \uplus \Phi_{2r}$ where

$$(W, \Phi_{1l}, \Phi_{2l}, \gamma_1) \in \mathcal{G}[\![\Omega]\!].$$

and

$$(W, \Phi_{1r}, \Phi_{2r}, \gamma_2) \in \mathcal{G}[\![\Omega]\!].$$

and for all $i \in \{1, 2\}$,

$$\mathrm{close}_i(\gamma_\Omega, \mathsf{e}_1{}^+) = \mathrm{close}_i(\gamma_1, \mathsf{e}_1{}^+)$$

and

$$\mathrm{close}_i(\gamma_\Omega, \mathsf{e}_2{}^+) = \mathrm{close}_i(\gamma_2, \mathsf{e}_2{}^+)$$

Thus, we refine the statement we need to prove to:

$$\begin{gathered}(W, (\Phi_{1l} \uplus \Phi_{1r}, \mathsf{let}\ \mathsf{x}_{\mathsf{fresh}} = \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathsf{e}_1{}^+)))\ \mathsf{in}\\ \mathsf{let}\ \mathsf{a}_\bullet = \mathsf{fst}\ \mathsf{x}_{\mathsf{fresh}}\ \mathsf{in}\ \mathsf{let}\ \mathsf{a}'_\bullet = \mathsf{snd}\ \mathsf{x}_{\mathsf{fresh}}\ \mathsf{in}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathsf{e}_2{}^+)))),\\ (\Phi_{2l} \uplus \Phi_{2r}, \mathsf{let}\ \mathsf{x}_{\mathsf{fresh}} = \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathsf{e}_1{}^+)))\ \mathsf{in}\\ \mathsf{let}\ \mathsf{a}_\bullet = \mathsf{fst}\ \mathsf{x}_{\mathsf{fresh}}\ \mathsf{in}\ \mathsf{let}\ \mathsf{a}'_\bullet = \mathsf{snd}\ \mathsf{x}_{\mathsf{fresh}}\ \mathsf{in}\ \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathsf{e}_2{}^+))))) \in \mathcal{E}[\![\tau]\!].\end{gathered}$$

Let e_1 and e_2 be the first and second expressions, respectively, in the tuple above. Expanding the definition of the expression relation, given:

$$\begin{gathered}\forall \Phi_{r1}, \Phi_{r2}, \mathsf{H}_1, \mathsf{H}_2{:}W,\ \mathsf{e}'_1,\ \mathsf{H}'_1,\ j < W.k.\\ \Phi_{r1} \# \Phi_{1l} \uplus \Phi_{1r} \wedge \Phi_{r2} \# \Phi_{2l} \uplus \Phi_{2r} \wedge \Phi_{r1} \uplus \Phi_{1l} \uplus \Phi_{1r}, \Phi_{r2} \uplus \Phi_{2l} \uplus \Phi_{2r} : W \wedge\\ \langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_{1l} \uplus \Phi_{1r}, \mathsf{H}_1, \mathsf{e}_1 \rangle \overset{j}{\dashrightarrow} \langle \Phi'_1, \mathsf{H}'_1, \mathsf{e}'_1 \rangle \nrightarrow\end{gathered}$$

we must show that either e'_1 is fail Conv or there exist $\Phi_{f1}, \Phi_{g1}, \Phi_{f2}, \Phi_{g2}, \mathsf{v}_2, \mathsf{H}'_2, W'$ such that:

$$\begin{aligned}&\langle \Phi_{r2} \uplus \mathrm{flags}(W, 2) \uplus \Phi_{2l} \uplus \Phi_{2r}, \mathsf{H}_2, \mathsf{e}_2 \rangle \overset{*}{\dashrightarrow} \langle \Phi_{r2} \uplus \mathrm{flags}(W', 2) \uplus \Phi_{f2} \uplus \Phi_{g2}, \mathsf{H}'_2, \mathsf{v}_2 \rangle \nrightarrow\\ &\wedge \Phi'_1 = \Phi_{r1} \uplus \mathrm{flags}(W', 1) \uplus \Phi_{f1} \uplus \Phi_{g1} \wedge\\ &\wedge\ W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W' \wedge\ \mathsf{H}'_1, \mathsf{H}'_2 : W'\\ &\wedge (W', (\Phi_{f1}, \mathsf{e}'_1), (\Phi_{f2}, \mathsf{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho)\end{aligned}$$

Therefore, we find that

$$\langle \Phi_{r1} \uplus \Phi_{1r} \uplus \mathrm{flags}(W, 1) \uplus \Phi_{1l}, \mathsf{H}_1, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathsf{e}_1{}^+))) \rangle$$

either reduces to fail Conv, in which case the original expression steps to fail Conv, or to some irreducible configuration $\langle \Phi_{r1} \uplus \Phi_{1r} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{f1l} \uplus \Phi_{g1l}, \mathsf{H}^*_1, \mathsf{e}^*_1 \rangle$, in which case

$$\langle \Phi_{r2} \uplus \Phi_{2r} \uplus \mathrm{flags}(W, 2) \uplus \Phi_{2l}, \mathsf{H}_2, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathsf{e}_1{}^+))) \rangle$$

also reduces to an irreducible configuration $\langle \Phi_{r2} \uplus \Phi_{2r} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{f2l} \uplus \Phi_{g2l}, \mathrm{H}_2^*, \mathrm{e}_1^\dagger \rangle$ and there exists some world W_1 where $W \sqsubseteq_{\Phi_{r1} \uplus \Phi_{1r}, \Phi_{r2} \uplus \Phi_{2r}} W_1, \mathrm{H}_1^*, \mathrm{H}_2^* : W_1$, and $(W_1, (\Phi_{f1l}, \mathrm{e}_1^*), (\Phi_{f2l}, \mathrm{e}_1^\dagger)) \in \mathcal{V}[\![\tau_1 \otimes \tau_2]\!]$..

By expanding the value relation, we find that

$$\Phi_{f1l} = \Phi_{f1ll} \uplus \Phi_{f1lr}$$
$$\mathrm{e}_1^* = (\mathrm{v}_1^*, \mathrm{v}_2^*)$$
$$\Phi_{f2l} = \Phi_{f2ll} \uplus \Phi_{f2lr}$$
$$\mathrm{e}_1^\dagger = (\mathrm{v}_1^\dagger, \mathrm{v}_2^\dagger)$$

where

$$(W_1, (\Phi_{f1ll}, \mathrm{v}_1^*), (\Phi_{f2ll}, \mathrm{v}_1^\dagger)) \in \mathcal{V}[\![\tau_1]\!].$$
$$(W_1, (\Phi_{f1lr}, \mathrm{v}_2^*), (\Phi_{f2lr}, \mathrm{v}_2^\dagger)) \in \mathcal{V}[\![\tau_2]\!].$$

Thus, the original configuration with H_1 steps as follows:

$$\begin{aligned}
&\langle \Phi_{r1} \uplus \mathrm{flags}(W, 1) \uplus \Phi_{1l} \uplus \Phi_{1r}, \mathrm{H}_1, \mathtt{let}\ \mathrm{x_{fresh}} = \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathrm{e}_1{}^+)))\ \mathtt{in}\\
&\quad \mathtt{let}\ \mathrm{a}_\bullet = \mathtt{fst}\ \mathrm{x_{fresh}}\ \mathtt{in}\ \mathtt{let}\ \mathrm{a}'_\bullet = \mathtt{snd}\ \mathrm{x_{fresh}}\ \mathtt{in}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e}_2{}^+)))\rangle \overset{*}{\dashrightarrow}\\
&\langle \Phi_{r1} \uplus \Phi_{1r} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{f1ll} \uplus \Phi_{f1lr} \uplus \Phi_{g1l}, \mathrm{H}_1^*, \mathtt{let}\ \mathrm{x_{fresh}} = \ (\mathrm{v}_1^*, \mathrm{v}_2^*)\ \mathtt{in}\\
&\quad \mathtt{let}\ \mathrm{a}_\bullet = \mathtt{fst}\ \mathrm{x_{fresh}}\ \mathtt{in}\ \mathtt{let}\ \mathrm{a}'_\bullet = \mathtt{snd}\ \mathrm{x_{fresh}}\ \mathtt{in}\ \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e}_2{}^+)))\rangle \overset{*}{\dashrightarrow}\\
&\langle \Phi_{r1} \uplus \Phi_{1r} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{f1ll} \uplus \Phi_{f1lr} \uplus \Phi_{g1l} \uplus \{f_{1l}, f_{2l}\}, \mathrm{H}_1^*,\\
&[\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{v}_1^*, f_{1l})][\mathrm{a}'_\bullet \mapsto \mathrm{protect}(\mathrm{v}_2^*, f_{2l})]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e}_2{}^+)))\rangle
\end{aligned}$$

where $f_{1l} \neq f_{2l}$ and $f_{1l}, f_{2l} \notin \Phi_{r1} \uplus \Phi_{1r} \uplus \Phi_{f1ll} \uplus \Phi_{f1lr} \uplus \Phi_{g1l}$.

By similar reasoning, the configuration on the other side with H_2 steps to:

$$\begin{aligned}
&\langle \Phi_{r2} \uplus \Phi_{2r} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{f2ll} \uplus \Phi_{f2lr} \uplus \Phi_{g2l} \uplus \{f_{1r}, f_{2r}\}, \mathrm{H}_2^*,\\
&[\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{v}_1^\dagger, f_{1r})][\mathrm{a}'_\bullet \mapsto \mathrm{protect}(\mathrm{v}_2^\dagger, f_{2r})]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e}_2{}^+)))\rangle
\end{aligned}$$

where $f_{1r} \neq f_{2r}$ and $f_{1r}, f_{2r} \notin \Phi_{r2} \uplus \Phi_{2r} \uplus \Phi_{f2ll} \uplus \Phi_{f2lr} \uplus \Phi_{g2l}$.

Next, notice that:

$$\begin{aligned}
&(W_1, \Phi_{1r} \uplus \Phi_{f1ll} \uplus \Phi_{f1lr} \uplus \{f_{1l}, f_{2l}\}, \Phi_{2r} \uplus \Phi_{f2ll} \uplus \Phi_{f2lr} \uplus \{f_{1r}, f_{2r}\},\\
&\gamma_2[\mathrm{a}_\bullet \mapsto (\mathrm{protect}(\mathrm{v}_1^*, f_{1l}), \mathrm{protect}(\mathrm{v}_1^\dagger, f_{1r}))][\mathrm{a}'_\bullet \mapsto (\mathrm{protect}(\mathrm{v}_2^*, f_{2l}), \mathrm{protect}(\mathrm{v}_2^\dagger, f_{2r}))]) \in \mathcal{G}[\![\Omega_2, \mathrm{a}_\bullet : \tau_1, \mathrm{a}'_\bullet : \tau_2]\!].
\end{aligned}$$

Thus, we can instantiate the second induction hypothesis with

$$\begin{aligned}
&W_1, \gamma_\Gamma, \gamma_\Gamma,\\
&\gamma_2[\mathrm{a}_\bullet \mapsto (\mathrm{protect}(\mathrm{v}_1^*, f_{1l}), \mathrm{protect}(\mathrm{v}_1^\dagger, f_{1r}))][\mathrm{a}'_\bullet \mapsto (\mathrm{protect}(\mathrm{v}_2^*, f_{2l}), \mathrm{protect}(\mathrm{v}_2^\dagger, f_{2r}))], \rho
\end{aligned}$$

to find that:

$$\begin{aligned}
&(W_1,\\
&(\Phi_{1r} \uplus \Phi_{f1ll} \uplus \Phi_{f1lr} \uplus \{f_{1l}, f_{2l}\},\\
&[\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{v}_1^*, f_{1l})][\mathrm{a}'_\bullet \mapsto \mathrm{protect}(\mathrm{v}_2^*, f_{2l})]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e}_2{}^+)))),\\
&(\Phi_{2r} \uplus \Phi_{f2ll} \uplus \Phi_{f2lr} \uplus \{f_{1r}, f_{2r}\},\\
&[\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{v}_1^\dagger, f_{1r})][\mathrm{a}'_\bullet \mapsto \mathrm{protect}(\mathrm{v}_2^\dagger, f_{2r})]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e}_2{}^+))))) \in \mathcal{E}[\![\tau]\!].
\end{aligned}$$

Then, consider again the above configurations:

$$\begin{aligned}
&\langle \Phi_{r1} \uplus \Phi_{1r} \uplus \mathrm{flags}(W_1, 1) \uplus \Phi_{f1ll} \uplus \Phi_{f1lr} \uplus \Phi_{g1l} \uplus \{f_{1l}, f_{2l}\}, \mathrm{H}_1^*,\\
&[\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{v}_1^*, f_{1l})][\mathrm{a}'_\bullet \mapsto \mathrm{protect}(\mathrm{v}_2^*, f_{2l})]\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_2, \mathrm{e}_2{}^+)))\rangle
\end{aligned}$$

$$\begin{aligned}
&\langle \Phi_{r2} \uplus \Phi_{2r} \uplus \mathrm{flags}(W_1, 2) \uplus \Phi_{f2ll} \uplus \Phi_{f2lr} \uplus \Phi_{g2l} \uplus \{f_{1r}, f_{2r}\}, \mathrm{H}_2^*,\\
&[\mathrm{a}_\bullet \mapsto \mathrm{protect}(\mathrm{v}_1^\dagger, f_{1r})][\mathrm{a}'_\bullet \mapsto \mathrm{protect}(\mathrm{v}_2^\dagger, f_{2r})]\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_2, \mathrm{e}_2{}^+)))\rangle
\end{aligned}$$

By applying the above fact, we find that the first configuration either steps to fail Conv, in which case the original configuration steps to fail Conv, or steps to some irreducible configuration

$$\langle \Phi_{r1} \uplus \Phi_{g1l} \uplus \mathrm{flags}(W_2, 1) \uplus \Phi_{f1r} \uplus \Phi_{g1r}, \mathsf{H}_1^{\dagger}, \mathsf{e}_2^{*} \rangle$$

in which case the second configuration also steps to some irreducible configuration

$$\langle \Phi_{r2} \uplus \Phi_{g2l} \uplus \mathrm{flags}(W_2, 2) \uplus \Phi_{f2r} \uplus \Phi_{g2r}, \mathsf{H}_2^{\dagger}, \mathsf{e}_2^{\dagger} \rangle$$

and there exists some world W_2 such that $W_1 \sqsubseteq_{\Phi_{r1} \uplus \Phi_{g1l}, \Phi_{r2} \uplus \Phi_{g2l}} W_2, \mathsf{H}_1^{\dagger}, \mathsf{H}_2^{\dagger} : W_2$, and

$$(W_2, (\Phi_{f1r}, \mathsf{e}_2^{*}), (\Phi_{f2r}, \mathsf{e}_2^{\dagger})) \in \mathcal{V}[\![\tau]\!].$$

Finally, since $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_1$ and $W_1 \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_2$, we have $W \sqsubseteq_{\Phi_{r1}, \Phi_{r2}} W_2$, which suffices to finish the proof. □

Lemma 3.47 (Compat $\llparenthesis \mathsf{e} \rrparenthesis_{\tau}$).

$$\begin{aligned} &\Delta = \Delta' \wedge \Gamma = \Gamma' \wedge \Gamma; \Omega; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau \rightsquigarrow \Gamma; \Omega' \wedge \_ : \tau \sim \tau \\ \implies\ &\Delta; \Gamma; \Gamma; \Omega \vdash \llparenthesis \mathsf{e} \rrparenthesis_{\tau} \preceq \llparenthesis \mathsf{e} \rrparenthesis_{\tau} : \tau \rightsquigarrow \Delta'; \Gamma' \end{aligned}$$

Proof. Expanding the third hypothesis, there exists some Ω_{e} such that $\Omega = \Omega_{\mathsf{e}} \uplus \Omega'$ and $\Gamma; \Omega_{\mathsf{e}}; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau$.

We have $\Delta = \Delta'$ and $\Gamma = \Gamma'$ by the first two assumptions. Moreover, $\Delta; \Gamma; \Gamma; \Omega \vdash \llparenthesis \mathsf{e} \rrparenthesis_{\tau} : \tau \rightsquigarrow \Delta'; \Gamma'$ by the conversion typing rule. Thus, to prove the conclusion, it suffices to show $\Delta; \Gamma; \Gamma; \Omega \vdash \llparenthesis \mathsf{e} \rrparenthesis_{\tau} \preceq \llparenthesis \mathsf{e} \rrparenthesis_{\tau} : \tau$.

Expanding the conclusion, given

$$\forall W. \forall \rho\, \gamma_{\Gamma}\, \gamma_{\Gamma}\, \gamma_{\Omega}. \rho \in \mathcal{D}[\![\Delta]\!] \wedge (W, \emptyset, \emptyset, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]_{\rho} \wedge (W, \emptyset, \emptyset, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]. \wedge (W, \Phi_1, \Phi_2, \gamma_{\Omega}) \in \mathcal{G}[\![\Omega]\!].$$

we must show

$$(W, (\Phi_1, \mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Omega}, \llparenthesis \mathsf{e} \rrparenthesis_{\tau}{}^{+})))), (\Phi_2, \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Omega}, \llparenthesis \mathsf{e} \rrparenthesis_{\tau}{}^{+}))))) \in \mathcal{E}[\![\tau]\!].$$

We can push the compiler and substitutions through the pair to refine that to:

$$\begin{aligned} &(W, (\Phi_1, C_{\tau \mapsto \tau}(\mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Omega}, \mathsf{e}^{+}))))), \\ &(\Phi_2, C_{\tau \mapsto \tau}(\mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Omega}, \mathsf{e}^{+})))))) \in \mathcal{E}[\![\tau]\!]. \end{aligned}$$

By Lemma 3.3, it suffices to show:

$$\begin{aligned} &(W, (\emptyset, C_{\tau \mapsto \tau}(\mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Omega}, \mathsf{e}^{+}))))), \\ &(\emptyset, C_{\tau \mapsto \tau}(\mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Omega}, \mathsf{e}^{+})))))) \in \mathcal{E}[\![\tau]\!]. \end{aligned}$$

Next, by Lemma 3.5, we have that $\gamma_{\Omega} = \gamma_1 \uplus \gamma_2$, $\Phi_1 = \Phi_{1l} \uplus \Phi_{1r}$, and $\Phi_2 = \Phi_{2l} \uplus \Phi_{2r}$ where

$$(W, \Phi_{1l}, \Phi_{2l}, \gamma_1) \in \mathcal{G}[\![\Omega_{\mathsf{e}}]\!].$$

and

$$(W, \Phi_{1r}, \Phi_{2r}, \gamma_2) \in \mathcal{G}[\![\Omega']\!].$$

and for all $i \in \{1, 2\}$,

$$\mathrm{close}_i(\gamma_{\Omega}, \mathsf{e_1}^{+}) = \mathrm{close}_i(\gamma_1, \mathsf{e}^{+})$$

Thus, we refine the statement we need to prove to:

$$\begin{aligned} &(W, (\emptyset, C_{\tau \mapsto \tau}(\mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_1, \mathsf{e}^{+}))))), \\ &(\emptyset, C_{\tau \mapsto \tau}(\mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_1, \mathsf{e}^{+})))))) \in \mathcal{E}[\![\tau]\!]. \end{aligned}$$

Now, by instantiating our induction hypothesis with $W, \gamma_{\Gamma}, \gamma_{\Gamma}, \gamma_1, \rho$, we find that:

$$(W, (\emptyset, \mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_{\Gamma}, \mathrm{close}_1(\gamma_1, \mathsf{e}^{+})))), (\emptyset, \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_{\Gamma}, \mathrm{close}_2(\gamma_1, \mathsf{e}^{+}))))) \in \mathcal{E}[\![\tau]\!]_{\rho}$$

By Lemma 3.14, it follows that:

$$(W, (\emptyset, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathsf{e}^+)))), (\emptyset, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathsf{e}^+))))) \in \mathcal{E}[\![\tau]\!].$$

Therefore, by Theorem 3.18, we have

$$\begin{gathered}(W, (\emptyset, C_{\tau \mapsto \tau}(\mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_\Gamma, \mathrm{close}_1(\gamma_1, \mathsf{e}^+))))),\\ (\emptyset, C_{\tau \mapsto \tau}(\mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_\Gamma, \mathrm{close}_2(\gamma_1, \mathsf{e}^+)))))) \in \mathcal{E}[\![\tau]\!].\end{gathered}$$

as was to be proven. □

4 CASE STUDY: MEMORY MANAGEMENT AND POLYMORPHISM

4.1 LCVM Language

Our target is an untyped lambda calculus with pairs, sums, and references.

4.1.1 *Syntax.*

$$\begin{array}{lll}
\text{Expressions } e & := & () \mid \mathbb{Z} \mid \ell \mid x \mid (e, e) \mid \text{fst } e \mid \text{snd } e \mid \text{inl } e \mid \text{inr } e \mid \text{if } e\ \{e\}\ \{e\} \\
 & & \mid \text{match } e\ x\{e\}\ y\{e\} \mid \text{let } x = e \text{ in } e \mid \lambda x\{e\} \mid e\ e \mid \text{ref } e \mid \text{alloc } e \mid \text{free } e \\
 & & \mid \text{callgc} \mid \text{gcmov } e \mid !e \mid e := e \mid \text{fail } c \\
\text{Values } v & ::= & () \mid \mathbb{Z} \mid \ell \mid (v, v) \mid \lambda x.e \\
\text{Error Code } c & ::= & \text{\textsc{Type}} \mid \text{\textsc{Conv}} \mid \text{\textsc{Ptr}} \\
\text{Heap } H & ::= & \ell \overset{gc}{\mapsto} v, \ldots \mid \ell \overset{m}{\mapsto} v, \ldots \\
\text{Evaluation Context } K & ::= & [\cdot] \mid (K, e) \mid (v, K) \mid \text{inl } K \mid \text{inr } K \mid \text{match } K\ x\{e\}\ y\{e\} \mid \text{if } K\ \{e\}\ \{e\} \mid \\
 & & \text{let } x = K \text{ in } e \mid K\ e \mid v\ K \mid \text{ref } K \mid \text{alloc } K \mid \text{free } K \mid \text{gcmov } K \mid !K \mid K := e \mid \\
 & & v := K
\end{array}$$

4.1.2 *Dynamics.*

Our operational semantics uses evaluation contexts to lift steps on subterms into steps on whole programs.

$$\frac{}{\langle H, \text{fst } (v, v')\rangle \Mapsto \langle H, v\rangle} \qquad \frac{v \neq (v_1, v_2)}{\langle H, \text{fst } v\rangle \Mapsto \langle H, \text{fail } \text{\textsc{Type}}\rangle} \qquad \frac{}{\langle H, \text{snd } (v', v)\rangle \Mapsto \langle H, v\rangle}$$

$$\frac{v \neq (v_1, v_2)}{\langle H, \text{snd } v\rangle \Mapsto \langle H, \text{fail } \text{\textsc{Type}}\rangle} \qquad \frac{}{\langle H, \text{if } 0\ \{e_1\}\ \{e_2\}\rangle \Mapsto \langle H, e_1\rangle} \qquad \frac{n \neq 0}{\langle H, \text{if } n\ \{e_1\}\ \{e_2\}\rangle \Mapsto \langle H, e_2\rangle}$$

$$\frac{v \notin \mathbb{Z}}{\langle H, \text{if } v\ \{e_1\}\ \{e_2\}\rangle \Mapsto \langle H, \text{fail } \text{\textsc{Type}}\rangle} \qquad \frac{}{\langle H, \text{match inl } v\ x\{e_1\}\ y\{e_2\}\rangle \Mapsto \langle H, [x \mapsto v]e_1\rangle}$$

$$\frac{}{\langle H, \text{match inr } v\ x\{e_1\}\ y\{e_2\}\rangle \Mapsto \langle H, [y \mapsto v]e_2\rangle} \qquad \frac{v \notin \{\text{inr } v', \text{inl } v'\}}{\langle H, \text{match } v\ x\{e_1\}\ y\{e_2\}\rangle \Mapsto \langle H, \text{fail } \text{\textsc{Type}}\rangle}$$

$$\frac{}{\langle H, \text{let } x = v \text{ in } e\rangle \Mapsto \langle H, [x \mapsto v]e\rangle} \qquad \frac{}{\langle H, \lambda x\{e_b\}\ v\rangle \Mapsto \langle H, [x \mapsto v]e_b\rangle}$$

$$\frac{v \neq \lambda x\{e\}}{\langle H, v\ v'\rangle \Mapsto \langle H, \text{fail } \text{\textsc{Type}}\rangle} \qquad \frac{\ell \notin \text{dom}(H)}{\langle H, \text{ref } v\rangle \Mapsto \langle H[\ell \overset{gc}{\mapsto} v], \ell\rangle} \qquad \frac{\ell \notin \text{dom}(H)}{\langle H, \text{alloc } v\rangle \Mapsto \langle H[\ell \overset{m}{\mapsto} v], \ell\rangle}$$

$$\frac{\ell \overset{m}{\mapsto} v \in H}{\langle H, \text{free } \ell\rangle \Mapsto \langle H \setminus \ell, ()\rangle} \qquad \frac{\ell \overset{gc}{\mapsto} v \in H}{\langle H, \text{free } \ell\rangle \Mapsto \langle H, \text{fail } \text{\textsc{Ptr}}\rangle} \qquad \frac{\ell \notin \text{dom}(H)}{\langle H, \text{free } \ell\rangle \Mapsto \langle H, \text{fail } \text{\textsc{Ptr}}\rangle}$$

$$\frac{\ell \overset{m}{\mapsto} v \in H}{\langle H, \text{gcmov } \ell\rangle \Mapsto \langle H[\ell \overset{gc}{\mapsto} v], \ell\rangle} \qquad \frac{H[\ell] = v}{\langle H, !\ell\rangle \Mapsto \langle H, v\rangle} \qquad \frac{\ell \notin \text{dom}(H)}{\langle H, !\ell\rangle \Mapsto \langle H, \text{fail } \text{\textsc{Ptr}}\rangle}$$

$$\frac{\mathsf{v} \neq \ell}{\langle \mathsf{H}, !\mathsf{v}\rangle \Mapsto \langle \mathsf{H}, \mathsf{fail}\ \textsc{Type}\rangle} \qquad \frac{\ell \overset{m}{\mapsto} \mathsf{v} \in \mathsf{H}}{\langle \mathsf{H}, \ell := \mathsf{v}'\rangle \Mapsto \langle \mathsf{H}[\ell \overset{m}{\mapsto} \mathsf{v}'], ()\rangle} \qquad \frac{\ell \overset{gc}{\mapsto} \mathsf{v} \in \mathsf{H}}{\langle \mathsf{H}, \ell := \mathsf{v}'\rangle \Mapsto \langle \mathsf{H}[\ell \overset{gc}{\mapsto} \mathsf{v}'], ()\rangle}$$

$$\frac{\ell \notin \mathrm{dom}(\mathsf{H})}{\langle \mathsf{H}, \ell := \mathsf{v}'\rangle \Mapsto \langle \mathsf{H}, \mathsf{fail}\ \textsc{Ptr}\rangle} \qquad \frac{\mathsf{v} \neq \ell}{\langle \mathsf{H}, \mathsf{v} := \mathsf{v}'\rangle \Mapsto \langle \mathsf{H}, \mathsf{fail}\ \textsc{Type}\rangle}$$

Let $\mathsf{H} : \mathit{MHeap}$ denote that H only contains mappings of the form $\ell \overset{m}{\mapsto} \mathsf{v}$ and let $\mathsf{H} : \mathit{GCHeap}$ denote that H only contains mappings of the form $\ell \overset{gc}{\mapsto} \mathsf{v}$.

Next, let $\mathit{FL}(\mathsf{e})$ and $\mathit{FL}(\mathsf{K}[\cdot])$ be the set of locations that appear free in e and K, respectively. Then, we say that a location ℓ is directly reachable from a location ℓ' in the heap H if $\ell' \in \mathrm{dom}(\mathsf{H})$ and $\ell \in \mathit{FL}(\mathsf{H}(\ell'))$. We say that ℓ is reachable from ℓ' in H if one can construct a sequence of locations $\ell_0 = \ell', \ell_1, \ell_2, \ldots, \ell_n = \ell$ where ℓ_i is directly reachable from ℓ_{i-1} in H for all $1 \leq i \leq n$. (Note that, for any location ℓ and heap H, ℓ is reachable from ℓ in H because we can construct the singleton sequence $\ell_0 = \ell$.)

Finally, let $\mathrm{reachablelocs}(\mathsf{H}, L)$ be the set of all locations in $\mathrm{dom}(\mathsf{H})$ reachable from L in H. (Note that $L \subseteq \mathrm{reachablelocs}(\mathsf{H}, L)$ by the previous parenthetical obversation.)

Using the above definitions, we further define a step on whole programs that performs garbage collection. This step is indexed by a set of locations L denoting the locations that must be preserved and can not be garbage collected. The step shrinks the heap non-deterministically, ensuring that garbage-collectable locations which are reachable from either the program or L are not removed from the heap.

$$\frac{\begin{array}{c}\mathsf{H}_{gc} : \mathit{GCHeap} \qquad \mathsf{H}_m : \mathit{MHeap} \\ \mathrm{reachablelocs}(\mathsf{H}_{gc} \uplus \mathsf{H}_m, \mathrm{dom}(\mathsf{H}_m) \cup \mathit{FL}(\mathsf{K}[\cdot]) \cup L) \cap \mathrm{dom}(\mathsf{H}_{gc}) \subseteq \mathrm{dom}(\mathsf{H}'_{gc}) \qquad \mathsf{H}'_{gc} \subseteq \mathsf{H}_{gc}\end{array}}{\langle \mathsf{H}_{gc} \uplus \mathsf{H}_m, \mathsf{K}[\mathsf{callgc}]\rangle \rightarrow_L \langle \mathsf{H}'_{gc} \uplus \mathsf{H}_m, \mathsf{K}[()]\rangle}$$

Finally, we also let steps on whole programs to take steps according to $\Mapsto$ and to lift fail c errors out of evaluation contexts:

$$\frac{\langle \mathsf{H}, \mathsf{e}\rangle \Mapsto \langle \mathsf{H}', \mathsf{e}'\rangle}{\langle \mathsf{H}, \mathsf{K}[\mathsf{e}]\rangle \rightarrow_L \langle \mathsf{H}', \mathsf{K}[\mathsf{e}']\rangle} \qquad \frac{\mathsf{K} \neq [\cdot]}{\langle \mathsf{H}, \mathsf{K}[\mathsf{fail}\ \mathsf{c}]\rangle \rightarrow_L \langle \mathsf{H}, \mathsf{fail}\ \mathsf{c}\rangle}$$

Note that we use $\rightarrow$ to denote $\rightarrow_{\emptyset}$.

4.1.3 Properties.

Lemma 4.1 (Lifting Steps Out of Evaluation Context). *If* $(\mathsf{H}, \mathsf{K}[\mathsf{e}]) \rightarrow_L (\mathsf{H}', \mathsf{K}[\mathsf{e}'])$ *and* $\mathsf{K}[\mathsf{e}']$ *is not of the form* fail c*, then* $(\mathsf{H}, \mathsf{e}) \rightarrow_{L \cup FL(K[\cdot])} (\mathsf{H}, \mathsf{e}')$*.*

Proof. Since it is given that $\mathsf{K}[\mathsf{e}']$ is not of the form fail c, there are two cases:

(1) The given $\rightarrow_L$ is the result of a callgc instruction. In this case, e must be of the form $\mathsf{K}'[\mathsf{callgc}]$ and e' must be of the form $\mathsf{K}'[()]$ for some evaluation context K'. Moreover, there exist $\mathsf{H}_{gc} : \mathit{GCHeap}, \mathsf{H}_m : \mathit{MHeap}, \mathsf{H}'_{gc}$ such that $\mathsf{H} = \mathsf{H}_{gc} \uplus \mathsf{H}_m$, $\mathsf{H}' = \mathsf{H}'_{gc} \uplus \mathsf{H}_m$, $\mathsf{H}'_{gc} \subseteq \mathsf{H}_{gc}$ and

$$\mathrm{reachablelocs}(\mathsf{H}_{gc} \uplus \mathsf{H}_m, \mathit{FL}(K[K'[\cdot]]) \cup L) \cap \mathrm{dom}(\mathsf{H}_{gc}) \subseteq \mathrm{dom}(\mathsf{H}'_{gc})$$

Then, notice that $\mathit{FL}(K[K'[\cdot]]) = \mathit{FL}(K'[\cdot]) \cup \mathit{FL}(K[\cdot])$. Ergo,

$$(\mathsf{H}_{gc} \uplus \mathsf{H}_m, \mathsf{K}'[\mathsf{callgc}]) \rightarrow_{L \cup FL(K[\cdot])} (\mathsf{H}'_{gc} \uplus \mathsf{H}_m, \mathsf{K}'[()])$$

as was to be proven.

(2) The given $\rightarrow_L$ is the result of a $\Mapsto$. In this case, e must be of the form $K'[e_\bullet]$ and e' must be of the form $K'[e'_\bullet]$ for some evaluation context K and expressions $e_\bullet, e'_\bullet$ such that $(H, e_\bullet) \Mapsto (H', e'_\bullet)$. It then follows that $(H, K'[e_\bullet]) \Mapsto (H', K'[e'_\bullet])$, as was to be proven.

□

Lemma 4.2 (Stepping Respects Evaluation Context). *If* $(H, e) \rightarrow_{L \cup FL(K[\cdot])} (H', e')$ *and* e' *is not of the form* fail c*, then*

(1) $(H, K[e]) \rightarrow_L (H', K[e'])$

(2) *for any* $H_\bullet, e_\bullet$ *such that* $(H, K[e]) \rightarrow_L (H_\bullet, e_\bullet)$*, there exists a* $e_{\bullet\bullet}$ *such that* $e_\bullet = K[e_{\bullet\bullet}]$.

Proof. Proving (1) is trivally similar to the proof of Lemma 4.1, so we focus on proving (2). We do case analysis on the reduction $(H, e) \rightarrow_{L \cup FL(K[\cdot])} (H', e')$:

(1) The given $\rightarrow_{L \cup FL(K[\cdot])}$ is the result of a callgc instruction. In this case, e must be of the form $K'[\text{callgc}]$. Then, for any $H_\bullet, e_\bullet$ such that $(H, K[e]) \rightarrow_L (H_\bullet, e_\bullet)$, because $K[e] = K[K'[\text{callgc}]]$, that step must be a callgc instruction, so $e_\bullet = K[K'[()]]$, and thus choosing $e_{\bullet\bullet} = K'[()]$ suffices to finish the proof.

(2) The given $\rightarrow_{L \cup FL(K[\cdot])}$ is the result of a $\Mapsto$. In this case, e must be of the form $K'[e^*]$ and e' must be of the form $K'[e^{*\prime}]$ for some evaluation context K' and expressions $e^*, e^{*\prime}$ such that $(H, e^*) \Mapsto (H', e^{*\prime})$. Moreover, $e^* \neq \text{callgc}$, because $(H, \text{callgc}) \not\Mapsto$, and e^* is not of the form fail c, because $(H, \text{fall c}) \not\Mapsto$.
Ergo, for any $H_\bullet, e_\bullet$ such that $(H, K[e]) \rightarrow_L (H_\bullet, e_\bullet)$, because $K[e] = K[K'[e^*]]$, this step must be the result of a $\Mapsto$. Thus, there exists some $e^{*\prime\prime}$ such that $(H, e^*) \Mapsto (H_\bullet, e^{*\prime\prime})$ and $e_\bullet = K[K'[e^{*\prime\prime}]]$, so choosing $e_{\bullet\bullet} = K'[e^{*\prime\prime}]$ suffices to finish the proof.

□

Lemma 4.3 (Subterm Termination). *If* $(H, e) \overset{*}{\rightarrow}_L (H', e') \not\rightarrow_L$ *where* e' *is not of the form* fail c *and* $(H, e) \overset{*}{\rightarrow}_L (H_\bullet, K[e_\bullet])$ *is a prefix of the aforementioned reduction, then* $(H, e) \overset{*}{\rightarrow}_L (H'_\bullet, K[e'_\bullet])$ *is also a prefix of the original reduction for some* $H'_\bullet, e_\bullet{}'$ *such that* $(H_\bullet, e_\bullet) \overset{*}{\rightarrow}_{L \cup FL(K[\cdot])} (H'_\bullet, e'_\bullet) \not\rightarrow_L$.

Proof. Consider the largest integer n such that there is a reduction

$$(H, e) \overset{*}{\rightarrow}_L (H_\bullet, K[e_\bullet]) \rightarrow_L (H_{\bullet,1}, K[e_{\bullet,1}]) \rightarrow_L \cdots \rightarrow_L (H_{\bullet,n}, K[e_{\bullet,\mathrm{n}}]) \tag{25}$$

that is a prefix of the original reduction $(H, e) \overset{*}{\rightarrow}_L (H', e') \not\rightarrow_L$.

There exists such an integer n because we can choose n = 0. Moreover, there is an upper bound on such integers n because the original reduction is terminating and thus has finite length. Also, since $(H_\bullet, K[e_\bullet]) \overset{*}{\rightarrow}_L (H_{\bullet,n}, K[e_{\bullet,\mathrm{n}}])$, by Lemma 4.1, $(H_\bullet, e_\bullet) \overset{*}{\rightarrow}_L (H_{\bullet,n}, e_{\bullet,\mathrm{n}})$. There are two cases:

(1) This prefix is the entire reduction $(H, e) \overset{*}{\rightarrow}_L (H', e') \not\rightarrow_L$, implying that $H' = H_{\bullet,n}$ and $e' = K[e_{\bullet,\mathrm{n}}]$. Thus, $(H_{\bullet,n}, K[e_{\bullet,\mathrm{n}}]) \not\rightarrow_L$, so by Lemma 4.2, $(H_{\bullet,n}, e_{\bullet,\mathrm{n}}) \not\rightarrow_{L \cup FL(K[\cdot])}$. Thus, choosing $H'_\bullet = H_{\bullet,n}$ and $e'_\bullet = e_{\bullet,\mathrm{n}}$ suffices to finish the proof.

(2) This prefix is not the entire reduction, so $(H, e) \overset{*}{\rightarrow}_L (H_{\bullet,n}, K[e_{\bullet,\mathrm{n}}]) \rightarrow_L (H'', e'')$ is also a prefix of the original reduction. e'' can not be of the form $K[e''']$ because if it were, then we could choose $H_{\bullet,n+1} = H''$ and $e_{\bullet,\mathrm{n+1}} = e''$ to create a longer reduction of the form (25), which would contradict the maximality of n. Ergo, if $(H_{\bullet,n}, e_{\bullet,\mathrm{n}})$ were not irreducible under $\rightarrow_{L \cup FL(K[\cdot])}$, that would contradict Lemma 4.2. Thus, $(H_{\bullet,n}, e_{\bullet,\mathrm{n}}) \not\rightarrow_{L \cup FL(K[\cdot])}$, so choosing $H'_\bullet = H_{\bullet,n}$ and $e'_\bullet = e_{\bullet,\mathrm{n}}$ suffices to finish the proof.

□

Note that when applying Lemma 4.3, we sometimes leave K implicit and we often write "$e'_{\bullet}$" as "v", even though it must actually be proven to be a value.

Moreover, in the proofs of the compatibility lemma, we are often given that $(H, e) \overset{*}{\rightarrow}_L (H_1, v_1) \nrightarrow$ and then we apply Lemma 4.3, possibly multiple times, to show a reduction $(H, e) \overset{*}{\rightarrow}_L (H', v') \nrightarrow$ for some other configuration (H', v'). We then conclude that $(H_1, v_1) = (H', v')$ because, even though $\rightarrow_L$ is not confluent, we implicitly deduce that since we applied Lemma 4.3, the reduction $(H, e) \overset{*}{\rightarrow}_L (H', v') \nrightarrow$ is a prefix of the original given reduction $(H, e) \overset{*}{\rightarrow}_L (H_1, v_1) \nrightarrow$.

4.2 MiniML Source Language

4.2.1 *Syntax.*

$$\begin{array}{lcl}
\text{Type } \tau & := & \alpha \mid \mathtt{unit} \mid \tau \rightarrow \tau \mid \forall \alpha.\tau \mid \mathtt{ref}\ \tau \mid \langle \tau \rangle \\
\text{Expression } e & := & x \mid () \mid \lambda x : \tau.e \mid \Lambda \alpha.e \mid e\ e \mid e\ [\tau] \mid \mathtt{ref}\ e \mid !e \mid e := e \mid \llparenthesis e \rrparenthesis_\tau
\end{array}$$

4.2.2 *Statics.* $\boxed{\Delta; \Gamma; \Delta; \Gamma \vdash e : \tau}$

$$\frac{x : \tau \in \Gamma}{\Delta; !\Gamma; \Delta; \Gamma \vdash x : \tau} \qquad \frac{}{\Delta; !\Gamma; \Delta; \Gamma \vdash () : \mathtt{unit}} \qquad \frac{\Delta; !\Gamma; \Delta; \Gamma, x : \tau_1 \vdash e : \tau_2}{\Delta; !\Gamma; \Delta; \Gamma \vdash \lambda x : \tau_1.e : \tau_1 \rightarrow \tau_2}$$

$$\frac{\Delta; !\Gamma; \Delta; \Gamma \vdash e_1 : \tau_1 \rightarrow \tau_2 \qquad \Delta; !\Gamma; \Delta; \Gamma \vdash e_2 : \tau_1}{\Delta; !\Gamma; \Delta; \Gamma \vdash e_1\ e_2 : \tau_2} \qquad \frac{\Delta; !\Gamma; \Delta, \alpha; \Gamma \vdash e : \tau}{\Delta; !\Gamma; \Delta; \Gamma \vdash \Lambda \alpha.e : \forall \alpha.\tau}$$

$$\frac{\Delta; !\Gamma; \Delta; \Gamma \vdash e : \forall \alpha.\tau_2}{\Delta; !\Gamma; \Delta; \Gamma \vdash e\ [\tau_1] : [\alpha \mapsto \tau_1]\tau_2} \qquad \frac{\Delta; !\Gamma; \Delta; \Gamma \vdash e : \tau}{\Delta; !\Gamma; \Delta; \Gamma \vdash \mathtt{ref}\ e : \mathtt{ref}\ \tau} \qquad \frac{\Delta; !\Gamma; \Delta; \Gamma \vdash e : \mathtt{ref}\ \tau}{\Delta; !\Gamma; \Delta; \Gamma \vdash !e : \tau}$$

$$\frac{\Delta; !\Gamma; \Delta; \Gamma \vdash e_1 : \mathtt{ref}\ \tau \qquad \Delta; !\Gamma; \Delta; \Gamma \vdash e_2 : \tau}{\Delta; !\Gamma; \Delta; \Gamma \vdash e_1 := e_2 : \mathtt{unit}} \qquad \frac{\Delta; \Gamma; \Delta; !\Gamma \vdash e : \tau \qquad \tau\ \tau}{\Delta; !\Gamma; \Delta; \Gamma \vdash \llparenthesis e \rrparenthesis_\tau : \tau}$$

4.2.3 *Compiler.*

$$\begin{array}{lcl}
x & \rightsquigarrow & x \\
() & \rightsquigarrow & () \\
\lambda x : \tau.e & \rightsquigarrow & \lambda x.e^+ \\
e_1 e_2 & \rightsquigarrow & {e_1}^+ {e_2}^+ \\
\Lambda \alpha.e & \rightsquigarrow & \lambda\_.e^+ \\
e\ [\tau] & \rightsquigarrow & e^+() \\
\mathtt{ref}\ e & \rightsquigarrow & \text{let } \_ = \text{callgc in ref } e^+ \\
!e & \rightsquigarrow & !e^+ \\
e_1 := e_2 & \rightsquigarrow & {e_1}^+ := {e_2}^+ \\
\llparenthesis e \rrparenthesis_\tau & \rightsquigarrow & C_{\tau \mapsto \tau}(e^+)
\end{array}$$

4.3 L^3 Source Language

4.3.1 Syntax.

$$\begin{array}{lcl}
\text{Type } \tau & := & \mathrm{unit} \mid \mathrm{bool} \mid \tau \otimes \tau \mid \tau \multimap \tau \mid !\tau \mid \mathrm{ptr}\,\zeta \mid \mathrm{cap}\,\zeta\,\tau \mid \forall \zeta.\tau \mid \exists \zeta.\tau \\
\text{Value } \mathrm{v} & := & \lambda \mathrm{x} : \tau.\mathrm{e} \mid () \mid \mathbb{B} \mid (\mathrm{v}, \mathrm{v}) \mid !\mathrm{v} \mid \Lambda \zeta.\mathrm{e} \mid \ulcorner \zeta,\ \mathrm{v} \urcorner \\
\text{Expression } \mathrm{e} & := & \mathrm{v} \mid \mathrm{x} \mid (\mathrm{e},\ \mathrm{e}) \\
 & & \mid \mathrm{e}\ \mathrm{e} \mid \mathrm{let}\ ()\ =\ \mathrm{e}\ \mathrm{in}\ \mathrm{e} \mid \mathrm{if}\ \mathrm{e}\ \mathrm{e}\ \mathrm{e} \mid \mathrm{let}\ (\mathrm{x},\ \mathrm{x})\ =\ \mathrm{e}\ \mathrm{in}\ \mathrm{e} \mid \mathrm{let}\ !\mathrm{x}\ =\ \mathrm{e}\ \mathrm{in}\ \mathrm{e} \\
 & & \mid \mathrm{dupl}\ \mathrm{e} \mid \mathrm{drop}\ \mathrm{e} \mid \mathrm{new}\ \mathrm{e} \mid \mathrm{free}\ \mathrm{e} \mid \mathrm{swap}\ \mathrm{e}\ \mathrm{e}\ \mathrm{e} \\
 & & \mid \mathrm{e}\ [\zeta] \mid \ulcorner \zeta,\ \mathrm{e} \urcorner \mid \mathrm{let}\ \ulcorner \zeta,\ \mathrm{x} \urcorner\ =\ \mathrm{e}\ \mathrm{in}\ \mathrm{e} \\
 & & \mid (\!|\mathsf{e}|\!)_{\tau} \\
\textsc{Duplicable} & := & \mathrm{unit} \mid \mathrm{bool} \mid \mathrm{ptr}\,\zeta \mid !\tau
\end{array}$$

4.3.2 *Statics.* $\boxed{\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{e} : \tau}$

$$\dfrac{}{\Delta; \Gamma; \Delta; \mathrm{x} : \tau \vdash \mathrm{x} : \tau} \qquad \dfrac{\Delta; \Gamma; \Delta; \Gamma, \mathrm{x} : \tau_1 \vdash \mathrm{e} : \tau_2}{\Delta; \Gamma; \Delta; \Gamma \vdash \lambda \mathrm{x} : \tau_1 \mathrm{e} : \tau_1 \multimap \tau_2}$$

$$\dfrac{\Delta; \Gamma; \Delta; \Gamma_1 \vdash \mathrm{e}_1 : \tau_1 \multimap \tau_2 \qquad \Delta; \Gamma; \Delta; \Gamma_2 \vdash \mathrm{e}_2 : \tau_1}{\Delta; \Gamma; \Delta; \Gamma_1 \uplus \Gamma_2 \vdash \mathrm{e}_1\ \mathrm{e}_2 : \tau_2} \qquad \dfrac{}{\Delta; \Gamma; \Delta; \emptyset \vdash () : \mathrm{unit}}$$

$$\dfrac{\Delta; \Gamma; \Delta; \Gamma_1 \vdash \mathrm{e}_1 : \mathrm{unit} \qquad \Delta; \Gamma; \Delta; \Gamma_2 \vdash \mathrm{e}_2 : \tau}{\Delta; \Gamma; \Delta; \Gamma_1 \uplus \Gamma_2 \vdash \mathrm{let}\ ()\ = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_1 : \tau} \qquad \dfrac{}{\Delta; \Gamma; \Delta; \emptyset \vdash \mathbb{B} : \mathrm{bool}}$$

$$\dfrac{\Delta; \Gamma; \Delta; \Gamma_1 \vdash \mathrm{e}_1 : \mathrm{bool} \qquad \Delta; \Gamma; \Delta; \Gamma_2 \vdash \mathrm{e}_2 : \tau \qquad \Delta; \Gamma; \Delta; \Gamma_2 \vdash \mathrm{e}_3 : \tau}{\Delta; \Gamma; \Delta; \Gamma_1 \uplus \Gamma_2 \vdash \mathrm{if}\ \mathrm{e}_1\ \mathrm{e}_2\ \mathrm{e}_3 : \tau}$$

$$\dfrac{\Delta; \Gamma; \Delta; \Gamma_1 \vdash \mathrm{e}_1 : \tau_1 \qquad \Delta; \Gamma; \Delta; \Gamma_2 \vdash \mathrm{e}_2 : \tau_2}{\Delta; \Gamma; \Delta; \Gamma_1 \uplus \Gamma_2 \vdash (\mathrm{e}_1,\ \mathrm{e}_2) : \tau_1 \otimes \tau_2}$$

$$\dfrac{\Delta; \Gamma; \Delta; \Gamma_1 \vdash \mathrm{e}_1 : \tau_1 \otimes \tau_2 \qquad \Delta; \Gamma; \Delta; \Gamma_2, \mathrm{x}_1 : \tau_1, \mathrm{x}_2 : \tau_2 \vdash \mathrm{e}_2 : \tau}{\Delta; \Gamma; \Delta; \Gamma_1 \uplus \Gamma_2 \vdash \mathrm{let}\ (\mathrm{x}_1,\ \mathrm{x}_2)\ = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 : \tau} \qquad \dfrac{\Delta; \Gamma; \Delta; !\Gamma \vdash \mathrm{v} : \tau}{\Delta; \Gamma; \Delta; !\Gamma \vdash !\mathrm{v} : !\tau}$$

$$\dfrac{\Delta; \Gamma; \Delta; \Gamma_1 \vdash \mathrm{e}_1 : !\tau_1 \qquad \Delta; \Gamma; \Delta; \Gamma_2, \mathrm{x} : \tau_1 \vdash \mathrm{e}_2 : \tau_2}{\Delta; \Gamma; \Delta; \Gamma_1 \uplus \Gamma_2 \vdash \mathrm{let}\ !\mathrm{x}\ = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 : \tau_2} \qquad \dfrac{\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{e} : !\tau}{\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{dupl}\ \mathrm{e} : !\tau \otimes !\tau}$$

$$\dfrac{\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{e} : !\tau}{\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{drop}\ \mathrm{e} : \mathrm{unit}} \qquad \dfrac{\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{e} : \tau}{\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{new}\ \mathrm{e} : \exists \zeta.\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta}$$

$$\dfrac{\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{e} : \exists \zeta.\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta}{\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{free}\ \mathrm{e} : \exists \zeta.\tau}$$

$$\dfrac{\Delta; \Gamma; \Delta; \Gamma_1 \vdash \mathrm{e}_1 : \mathrm{cap}\ \zeta\ \tau_1 \qquad \Delta; \Gamma; \Delta; \Gamma_2 \vdash \mathrm{e}_2 : \mathrm{ptr}\ \zeta \qquad \Delta; \Gamma; \Delta; \Gamma_3 \vdash \mathrm{e}_3 : \tau_3}{\Delta; \Gamma; \Delta; \Gamma_1 \uplus \Gamma_2 \uplus \Gamma_3 \vdash \mathrm{swap}\ \mathrm{e}_1\ \mathrm{e}_2\ \mathrm{e}_3 : \mathrm{cap}\ \zeta\ \tau_3\ \otimes\ \tau_1}$$

$$\dfrac{\Delta; \Gamma; \Delta, \zeta; \Gamma \vdash \mathrm{e} : \tau}{\Delta; \Gamma; \Delta; \Gamma \vdash \Lambda \zeta.\mathrm{e} : \forall \zeta.\tau} \qquad \dfrac{\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{e} : \forall \zeta.\tau \qquad \zeta' \in \Delta}{\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{e}\ [\zeta'] : [\zeta \mapsto \zeta']\tau}$$

$$\dfrac{\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{e} : [\zeta \mapsto \zeta']\tau \qquad \zeta' \in \Delta}{\Delta; \Gamma; \Delta; \Gamma \vdash \ulcorner \zeta',\ \mathrm{e} \urcorner : \exists \zeta.\tau}$$

$$\dfrac{\Delta; \Gamma; \Delta; \Gamma_1 \vdash \mathrm{e}_1 : \exists \zeta.\tau_1 \qquad \Delta; \Gamma; \Delta, \zeta; \Gamma_2, \mathrm{x} : \tau_1 \vdash \mathrm{e}_2 : \tau_2 \qquad \mathit{FLV}(\tau_2) \subseteq \Delta}{\Delta; \Gamma; \Delta; \Gamma_1 \vdash \mathrm{let}\ \ulcorner \zeta,\ \mathrm{x} \urcorner\ =\ \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2}$$

$$\dfrac{\Delta; !\Gamma; \Delta; \Gamma \vdash \mathrm{e} : \tau \qquad \tau \sim \tau}{\Delta; \Gamma; \Delta; !\Gamma \vdash (\!|\mathrm{e}|\!)_{\tau} : \tau}$$

4.3.3 *Compiler.*

$$
\begin{aligned}
&x &&\rightsquigarrow\quad x\\
&\lambda x : \tau.e &&\rightsquigarrow\quad \lambda x.e^{+}\\
&e_1\ e_2 &&\rightsquigarrow\quad {e_1}^{+}\ {e_2}^{+}\\
&() &&\rightsquigarrow\quad ()\\
&\text{let } () \ = e_1 \text{ in } e_2 &&\rightsquigarrow\quad \text{let } \_ = {e_1}^{+} \text{ in } {e_2}^{+}\\
&\text{true} &&\rightsquigarrow\quad 0\\
&\text{false} &&\rightsquigarrow\quad 1\\
&\text{if } e_1\ e_2\ e_3 &&\rightsquigarrow\quad \text{if } {e_1}^{+}\ {e_2}^{+}\ {e_3}^{+}\\
&(e_1,\ e_2) &&\rightsquigarrow\quad ({e_1}^{+},\ {e_2}^{+})\\
&\text{let } (x_1,\ x_2) \ = e_1 \text{ in } e_2 &&\rightsquigarrow\quad \text{let } p = {e_1}^{+} \text{ in let } x_1 = \text{fst } p \text{ in let } x_2 = \text{snd } p \text{ in } {e_2}^{+}\\
&!v &&\rightsquigarrow\quad v^{+}\\
&\text{let } !x = e_1 \text{ in } e_2 &&\rightsquigarrow\quad \text{let } x = {e_1}^{+} \text{ in } {e_2}^{+}\\
&\text{dupl } e &&\rightsquigarrow\quad \text{let } x = e^{+} \text{ in } (x,\ x)\\
&\text{drop } e &&\rightsquigarrow\quad \text{let } \_ = e^{+} \text{ in } ()\\
&\text{new } e &&\rightsquigarrow\quad \text{let } \_ = \text{callgc in let } x_{\ell} = \text{alloc } e^{+} \text{ in } ((),\ x_{\ell})\\
&\text{free } e &&\rightsquigarrow\quad \text{let } x = e^{+} \text{ in let } x_r =!(\text{snd } x) \text{ in let } \_ = \text{free } (\text{snd } x) \text{ in } x_r\\
&\text{swap } e_c\ e_p\ e_v &&\rightsquigarrow\quad \text{let } x_p = {e_p}^{+} \text{ in let } \_ = e_c \text{ in let } x_{v'} = !x_p \text{ in let } \_ = (x_p := {e_v}^{+}) \text{ in } ((), x_{v'})\\
&\Lambda\zeta.e &&\rightsquigarrow\quad \lambda\_.e^{+}\\
&e\ [\zeta] &&\rightsquigarrow\quad e^{+}\ ()\\
&\ulcorner\zeta,\ e\urcorner &&\rightsquigarrow\quad e^{+}\\
&\text{let } \ulcorner\zeta,\ x\urcorner = e_1 \text{ in } e_2 &&\rightsquigarrow\quad \text{let } x = {e_1}^{+} \text{ in } {e_2}^{+}\\
&\llparenthesis e \rrparenthesis_{\tau} &&\rightsquigarrow\quad C_{\tau \mapsto \tau}(e^{+})
\end{aligned}
$$

4.4 Logical Relation

4.4.1 Worlds. A world W is drawn from:

$$World_n = \{(k, \Psi) \mid k < n \wedge \Psi \subset HeapTy_k \wedge \text{dom}(\Psi) \text{ is a bijection}\}$$

$$World = \bigcup_n World_n$$

where k is the step index and Ψ is a heap typing.
This heap typing has the following shape:

$$HeapTy_n = \{(\ell_1, \ell_2) \mapsto Typ_n, \ldots\}$$

where ℓ are heap locations.

$$
\begin{aligned}
Atom_n = \{(W, (H_1, e_1), (H_2, e_2)) \mid \quad & W \in World_n \wedge \text{dom}(H_1)\#\text{dom}((W.\Psi)^1) \wedge \text{dom}(H_2)\#\text{dom}((W.\Psi)^2)\\
& \wedge H_1 : MHeap \wedge H_2 : MHeap\}
\end{aligned}
$$

H_1 and H_2 represent the manually managed locations owned by e_1 and e_2, respectively. As stated in the definition above, none of the locations in H_1, H_2 can be in the world and all locations in H_1, H_2 must be manually managed.

$$AtomVal_n = \{(W, (H_1, v_1), (H_2, v_2)) \in Atom_n\}$$

$$Atom = \bigcup_n Atom_n$$

$$AtomVal = \bigcup_n AtomVal_n$$

Restrictions. We define restriction based on indexing over relations as:

$$\lfloor R \rfloor_j = \{(W, (\mathsf{H}_1, \mathsf{e}_1), (\mathsf{H}_2, \mathsf{e}_2)) \mid (W, (\mathsf{H}_1, \mathsf{e}_1), (\mathsf{H}_2, \mathsf{e}_2)) \in R \land W.k < j\}$$

$$\lfloor \Psi \rfloor_j = \{(\ell_1, \ell_2) \mapsto \lfloor R \rfloor_j \mid (\ell_1, \ell_2) \mapsto R \in \Psi\}$$

Later. We define a $\triangleright$ (later) modality defined as restricting the index to the current one, which forces the worlds "forward" one step (as it cuts out everything with the current step index). On a world W, $\triangleright W = (W.k - 1, \lfloor W.\Psi \rfloor_{W.k-1})$.

Heaps. A heap H is:

$$\mathsf{H} = \{\ell \overset{m}{\mapsto} \mathsf{v}, \dots\} \uplus \{\ell \overset{gc}{\mapsto} \mathsf{v}, \dots\}$$

And we define when a pair of heaps $\mathsf{H}_1, \mathsf{H}_2$ satisfy a world as $\mathsf{H}_1, \mathsf{H}_2 : W$:

$$\begin{array}{l} \mathsf{H}_1 : GCHeap \land \mathsf{H}_2 : GCHeap \land \\ \forall (\ell_1, \ell_2) \mapsto R \in W.\Psi.\ \exists \mathsf{v}_1, \mathsf{v}_2.\ell_1 \overset{gc}{\mapsto} \mathsf{v}_1 \in \mathsf{H}_1 \land \ell_2 \overset{gc}{\mapsto} \mathsf{v}_2 \in \mathsf{H}_2 \land (\triangleright W, (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in R \end{array}$$

i.e., locations must point to closed values that are in the relation specified by the heap typing. Notice that these locations must be garbage-collectable.

World Extension. In $Atom$, the tuple $(W, (\mathsf{H}_1, \mathsf{e}_1), (\mathsf{H}_2, \mathsf{e}_2))$ contains manually managed locations owned by the heaps in $\mathsf{H}_1, \mathsf{H}_2$ and garbage-collectable locations in the world W. Moreover, $\mathsf{e}_1, \mathsf{e}_2$ contain locations that are reachable which must remain valid and not be garbage-collected for the tuple to still be well-defined. Therefore, to define world extension, we must index world extension both by the sets of locations owned by $\mathsf{H}_1, \mathsf{H}_2$ and the sets of locations reachable from e_1 and e_2.

Let $\mathbb{L}$ denote a pair of sets of locations and η denote a bijection of locations. For any worlds $(k, \Psi), (j, \Psi') \in World$, if $\mathbb{L}.1 \# \mathrm{dom}(\Psi^1)$, $\mathbb{L}.2 \# \mathrm{dom}(\Psi^2)$, and $\eta \subseteq \mathrm{dom}(\Psi)$, we define that (j, Ψ') *is a world extension of* (k, Ψ) *while avoiding* $\mathbb{L}$ *and preserving* η, denoted by $(k, \Psi) \sqsubseteq_{\mathbb{L},\eta} (j, \Psi')$, when:

$$\begin{array}{l} j \leq k \\ \land\ \mathbb{L}.1 \# \mathrm{dom}((\Psi')^1) \land \mathbb{L}.2 \# \mathrm{dom}((\Psi')^2) \\ \land\ \forall (\ell_1, \ell_2) \in \eta. \Psi'(\ell_1, \ell_2) = \lfloor \Psi(\ell_1, \ell_2) \rfloor_j \end{array}$$

We also define a strict version, that requires that the step index actually decreased:

$$W_1 \sqsubset_{\mathbb{L},\eta} W_2 \triangleq W_1.k > W_2.k \land W_1 \sqsubseteq_{\mathbb{L},\eta} W_2$$

For any set of locations L_1, L_2, let $\mathrm{rchgclocs}(W, L_1, L_2)$ be the subset of pairs of locations in $\mathrm{dom}(W.\Psi)$ whose first component is in L_1 and whose second component is in L_2.

Then, we define a shorthand notation for world extension indexed by heaps and expressions, since $\mathbb{L}.1, \mathbb{L}.2$ are usually domains of heaps and η^1, η^2 are usually sets of free locations in expressions:

$$W_1 \mathrel{\dot{\sqsubseteq}}_{\mathsf{H}_1,\mathsf{H}_2,\mathsf{e}_1,\mathsf{e}_2} W_2 \triangleq W_1 \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_1),\mathrm{dom}(\mathsf{H}_2)),\eta} W_2$$

where

$$\eta = \mathrm{rchgclocs}(W_1, FL(\mathrm{cod}(\mathsf{H}_1)) \cup FL(\mathsf{e}_1), FL(\mathrm{cod}(\mathsf{H}_2)) \cup FL(\mathsf{e}_2))$$

Finally, we define *Typ* in terms of world extension as follows:

$$\begin{aligned} Typ_n &= \{R \in 2^{AtomVal_n} \mid \forall (W, (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in R.\ \forall W'.\ W \mathrel{\dot{\sqsubseteq}}_{\mathsf{H}_1,\mathsf{H}_2,\mathsf{v}_1,\mathsf{v}_2} W' \\ &\qquad\qquad \implies (W', (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in R\} \\ Typ &= \{R \in 2^{AtomVal} \mid \forall k. \lfloor R \rfloor_k \in Typ_k\} \end{aligned}$$

4.4.2 Expression Relation.

$$\begin{aligned} \mathcal{E}\llbracket\tau\rrbracket_\rho \quad = \quad & \{(W, (\mathsf{H}_1, \mathsf{e}_1), (\mathsf{H}_2, \mathsf{e}_2)) \mid \\ & \quad \forall L_1, L_2, \mathsf{v}_1, \mathsf{H}_{1g+}, \mathsf{H}_{2g+} : W, \mathsf{H}_{1+} : MHeap, \mathsf{H}_{1*}. \\ & \quad (\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{e}_1) \overset{*}{\longrightarrow}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \twoheadrightarrow_{L_1} \\ & \quad \implies \exists \mathsf{H}'_1, \mathsf{H}'_{1g}. \forall \mathsf{H}_{2+} : MHeap. \exists \mathsf{H}'_2, W', \mathsf{H}'_{2g}, \mathsf{v}_2. \\ & \qquad \mathsf{H}_{1*} = \mathsf{H}'_{1g} \uplus \mathsf{H}'_1 \uplus \mathsf{H}_{1+} \ \wedge \mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W' \ \wedge \\ & \qquad W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W, L_1 \cup FL(\mathrm{cod}(\mathsf{H}_{1+})), L_2 \cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W' \ \wedge \\ & \qquad (W', (\mathsf{H}'_1, \mathsf{v}_1), (\mathsf{H}'_2, \mathsf{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho \ \wedge \\ & \qquad (\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \mathsf{e}_2) \overset{*}{\longrightarrow}_{L_2} (\mathsf{H}'_{2g} \uplus \mathsf{H}'_2 \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \twoheadrightarrow_{L_2} \\ & \qquad \wedge\ \mathsf{H}_{1'} = \mathsf{H}_{2'} = \emptyset\} \end{aligned}$$

Note that the parts highlighted in `MiniML` colors only apply to types τ from `MiniML`, not types τ from $\mathbf{L^3}$.

4.4.3 Value Relation.

$$\begin{aligned} \mathcal{V}\llbracket\alpha\rrbracket_\rho \quad &= \quad \rho.\mathsf{F}(\alpha) \\ \mathcal{V}\llbracket\mathtt{unit}\rrbracket_\rho \quad &= \quad \{(W, (\emptyset, ()), (\emptyset, ()))\} \\ \mathcal{V}\llbracket\tau_1 \to \tau_2\rrbracket_\rho \quad &= \quad \{(W, (\emptyset, \lambda \mathsf{x}_1.\mathsf{e}_1), (\emptyset, \lambda \mathsf{x}_2.\mathsf{e}_2)) \mid \\ & \qquad \forall W', \mathsf{v}_1, \mathsf{v}_2. W \mathrel{\dot{\sqsubseteq}}_{\emptyset,\emptyset,\mathsf{e}_1,\mathsf{e}_2} W' \wedge (W', (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}\llbracket\tau_1\rrbracket_\rho \implies \\ & \qquad\quad (W', (\emptyset, [\mathsf{x}_1 \mapsto \mathsf{v}_1]\mathsf{e}_1), (\emptyset, [\mathsf{x}_2 \mapsto \mathsf{v}_2]\mathsf{e}_2)) \in \mathcal{E}\llbracket\tau_2\rrbracket_\rho\} \\ \mathcal{V}\llbracket\forall\alpha.\tau\rrbracket_\rho \quad &= \quad \{(W, (\emptyset, \lambda_.\mathsf{e}_1), (\emptyset, \lambda_.\mathsf{e}_2)) \mid \\ & \qquad \forall R \in RelT, W'. W \mathrel{\dot{\sqsubset}}_{\emptyset,\emptyset,\mathsf{e}_1,\mathsf{e}_2} W' \implies (W', (\emptyset, \mathsf{e}_1), (\emptyset, \mathsf{e}_2)) \in \mathcal{E}\llbracket\tau\rrbracket_{\rho[\mathsf{F}(\alpha) \mapsto R]}\} \\ \mathcal{V}\llbracket\mathtt{ref}\ \tau\rrbracket_\rho \quad &= \quad \{(W, (\emptyset, \ell_1), (\emptyset, \ell_2)) \mid W.\Psi(\ell_1, \ell_2) = \lfloor \mathcal{V}\llbracket\tau\rrbracket_\rho \rfloor_{W.k}\} \\ \mathcal{V}\llbracket\langle\tau\rangle\rrbracket_\rho \quad &= \quad \mathcal{V}\llbracket\tau\rrbracket_\rho \\ \mathcal{V}\llbracket\mathrm{unit}\rrbracket_\rho \quad &= \quad \{(W, (\emptyset, ()), (\emptyset, ()))\} \\ \mathcal{V}\llbracket\mathrm{bool}\rrbracket_\rho \quad &= \quad \{(W, (\emptyset, \mathsf{b}), (\emptyset, \mathsf{b})) \mid \mathsf{b} \in \{0, 1\}\} \\ \mathcal{V}\llbracket\tau_1 \otimes \tau_2\rrbracket_\rho \quad &= \quad \{(W, (\mathsf{H}_{1l} \uplus \mathsf{H}_{1r}, (\mathsf{v}_{1\mathsf{l}}, \mathsf{v}_{1\mathsf{r}})), (\mathsf{H}_{2l} \uplus \mathsf{H}_{2r}, (\mathsf{v}_{2\mathsf{l}}, \mathsf{v}_{2\mathsf{r}}))) \mid \\ & \qquad (W, (\mathsf{H}_{1l}, \mathsf{v}_{1\mathsf{l}}), (\mathsf{H}_{2l}, \mathsf{v}_{2\mathsf{l}})) \in \mathcal{V}\llbracket\tau_1\rrbracket_\rho \wedge \\ & \qquad (W, (\mathsf{H}_{1r}, \mathsf{v}_{1\mathsf{r}}), (\mathsf{H}_{2r}, \mathsf{v}_{2\mathsf{r}})) \in \mathcal{V}\llbracket\tau_2\rrbracket_\rho\} \\ \mathcal{V}\llbracket\tau_1 \multimap \tau_2\rrbracket_\rho \quad &= \quad \{(W, (\mathsf{H}_1, \lambda \mathsf{x}_1.\mathsf{e}_1), (\mathsf{H}_2, \lambda \mathsf{x}_2.\mathsf{e}_2)) \mid \forall W', \mathsf{H}_{1v}, \mathsf{v}_1, \mathsf{H}_{2v}, \mathsf{v}_2. \\ & \qquad W \mathrel{\dot{\sqsubseteq}}_{\mathsf{H}_1,\mathsf{H}_2,\mathsf{e}_1,\mathsf{e}_2} W' \wedge (W', (\mathsf{H}_{1v}, \mathsf{v}_1), (\mathsf{H}_{2v}, \mathsf{v}_2)) \in \mathcal{V}\llbracket\tau_1\rrbracket_\rho \\ & \qquad \implies (W', (\mathsf{H}_1 \uplus \mathsf{H}_{1v}, [\mathsf{x}_1 \mapsto \mathsf{v}_1]\mathsf{e}_1), (\mathsf{H}_2 \uplus \mathsf{H}_{2v}, [\mathsf{x}_2 \mapsto \mathsf{v}_2]\mathsf{e}_2)) \in \mathcal{E}\llbracket\tau_2\rrbracket_\rho\} \\ \mathcal{V}\llbracket!\tau\rrbracket_\rho \quad &= \quad \{(W, (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \mid (W, (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho\} \\ \mathcal{V}\llbracket\mathrm{ptr}\ \zeta\rrbracket_\rho \quad &= \quad \{(W, (\emptyset, \ell_1), (\emptyset, \ell_2)) \mid \rho.\mathrm{L3}(\zeta) = (\ell_1, \ell_2)\} \\ \mathcal{V}\llbracket\mathrm{cap}\ \zeta\ \tau\rrbracket_\rho \quad &= \quad \{(W, (\mathsf{H}_1 \uplus \{\ell_1 \mapsto \mathsf{v}_1\}, ()), (\mathsf{H}_2 \uplus \{\ell_2 \mapsto \mathsf{v}_2\}, ())) \mid \\ & \qquad \rho.\mathrm{L3}(\zeta) = (\ell_1, \ell_2) \wedge (W, (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho\} \\ \mathcal{V}\llbracket\forall\zeta.\tau\rrbracket_\rho \quad &= \quad \{(W, (\mathsf{H}_1, \lambda_.\mathsf{e}_1), (\mathsf{H}_2, \lambda_.\mathsf{e}_2)) \mid \forall \ell_1 \ell_2. (W, (\mathsf{H}_1, \mathsf{e}_1), (\mathsf{H}_2, \mathsf{e}_2)) \in \mathcal{E}\llbracket\tau\rrbracket_{\rho[\mathrm{L3}(\zeta) \mapsto (\ell_1, \ell_2)]}\} \\ \mathcal{V}\llbracket\exists\zeta.\tau\rrbracket_\rho \quad &= \quad \{(W, (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2) \mid \exists \ell_1 \ell_2. (W, (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_{\rho[\mathrm{L3}(\zeta) \mapsto (\ell_1, \ell_2)]}\} \end{aligned}$$

4.4.4 Extending to Open Terms.

$$\begin{array}{lcl}
\mathcal{G}\llbracket\cdot\rrbracket_\rho & = & \{(W,\cdot)\} \\
\mathcal{G}\llbracket\Gamma, \mathrm{x} : \tau\rrbracket_\rho & = & \{(W, \gamma[\mathrm{x} \mapsto (\mathrm{v}_1, \mathrm{v}_2)]) \mid (W,\gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho\} \\
\mathcal{G}\llbracket\cdot\rrbracket_\rho & = & \{(W, \emptyset, \emptyset, \cdot)\} \\
\mathcal{G}\llbracket\Gamma, \mathrm{x} : \tau\rrbracket_\rho & = & \{(W, \mathrm{H}_1 \uplus \mathrm{H}_{1x}, \mathrm{H}_2 \uplus \mathrm{H}_{2x}, \gamma[\mathrm{x} \mapsto (\mathrm{v}_1, \mathrm{v}_2)]) \mid \\
 & & \quad (W, \mathrm{H}_1, \mathrm{H}_2, \gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, (\mathrm{H}_{1x}, \mathrm{v}_1), (\mathrm{H}_{2x}, \mathrm{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho\} \\
\mathcal{D}\llbracket\cdot\rrbracket & = & \{\cdot\} \\
\mathcal{D}\llbracket\Delta, \alpha\rrbracket & = & \{\rho[\alpha \mapsto R] \mid \rho \in \mathcal{D}\llbracket\Delta\rrbracket \wedge R \in \mathit{RelT}\} \\
\mathcal{D}\llbracket\Delta, \zeta\rrbracket & = & \{\rho[\zeta \mapsto (\ell_1, \ell_2)] \mid \rho \in \mathcal{D}\llbracket\Delta\rrbracket\}
\end{array}$$

$$\begin{array}{lcl}
\Delta;\Gamma;\Delta;\Gamma \vdash \mathrm{e}_1 \preceq \mathrm{e}_2 : \tau & \equiv & \forall \rho, \gamma_{\mathrm{L}}, \gamma_{\Gamma}, W. \\
 & & \quad \rho.\mathrm{L3} \in \mathcal{D}\llbracket\Delta\rrbracket \wedge \rho.\mathrm{F} \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \emptyset, \emptyset, \gamma_{\mathrm{L}}) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, \gamma_{\Gamma}) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \\
 & & \quad \Longrightarrow (W, (\emptyset, \gamma_{\mathrm{L}}^1(\gamma_{\Gamma}^1(\mathrm{e}_1{}^+))), (\emptyset, \gamma_{\mathrm{L}}^2(\gamma_{\Gamma}^2(\mathrm{e}_2{}^+)))) \in \mathcal{E}\llbracket\tau\rrbracket_\rho \\
\Delta;\Gamma;\Delta;\Gamma \vdash \mathrm{e}_1 \preceq \mathrm{e}_2 : \tau & \equiv & \forall \rho, \gamma_{\Gamma}, \gamma_{\mathrm{L}}, W, \mathrm{H}_1, \mathrm{H}_2. \\
 & & \quad \rho.\mathrm{F} \in \mathcal{D}\llbracket\Delta\rrbracket \wedge \rho.\mathrm{L3} \in \mathcal{D}\llbracket\Delta\rrbracket \wedge (W, \gamma_{\Gamma}) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \\
 & & \quad \Longrightarrow (W, (\mathrm{H}_1, \gamma_{\mathrm{L}}^1(\gamma_{\Gamma}^1(\mathrm{e}_1{}^+))), (\mathrm{H}_2, \gamma_{\mathrm{L}}^2(\gamma_{\Gamma}^2(\mathrm{e}_2{}^+)))) \in \mathcal{E}\llbracket\tau\rrbracket_\rho
\end{array}$$

4.5 Convertibility

$$\frac{\tau \in \textsc{Duplicable}}{\mathrm{C}_{\langle\tau\rangle\mapsto\tau}, \mathrm{C}_{\tau\mapsto\langle\tau\rangle} : \langle\tau\rangle \sim \tau}$$

$$\frac{}{\mathrm{C}_{\forall\alpha.\alpha \to (\alpha \to \alpha)\mapsto\mathrm{bool}}, \mathrm{C}_{\mathrm{bool}\mapsto\forall\alpha.\alpha \to (\alpha \to \alpha)} : \forall\alpha.\alpha \to (\alpha \to \alpha) \sim \mathrm{bool}}$$

$$\frac{\tau_1 \in \textsc{Duplicable} \qquad \mathrm{C}_{\tau_1\mapsto\tau_1}, \mathrm{C}_{\tau_1\mapsto\tau_1} : \tau_1 \sim \tau_1 \qquad \mathrm{C}_{\tau_2\mapsto\tau_2}, \mathrm{C}_{\tau_2\mapsto\tau_2} : \tau_2 \sim \tau_2}{\mathrm{C}_{\tau_1 \to \tau_2\mapsto!(!\tau_1\multimap\tau_2)}, \mathrm{C}_{!(!\tau_1\multimap\tau_2)\mapsto\tau_1 \to \tau_2} : \tau_1 \to \tau_2 \sim !(!\tau_1 \multimap \tau_2)}$$

$$\frac{\mathrm{C}_{\tau\mapsto\tau}, \mathrm{C}_{\tau\mapsto\tau} : \tau \sim \tau}{\mathrm{C}_{\mathtt{ref}\ \tau\mapsto\exists\zeta.\mathrm{cap}\ \zeta\ \tau\ \otimes\ !\mathrm{ptr}\ \zeta}, \mathrm{C}_{\exists\zeta.\mathrm{cap}\ \zeta\ \tau\ \otimes\ !\mathrm{ptr}\ \zeta\mapsto\mathtt{ref}\ \tau} : \mathtt{ref}\ \tau \sim \exists\zeta.\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta}$$

$$\begin{array}{lcl}
\mathrm{C}_{\langle\tau\rangle\mapsto\tau}\ \mathrm{e} & \triangleq & \mathrm{e} \\
\mathrm{C}_{\tau\mapsto\langle\tau\rangle}\ \mathrm{e} & \triangleq & \mathrm{e} \\
\mathrm{C}_{\forall\alpha.\alpha \to (\alpha \to \alpha)\mapsto\mathrm{bool}}\ \mathrm{e} & \triangleq & \mathrm{let\ f = e\ in\ ((f\ \ ())\ \ 0)\ 1} \\
\mathrm{C}_{\mathrm{bool}\mapsto\forall\alpha.\alpha \to (\alpha \to \alpha)}\ \mathrm{e} & \triangleq & \mathrm{let\ x = e\ in}\ \lambda\_.\lambda \mathrm{t}.\lambda \mathrm{f.if\ x\ t\ f} \\
\mathrm{C}_{\tau_1 \to \tau_2\mapsto!(!\tau_1\multimap\tau_2)}\ \mathrm{e} & \triangleq & \mathrm{let\ f = e\ in}\ \lambda \mathrm{x}.\left(\mathrm{C}_{\tau_2\mapsto\tau_2}\ \left(\mathrm{f}\ \left(\mathrm{C}_{\tau_1\mapsto\tau_1}\ \mathrm{x}\right)\right)\right) \\
\mathrm{C}_{!(!\tau_1\multimap\tau_2)\mapsto\tau_1 \to \tau_2}\ \mathrm{e} & \triangleq & \mathrm{let\ f = e\ in}\ \lambda \mathrm{x}.\left(\mathrm{C}_{\tau_2\mapsto\tau_2}\ \left(\mathrm{f}\ \left(\mathrm{C}_{\tau_1\mapsto\tau_1}\ \mathrm{x}\right)\right)\right) \\
\mathrm{C}_{\mathtt{ref}\ \tau\mapsto\exists\zeta.\mathrm{cap}\ \zeta\ \tau\ \otimes\ !\mathrm{ptr}\ \zeta}\ \mathrm{e} & \triangleq & \mathrm{let\ x}_\ell = \mathrm{alloc\ C}_{\tau\mapsto\tau}(!\mathrm{e})\ \mathrm{in}\ ((), \mathrm{x}_\ell) \\
\mathrm{C}_{\exists\zeta.\mathrm{cap}\ \zeta\ \tau\ \otimes\ !\mathrm{ptr}\ \zeta\mapsto\mathtt{ref}\ \tau}\ \mathrm{e} & \triangleq & \mathrm{let\ x}_\ell = \mathrm{snd\ e\ in\ let}\ \_ = (\mathrm{x}_\ell := \mathrm{C}_{\tau\mapsto\tau}(!\mathrm{x}_\ell))\ \mathrm{in\ gcmov\ x}_\ell
\end{array}$$

Theorem 4.4 (Convertibility Soundness). *If $\tau_A \sim \tau_B$ then for all ρ,*

(1) $\forall(W, (\mathrm{H}_1, \mathrm{e}_1), (\mathrm{H}_2, \mathrm{e}_2)) \in \mathcal{E}\llbracket\tau_A\rrbracket_\rho.\ \left(W, \left(\mathrm{H}_1, \mathrm{C}_{\tau_A\mapsto\tau_B}\ \mathrm{e}_1\right), \left(\mathrm{H}_2, \mathrm{C}_{\tau_A\mapsto\tau_B}\ \mathrm{e}_2\right)\right) \in \mathcal{E}\llbracket\tau_B\rrbracket_\rho$*; and*

(2) $\forall(W, (\mathrm{H}_1, \mathrm{e}_1), (\mathrm{H}_2, \mathrm{e}_2)) \in \mathcal{E}\llbracket\tau_B\rrbracket_\rho.\ \left(W, \left(\mathrm{H}_1, \mathrm{C}_{\tau_B\mapsto\tau_A}\ \mathrm{e}_1\right), \left(\mathrm{H}_2, \mathrm{C}_{\tau_B\mapsto\tau_A}\ \mathrm{e}_2\right)\right) \in \mathcal{E}\llbracket\tau_A\rrbracket_\rho$

Proof. By simultaneous induction on the structure of the convertibility relation.

$\boxed{\langle\tau\rangle \sim \tau}$

(1) We are to show that

$$\forall (W, (\mathrm{H}_1, \mathrm{e}_1), (\mathrm{H}_2, \mathrm{e}_2)) \in \mathcal{E}[\![\langle\tau\rangle]\!]_\rho.\, \Big(W, (\mathrm{H}_1, \mathrm{C}_{\langle\tau\rangle\mapsto\tau}\ \mathrm{e}_1), (\mathrm{H}_2, \mathrm{C}_{\langle\tau\rangle\mapsto\tau}\ \mathrm{e}_2)\Big) \in \mathcal{E}[\![\tau]\!]_\rho$$

Expanding the definition of $\mathrm{C}_{\langle\tau\rangle\mapsto\tau}$, $\mathcal{E}[\![\cdot]\!]_\cdot$ and pushing substitutions in the goal, we are to show that

$$\begin{aligned}&\exists \mathrm{H}_1', \mathrm{H}_{1g}'.\forall \mathrm{H}_{2+} : MHeap.\exists \mathrm{H}_2', W', \mathrm{H}_{2g}', \mathrm{v}_2.\\ &\mathrm{H}_{1*} = \mathrm{H}_{1g}' \uplus \mathrm{H}_1' \uplus \mathrm{H}_{1+}\ \wedge \mathrm{H}_{1g}', \mathrm{H}_{2g'} : W' \wedge\\ &W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W, L_1\cup FL(\mathrm{cod}(\mathrm{H}_{1+})), L_2\cup FL(\mathrm{cod}(\mathrm{H}_{2+})))}\ W' \wedge\\ &(W', (\mathrm{H}_1', \mathrm{v}_1), (\mathrm{H}_2', \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho \wedge\\ &(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathrm{e}_2) \overset{*}{\rightarrow}_{L_2} (\mathrm{H}_{2g}' \uplus \mathrm{H}_2' \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \twoheadrightarrow_{L_2}\end{aligned}$$

given arbitrary $W, L_1, L_2, \mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W, \mathrm{v}_1, \mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_{1+} : MHeap, \mathrm{H}_{1*}$ such that

$$(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \mathrm{e}_1) \overset{*}{\rightarrow}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \not\rightarrow_{L_1}$$

Because $(W, (\mathrm{H}_1, \mathrm{e}_1), (\mathrm{H}_2, \mathrm{e}_2)) \in \mathcal{E}[\![\langle\tau\rangle]\!]_\rho$, we find that $\mathrm{H}_{1*} = \mathrm{H}_{1g}' \uplus \mathrm{H}_{1+}$ and

$$(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathrm{e}_2) \overset{*}{\rightarrow}_{L_2} (\mathrm{H}_{2g}' \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \not\rightarrow_{L_2}$$

where $\mathrm{H}_{1g}', \mathrm{H}_{2g}' : W'$ for some world $W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W, L_1\cup FL(\mathrm{cod}(\mathrm{H}_{1+})), L_2\cup FL(\mathrm{cod}(\mathrm{H}_{2+})))}$ W' such that

$$(W', (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}[\![\langle\tau\rangle]\!]_\rho$$

From here, we can take $W' = W'$, $\mathrm{H}_1' = \emptyset$, $\mathrm{H}_2' = \emptyset$, $\mathrm{H}_{1g}' = \mathrm{H}_{1g}'$, and $\mathrm{H}_{2g}' = \mathrm{H}_{2g}'$. Then, from expanding $(W', (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}[\![\langle\tau\rangle]\!]_\rho$, we find $(W', (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho$, which suffices to finish the proof.

(2) We are to show that

$$\forall (W, (\mathrm{H}_1, \mathrm{e}_1), (\mathrm{H}_2, \mathrm{e}_2)) \in \mathcal{E}[\![\tau]\!]_\rho.\, \Big(W, (\mathrm{H}_1, \mathrm{C}_{\langle\tau\rangle\mapsto\tau}\ \mathrm{e}_1), (\mathrm{H}_2, \mathrm{C}_{\langle\tau\rangle\mapsto\tau}\ \mathrm{e}_2)\Big) \in \mathcal{E}[\![\langle\tau\rangle]\!]_\rho$$

Expanding the definition of $\mathrm{C}_{\langle\tau\rangle\mapsto\tau}$, $\mathcal{E}[\![\cdot]\!]_\cdot$ and pushing substitutions in the goal, we are to show that

$$\begin{aligned}&\exists \mathrm{H}_{1g}'.\forall \mathrm{H}_{2+} : MHeap.\exists W', \mathrm{H}_{2g}', \mathrm{v}_2.\\ &\mathrm{H}_{1*} = \mathrm{H}_{1g}' \uplus \mathrm{H}_1' \uplus \mathrm{H}_{1+}\ \wedge \mathrm{H}_{1g}', \mathrm{H}_{2g'} : W' \wedge\\ &W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W, L_1\cup FL(\mathrm{cod}(\mathrm{H}_{1+})), L_2\cup FL(\mathrm{cod}(\mathrm{H}_{2+})))}\ W' \wedge\\ &(W', (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}[\![\langle\tau\rangle]\!]_\rho \wedge\\ &(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathrm{e}_2) \overset{*}{\rightarrow}_{L_2} (\mathrm{H}_{2g}' \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \twoheadrightarrow_{L_2}\end{aligned}$$

given arbitrary $W, L_1, L_2, \mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W, \mathrm{v}_1, \mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_{1+} : MHeap, \mathrm{H}_{1*}$ such that

$$(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \mathrm{e}_1) \overset{*}{\rightarrow}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \not\rightarrow_{L_1}$$

Because $(W, (\emptyset, \mathrm{e}_1), (\emptyset, \mathrm{e}_2)) \in \mathcal{E}[\![\tau]\!]_\rho$, we find that $\mathrm{H}_{1*} = \mathrm{H}_{1g}' \uplus \mathrm{H}_1' \uplus \mathrm{H}_{1+}$ and

$$(\mathrm{H}_{2g+} \uplus \mathrm{H}_{2+}, \mathrm{e}_2) \overset{*}{\rightarrow}_{L_2} (\mathrm{H}_{2g}' \uplus \mathrm{H}_2' \uplus \mathrm{H}_{2+}, \mathrm{v}_1) \not\rightarrow_{L_2}$$

where $\mathrm{H}_{1g}', \mathrm{H}_{2g}' : W'$ for some world $W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W, L_1\cup FL(\mathrm{cod}(\mathrm{H}_{1+})), L_2\cup FL(\mathrm{cod}(\mathrm{H}_{2+})))}$ W' such that

$$(W', (\mathrm{H}_1', \mathrm{v}_1), (\mathrm{H}_2', \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho$$

Recall that $\tau \in$ Duplicable $= \{\mathrm{unit}, \mathrm{bool}, \mathrm{ptr}\ \zeta, !\tau\}$. Then by inspecting definitions of $\mathcal{V}[\![\tau]\!]_\rho$ for all four of these cases, we have that $\mathrm{H}_1' = \mathrm{H}_2' = \emptyset$.

We then take $W' = W'$, $H_1' = \emptyset$, $H_2' = \emptyset$, $H_{1g}' = H_{1g}'$, and $H_{2g}' = H_{2g}'$. Finally, given $(W', (\emptyset, v_1), (\emptyset, v_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho$, it follows that $(W', (\emptyset, v_1), (\emptyset, v_2)) \in \mathcal{V}\llbracket\langle\tau\rangle\rrbracket_\rho$.

$\boxed{\forall\alpha.\alpha \rightarrow (\alpha \rightarrow \alpha) \sim \mathrm{bool}}$

(1) We are to show that

$$\forall\, (W, (H_1, e_1), (H_2, e_2)) \in \mathcal{E}\llbracket\forall\alpha.\alpha \rightarrow (\alpha \rightarrow \alpha)\rrbracket_\rho.$$

$$\left(W, (H_1, C_{\forall\alpha.\alpha \rightarrow (\alpha \rightarrow \alpha)\mapsto\mathrm{bool}}\ e_1), (H_2, C_{\forall\alpha.\alpha \rightarrow (\alpha \rightarrow \alpha)\mapsto\mathrm{bool}}\ e_2)\right) \in \mathcal{E}\llbracket\mathrm{bool}\rrbracket_\rho$$

Expanding the definition of $C_{\forall\alpha.\alpha \rightarrow (\alpha \rightarrow \alpha)\mapsto\mathrm{bool}}$, we are to show that

$$(W, (H_1, \mathsf{let}\ f_1 = e_1\ \mathsf{in}\ ((f_1\ \ ())\ \ 0)\ 1), (H_2, \mathsf{let}\ f_2 = e_2\ \mathsf{in}\ ((f_2\ \ ())\ \ 0)\ 1)) \in \mathcal{E}\llbracket\mathrm{bool}\rrbracket_\rho$$

given arbitrary e_1, e_2 such that $(W, (H_1, e_1), (H_2, e_2)) \in \mathcal{E}\llbracket\forall\alpha.\alpha \rightarrow (\alpha \rightarrow \alpha)\rrbracket_\rho$. Expanding the definition of $C_{\forall\alpha.\alpha \rightarrow (\alpha \rightarrow \alpha)\mapsto\mathrm{bool}}$, $\mathcal{E}\llbracket\cdot\rrbracket$. and pushing substitutions in the goal, we are to show that

$$\begin{aligned}
&\exists H_1', H_{1g}'.\forall H_{2+} : \mathit{MHeap}.\exists H_2', W', H_{2g}', v_2.\\
&H_{1*} = H_{1g}' \uplus H_1' \uplus H_{1+}\ \wedge H_{1g}', H_{2g'} : W' \wedge\\
&W \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(H_{1+})),L_2\cup FL(\mathrm{cod}(H_{2+})))}\ W' \wedge\\
&(W', (H_1', v_1), (H_2', v_2)) \in \mathcal{V}\llbracket\mathrm{bool}\rrbracket_\rho \wedge\\
&(H_{2g+} \uplus H_2 \uplus H_{2+}, \mathsf{let}\ f_2 = e_2\ \mathsf{in}\ ((f_2\ \ ())\ \ 0)\ 1) \overset{*}{\rightarrow}_{L_2} (H_{2g}' \uplus H_2' \uplus H_{2+}, v_2) \not\twoheadrightarrow_{L_2}
\end{aligned}$$

given arbitrary $W, L_1, L_2, H_{1g+}, H_{2g+} : W, v_1, H_1, H_2, H_{1+} : \mathit{MHeap}, H_{1*}$ such that

$$(H_{1g+} \uplus H_1 \uplus H_{1+}, \mathsf{let}\ f_1 = e_1\ \mathsf{in}\ ((f_1\ \ ())\ \ 0)\ 1) \overset{*}{\rightarrow}_{L_1} (H_{1*}, v_1) \not\twoheadrightarrow_{L_1}$$

By Lemma 4.3, we have that $(H_{1g+} \uplus H_1 \uplus H_{1+}, e_1) \overset{*}{\rightarrow}_{L_1} (H_{1*}^1, v_1^1) \not\twoheadrightarrow_{L_1}$ for some H_{1*}^1, v_1^1. Expanding the definition of $\mathcal{E}\llbracket\cdot\rrbracket_\rho$ in the premise and specializing where appropriate, we have that $H_{1*}^1 = H_{1g}' \uplus H_{1+}$ and

$$(H_{2g+} \uplus H_2 \uplus H_{2+}, e_2) \overset{*}{\rightarrow}_{L_2} (H_{2g}' \uplus H_{2+}, v_2^1) \not\twoheadrightarrow_{L_2}$$

where $H_{1g}', H_{2g}' : W'$ for some

$$W \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(H_{1+})),L_2\cup FL(\mathrm{cod}(H_{2+})))}\ W'$$

such that

$$(W', (\emptyset, v_1^1), (\emptyset, v_2^1)) \in \mathcal{V}\llbracket\forall\alpha.\alpha \rightarrow (\alpha \rightarrow \alpha)\rrbracket_\rho$$

Expanding the definition of $\mathcal{V}\llbracket\forall\alpha.\alpha \rightarrow (\alpha \rightarrow \alpha)\rrbracket_\rho$, we have that

$$\begin{aligned}
&v_1^1 = \lambda\_.e_1^1 \wedge v_2^1 = \lambda\_.e_2^1 \wedge\\
&\forall R \in \mathit{RelT}.(W', (\emptyset, e_1^1), (\emptyset, e_2^1)) \in \mathcal{E}\llbracket\alpha \rightarrow (\alpha \rightarrow \alpha)\rrbracket_{\rho[\mathsf{F}(\alpha)\mapsto R]}
\end{aligned}$$

To proceed, we take $R = \mathcal{V}\llbracket\langle\mathrm{bool}\rangle\rrbracket_\rho$. We do this because we expect the reduction to eventually need a value in $\mathcal{V}\llbracket\mathrm{bool}\rrbracket_\rho$, but by using the type $\langle\mathrm{bool}\rangle$ instead (which has the same interpretation in our model), we can apply Lemma 4.9 to get that:

$$(W', (\emptyset, e_1^1), (\emptyset, e_2^1)) \in \mathcal{E}\llbracket\langle\mathrm{bool}\rangle \rightarrow (\langle\mathrm{bool}\rangle \rightarrow \langle\mathrm{bool}\rangle)\rrbracket_\rho$$

By the operational semantics of LCVM, we now have that

$$\begin{aligned}(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{f}_1 = \mathsf{e}_1\ \mathsf{in}\ ((\mathsf{f}_1\ ())\ 0)\ 1) &\xrightarrow{*}_{L_1} (\mathsf{H}'_{1g} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{f}_1 = \lambda\_.\mathsf{e}^1_1\ \mathsf{in}\ ((\mathsf{f}_1\ ())\ 0)\ 1)\\ &\xrightarrow{1}_{L_1} (\mathsf{H}'_{1g} \uplus \mathsf{H}_{1+}, [\mathsf{f}_1 \mapsto \lambda\_.\mathsf{e}^1_1]\,((\mathsf{f}_1\ ())\ 0)\ 1)\\ &= (\mathsf{H}'_{1g} \uplus \mathsf{H}_{1+}, \big(\big((\lambda\_.\mathsf{e}^1_1)\ ()\big)\ 0\big)\ 1)\\ &\xrightarrow{1}_{L_1} (\mathsf{H}'_{1g} \uplus \mathsf{H}_{1+}, (\mathsf{e}^1_1\ 0)\ 1)\\ &\xrightarrow{*}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \not\rightarrow_{L_1}\end{aligned}$$

By Lemma 4.3, we have that

$$\left(\mathsf{H}'_{1g} \uplus \mathsf{H}_{1+}, \mathsf{e}^1_1\right) \xrightarrow{*}_{L_1} (\mathsf{H}^2_{1*}, \mathsf{v}^2_1) \not\rightarrow_{L_1}$$

for some $\mathsf{H}^2_{1*}, \mathsf{v}^2_1$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]_\rho$ and specializing where appropriate, we have that $\mathsf{H}^2_{1*} = \mathsf{H}''_{1g} \uplus \mathsf{H}_{1+}$ and

$$(\mathsf{H}'_{2g} \uplus \mathsf{H}_{2+}, \mathsf{e}^1_2) \xrightarrow{*}_{L_2} (\mathsf{H}''_{2g} \uplus \mathsf{H}_{2+}, \mathsf{v}^2_2) \not\rightarrow_{L_2}$$

where $\mathsf{H}''_{1g}, \mathsf{H}''_{2g} : W''$ for some $W' \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathsf{H}_{2+})))}$ W'' such that

$$(W'', (\emptyset, \mathsf{v}^2_1), (\emptyset, \mathsf{v}^2_2)) \in \mathcal{V}[\![\langle\mathsf{bool}\rangle \to (\langle\mathsf{bool}\rangle \to \langle\mathsf{bool}\rangle)]\!]_\rho$$

Expanding the definition of $\mathcal{V}[\![\langle\mathsf{bool}\rangle \to (\langle\mathsf{bool}\rangle \to \langle\mathsf{bool}\rangle)]\!]_\rho$, we have that

$$\begin{aligned}&\mathsf{v}^2_1 = \lambda \mathsf{x}^2_1.\mathsf{e}^2_1 \wedge \mathsf{v}^2_2 = \lambda \mathsf{x}^2_2.\mathsf{e}^2_2 \wedge\\ &\forall (W'', (\emptyset, \mathsf{v}^a_1), (\emptyset, \mathsf{v}^a_2)) \in \mathcal{V}[\![\langle\mathsf{bool}\rangle]\!]_\rho.\\ &\quad (W'', (\emptyset, [\mathsf{x}^2_1 \mapsto \mathsf{v}^a_1]\mathsf{e}^2_1), (\emptyset, [\mathsf{x}^2_2 \mapsto \mathsf{v}^a_2]\mathsf{e}^2_2)) \in \mathcal{E}[\![\langle\mathsf{bool}\rangle \to \langle\mathsf{bool}\rangle]\!]_\rho\end{aligned}$$

Observe that $\mathcal{V}[\![\langle\mathsf{bool}\rangle]\!]_\rho = \mathcal{V}[\![\mathsf{bool}]\!]_\rho$ and $(W'', (\emptyset, 0), (\emptyset, 0)) \in \mathcal{V}[\![\mathsf{bool}]\!]_\rho$ by definition, so $(W'', (\emptyset, [\mathsf{x}^2_1 \mapsto 0]\mathsf{e}^2_1), (\emptyset, [\mathsf{x}^2_2 \mapsto 0]\mathsf{e}^2_2)) \in \mathcal{E}[\![\langle\mathsf{bool}\rangle \to \langle\mathsf{bool}\rangle]\!]_\rho$. By Lemma 4.3, we now have that

$$\left(\mathsf{H}''_{1g} \uplus \mathsf{H}_{1+}, (\lambda \mathsf{x}^2_1.\mathsf{e}^2_1)\ 0\right) \xrightarrow{1}_{L_1} \left(\mathsf{H}''_{1g} \uplus \mathsf{H}_{1+}, [\mathsf{x}^2_1 \mapsto 0]\mathsf{e}^2_1\right) \xrightarrow{*}_{L_1} (\mathsf{H}^3_{1*}, \mathsf{v}^3_1) \not\rightarrow$$

for some $\mathsf{H}^3_{1*}, \mathsf{v}^3_1$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]_\rho$, we have that $\mathsf{H}^3_{1*} = \mathsf{H}'''_{1g} \uplus \mathsf{H}_{1+}$ and

$$(\mathsf{H}''_{2g} \uplus \mathsf{H}_{2+}, [\mathsf{x}^2_2 \mapsto 0]\mathsf{e}^2_2) \rightarrow_{L_2} (\mathsf{H}'''_{2g} \uplus \mathsf{H}_{2+}, \mathsf{v}^3_2) \not\rightarrow_{L_2}$$

where $\mathsf{H}'''_{1g}, \mathsf{H}'''_{2g} : W'''$ for some $W'' \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathsf{H}_{2+})))}$ W''' such that

$$(W''', (\emptyset, \mathsf{v}^3_1), (\emptyset, \mathsf{v}^3_1)) \in \mathcal{V}[\![\langle\mathsf{bool}\rangle \to \langle\mathsf{bool}\rangle]\!]_\rho$$

Expanding the definition of $\mathcal{V}[\![\langle\mathsf{bool}\rangle \to \langle\mathsf{bool}\rangle]\!]_\rho$, we have that

$$\begin{aligned}&\mathsf{v}^3_1 = \lambda \mathsf{x}^3_1.\mathsf{e}^3_1 \wedge \mathsf{v}^3_2 = \lambda \mathsf{x}^3_2.\mathsf{e}^3_2 \wedge\\ &\forall (W''', (\emptyset, \mathsf{v}^a_1), (\emptyset, \mathsf{v}^a_2)) \in \mathcal{V}[\![\langle\mathsf{bool}\rangle]\!]_\rho.\ (W''', (\emptyset, [\mathsf{x}^3_1 \mapsto \mathsf{v}^a_1]\mathsf{e}^3_1), (\emptyset, [\mathsf{x}^3_2 \mapsto \mathsf{v}^a_2]\mathsf{e}^3_2)) \in \mathcal{E}[\![\langle\mathsf{bool}\rangle]\!]_\rho\end{aligned}$$

Recall that $\mathcal{V}[\![\langle\mathsf{bool}\rangle]\!]_\rho = \mathcal{V}[\![\mathsf{bool}]\!]_\rho$ and $(W''', (\emptyset, 1), (\emptyset, 1)) \in \mathcal{V}[\![\mathsf{bool}]\!]_\rho$ by definition, so $(W''', (\emptyset, [\mathsf{x}^3_1 \mapsto 1]\mathsf{e}^3_1), (\emptyset, [\mathsf{x}^3_2 \mapsto 1]\mathsf{e}^3_2)) \in \mathcal{E}[\![\langle\mathsf{bool}\rangle]\!]_\rho$. We now have that

$$\left(\mathsf{H}'''_{1g} \uplus \mathsf{H}_{1+}, (\lambda \mathsf{x}^3_1.\mathsf{e}^3_1)\ 1\right) \xrightarrow{1}_{L_1} \left(\mathsf{H}'''_{1g} \uplus \mathsf{H}_{1+}, [\mathsf{x}^3_1 \mapsto 1]\mathsf{e}^3_1\right) \xrightarrow{*}_{L_1} (\mathsf{H}^4_{1*}, \mathsf{v}^4_1) \not\rightarrow$$

Expanding the definition of $\mathcal{E}[\![\cdot]\!]_\rho$, we have that $\mathrm{H}^4_{1*} = \mathrm{H}''''_{1g} \uplus \mathrm{H}_{1+}$ and

$$(\mathrm{H}'''_{2g} \uplus \mathrm{H}_{2+}, [\mathrm{x}^3_2 \mapsto 1]\mathrm{e}^3_2) \xrightarrow{*}_{L_2} (\mathrm{H}''''_{2g} \uplus \mathrm{H}_{2+}, \mathrm{v}^4_2) \nrightarrow_{L_2}$$

where $\mathrm{H}''''_{1g}, \mathrm{H}''''_{2g} : W''''$ for some $W''' \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W''''$ and

$$(W'''', (\emptyset, \mathrm{v}^4_1), (\emptyset, \mathrm{v}^4_2)) \in \mathcal{V}[\![\langle\mathrm{bool}\rangle]\!]_\rho$$

It follows that $\mathrm{H}_{1*} = \mathrm{H}''''_{1g} \uplus \mathrm{H}_{1+}$ and $\mathrm{v}_1 = \mathrm{v}^4_1$. Thus, we choose $\mathrm{H}'_1 = \emptyset$, $\mathrm{H}'_2 = \emptyset$, $\mathrm{H}'_{1g} = \mathrm{H}''''_{1g}$, $\mathrm{H}'_{2g} = \mathrm{H}''''_{2g}$, and $W' = W''''$. The fact that $(W'''', (\emptyset, \mathrm{v}^4_1), (\emptyset, \mathrm{v}^4_2)) \in \mathcal{V}[\![\mathrm{bool}]\!]_\rho$ follows trivially from the above statement and that $\mathcal{V}[\![\langle\mathrm{bool}\rangle]\!]_\rho = \mathcal{V}[\![\mathrm{bool}]\!]_\rho$.

Finally, all that remains to show that

$$(\mathrm{H}_{2g+} \uplus \mathrm{H}_{2+}, \mathrm{let}\ \mathrm{f}_2 = \mathrm{e}_2\ \mathrm{in}\ ((\mathrm{f}_2\ \ ())\ \ 0)\ 1) \xrightarrow{*}_{L_2} (\mathrm{H}''''_{2g} \uplus \mathrm{H}_{2+}, \mathrm{v}^4_2) \nrightarrow_{L_2}$$

given arbitrary H_{2+}.

We have that

$$\begin{aligned}
(\mathrm{H}_{2g+} \uplus \mathrm{H}_{2+}, \mathrm{let}\ \mathrm{f}_2 = \mathrm{e}_2\ \mathrm{in}\ ((\mathrm{f}_2\ \ ())\ \ 0)\ 1) &\xrightarrow{*}_{L_2} (\mathrm{H}'_{2g} \uplus \mathrm{H}_{2+}, \mathrm{let}\ \mathrm{f}_2 = \lambda\_.\mathrm{e}^1_2\ \mathrm{in}\ ((\mathrm{f}_2\ \ ())\ \ 0)\ 1)\\
&\xrightarrow{1}_{L_2} (\mathrm{H}'_{2g} \uplus \mathrm{H}_{2+}, [\mathrm{f}_2 \mapsto \lambda\_.\mathrm{e}^1_2]\ ((\mathrm{f}_2\ \ ())\ \ 0)\ 1)\\
&= (\mathrm{H}'_{2g} \uplus \mathrm{H}_{2+}, \big((\lambda\_.\mathrm{e}^1_2\ \ ())\ \ 0\big)\ 1)\\
&\xrightarrow{1}_{L_2} (\mathrm{H}'_{2g} \uplus \mathrm{H}_{2+}, \big(\mathrm{e}^1_2\ 0\big)\ 1)\\
&\xrightarrow{*}_{L_2} (\mathrm{H}''_{2g} \uplus \mathrm{H}_{2+}, \big(\big(\lambda \mathrm{x}^2_2.\mathrm{e}^2_2\big)\ \ 0\big)\ 1)\\
&\xrightarrow{1}_{L_2} (\mathrm{H}''_{2g} \uplus \mathrm{H}_{2+}, [\mathrm{x}^2_2 \mapsto 0]\mathrm{e}^2_2 1)\\
&\xrightarrow{*}_{L_2} (\mathrm{H}'''_{2g} \uplus \mathrm{H}_{2+}, \lambda \mathrm{x}^3_2.\mathrm{e}^3_2 1)\\
&\xrightarrow{1}_{L_2} (\mathrm{H}'''_{2g} \uplus \mathrm{H}_{2+}, [\mathrm{x}^3_2 \mapsto 1]\mathrm{e}^3_2)\\
&\xrightarrow{*}_{L_2} (\mathrm{H}''''_{2g} \uplus \mathrm{H}_{2+}, \mathrm{v}^4_2)\\
&\nrightarrow_{L_2}
\end{aligned}$$

as was to be demonstrated.

(2) We are to show that

$\forall\, (W, (\mathrm{H}_1, \mathrm{e}_1), (\mathrm{H}_2, \mathrm{e}_2)) \in \mathcal{E}[\![\mathrm{bool}]\!]_\rho.$

$$\Big(W, (\mathrm{H}_1, \mathrm{C}_{\mathrm{bool} \mapsto \forall \alpha.\alpha \to (\alpha \to \alpha)}\ \mathrm{e}_1), (\mathrm{H}_2, \mathrm{C}_{\mathrm{bool} \mapsto \forall \alpha.\alpha \to (\alpha \to \alpha)}\ \mathrm{e}_2)\Big) \in \mathcal{E}[\![\forall \alpha.\alpha \to (\alpha \to \alpha)]\!]_\rho$$

Expanding the definition of $\mathrm{C}_{\mathrm{bool} \mapsto \forall \alpha.\alpha \to (\alpha \to \alpha)}$, we are to show that

$$\begin{aligned}
&(W, (\mathrm{H}_1, \mathrm{let}\ \mathrm{x}_1 = \mathrm{e}_1\ \mathrm{in}\ (\lambda\_.\lambda \mathrm{t}_1.\lambda \mathrm{f}_1.\mathrm{if}\ \mathrm{x}_1\ \mathrm{t}_1\ \mathrm{f}_1)),\\
&\quad (\mathrm{H}_2, \mathrm{let}\ \mathrm{x}_2 = \mathrm{e}_2\ \mathrm{in}\ (\lambda\_.\lambda \mathrm{t}_2.\lambda \mathrm{f}_2.\mathrm{if}\ \mathrm{x}_2\ \mathrm{t}_2\ \mathrm{f}_2))) \in \mathcal{E}[\![\forall \alpha.\alpha \to (\alpha \to \alpha)]\!]_\rho
\end{aligned}$$

given arbitrary e_1, e_2 such that $(W, (H_1, e_1), (H_2, e_2)) \in \mathcal{E}\llbracket \mathrm{bool} \rrbracket_\rho$. Expanding the definition of $\mathcal{E}\llbracket \cdot \rrbracket_\rho$, we are to show that

$$\begin{array}{l}
\exists H'_{1g}.\forall H_{2+} : \mathit{MHeap}.\exists W', H'_{2g}, v_2. \\
H_{1*} = H'_{1g} \uplus H_{1+} \ \wedge H'_{1g}, H_{2g'} : W' \wedge \\
W \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(H_{1+})),L_2 \cup FL(\mathrm{cod}(H_{2+})))} W' \wedge \\
(W', (\emptyset, v_1), (\emptyset, v_2)) \in \mathcal{V}\llbracket \forall \alpha.\alpha \rightarrow (\alpha \rightarrow \alpha) \rrbracket_\rho \wedge \\
(H_{2g+} \uplus H_2 \uplus H_{2+}, \text{let } x_1 = e_1 \text{ in } (\lambda\_.\lambda t_1.\lambda f_1.\text{if } x_1\ t_1\ f_1)) \xrightarrow{*}_{L_2} (H'_{2g} \uplus H_{2+}, v_2) \not\twoheadrightarrow_{L_2}
\end{array}$$

given arbitrary $W, L_1, L_2, H_{1g+}, H_{2g+} : W, v_1, H_1, H_2, H_{1+} : \mathit{MHeap}, H_{1*}$ such that

$$(H_{1g+} \uplus H_1 \uplus H_{1+}, \text{let } x_2 = e_2 \text{ in } (\lambda\_.\lambda t_2.\lambda f_2.\text{if } x_2\ t_2\ f_2)) \xrightarrow{*}_{L_1} (H_{1*}, v_1) \nrightarrow_{L_1}$$

By Lemma 4.3, we have that $(H_{1g+} \uplus H_1 \uplus H_{1+}, e_1) \xrightarrow{*}_{L_1} (H^1_{1*}, v^1_1) \not\twoheadrightarrow_{L_1}$. Expanding the definition of $\mathcal{E}\llbracket \cdot \rrbracket_\rho$ in the premise and specializing where appropriate, we have that $H^1_{1*} = H'_{1g} \uplus H'_1 \uplus H_{1+}$ and

$$(H_{2g+} \uplus H_2 \uplus H_{2+}, e_2) \xrightarrow{*}_{L_2} (H'_{2g} \uplus H'_2 \uplus H_{2+}, v^1_2) \not\twoheadrightarrow_{L_2}$$

where $H'_{1g}, H'_{2g} : W'$ for some

$$W \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(H_{1+})),L_2 \cup FL(\mathrm{cod}(H_{2+})))} W'$$

such that

$$(W', (H'_1, v^1_1), (H'_2, v^1_2)) \in \mathcal{V}\llbracket \mathrm{bool} \rrbracket_\rho$$

Expanding the definition of $\mathcal{V}\llbracket \mathrm{bool} \rrbracket_\rho$, we have that

$$H'_1 = \emptyset \ \wedge H'_2 = \emptyset \ \wedge v^1_1 = v^2_2 = b \ \wedge b \in \{0, 1\}$$

By Lemma 4.3, we now have that

$$\begin{aligned}
(H'_{1g} \uplus H_1 \uplus H_{1+}, \text{let } x_1 = b \text{ in } (\lambda\_.\lambda t_1.\lambda f_1.\text{if } x_1\ t_1\ f_1)) &\xrightarrow{1}_{L_1} (H'_{1g} \uplus H_{1+}, [x_1 \mapsto b]\ (\lambda\_.\lambda t_1.\lambda f_1.\text{if } x_1\ t_1\ f_1)) \\
&= (H'_{1g} \uplus H_{1+}, (\lambda\_.\lambda t_1.\lambda f_1.\text{if } b\ t_1\ f_1)) \\
&\xrightarrow{*}_{L_1} (H_{1*}, v_1) \\
&\not\twoheadrightarrow
\end{aligned}$$

from which we conclude that $H_{1*} = H'_{1g} \uplus H_{1+}$ and $v_1 = (\lambda\_.\lambda t_1.\lambda f_1.\text{if } b\ t_1\ f_1)$ since configurations with values as programs do not step.
Then, to prove the goal, we take $W' = W'$, $H'_{1g} = H'_{1g}$, and $H'_{2g} = H'_{2g}$.
To show the configuration with the heap $H_{2g+} \uplus H_2 \uplus H_{2+}$ terminates, we have

$$\begin{aligned}
(H_{2g+} \uplus H_2 \uplus H_{2+}, \text{let } x_2 = e_2 \text{ in } (\lambda\_.\lambda t_2.\lambda f_2.\text{if } x_2\ t_2\ f_2)) &\xrightarrow{*}_{L_2} (H'_{2g} \uplus H_{2+}, \text{let } x_2 = b \text{ in } (\lambda\_.\lambda t_2.\lambda f_2.\text{if } x_2\ t_2\ f_2)) \\
&\xrightarrow{1}_{L_2} (H'_{2g} \uplus H_{2+}, [x_2 \mapsto b]\ (\lambda\_.\lambda t_2.\lambda f_2.\text{if } x_2\ t_2\ f_2)) \\
&= (H'_{2g} \uplus H_{2+}, (\lambda\_.\lambda t_2.\lambda f_2.\text{if } b\ t_2\ f_2)) \\
&\not\twoheadrightarrow
\end{aligned}$$

Then take $H'_{2+} = H^1_{2+}$.

All that remains to show is

$$(W', (\emptyset, (\lambda\_.\lambda t_1.\lambda f_1.\text{if } b\ t_1\ f_1)), (\emptyset, (\lambda\_.\lambda t_2.\lambda f_2.\text{if } b\ t_2\ f_2))) \in \mathcal{V}\llbracket \forall \alpha.\alpha \rightarrow (\alpha \rightarrow \alpha) \rrbracket_\rho$$

Expanding the definition of $\mathcal{V}\llbracket\cdot\rrbracket_\rho$ and applying Lemma 4.12, we are to show that

$$(W'', (\emptyset, (\lambda t_1.\lambda f_1.\text{if } b\ t_1\ f_1)), (\emptyset, (\lambda t_2.\lambda f_2.\text{if } b\ t_2\ f_2))) \in \mathcal{V}\llbracket\alpha \rightarrow (\alpha \rightarrow \alpha)\rrbracket_{\rho[\mathsf{F}(\alpha)\mapsto R]}$$

given arbitrary $R \in RelT$ and worlds W'' such that $W' \sqsubseteq_{\emptyset,\emptyset,\lambda t_1.\lambda f_1.\text{if } b\ t_1\ f_1,\lambda t_2.\lambda f_2.\text{if } b\ t_2\ f_2} W''$. Expanding the definition of $\mathcal{V}\llbracket\alpha \rightarrow (\alpha \rightarrow \alpha)\rrbracket_{\rho[\mathsf{F}(\alpha)\mapsto R]}$, pushing substitutions, and applying Lemma 4.12, we are to show that

$$(W''', (\emptyset, (\lambda f_1.\text{if } b\ v_{1t}\ f_1)), (\emptyset, (\lambda f_2.\text{if } b\ v_{2t}\ f_2))) \in \mathcal{V}\llbracket\alpha \rightarrow \alpha\rrbracket_{\rho[\mathsf{F}(\alpha)\mapsto R]}$$

given arbitrary worlds W''' such that $W'' \sqsubseteq_{\emptyset,\emptyset,\lambda f_1.\text{if } b\ v_{1t}\ f_1,\lambda f_2.\text{if } b\ v_{2t}\ f_2} W'''$ and arbitrary v_{1t}, v_{2t} such that $(W''', (\emptyset, v_{1t}), (\emptyset, v_{2t})) \in \mathcal{V}\llbracket\alpha\rrbracket_{\rho[\mathsf{F}(\alpha)\mapsto R]}$. Expanding the definition of $\mathcal{V}\llbracket\alpha \rightarrow \alpha\rrbracket_{\rho[\mathsf{F}(\alpha$ and pushing substitutions, we are to show that

$$(W'''', (\emptyset, (\text{if } b\ v_{1t}\ v_{1f})), (\emptyset, (\text{if } b\ v_{2t}\ v_{2f}))) \in \mathcal{E}\llbracket\alpha\rrbracket_{\rho[\mathsf{F}(\alpha)\mapsto R]}$$

given arbitrary worlds W'''' such that $W''' \sqsubseteq_{\emptyset,\emptyset,\text{if } b\ v_{1t}\ v_{1f},\text{if } b\ v_{2t}\ v_{2f}} W''''$ and arbitrary v_{1f}, v_{2f} such that $(\emptyset, v_{1f}, \emptyset, v_{2f}) \in \mathcal{V}\llbracket\alpha\rrbracket_{\rho[\mathsf{F}(\alpha)\mapsto R]}$. Expanding the definition of $\mathcal{E}\llbracket\cdot\rrbracket_\rho$, we are to show that

$$\begin{aligned}
&\exists H'_{1g}.\forall H_{2+} : MHeap.\exists W', H'_{2g}, v_2.\\
&H_{1*} = H'_{1g} \uplus H_{1+} \ \wedge H'_{1g}, H_{2g'} : W' \wedge\\
&W'''' \sqsubseteq_{(\text{dom}(H_{1+}),\text{dom}(H_{2+})),\text{rchgclocs}(W,L_1\cup FL(\text{cod}(H_{1+})),L_2\cup FL(\text{cod}(H_{2+})))} W' \wedge\\
&(W', (\emptyset, v_1), (\emptyset, v_2)) \in \mathcal{V}\llbracket\forall\alpha.\alpha \rightarrow (\alpha \rightarrow \alpha)\rrbracket_\rho \wedge\\
&(H_{2g+} \uplus H_{2+}, \text{if } b\ v_{1t}\ v_{1f}) \overset{*}{\rightarrow}_{L_2} (H'_{2g} \uplus H_{2+}, v_2) \not\twoheadrightarrow_{L_2}
\end{aligned}$$

given arbitrary $L_1, L_2, H_{1g+}, H_{2g+} : W'''', v_1, H_1, H_2, H_{1+} : MHeap, H_{1*}$ such that

$$(H_{1g+} \uplus H_{1+}, \text{if } b\ v_{2t}\ v_{2f}) \overset{*}{\rightarrow}_{L_1} (H_{1*}, v_1) \not\rightarrow_{L_1}$$

The operational semantics of LCVM offers two cases depending on the value of b. Suppose, without loss of generality, that $b = 0$. Then we have

$$(H_{1g+} \uplus H_{1+}, \text{if } b\ v_{1t}\ v_1) \overset{1}{\rightarrow}_{L_1} (H_{1g+} \uplus H_{1+}, v_{1t}) \overset{*}{\rightarrow}_{L_1} (H_{1*}, v_1) \not\twoheadrightarrow_{L_1}$$

from which we conclude that $v_1 = v_{1t}$, $H_{1*} = H_{1g+} \uplus H_{1+}$ since configurations with values as programs do not step. Then we can take $W' = W''''$, $H'_{1g} = H_{1g+}$, $H'_{2g} = H_{2g+}$, and $v_2 = v_{2t}$. All that remains is to show that

$$(H_{2g+} \uplus H_{2+}, \text{if } 0\ v_{2t}\ v_{2f}) \overset{*}{\rightarrow}_{L_2} (H_{2g+} \uplus H_{2+}, v_{2t}) \not\twoheadrightarrow_{L_2}$$

This is actually just one step by the operational semantics of LCVM.
The case in which $b = 1$ is analogous, exchanging v_{it} with v_{if} where appropriate.

$\boxed{\tau_1 \rightarrow \tau_2 \sim\ !(!\tau_1 \multimap \tau_2)}$

(1) We are to show that

$$\forall\,(W, (\emptyset, e_1), (\emptyset, e_2)) \in \mathcal{E}\llbracket\tau_1 \rightarrow \tau_2\rrbracket_\rho.$$

$$\big(W, (\emptyset, C_{\tau_1 \rightarrow \tau_2 \mapsto !(!\tau_1\multimap\tau_2)}\ e_1), (\emptyset, C_{\tau_1 \rightarrow \tau_2 \mapsto !(!\tau_1\multimap\tau_2)}\ e_2)\big) \in \mathcal{E}\llbracket !(!\tau_1 \multimap \tau_2)\rrbracket_\rho$$

Expanding the definition of $C_{\tau_1 \rightarrow \tau_2 \mapsto !(!\tau_1\multimap\tau_2)}\ e_1$, we are to show that

$$\big(W, (\emptyset, \text{let } f_1 = e_1 \text{ in } \lambda x_1.\big(C_{\tau_2\mapsto\tau_2}\ (\ldots)\big)), (\emptyset, \text{let } f_2 = e_2 \text{ in } \lambda x_2.\big(C_{\tau_2\mapsto\tau_2}\ (\ldots)\big))\big) \in \mathcal{E}\llbracket !(!\tau_1 \multimap \tau_2)\rrbracket_\rho$$

given arbitrary $\mathrm{e}_1, \mathrm{e}_2$ such that $(\emptyset, \mathrm{e}_1, \emptyset, \mathrm{e}_2) \in \mathcal{E}\llbracket \tau_1 \longrightarrow \tau_2 \rrbracket_\rho$. Expanding the definition of $\mathcal{E}\llbracket \cdot \rrbracket_\rho$, we are to show that

$\exists \mathrm{H}_1', \mathrm{H}_{1g}'. \forall \mathrm{H}_{2+} : \mathit{MHeap}. \exists \mathrm{H}_2', W', \mathrm{H}_{2g}', \mathrm{v}_2.$
$\mathrm{H}_{1*} = \mathrm{H}_{1g}' \uplus \mathrm{H}_1' \uplus \mathrm{H}_{1+} \ \wedge \mathrm{H}_{1g}', \mathrm{H}_{2g'} : W' \wedge$
$W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}), \mathrm{dom}(\mathrm{H}_{2+})), \mathrm{rchgclocs}(W, L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})), L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W' \wedge$
$(W', (\mathrm{H}_1', \mathrm{v}_1), (\mathrm{H}_2', \mathrm{v}_2)) \in \mathcal{V}\llbracket !(!\tau_1 \multimap \tau_2) \rrbracket_\rho \wedge$
$(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathrm{let}\ \mathrm{f}_2 = \mathrm{e}_2\ \mathrm{in}\ \lambda \mathrm{x}_2. \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ (\ldots)\right)) \xrightarrow{*}_{L_2} (\mathrm{H}_{2g}' \uplus \mathrm{H}_2' \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \not\twoheadrightarrow_{L_2}$

given arbitrary $W, L_1, L_2, \mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W, \mathrm{v}_1, \mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_{1+} : \mathit{MHeap}, \mathrm{H}_{1*}$ such that

$$(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \mathrm{let}\ \mathrm{f}_1 = \mathrm{e}_1\ \mathrm{in}\ \lambda \mathrm{x}_1. \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ (\ldots)\right)) \xrightarrow{*}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \not\rightarrow_{L_1}$$

By Lemma 4.3, we have that $(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \mathrm{e}_1) \xrightarrow{*}_{L_1} (\mathrm{H}_{1*}^1, \mathrm{v}_1^1) \not\twoheadrightarrow_{L_1}$ for some $\mathrm{H}_{1*}^1, \mathrm{v}_1^1$. Expanding the definition of $\mathcal{E}\llbracket \tau_1 \longrightarrow \tau_2 \rrbracket_\rho$ in the premise and specializing where appropriate, we have that $\mathrm{H}_{1*}^1 = \mathrm{H}_{1g}' \uplus \mathrm{H}_{1+}$ and

$$(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathrm{e}_2) \xrightarrow{*}_{L_2} (\mathrm{H}_{2g}' \uplus \mathrm{H}_{2+}, \mathrm{v}_2^1)$$

where $\mathrm{H}_{1g}', \mathrm{H}_{2g}' : W'$ for some $W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}), \mathrm{dom}(\mathrm{H}_{2+})), \mathrm{rchgclocs}(W, L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})), L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))}$ W' such that

$$(W', (\emptyset, \mathrm{v}_1^1), (\emptyset, \mathrm{v}_2^1)) \in \mathcal{V}\llbracket \tau_1 \longrightarrow \tau_2 \rrbracket_\rho$$

Expanding the definition of $\mathcal{V}\llbracket \tau_1 \longrightarrow \tau_2 \rrbracket_\rho$, we have that

$$\begin{gathered}\mathrm{v}_1^1 = \lambda \mathrm{x}_1^1.\mathrm{e}_1^1 \wedge \mathrm{v}_2^1 = \lambda \mathrm{x}_2^1.\mathrm{e}_2^1 \wedge \\ \forall W''. W' \sqsubseteq_{\emptyset, \emptyset, \mathrm{e}_1^1, \mathrm{e}_2^1} W'' \wedge \forall (W'', (\emptyset, \mathrm{v}_1^a), (\emptyset, \mathrm{v}_2^a)) \in \mathcal{V}\llbracket \tau_1 \rrbracket_\rho . (W'', (\emptyset, [\mathrm{x}_1^1 \mapsto \mathrm{v}_1^a]\mathrm{e}_1^1), (\emptyset, [\mathrm{x}_2^1 \mapsto \mathrm{v}_2^a]\mathrm{e}_2^1)) \in \mathcal{E}\llbracket \tau_2 \rrbracket_\rho\end{gathered} \tag{26}$$

By the operational semantics of LCVM, we now have that

$$\begin{aligned}(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \mathrm{let}\ \mathrm{f}_1 = \mathrm{e}_1\ \mathrm{in}\ \lambda \mathrm{x}_1.(\ldots)) &\xrightarrow{*}_{L_1} (\mathrm{H}_{1g}' \uplus \mathrm{H}_{1+}, \mathrm{let}\ \mathrm{f}_1 = \lambda \mathrm{x}_1^1.\mathrm{e}_1^1\ \mathrm{in}\ \lambda \mathrm{x}_1.(\ldots)) \\ &\xrightarrow{1}_{L_1} (\mathrm{H}_{1g}' \uplus \mathrm{H}_{1+}, [\mathrm{f}_1 \mapsto \lambda \mathrm{x}_1^1.\mathrm{e}_1^1]\lambda \mathrm{x}_1.(\ldots)) \\ &= \left(\mathrm{H}_{1g}' \uplus \mathrm{H}_{1+}, \lambda \mathrm{x}_1. \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \left((\lambda \mathrm{x}_1^1.\mathrm{e}_1^1)\ \left(\mathrm{C}_{\tau_1 \mapsto \tau_1}\ \mathrm{x}_1\right)\right)\right)\right) \\ &\not\twoheadrightarrow\end{aligned}$$

so $\mathrm{H}_{1*} = \mathrm{H}_{1g}' \uplus \mathrm{H}_{1+}$ and

$$\mathrm{v}_1 = \lambda \mathrm{x}_1. \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \left((\lambda \mathrm{x}_1^1.\mathrm{e}_1^1)\ \left(\mathrm{C}_{\tau_1 \mapsto \tau_1}\ \mathrm{x}_1\right)\right)\right)$$

Then we show the goal by taking $W' = W'$, $\mathrm{H}_{1g}' = \mathrm{H}_{1g}'$, $\mathrm{H}_{2g}' = \mathrm{H}_{2g}'$, $\mathrm{H}_1' = \emptyset$, $\mathrm{H}_2' = \emptyset$, and

$$\mathrm{v}_2 = \lambda \mathrm{x}_2. \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \left((\lambda \mathrm{x}_2^1.\mathrm{e}_2^1)\ \left(\mathrm{C}_{\tau_1 \mapsto \tau_1}\ \mathrm{x}_2\right)\right)\right)$$

To show the configuration with $\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}$ terminates, we have

$$\begin{aligned}(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathrm{let}\ \mathrm{f}_2 = \mathrm{e}_2\ \mathrm{in}\ \lambda \mathrm{x}_2.(\ldots)) &\xrightarrow{*}_{L_2} (\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathrm{let}\ \mathrm{f}_2 = \lambda \mathrm{x}_2^1.\mathrm{e}_2^1\ \mathrm{in}\ \lambda \mathrm{x}_1.(\ldots)) \\ &\xrightarrow{1}_{L_2} (\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, [\mathrm{f}_2 \mapsto \lambda \mathrm{x}_2^1.\mathrm{e}_2^1]\lambda \mathrm{x}_2.(\ldots)) \\ &= (\mathrm{H}_{2g+} \uplus \mathrm{H}_{2+}, \lambda \mathrm{x}_2. \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \left((\lambda \mathrm{x}_2^1.\mathrm{e}_2^1)\ \left(\mathrm{C}_{\tau_1 \mapsto \tau_1}\ \mathrm{x}_2\right)\right)\right)) \\ &\not\twoheadrightarrow_{L_2}\end{aligned}$$

Then take $\mathrm{H}_2' = \emptyset$, $\mathrm{H}_{2+}' = \mathrm{H}_{2+}^1$.

All that remains to show is that:

$$\big(W', (\emptyset, (\lambda x_1.\, (C_{\tau_2 \mapsto \tau_2}\ ((\lambda x_1^1.e_1^1)\ (C_{\tau_1 \mapsto \tau_1}\ x_1))))), (\emptyset, (\lambda x_2.\, (C_{\tau_2 \mapsto \tau_2}\ ((\lambda x_2^1.e_2^1)\ (C_{\tau_1 \mapsto \tau_1}\ x_2)))))\big)$$
$$\in \mathcal{V}[\![!(!\tau_1 \multimap \tau_2)]\!]_\rho$$

Expanding the definitions of $\mathcal{V}[\![!(!\tau_1 \multimap \tau_2)]\!]_\rho$, $\mathcal{V}[\![!\cdot]\!]_\rho$ (twice), and pushing substitutions, we are to show that

$$\big(W'', (\emptyset, (C_{\tau_2 \mapsto \tau_2}\ ((\lambda x_1^1.e_1^1)\ (C_{\tau_1 \mapsto \tau_1}\ v_1^a)))), (\emptyset, (C_{\tau_2 \mapsto \tau_2}\ ((\lambda x_2^1.e_2^1)\ (C_{\tau_1 \mapsto \tau_1}\ v_2^a))))\big)$$
$$\in \mathcal{E}[\![\tau_2]\!]_\rho$$

given arbitrary worlds W'' such that $W' \sqsubseteq_{\emptyset,\emptyset,e_1^1,e_2^1} W''$ and arbitrary v_1^a, v_2^a such that $(W'', (\emptyset, v_1^a), (\emptyset, v_2^a)) \in \mathcal{V}[\![\tau_1]\!]_\rho$. Expanding the definition of $\mathcal{E}[\![\cdot]\!]$., we are to show that

$$\begin{array}{l}
\exists H_1', H_{1g}'.\forall H_{2+} : \mathit{MHeap}.\exists H_2', W', H_{2g}', v_2.\\
H_{1*} = H_{1g}' \uplus H_1' \uplus H_{1+} \ \wedge H_{1g}', H_{2g'} : W' \wedge\\
W'' \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W'',L_1 \cup FL(\mathrm{cod}(H_{1+})),L_2 \cup FL(\mathrm{cod}(H_{2+})))} W' \wedge\\
(W', (H_1', v_1), (H_2', v_2)) \in \mathcal{V}[\![\tau]\!]_\rho \wedge\\
(H_{2g+} \uplus H_{2+}, (C_{\tau_2 \mapsto \tau_2}\ ((\lambda x_1^1.e_1^1)\ (C_{\tau_1 \mapsto \tau_1}\ v_1^a)))) \xrightarrow{*}_{L_2} (H_{2g}' \uplus H_2' \uplus H_{2+}, v_2) \twoheadrightarrow_{L_2}
\end{array}$$

given arbitrary $L_1, L_2, H_{1g+}, H_{2g+} : W, v_1, H_1, H_2, H_{1+} : \mathit{MHeap}, H_{1*}$ such that

$$(H_{1g+} \uplus H_{1+}, (C_{\tau_2 \mapsto \tau_2}\ ((\lambda x_1^1.e_1^1)\ (C_{\tau_1 \mapsto \tau_1}\ v_1^a))) \xrightarrow{*}_{L_1} (H_{1*}, v_1) \not\twoheadrightarrow_{L_1}$$

By Lemma 4.3, we have that $(H_{1g+} \uplus H_1 \uplus H_{1+}, C_{\tau_1 \mapsto \tau_1}\ v_1^a) \xrightarrow{*}_{L_1 \cup FL(e_1^1)} (H_{1*}^1, v_1^1) \twoheadrightarrow_{L_1 \cup FL(e_1^1)}$ for some H_{1*}^1, v_1^1. Recall that $(W'', (\emptyset, v_1^a), (\emptyset, v_2^a)) \in \mathcal{V}[\![\tau_1]\!]_\rho$ by assumption, so $(W'', (\emptyset, v_1^a), (\emptyset, v_2^a)) \in \mathcal{E}[$ by Lemma 4.12. Then, appealing to the induction hypothesis that $\tau_1 \sim \tau_1$ is sound, expanding the definition of $\mathcal{E}[\![\cdot]\!]_\rho$, and specializing as appropriate, we have that $H_{1*}^1 = H_{1g}' \uplus H_{1+}$ and

$$(H_{2g+} \uplus H_{2+}, C_{\tau_1 \mapsto \tau_1}\ v_2^a) \xrightarrow{*}_{L_2 \cup FL(e_2^1)} (H_{2g}' \uplus H_{2+}, v_2^1) \twoheadrightarrow_{L_2 \cup FL(e_2^1)}$$

where $H_{1g}', H_{2g}' : W'''$ for some $W'' \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W'',L_1 \cup FL(e_1^1) \cup FL(\mathrm{cod}(H_{1+})),L_2 \cup FL(e_2^1) \cup FL(\mathrm{cod}(H_2}$ W''' such that

$$(W''', (\emptyset, v_1^1), (\emptyset, v_2^1)) \in \mathcal{V}[\![\tau_1]\!]_\rho$$

Now, by the operational semantics of LCVM, we have that

$$\begin{aligned}
(H_{1g+} \uplus H_{1+}, (C_{\tau_2 \mapsto \tau_2}\ ((\lambda x_1^1.e_1^1)\ (C_{\tau_1 \mapsto \tau_1}\ v_1^a)))) &\xrightarrow{*}_{L_1} \big(H_{1g}' \uplus H_{1+}, (C_{\tau_2 \mapsto \tau_2}\ ((\lambda x_1^1.e_1^1)\ v_1^1))\big)\\
&\xrightarrow{1}_{L_1} \big(H_{1g}' \uplus H_{1+}, (C_{\tau_2 \mapsto \tau_2}\ [x_1^1 \mapsto v_1^1]e_1^1)\big)\\
&\xrightarrow{*}_{L_1} (H_{1*}, v_1)\\
&\twoheadrightarrow_{L_1}
\end{aligned}$$

Then applying Lemma 4.3 again, we have that $\big(H_{1g}' \uplus H_{1+}, [x_1^1 \mapsto v_1^1]e_1^1\big) \xrightarrow{*}_{L_1} (H_{1*}^2, v_1^2) \twoheadrightarrow_{L_1}$ for some H_{1*}^2, v_1^2. Since $(W''', (\emptyset, v_1^1), (\emptyset, v_2^1)) \in \mathcal{V}[\![\tau_1]\!]_\rho$ and $W' \sqsubseteq_{\emptyset,\emptyset,e_1^1,e_2^1} W'''$ (by Lemma 4.6), we have $(W''', (\emptyset, [x_1^1 \mapsto v_1^1]e_1^1), (\emptyset, [x_2^2 \mapsto v_2^1]e_2^1)) \in \mathcal{E}[\![\tau_2]\!]_\rho$ by (26). Expanding the definition of $\mathcal{E}[\![\cdot]\!]_\rho$, we have that $H_{1*}^2 = H_{1g}'' \uplus H_{1+}$ and

$$(H_{2g}' \uplus H_{2+}, [x_2^2 \mapsto v_2^1]e_2^1) \xrightarrow{*}_{L_2} (H_{2g}'' \uplus H_{2+}, v_2^2) \twoheadrightarrow_{L_2}$$

where $H''_{1g}, H''_{2g} : W''''$ for some $W''' \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W''',L_1 \cup FL(\mathrm{cod}(H_{1+})),L_2 \cup FL(\mathrm{cod}(H_{2+})))}$ W'''' such that

$$(W'''', (\emptyset, v_1^2), (\emptyset, v_2^2)) \in \mathcal{V}\llbracket \tau_2 \rrbracket_\rho$$

Now, by the operational semantics of LCVM, we have that

$$\begin{aligned}\left(H'_{1g} \uplus H_{1+}, \left(C_{\tau_2 \mapsto \tau_2}\ [x_1^1 \mapsto v_1^1]e_1^1\right)\right) &\xrightarrow{*}_{L_1} \left(H''_{1g} \uplus H_{1+}, \left(C_{\tau_2 \mapsto \tau_2}\ v_1^2\right)\right)\\ &\xrightarrow{*}_{L_1} (H_{1*}, v_1)\\ &\nrightarrow_{L_1}\end{aligned}$$

Recall that $(W'''', (\emptyset, v_1^2), (\emptyset, v_2^2)) \in \mathcal{V}\llbracket \tau_2 \rrbracket_\rho$, so $(W'''', (\emptyset, v_1^2), (\emptyset, v_2^2)) \in \mathcal{E}\llbracket \tau_2 \rrbracket_\rho$ by Lemma 4.12. Then, appealing to the induction hypothesis that $\tau_2 \sim \tau_2$ is sound, expanding the definition of $\mathcal{E}\llbracket \cdot \rrbracket_\rho$, and specializing as appropriate, we have that $H_{1*} = H'''_{1g} \uplus H'''_1 \uplus H_{1+}$ and

$$(H''_{2g} \uplus H_{2+}, C_{\tau_2 \mapsto \tau_2} v_2^2) \xrightarrow{*}_{L_2} (H'''_{2g} \uplus H'''_2 \uplus H_{2+}, v_2) \nrightarrow_{L_2}$$

where $H'''_{1g}, H'''_{2g} : W'''''$ for some $W'''' \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W'''',L_1 \cup FL(\mathrm{cod}(H_{1+})),L_2 \cup FL(\mathrm{cod}(H_{2+})))}$ W''''' such that

$$(W''''', (H'''_1, v_1), (H'''_2, v_2)) \in \mathcal{V}\llbracket \tau_2 \rrbracket_\rho$$

Then we show the goal by taking $W' = W'''''$, $H'_1 = H'''_1$, $H'_2 = H'''_2$, $H'_{1g} = H'''_{1g}$, and $H'_{2g} = H'''_{2g}$. Finally, to show the configuration with $H_{2g+} \uplus H_{2+}$ terminates, we have:

$$\begin{aligned}\left(H_{2g+} \uplus H_{2+}, \left(C_{\tau_2 \mapsto \tau_2}\ \left(\left(\lambda x_2^1.e_2^1\right)\ \left(C_{\tau_1 \mapsto \tau_1}\ v_2^a\right)\right)\right)\right) &\xrightarrow{*}_{L_2} \left(H'_{2g} \uplus H_{2+}, \left(C_{\tau_2 \mapsto \tau_2}\ \left(\left(\lambda x_2^1.e_2^1\right)\ v_2^1\right)\right)\right)\\ &\xrightarrow{1}_{L_2} \left(H'_{2g} \uplus H_{2+}, \left(C_{\tau_2 \mapsto \tau_2}\ [x_2^1 \mapsto v_2^1]e_2^1\right)\right)\\ &\xrightarrow{*}_{L_2} \left(H''_{2g} \uplus H_{2+}, \left(C_{\tau_2 \mapsto \tau_2}\ v_2^2\right)\right)\\ &\xrightarrow{*}_{L_2} \left(H'''_{2g} \uplus H'''_2 \uplus H_{2+}, v_2\right)\\ &\nrightarrow_{L_2}\end{aligned}$$

(2) We are to show that

$$\forall (W, (\emptyset, e_1), (\emptyset, e_2)) \in \mathcal{E}\llbracket !(!\tau_1 \multimap \tau_2) \rrbracket_\rho.$$
$$\left(W, \left(\emptyset, C_{!(!\tau_1 \multimap \tau_2) \mapsto \tau_1\ \longrightarrow\ \tau_2}\ e_1\right), \left(\emptyset, C_{!(!\tau_1 \multimap \tau_2) \mapsto \tau_1\ \longrightarrow\ \tau_2}\ e_2\right)\right) \in \mathcal{E}\llbracket \tau_1 \longrightarrow \tau_2 \rrbracket_\rho$$

Expanding the definition of $C_{!(!\tau_1 \multimap \tau_2) \mapsto \tau_1\ \longrightarrow\ \tau_2}\ e_1$, we are to show that

$$\left(W, \left(\emptyset, \mathrm{let}\ f_1 = e_1\ \mathrm{in}\ \lambda x_1. \left(C_{\tau_2 \mapsto \tau_2}\ (\ldots)\right)\right), \left(\emptyset, \mathrm{let}\ f_2 = e_2\ \mathrm{in}\ \lambda x_2. \left(C_{\tau_2 \mapsto \tau_2}\ (\ldots)\right)\right)\right) \in \mathcal{E}\llbracket \tau_1 \longrightarrow \tau_2 \rrbracket_\rho$$

given arbitrary e_1, e_2 such that $(\emptyset, e_1, \emptyset, e_2) \in \mathcal{E}\llbracket !(!\tau_1 \multimap \tau_2) \rrbracket_\rho$. Expanding the definition of $\mathcal{E}\llbracket \cdot \rrbracket_\rho$, we are to show that

$$\begin{aligned}&\exists H'_{1g}.\forall H_{2+} : MHeap.\exists W', H'_{2g}, v_2.\\ &H_{1*} = H'_{1g} \uplus H'_1 \uplus H_{1+}\ \wedge H'_{1g}, H_{2g'} : W' \wedge\\ &W \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(H_{1+})),L_2 \cup FL(\mathrm{cod}(H_{2+})))}\ W' \wedge\\ &(W', (\emptyset, v_1), (\emptyset, v_2)) \in \mathcal{V}\llbracket \tau_1 \longrightarrow \tau_2 \rrbracket_\rho \wedge\\ &(H_{2g+} \uplus H_2 \uplus H_{2+}, \mathrm{let}\ f_2 = e_2\ \mathrm{in}\ \lambda x_2. \left(C_{\tau_2 \mapsto \tau_2}\ (\ldots)\right)) \xrightarrow{*}_{L_2} (H'_{2g} \uplus H_{2+}, v_2) \nrightarrow_{L_2}\end{aligned}$$

given arbitrary $W, L_1, L_2, H_{1g+}, H_{2g+} : W, v_1, H_1, H_2, H_{1+} : MHeap, H_{1*}$ such that

$$(H_{1g+} \uplus H_1 \uplus H_{1+}, \mathrm{let}\ f_1 = e_1\ \mathrm{in}\ \lambda x_1. \left(C_{\tau_2 \mapsto \tau_2}\ (\ldots)\right)) \xrightarrow{*}_{L_1} (H_{1*}, v_1) \not\rightarrow_{L_1}$$

By Lemma 4.3, we have that $\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \mathrm{e}_1) \xrightarrow{*}_{L_1} (\mathrm{H}^1_{1*}, \mathrm{v}^1_1) \not\twoheadrightarrow_{L_1}$ for some $\mathrm{H}^1_{1*}, \mathrm{v}^1_1$. Expanding the definition of $\mathcal{E}\llbracket !(!\tau_1 \multimap \tau_2) \rrbracket_\rho$ in the premise and specializing where appropriate, we have that $\mathrm{H}^1_{1*} = \mathrm{H}'_{1g} \uplus \mathrm{H}'_1 \mathrm{H}_{1+}$ and

$$(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathrm{e}_2) \xrightarrow{*}_{L_2} (\mathrm{H}'_{2g} \uplus \mathrm{H}'_2 \uplus \mathrm{H}_{2+}, \mathrm{v}^1_2)$$

where $\mathrm{H}'_{1g}, \mathrm{H}'_{2g} : W'$ for some $W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}), \mathrm{dom}(\mathrm{H}_{2+})), \mathrm{rchgclocs}(W, L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})), L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W'$ such that

$$(W', (\mathrm{H}'_1, \mathrm{v}^1_1), (\mathrm{H}'_2, \mathrm{v}^1_2)) \in \mathcal{V}\llbracket !(!\tau_1 \multimap \tau_2) \rrbracket_\rho$$

Expanding the definition of $\mathcal{V}\llbracket ! \cdot \rrbracket.$ (twice) and $\mathcal{V}\llbracket \cdot \multimap \cdot \rrbracket.$, we have that

$$\begin{aligned}
&\mathrm{v}^1_1 = \lambda \mathrm{x}^1_1.\mathrm{e}^1_1 \wedge \mathrm{v}^1_2 = \lambda \mathrm{x}^1_2.\mathrm{e}^1_2 \;\wedge \mathrm{H}'_1 = \emptyset \wedge \mathrm{H}'_2 = \emptyset \\
&\forall W''. W' \sqsubseteq_{\emptyset, \emptyset, \mathrm{e}^1_1, \mathrm{e}^1_2} W'' \implies \\
&\forall (W'', (\emptyset, \mathrm{v}^a_1), (\emptyset, \mathrm{v}^a_2)) \in \mathcal{V}\llbracket \tau_1 \rrbracket_\rho . (\emptyset, [\mathrm{x}^1_1 \mapsto \mathrm{v}^a_1]\mathrm{e}^1_1, \emptyset, [\mathrm{x}^1_2 \mapsto \mathrm{v}^a_2]\mathrm{e}^1_2) \in \mathcal{E}\llbracket \tau_2 \rrbracket_\rho
\end{aligned} \tag{27}$$

where we associate empty heaps with the v^a_i because the tuple comes from $\mathcal{V}\llbracket !\tau_1 \rrbracket_\rho$. By the operational semantics of LCVM, we now have that

$$\begin{aligned}
(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \mathrm{let}\ \mathrm{f}_1 = \mathrm{e}_1\ \mathrm{in}\ \lambda \mathrm{x}_1.(\ldots)) &\xrightarrow{*}_{L_1} (\mathrm{H}'_{1g} \uplus \mathrm{H}_{1+}, \mathrm{let}\ \mathrm{f}_1 = \lambda \mathrm{x}^1_1.\mathrm{e}^1_1\ \mathrm{in}\ \lambda \mathrm{x}_1.(\ldots)) \\
&\xrightarrow{1}_{L_1} (\mathrm{H}'_{1g} \uplus \mathrm{H}_{1+}, [\mathrm{f}_1 \mapsto \lambda \mathrm{x}^1_1.\mathrm{e}^1_1]\lambda \mathrm{x}_1.(\ldots)) \\
&= \left(\mathrm{H}'_{1g} \uplus \mathrm{H}_{1+}, \lambda \mathrm{x}_1. \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \left(\left(\lambda \mathrm{x}^1_1.\mathrm{e}^1_1\right)\ \left(\mathrm{C}_{\tau_1 \mapsto \tau_1}\ \mathrm{x}_1\right)\right)\right)\right) \\
&\not\twoheadrightarrow_{L_1}
\end{aligned}$$

so $\mathrm{H}_{1*} = \mathrm{H}'_{1g} \uplus \mathrm{H}_{1+}$ and

$$\mathrm{v}_1 = \lambda \mathrm{x}_1. \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \left(\left(\lambda \mathrm{x}^1_1.\mathrm{e}^1_1\right)\ \left(\mathrm{C}_{\tau_1 \mapsto \tau_1}\ \mathrm{x}_1\right)\right)\right)$$

Then we show the goal by taking $W' = W'$, $\mathrm{H}'_{1g} = \mathrm{H}'_{1g}$, $\mathrm{H}'_{2g} = \mathrm{H}'_{2g}$ and

$$\mathrm{v}_2 = \lambda \mathrm{x}_2. \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \left(\left(\lambda \mathrm{x}^1_2.\mathrm{e}^1_2\right)\ \left(\mathrm{C}_{\tau_1 \mapsto \tau_1}\ \mathrm{x}_2\right)\right)\right)$$

To show the configuration $\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}$ terminates, we have

$$\begin{aligned}
(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathrm{let}\ \mathrm{f}_2 = \mathrm{e}_2\ \mathrm{in}\ \lambda \mathrm{x}_2.(\ldots)) &\xrightarrow{*}_{L_2} (\mathrm{H}'_{2g} \uplus \mathrm{H}_{2+}, \mathrm{let}\ \mathrm{f}_2 = \lambda \mathrm{x}^1_2.\mathrm{e}^1_2\ \mathrm{in}\ \lambda \mathrm{x}_1.(\ldots)) \\
&\xrightarrow{1}_{L_2} (\mathrm{H}'_{2g} \uplus \mathrm{H}_{2+}, [\mathrm{f}_2 \mapsto \lambda \mathrm{x}^1_2.\mathrm{e}^1_2]\lambda \mathrm{x}_2.(\ldots)) \\
&= \left(\mathrm{H}'_{2g} \uplus \mathrm{H}_{2+}, \lambda \mathrm{x}_2. \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \left(\left(\lambda \mathrm{x}^1_2.\mathrm{e}^1_2\right)\ \left(\mathrm{C}_{\tau_1 \mapsto \tau_1}\ \mathrm{x}_2\right)\right)\right)\right) \\
&\not\twoheadrightarrow_{L_2}
\end{aligned}$$

All that remains to show is that

$$\begin{aligned}
&\left(W', \left(\emptyset, \left(\lambda \mathrm{x}_1. \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \left(\left(\lambda \mathrm{x}^1_1.\mathrm{e}^1_1\right)\ \left(\mathrm{C}_{\tau_1 \mapsto \tau_1}\ \mathrm{x}_1\right)\right)\right)\right)\right), \left(\emptyset, \left(\lambda \mathrm{x}_2. \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \left(\left(\lambda \mathrm{x}^1_2.\mathrm{e}^1_2\right)\ \left(\mathrm{C}_{\tau_1 \mapsto \tau_1}\ \mathrm{x}_2\right)\right)\right)\right)\right)\right) \\
&\in \mathcal{V}\llbracket \tau_1 \to \tau_2 \rrbracket_\rho
\end{aligned}$$

Expanding the definition of $\mathcal{V}\llbracket \tau_1 \to \tau_2 \rrbracket_\rho$ and pushing substitutions, we are to show that

$$\begin{aligned}
&\left(W'', \left(\emptyset, \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \left(\left(\lambda \mathrm{x}^1_1.\mathrm{e}^1_1\right)\ \left(\mathrm{C}_{\tau_1 \mapsto \tau_1}\ \mathrm{v}^a_1\right)\right)\right)\right), \left(\emptyset, \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \left(\left(\lambda \mathrm{x}^1_2.\mathrm{e}^1_2\right)\ \left(\mathrm{C}_{\tau_1 \mapsto \tau_1}\ \mathrm{v}^a_2\right)\right)\right)\right)\right) \\
&\in \mathcal{E}\llbracket \tau_2 \rrbracket_\rho
\end{aligned}$$

given arbitrary worlds W'' such that $W' \sqsubseteq_{\emptyset,\emptyset,e_1^1,e_2^1} W''$ and v_1^a, v_2^a such that $(W'', (\emptyset, v_1^a), (\emptyset, v_2^a)) \in \mathcal{V}\llbracket \tau_1 \rrbracket$
Expanding the definition of $\mathcal{E}\llbracket \cdot \rrbracket_\cdot$, we are to show that

$$\begin{array}{l}
\exists H'_{1g}.\forall H_{2+} : \mathit{MHeap}.\exists W', H'_{2g}, v_2. \\
H_{1*} = H'_{1g} \uplus H'_1 \uplus H_{1+} \ \wedge H'_{1g}, H_{2g'} : W' \wedge \\
W'' \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W, L_1 \cup FL(\mathrm{cod}(H_{1+})), L_2 \cup FL(\mathrm{cod}(H_{2+})))} W' \wedge \\
(W', (\emptyset, v_1), (\emptyset, v_2)) \in \mathcal{V}\llbracket \tau_2 \rrbracket_\rho \wedge \\
(H_{2g+} \uplus H_{2+}, (C_{\tau_2 \mapsto \tau_2} \ ((\lambda x_1^1.e_1^1) \ (C_{\tau_1 \mapsto \tau_1} \ v_1^a)))) \overset{*}{\longrightarrow}_{L_2} (H'_{2g} \uplus H_{2+}, v_2) \not\twoheadrightarrow_{L_2}
\end{array}$$

given arbitrary $L_1, L_2, H_{1g+}, H_{2g+} : W, v_1, H_1, H_2, H_{1+} : \mathit{MHeap}, H_{1*}$ such that

$$(H_{1g+} \uplus H_{1+}, (C_{\tau_2 \mapsto \tau_2} \ ((\lambda x_2^1.e_2^1) \ (C_{\tau_1 \mapsto \tau_1} \ v_2^a)))) \overset{*}{\longrightarrow}_{L_1} (H_{1*}, v_1) \nrightarrow_{L_1}$$

By Lemma 4.3, we have that $(H_{1g+} \uplus H_{1+}, C_{\tau_1 \mapsto \tau_1} \ v_1^a) \overset{*}{\longrightarrow}_{L_1 \cup FL(e_1^1)} (H_{1*}^1, v_1^1) \not\twoheadrightarrow_{L_1 \cup FL(e_1^1)}$ for some H_{1*}^1, v_1^1. Recall that $(W'', (\emptyset, v_1^a), (\emptyset, v_2^a)) \in \mathcal{V}\llbracket \tau_1 \rrbracket_\rho$ by assumption, so $(W'', (\emptyset, v_1^a), (\emptyset, v_2^a)) \in \mathcal{E}\llbracket \tau_1 \rrbracket$ by Lemma 4.12. Then, appealing to the inductive hypothesis that $\tau_1 \sim \tau_1$ is sound, expanding the definition of $\mathcal{E}\llbracket \cdot \rrbracket_\rho$, and specializing as appropriate, we have that $H_{1*}^1 = H'_{1g} \uplus H'_1 \uplus H_{1+}$ and

$$(H_{2g+} \uplus H_{2+}, C_{\tau_2 \mapsto \tau_2} v_2^a) \overset{*}{\longrightarrow}_{L_2 \cup FL(e_2^1)} (H'_{2g} \uplus H'_2 \uplus H_{2+}, v_2^1) \not\twoheadrightarrow_{L_2 \cup FL(e_2^1)}$$

where $H'_{1g}, H'_{2g} : W'''$ for some $W'' \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W'', L_1 \cup FL(e_1^1) \cup FL(\mathrm{cod}(H_{1+})), L_2 \cup FL(e_2^1) \cup FL(\mathrm{cod}(H_2}$
W''' such that

$$(W''', (H'_1, v_1^1), (H'_2, v_2^1)) \in \mathcal{V}\llbracket \tau_1 \rrbracket_\rho$$

Since $\tau_1 \in$ Duplicable, expanding the definition of Duplicable and $\mathcal{V}\llbracket \cdot \rrbracket_\cdot$ reveals that we have $H'_1 = H'_2 = \emptyset$.
Now, by the operational semantics of LCVM, we have that

$$\begin{array}{rl}
(H_{1g+} \uplus H_{1+}, (C_{\tau_2 \mapsto \tau_2} \ ((\lambda x_1^1.e_1^1) \ (C_{\tau_1 \mapsto \tau_1} \ v_1^a)))) & \overset{*}{\longrightarrow}_{L_1} \left(H'_{1g} \uplus H_{1+}, (C_{\tau_2 \mapsto \tau_2} \ ((\lambda x_1^1.e_1^1) \ v_1^1))\right) \\
& \overset{1}{\longrightarrow}_{L_1} \left(H'_{1g} \uplus H_{1+}, (C_{\tau_2 \mapsto \tau_2} \ [x_1^1 \mapsto v_1^1]e_1^1)\right) \\
& \overset{*}{\longrightarrow}_{L_1} (H_{1*}, v_1) \\
& \not\twoheadrightarrow_{L_1}
\end{array}$$

Then applying Lemma 4.3 again, we have that $\left(H'_{1g} \uplus H_{1+}, [x_1^1 \mapsto v_1^1]e_1^1\right) \overset{*}{\longrightarrow}_{L_1} (H_{1*}^2, v_1^2) \not\twoheadrightarrow_{L_1}$ for some H_{1*}^2, v_1^2. Since $(W''', (\emptyset, v_1^1), (\emptyset, v_2^1)) \in \mathcal{V}\llbracket \tau_1 \rrbracket_\rho$ and $W' \sqsubseteq_{\emptyset,\emptyset,e_1^1,e_2^1} W'''$ (by Lemma 4.6), we have $(W''', (\emptyset, [x_1^1 \mapsto v_1^1]e_1^1), (\emptyset, [x_2^2 \mapsto v_2^1]e_2^1)) \in \mathcal{E}\llbracket \tau_2 \rrbracket_\rho$ by (27). Expanding the definition of $\mathcal{E}\llbracket \cdot \rrbracket_\rho$, we have that $H_{1*}^2 = H''_{1g} \uplus H''_1 \uplus H_{1+}$ and

$$(H_{2g+} \uplus H_{2+}, [x_2^2 \mapsto v_2^1]e_2^1) \overset{*}{\longrightarrow}_{L_2} (H''_{2g} \uplus H''_2 \uplus H_{2+}, v_2^2) \not\twoheadrightarrow_{L_2}$$

where $H''_{1g}, H''_{2g} : W''''$ for some $W''' \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W''', L_1 \cup FL(\mathrm{cod}(H_{1+})), L_2 \cup FL(\mathrm{cod}(H_{2+})))}$
W'''' such that

$$(W'''', (H''_1, v_1^2), (H''_2, v_2^2)) \in \mathcal{V}\llbracket \tau_2 \rrbracket_\rho$$

Now, by the operational semantics of LCVM, we have that

$$\begin{array}{rl}
\left(H'_{1g+} \uplus H_{1+}, (C_{\tau_2 \mapsto \tau_2} \ [x_1^1 \mapsto v_1^1]e_1^1)\right) & \overset{*}{\longrightarrow} \left(H'_{1g} \uplus H''_1 \uplus H_{1+}, (C_{\tau_2 \mapsto \tau_2} \ v_1^2)\right) \\
& \overset{*}{\longrightarrow} (H_{1*}, v_1) \\
& \not\twoheadrightarrow
\end{array}$$

Recall that $(W'''', (\mathrm{H}_1'', \mathrm{v}_1^2), (\mathrm{H}_2'', \mathrm{v}_2^2)) \in \mathcal{V}[\![\tau_2]\!]_\rho$, so $(W'''', (\mathrm{H}_1'', \mathrm{v}_1^2), (\mathrm{H}_2'', \mathrm{v}_2^2)) \in \mathcal{E}[\![\tau_2]\!]_\rho$ by Lemma 4.12. Then, appealing to the indcutive hypothesis that $\tau_2 \sim \tau_2$ is sound, expanding the definition of $\mathcal{E}[\![\cdot]\!]_\rho$, and specializing as appropriate, we have that $\mathrm{H}_{1*} = \mathrm{H}_{1g}''' \uplus \mathrm{H}_{1+}$ and

$$(\mathrm{H}_{2g}'' \uplus \mathrm{H}_2'' \uplus \mathrm{H}_{2+}, \mathrm{C}_{\tau_2 \mapsto \tau_2} \mathrm{v}_2^2) \xrightarrow{*}_{L_2} (\mathrm{H}_{2g}''' \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \nrightarrow_{L_2}$$

where $\mathrm{H}_{1g}''', \mathrm{H}_{2g}''' : W'''''$ for some $W'''' \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W'''',L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))}$ W''''' such that

$$(W''''', (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}[\![\tau_2]\!]_\rho$$

Then we show the goal by taking $W' = W'''''$, $\mathrm{H}_{1g}' = \mathrm{H}_{1g}'''$, $\mathrm{H}_{2g}' = \mathrm{H}_{2g}'''$, and $\mathrm{v}_2 = \mathrm{v}_2$. For showing the configuration with $\mathrm{H}_{2g+} \uplus \mathrm{H}_{2+}$ terminates, we have

$$\begin{aligned}
\left(\mathrm{H}_{2g+} \uplus \mathrm{H}_{2+}, \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \left(\left(\lambda \mathrm{x}_2^1.\mathrm{e}_2^1\right)\ \left(\mathrm{C}_{\tau_1 \mapsto \tau_1}\ \mathrm{v}_2^{\mathrm{a}}\right)\right)\right)\right) &\xrightarrow{*}_{L_2} \left(\mathrm{H}_{2g}' \uplus \mathrm{H}_{2+}, \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \left(\left(\lambda \mathrm{x}_2^1.\mathrm{e}_2^1\right)\ \mathrm{v}_2^1\right)\right)\right) \\
&\xrightarrow{1}_{L_2} \left(\mathrm{H}_{2g}' \uplus \mathrm{H}_{2+}, \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ [\mathrm{x}_2^1 \mapsto \mathrm{v}_2^1]\mathrm{e}_2^1\right)\right) \\
&\xrightarrow{*}_{L_2} \left(\mathrm{H}_{2g}'' \uplus \mathrm{H}_2'' \uplus \mathrm{H}_{2+}, \left(\mathrm{C}_{\tau_2 \mapsto \tau_2}\ \mathrm{v}_2^2\right)\right) \\
&\xrightarrow{*}_{L_2} \left(\mathrm{H}_{2g}''' \uplus \mathrm{H}_{2+}, \mathrm{v}_2\right) \\
&\nrightarrow_{L_2}
\end{aligned}$$

$\boxed{\mathtt{ref}\ \tau \sim \exists \zeta.\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta}$

(1) For the first direction, we show that

$$\forall (W, (\mathrm{H}_1, \mathrm{e}_1), (\mathrm{H}_2, \mathrm{e}_2)) \in \mathcal{E}[\![\mathtt{ref}\ \tau]\!]_\rho.$$
$$\left(W, (\mathrm{H}_1, \mathrm{C}_{\mathtt{ref}\ \tau \mapsto \exists \zeta.\mathrm{cap}\ \zeta\ \tau\ \otimes\ !\mathrm{ptr}\ \zeta}(\mathrm{e}_1)\right), \left(\mathrm{H}_2, \mathrm{C}_{\mathtt{ref}\ \tau \mapsto \exists \zeta.\mathrm{cap}\ \zeta\ \tau\ \otimes\ !\mathrm{ptr}\ \zeta}(\mathrm{e}_2))\right) \in \mathcal{E}[\![\exists \zeta.\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta]\!]_\rho$$

where we have, by our induction hypothesis, that we can convert τ to τ.
We first expand the conversions, noting that the terms in question are:

$$\mathrm{let}\ \mathrm{x}_\ell = \mathrm{alloc}\ \mathrm{C}_{\tau \mapsto \tau}(!\mathrm{e}_\mathrm{i})\ \mathrm{in}\ ((), \mathrm{x}_\ell)$$

Expanding the definition of $\mathcal{E}[\![\exists \zeta.\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta]\!]_\rho$, we see that what we need to show is that:

$$\begin{aligned}
&\exists \mathrm{H}_1', \mathrm{H}_{1g}'.\forall \mathrm{H}_{2+} : \mathit{MHeap}.\exists \mathrm{H}_2', W', \mathrm{H}_{2g}', \mathrm{v}_2. \\
&\mathrm{H}_{1*} = \mathrm{H}_{1g}' \uplus \mathrm{H}_1' \uplus \mathrm{H}_{1+}\ \wedge \mathrm{H}_{1g}', \mathrm{H}_{2g'} : W' \wedge \\
&W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))}\ W' \wedge \\
&(W', (\mathrm{H}_1', \mathrm{v}_1), (\mathrm{H}_2', \mathrm{v}_2)) \in \mathcal{V}[\![\exists \zeta.\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta]\!]_\rho \wedge \\
&(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathrm{let}\ \mathrm{x}_\ell = \mathrm{alloc}\ \mathrm{C}_{\tau \mapsto \tau}(!\mathrm{e}_2)\ \mathrm{in}\ ((), \mathrm{x}_\ell)) \xrightarrow{*}_{L_2} (\mathrm{H}_{2g}' \uplus \mathrm{H}_2' \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \nrightarrow_{L_2}
\end{aligned}$$

given arbitrary $L_1, L_2, \mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W, \mathrm{v}_1, \mathrm{H}_{1+} : \mathit{MHeap}, \mathrm{H}_{1*}$, such that

$$(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \mathrm{let}\ \mathrm{x}_\ell = \mathrm{alloc}\ \mathrm{C}_{\tau \mapsto \tau}(!\mathrm{e}_1)\ \mathrm{in}\ ((), \mathrm{x}_\ell)) \xrightarrow{*}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \nrightarrow_{L_1}$$

By Lemma 4.3, we have that $(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \mathrm{e}_1) \xrightarrow{*}_{L_1} (\mathrm{H}_{1*}^1, \mathrm{v}_1^1) \nrightarrow_{L_1}$ for some $\mathrm{H}_{1*}^1, \mathrm{v}_1^1$.

Our induction hypothesis, appropriately instantiated and simplified, then tells us that

$$\begin{aligned}&\exists W^1\ \mathsf{H}^1_{1g+}.\mathsf{H}^1_{1*} = \mathsf{H}^1_{1g+} \uplus \mathsf{H}_{1+} \wedge\ \mathsf{H}^1_{1g+}, \mathsf{H}^1_{2g+} : W^1 \wedge \\ &\quad W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathsf{H}_{2+})))}\ W^1 \wedge \\ &\quad \forall \mathsf{H}_{2+}.\exists \mathsf{v}^1_2, \mathsf{H}^1_{2g+}.(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, \mathsf{e}_2) \overset{*}{\longrightarrow}_{L_2} (\mathsf{H}^1_{2g+} \uplus \mathsf{H}_{2+}, \mathsf{v}^1_2) \twoheadrightarrow_{L_2}\ \wedge (W^1, (\emptyset, \mathsf{v}^1_1), (\emptyset, \mathsf{v}^1_2)) \in \mathcal{V}[\![\mathtt{ref}\ \tau]\!]_\rho \end{aligned} \tag{28}$$

This means, in particular, that v^1_1 and v^1_2 are locations, call them ℓ_1 and ℓ_2, and heap satisfaction means that $\mathsf{H}^1_{ig+}(\ell_i)$ are values (call them v_1 and v_2) related by $\mathcal{V}[\![\tau]\!]_\rho$. Also, since the value relation for MiniML doesn't allow heap fragments, this means that the locations in H_i have been consumed.

Thus, we can instantiate our induction hypothesis for $C_{\tau \mapsto \tau}$ with v_i and get reductions that we can use to again appeal to Lemma 4.3, with. In particular, we know that we proceed with the following reductions thus far (with related ones on the other side):

$$\begin{aligned}&(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x}_\ell = \mathsf{alloc}\ \mathsf{C}_{\tau \mapsto \tau}(!\mathsf{e}_1)\ \mathsf{in}\ ((), \mathsf{x}_\ell)) \\ &\overset{*}{\longrightarrow}_{L_1} (\mathsf{H}^1_{1g+} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x}_\ell = \mathsf{alloc}\ \mathsf{C}_{\tau \mapsto \tau}(!\ell_1)\ \mathsf{in}\ ((), \mathsf{x}_\ell)) \\ &\overset{*}{\longrightarrow}_{L_1} (\mathsf{H}^1_{1g+} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x}_\ell = \mathsf{alloc}\ \mathsf{C}_{\tau \mapsto \tau}(\mathsf{v}_1)\ \mathsf{in}\ ((), \mathsf{x}_\ell)) \\ &\overset{*}{\longrightarrow}_{L_1} (\mathsf{H}^2_{1g+} \uplus \mathsf{H}^2_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x}_\ell = \mathsf{alloc}\ \mathsf{v}_{1'}\ \mathsf{in}\ ((), \mathsf{x}_\ell))\end{aligned}$$

Where we know we have $W^1 \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W^1,L_1 \cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathsf{H}_{2+})))}$ W^2, $\mathsf{H}^2_{1g+}, \mathsf{H}^2_{2g+} : W^2$, and $(W^2, (\mathsf{H}^2_1, \mathsf{v}_{1'}), (\mathsf{H}^2_2, \mathsf{v}_{2'})) \in \mathcal{V}[\![\tau]\!]_\rho$.

Now, we can proceed with the remaining reductions, after which we have to complete all our original obligations at the resulting future world. The reductions are:

$$\begin{aligned}&(\mathsf{H}^2_{1g+} \uplus \mathsf{H}^2_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x}_\ell = \mathsf{alloc}\ \mathsf{v}_{1'}\ \mathsf{in}\ ((), \mathsf{x}_\ell)) \\ &\overset{*}{\longrightarrow}_{L_1} (\mathsf{H}^2_{1g+} \uplus \{\ell_{1'} \overset{m}{\mapsto} v'_1\} \uplus \mathsf{H}^2_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x}_\ell = \ell_{1'}\ \mathsf{in}\ ((), \mathsf{x}_\ell)) \\ &\overset{*}{\longrightarrow}_{L_1} (\mathsf{H}^2_{1g+} \uplus \mathsf{H}^2_1 \uplus \{\ell_{1'} \overset{m}{\mapsto} v'_1\} \uplus \mathsf{H}_{1+}, ((), \ell_{1'}))\end{aligned}$$

Where the latter has clearly terminated to a value. We know, analogously, that the other side will run in the same way, terminating with the configuration:

$$(\mathsf{H}^2_{2g+} \uplus \mathsf{H}^2_2 \uplus \{\ell_{2'} \overset{m}{\mapsto} v'_2\} \uplus \mathsf{H}_{2+}, ((), \ell_{2'}))$$

The world we choose is simply W^2 — our manual allocation doesn't change the garbage collected fragments of the heap (indicated by name with a subscript g), and thus the same world and heap satisfaction still holds. Since we already have the values to which both sides terminated, our remaining obligation is to show:

$$(W^2, (\mathsf{H}^2_1 \uplus \{\ell_{1'} \overset{m}{\mapsto} v'_1\}, ((), \ell_{1'})), (\mathsf{H}^2_2 \uplus \{\ell_{2'} \overset{m}{\mapsto} v'_2\}, ((), \ell_{2'}))) \in \mathcal{V}[\![\exists \zeta.\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta]\!]_\rho$$

Expanding the definition of $\mathcal{V}[\![\exists \zeta.\tau]\!]_\rho$, it suffices to show that:

$$(W^2, (\mathsf{H}^2_1 \uplus \{\ell_{1'} \overset{m}{\mapsto} v_{1'}\}, ((), \ell_{1'})), (\mathsf{H}^2_2 \uplus \{\ell_{2'} \overset{m}{\mapsto} v'_2\}, ((), \ell_{2'}))) \in \mathcal{V}[\![\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta]\!]_{\rho[\mathrm{L3}(\zeta) \mapsto (\ell_{1'}, \ell_{2'})]}$$

Now, we turn to the definition of $\mathcal{V}[\![\tau_1 \otimes \tau_2]\!]_\rho$, which says we need to split the heaps and then prove, using the split (we use empty heaps on one side of our split), the following two obligations:

$$(W^2, (\mathsf{H}^2_1 \uplus \{\ell_{1'} \overset{m}{\mapsto} v'_1\}, ()), (\mathsf{H}^2_2 \uplus \{\ell_{2'} \overset{m}{\mapsto} v'_2\}, ())) \in \mathcal{V}[\![\mathrm{cap}\ \zeta\ \tau]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_{1'},\ell_{2'})]}\}$$
$$(W^2, (\emptyset, \ell_{1'}), (\emptyset, \ell_{2'})) \in \mathcal{V}[\![!\mathrm{ptr}\ \zeta]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_{1'},\ell_{2'})]}$$

The second one holds trivially, since ! requires empty heaps and the ptr type requires that the locations are mapped to by the type environment, which they are. The first is only slightly less trivial: it requires, first, that $\rho[\mathrm{L3}(\zeta) \mapsto (\ell_{1'}, \ell_2)](\zeta) = (\ell_1, \ell_2)$, which it clearly does. Then, that those locations map to values in the heap, and that, for the rest of the heap, the following holds:

$$(W^2, (\mathsf{H}^2_{1'}, \mathsf{v}_{1'}), (\mathsf{H}^2_{2'}, \mathsf{v}_{21})) \in \mathcal{V}[\![\tau]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_{1'},\ell_{2'})]}\}$$

This holds by earlier assumption on $\mathsf{v}_{1'}$ and $\mathsf{v}_{2'}$ and weakening in the type substitution.

(2) The other direction, requires that we show

$$\forall (W, (\mathsf{H}_1, \mathsf{e}_1), (\mathsf{H}_2, \mathsf{e}_2)) \in \mathcal{E}[\![\exists\zeta.\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta]\!]_\rho.$$
$$\left(W, (\mathsf{H}_1, \mathsf{C}_{\exists\zeta.\mathrm{cap}\ \zeta\ \tau\ \otimes\ !\mathrm{ptr}\ \zeta\mapsto\mathtt{ref}\ \tau}(\mathsf{e}_1)), (\mathsf{H}_2, \mathsf{C}_{\exists\zeta.\mathrm{cap}\ \zeta\ \tau\ \otimes\ !\mathrm{ptr}\ \zeta\mapsto\mathtt{ref}\ \tau}(\mathsf{e}_2))\right) \in \mathcal{E}[\![\mathtt{ref}\ \tau]\!]_\rho$$

where we have, by our induction hypothesis, that we can convert τ to τ.
We first expand the conversions, noting that the terms in question are:

$$\mathsf{let}\ \mathsf{x}_\ell = \mathsf{snd}\ \mathsf{e}_\mathsf{i}\ \mathsf{in}\ \mathsf{let}\ \_ = (\mathsf{x}_\ell := \mathsf{C}_{\tau\mapsto\tau}(!\mathsf{x}_\ell))\ \mathsf{in}\ \mathsf{gcmov}\ \mathsf{x}_\ell$$

As before, we expand the definition our obligation, in this case $\mathcal{E}[\![\mathtt{ref}\ \tau]\!]_\rho$, to show that what we need is that:

$$\exists W', \mathsf{H}'_{1g}, \mathsf{H}'_{2g}.\forall \mathsf{H}_{2+}.\exists \mathsf{v}_2.$$
$$\mathsf{H}_{1*} = \mathsf{H}'_{1g} \uplus \mathsf{H}_{1+}\ \wedge \mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W' \wedge$$
$$W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathsf{H}_{2+})))}\ W' \wedge$$
$$(W', (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}[\![\mathtt{ref}\ \tau]\!]_\rho \wedge$$
$$(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \mathsf{let}\ \mathsf{x}_\ell = \mathsf{snd}\ \mathsf{e}_2\ \mathsf{in}\ \mathsf{let}\ \_ = (\mathsf{x}_\ell := \mathsf{C}_{\tau\mapsto\tau}(!\mathsf{x}_\ell))\ \mathsf{in}\ \mathsf{gcmov}\ \mathsf{x}_\ell) \overset{*}{\longrightarrow}_{L_2} (\mathsf{H}'_{2g} \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \not\twoheadrightarrow_{L_1}$$

given arbitrary $L_1, L_2, \mathsf{H}_{1g+}, \mathsf{H}_{2g+} : W, \mathsf{v}_1, \mathsf{H}_{1+}, \mathsf{H}_{1*}$, such that

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x}_\ell = \mathsf{snd}\ \mathsf{e}_1\ \mathsf{in}\ \mathsf{let}\ \_ = (\mathsf{x}_\ell := \mathsf{C}_{\tau\mapsto\tau}(!\mathsf{x}_\ell))\ \mathsf{in}\ \mathsf{gcmov}\ \mathsf{x}_\ell) \overset{*}{\longrightarrow}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \not\twoheadrightarrow_{L_1}$$

We appeal to Lemma 4.3, which tells us that $(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{e}_1) \overset{*}{\longrightarrow}_{L^1} (\mathsf{H}^1_{1*}, \mathsf{v}^1_1) \not\twoheadrightarrow_{L^1}$ for some $\mathsf{H}^1_{1*}, \mathsf{v}^1_1$.
Our induction hypothesis, appropriately instantiated and simplified, then tells us that

$$\begin{aligned}
\exists \mathsf{H}^1_1, \mathsf{H}^1_{1g}.\forall \mathsf{H}_{2+} : \mathit{MHeap}.\exists \mathsf{H}^1_2, W', \mathsf{H}^1_{2g}, {\mathsf{v}_2}^1.\\
\mathsf{H}_{1*} = \mathsf{H}^1_{1g} \uplus \mathsf{H}^1_1 \uplus \mathsf{H}_{1+}\ \wedge \mathsf{H}^1_{1g}, \mathsf{H}^1_{2g'} : W^1 \wedge\\
W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathsf{H}_{2+})))}\ W^1 \wedge\\
(W^1, (\mathsf{H}^1_1, {\mathsf{v}_1}^1), (\mathsf{H}^1_2, {\mathsf{v}_2}^1)) \in \mathcal{V}[\![\exists\zeta.\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta]\!]_\rho \wedge\\
(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, \mathsf{e}_1) \overset{*}{\longrightarrow}_{L_2} (\mathsf{H}^1_{2g} \uplus \mathsf{H}^1_2 \uplus \mathsf{H}_{2+}, {\mathsf{v}_2}^1) \not\twoheadrightarrow
\end{aligned} \tag{29}$$

In particular, that means that v^1_1 and v^1_2 have the form $((), \ell_\mathsf{i})$, where the value relation means that the heap fragments map ℓ_i to a v_i. Note that H^1_i is composed of $\{\ell_1 \overset{m}{\mapsto} \mathsf{v}_\mathsf{i}\} \uplus \mathsf{H}^{1'}_i$. This follows from the value relation.
If we continue evaluating our original terms, we step as follows:

$$\begin{array}{l}
(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x}_\ell = \mathsf{snd}\ \mathsf{e}_1\ \mathsf{in}\ \mathsf{let}\ \_ = (\mathsf{x}_\ell := \mathsf{C}_{\tau\mapsto\tau}(!\mathsf{x}_\ell))\ \mathsf{in}\ \mathsf{gcmov}\ \mathsf{x}_\ell) \overset{*}{\rightarrow}_{L_1} \\
(\mathsf{H}^1_{1g+} \uplus \{\ell_1 \overset{m}{\mapsto} \mathsf{v}_\mathsf{i}\} \uplus \mathsf{H}^{1'}_i \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x}_\ell = \mathsf{snd}\ ((), \ell_1)\ \mathsf{in}\ \mathsf{let}\ \_ = (\mathsf{x}_\ell := \mathsf{C}_{\tau\mapsto\tau}(!\mathsf{x}_\ell))\ \mathsf{in}\ \mathsf{gcmov}\ \mathsf{x}_\ell) \rightarrow_{L_1} \\
(\mathsf{H}^1_{1g+} \uplus \{\ell_1 \overset{m}{\mapsto} \mathsf{v}_\mathsf{i}\} \uplus \mathsf{H}^{1'}_i \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x}_\ell = \ell_1\ \mathsf{in}\ \mathsf{let}\ \_ = (\mathsf{x}_\ell := \mathsf{C}_{\tau\mapsto\tau}(!\mathsf{x}_\ell))\ \mathsf{in}\ \mathsf{gcmov}\ \mathsf{x}_\ell) \rightarrow_{L_1} \\
(\mathsf{H}^1_{1g+} \uplus \{\ell_1 \overset{m}{\mapsto} \mathsf{v}_1\} \uplus \mathsf{H}^{1'}_i \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = (\ell_1 := \mathsf{C}_{\tau\mapsto\tau}(!\ell_1))\ \mathsf{in}\ \mathsf{gcmov}\ \ell_1) \rightarrow_{L_1} \\
(\mathsf{H}^1_{1g+} \uplus \{\ell_1 \overset{m}{\mapsto} \mathsf{v}_1\} \uplus \mathsf{H}^{1'}_i \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = (\ell_1 := \mathsf{C}_{\tau\mapsto\tau}(\mathsf{v}_1))\ \mathsf{in}\ \mathsf{gcmov}\ \ell_1)
\end{array}$$

Since we know that v_1 was in the value relation at type τ, we can appeal to our induction hypothesis with the heap fragment $\mathsf{H}^{1'}_i$ to get that $C_{\tau\mapsto\tau}(\mathsf{v}_1)$ (and, correspondingly $C_{\tau\mapsto\tau}(\mathsf{v}_2)$) are in the expression relation at $\mathcal{E}[\![\tau]\!]_\rho$. That expression relation will tell us that once the term runs to a value, that heap fragment will be consumed.

This means, in particular, that we can combine Lemma 4.3 with the definition of the expression relation to get that $(\mathsf{H}^1_{1g+} \uplus \{\ell_1 \overset{m}{\mapsto} \mathsf{v}_1\} \uplus \mathsf{H}^{1'}_i \uplus \mathsf{H}_{1+}, C_{\tau\mapsto\tau}(\mathsf{v}_1)) \overset{*}{\rightarrow}_{L_1} (\mathsf{H}^2_{1g+} \uplus \{\ell_1 \overset{m}{\mapsto} \mathsf{v}_1\} \uplus \mathsf{H}_{1+}, \mathsf{v}^2_1) \nrightarrow_{L_1}$ for some $\mathsf{H}^2_{1g+}, \mathsf{v}^2_1$, where v^2_1 is related to a corresponding v^2_2 in $\mathcal{V}[\![\tau]\!]_\rho$ at a world W^2 that is an extension of W^1 (note that all the other steps did not change the garbage collected portion of the heap, so the only changes happened during the conversion, and are thus guided by the expression relation that our induction hypothesis produces).

This means our final sequence of steps are:

$$\begin{array}{l}
(\mathsf{H}^1_{1g+} \uplus \{\ell_1 \overset{m}{\mapsto} \mathsf{v}_1\} \uplus \mathsf{H}^{1'}_i \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = (\ell_1 := \mathsf{C}_{\tau\mapsto\tau}(\mathsf{v}_1))\ \mathsf{in}\ \mathsf{gcmov}\ \ell_1) \overset{*}{\rightarrow}_{L_1} \\
(\mathsf{H}^2_{1g+} \uplus \{\ell_1 \overset{m}{\mapsto} \mathsf{v}_1\} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = (\ell_1 := \mathsf{v}^2_1)\ \mathsf{in}\ \mathsf{gcmov}\ \ell_1) \rightarrow_{L_1} \\
(\mathsf{H}^2_{1g+} \uplus \{\ell_1 \overset{m}{\mapsto} \mathsf{v}^2_1\} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = ()\ \mathsf{in}\ \mathsf{gcmov}\ \ell_1) \rightarrow_{L_1} \\
(\mathsf{H}^2_{1g+} \uplus \{\ell_1 \overset{m}{\mapsto} \mathsf{v}^2_1\} \uplus \mathsf{H}_{1+}, \mathsf{gcmov}\ \ell_1) \rightarrow_{L_1} \\
(\mathsf{H}^2_{1g+} \uplus \{\ell_1 \overset{gc}{\mapsto} \mathsf{v}^2_1\} \uplus \mathsf{H}_{1+}, \ell_1)
\end{array}$$

And in particular, we can relate our final values, ℓ_1 and ℓ_2, at $\mathcal{V}[\![\mathtt{ref}\ \tau]\!]_\rho$ at a world W^3, which is W^2 extended with the mapping from (ℓ_1, ℓ_2) to $\mathcal{V}[\![\tau]\!]_\rho$. We note, critically, that the owned portion of the heap is now empty, a requirement of $\mathcal{V}[\![\tau]\!]_\rho$, having been moved into the garbage collected portion of the heap.

□

4.6 Logical Relation Soundness

4.6.1 Supporting Lemmas.

Lemma 4.5 (World Extension Weakening). *If $W \sqsubseteq_{\mathbb{L},\eta} W'$, then for any $\mathbb{L}'$ such that $\mathbb{L}'.j \subseteq \mathbb{L}.j$ for all $j \in \{1, 2\}$ and for any $\eta' \subseteq \eta$, $W \sqsubseteq_{\mathbb{L}',\eta'} W'$.*

Proof. Let $W = (k, \Psi)$ and $W' = (j, \Psi')$. From $W \sqsubseteq_{\mathbb{L},\eta} W'$, we have $j \leq k$. We also have $\mathbb{L}.1\#\mathrm{dom}((\Psi')^1)$ and $\mathbb{L}.2\#\mathrm{dom}((\Psi')^2)$. Since $\mathbb{L}'.1 \subseteq \mathbb{L}.1$ and $\mathbb{L}'.2 \subseteq \mathbb{L}.2$, this implies $\mathbb{L}'.1\#\mathrm{dom}((\Psi')^1)$ and $\mathbb{L}'.2\#\mathrm{dom}((\Psi')^2)$. Moreover, for all $(\ell_1, \ell_2) \in \eta$, $\Psi'(\ell_1, \ell_2) = \lfloor \Psi(\ell_1, \ell_2) \rfloor_j$. Since $\eta' \subseteq \eta$, it follows that for all $(\ell_1, \ell_2) \in \eta'$, $\Psi'(\ell_1, \ell_2) = \lfloor \Psi(\ell_1, \ell_2) \rfloor_j$. Ergo, $W \sqsubseteq_{\mathbb{L}',\eta'} W'$, as was to be proven. □

Lemma 4.6 (World Extension Transitive). *If $W_1 \sqsubseteq_{\mathbb{L}_1,\eta_1} W_2$ and $W_2 \sqsubseteq_{\mathbb{L}_2,\eta_2} W_3$ then*

$$W_1 \sqsubseteq_{(\mathbb{L}_1.1\cap\mathbb{L}_2.1, \mathbb{L}_1.2\cap\mathbb{L}_2.2),\eta_1\cap\eta_2} W_3$$

Proof. Let $\mathbb{L} = (\mathbb{L}_1.1 \cap \mathbb{L}_2.1, \mathbb{L}_1.2 \cap \mathbb{L}_2.2)$ and $\eta = \eta_1 \cap \eta_2$. By Lemma 4.5, $W_1 \sqsubseteq_{\mathbb{L},\eta} W_2$ and $W_2 \sqsubseteq_{\mathbb{L},\eta} W_3$. We would like to show $W_1 \sqsubseteq_{\mathbb{L},\eta} W_3$.

Let $W_1 = (k_1, \Psi_1)$, $W_2 = (k_2, \Psi_2)$, and $W_3 = (k_3, \Psi_3)$.

We know from world extension that $k_1 \leq k_2$ and $k_2 \leq k_3$, so by transitivity, $k_1 \leq k_3$.

By $W_2 \sqsubseteq_{\mathbb{L},\eta} W_3$, $\mathbb{L}.1\#\mathrm{dom}(\Psi_3^1)$ and $\mathbb{L}.2\#\mathrm{dom}(\Psi_3^2)$.

Finally, by both world extensions, for all $(\ell_1, \ell_2) \in \eta$,

$$\Psi_3(\ell_1, \ell_2) = \lfloor \Psi_2(\ell_1, \ell_2) \rfloor_{k_3} = \lfloor \lfloor \Psi_1(\ell_1, \ell_2) \rfloor_{k_2} \rfloor_{k_3}$$

Then, since $k_2 \leq k_3$, we find that $\Psi_3(\ell_1, \ell_2) = \lfloor \lfloor \Psi_1(\ell_1, \ell_2) \rfloor_{k_2} \rfloor_{k_3} = \lfloor \Psi_1(\ell_1, \ell_2) \rfloor_{k_3}$. This suffices to show that $W_1 \sqsubseteq_{\mathbb{L},\eta} W_3$, as was to be proven. □

Lemma 4.7 (World Extension).

(1) *If* $(W, (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_\rho$, *and* $W \sqsubseteq_{\mathsf{H}_1,\mathsf{H}_2,\mathsf{v}_1,\mathsf{v}_2} W'$, *then* $(W', (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_\rho$.

(2) *If* $(W, \mathsf{H}_1, \mathsf{H}_2, \gamma_{\mathrm{L}}.\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho$ *and* $W \sqsubseteq_{\mathsf{H}_1,\mathsf{H}_2,\gamma_{\mathrm{L}}.\Gamma^1(.),\gamma_{\mathrm{L}}.\Gamma^2(.)} W'$, *then* $(W', \mathsf{H}_1, \mathsf{H}_2, \gamma_{\mathrm{L}}.\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho$.

(3) *If* $(W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho$ *and* $W \sqsubseteq_{\emptyset,\emptyset,\gamma_\Gamma^1(.),\gamma_\Gamma^2(.)} W'$, *then* $(W', \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho$.

Proof. (1) By induction on τ. Most cases are trivial, relying on Lemma 4.6 where appropriate. The only non-trivial cases are $\tau = \mathtt{ref}\ \tau$ and $\tau = \mathsf{cap}\ \zeta\ \tau$.

- $\tau = \mathtt{ref}\ \tau$: Suppose that $(W, (\emptyset, \ell_1), (\emptyset, \ell_2)) \in \mathcal{V}\llbracket \mathtt{ref}\ \tau \rrbracket_\rho$ and $W \sqsubseteq_{\emptyset,\emptyset,\ell_1,\ell_2} W'$. We would like to show $(W', (\emptyset, \ell_1), (\emptyset, \ell_2)) \in \mathcal{V}\llbracket \mathtt{ref}\ \tau \rrbracket_\rho$. Expanding the premise, we have that $W.\Psi(\ell_1, \ell_2) = \lfloor \mathcal{V}\llbracket \tau \rrbracket_\rho \rfloor_{W.k}$. This shows that $(\ell_1, \ell_2) \in \mathrm{dom}(W.\Psi)$, so since ℓ_1 is free in the expression ℓ_1 and ℓ_2 is free in the expression ℓ_2, it follows that $(\ell_1, \ell_2) \in \mathrm{rchgclocs}(W, FL(\ell_1), FL(\ell_2))$. Ergo, by the definition of world extension,
$$W'.\Psi(\ell_1, \ell_2) = \lfloor W.\Psi(\ell_1, \ell_2) \rfloor_{W'.k} = \lfloor \lfloor \mathcal{V}\llbracket \tau \rrbracket_\rho \rfloor_{W.k} \rfloor_{W'.k} = \lfloor \mathcal{V}\llbracket \tau \rrbracket_\rho \rfloor_{W'.k},$$
which suffices to prove $(W', (\emptyset, \ell_1), (\emptyset, \ell_2)) \in \mathcal{V}\llbracket \mathtt{ref}\ \tau \rrbracket_\rho$.
(Note that $\lfloor \lfloor \mathcal{V}\llbracket \tau \rrbracket_\rho \rfloor_{W.k} \rfloor_{W'.k} = \lfloor \mathcal{V}\llbracket \tau \rrbracket_\rho \rfloor_{W'.k}$ follows from $W'.k \leq W.k$, which we get from world extension.)
- $\tau = \mathsf{cap}\ \zeta\ \tau$: Suppose that $(W, (\mathsf{H}_1 \uplus \{\ell_1 \mapsto \mathsf{v}_1\}, ()), (\mathsf{H}_2 \uplus \{\ell_2 \mapsto \mathsf{v}_2\})) \in \mathcal{V}\llbracket \mathsf{cap}\ \zeta\ \tau \rrbracket_\rho$ where $\rho.\mathrm{L3}(\zeta) = (\ell_1, \ell_2)$ and $W \sqsubseteq_{\mathsf{H}_1 \uplus \{\ell_1 \mapsto \mathsf{v}_1\},\mathsf{H}_2 \uplus \{\ell_2 \mapsto \mathsf{v}_2\},(),()} W'$. Expanding the definition of world extension, we find
$$W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_1) \uplus \{\ell_1\},\mathrm{dom}(\mathsf{H}_2) \uplus \{\ell_2\}),\mathrm{rchgclocs}(W,FL(\mathrm{cod}(\mathsf{H}_1)) \cup FL(\mathsf{v}_1),FL(\mathrm{cod}(\mathsf{H}_2)) \cup FL(\mathsf{v}_2))} W'$$
Thus, for $j \in \{1, 2\}$, $(\mathrm{dom}(\mathsf{H}_j) \uplus \{\ell_j\})\#\mathrm{dom}(W'.\Psi^j)$, so $(W', (\mathsf{H}_1 \uplus \{\ell_1 \mapsto \mathsf{v}_1\}, ()), (\mathsf{H}_2 \uplus \{\ell_2 \mapsto \mathsf{v}_2\}, ()))$ is still in *Atom*, which is required to show this tuple is in the value relation.
Moreover, by Lemma 4.5, we find $W \sqsubseteq_{\mathsf{H}_1,\mathsf{H}_2,\mathsf{v}_1,\mathsf{v}_2} W'$.
By expanding the value relation, we find $(W, (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_\rho$. Since $W \sqsubseteq_{\mathsf{H}_1,\mathsf{H}_2,\mathsf{v}_1,\mathsf{v}_2} W'$, by the induction hypothesis, we find $(W', (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_\rho$, which suffices to prove $(W', (\mathsf{H}_1 \uplus \{\ell_1 \mapsto \mathsf{v}_1\}, ()), (\mathsf{H}_2 \uplus \{\ell_2 \mapsto \mathsf{v}_2\}, ())) \in \mathcal{V}\llbracket \mathsf{cap}\ \zeta\ \tau \rrbracket_\rho$.

(2) By induction on $\gamma_{\mathrm{L}}.\Gamma$, appealing to the previous case where appropriate.

(3) By induction on γ_Γ, appealing to the previous case where appropriate.

□

Lemma 4.8 (World Extension and Garbage Collection). *Consider some world* W *and two sets of locations* L_1, L_2. *Then, consider arbitrary heaps* $\mathsf{H}_{1g}, \mathsf{H}_{2g} : W$ *and* $\mathsf{H}_{1m}, \mathsf{H}_{2m}$ *such that* $\mathsf{H}_{1m} : MHeap$, $\mathsf{H}_{2m} : MHeap$, $dom(\mathsf{H}_{1m})\#dom(W.\Psi^1)$, *and* $dom(\mathsf{H}_{2m})\#dom(W.\Psi^2)$. *Let* $L_1' = reachablelocs(\mathsf{H}_{1g} \uplus \mathsf{H}_{1m}, dom(\mathsf{H}_{1m}) \uplus FL(\mathsf{K}_1[\cdot]) \cup L_1)$ *and* $L_2' = reachablelocs(\mathsf{H}_{2g} \uplus \mathsf{H}_{2m}, dom(\mathsf{H}_{2m}) \uplus FL(\mathsf{K}_2[\cdot]) \cup L_2)$.

Then, if

$$(\mathsf{H}_{1g} \uplus \mathsf{H}_{1m}, \mathsf{K}_1[\mathsf{callgc}]) \rightarrow_{L_1} (\mathsf{H}'_{1g} \uplus \mathsf{H}_{1m}, \mathsf{K}_1[()])$$

and

$$(\mathsf{H}_{2g} \uplus \mathsf{H}_{2m}, \mathsf{K}_2[\mathsf{callgc}]) \rightarrow_{L_2} (\mathsf{H}'_{2g} \uplus \mathsf{H}_{2m}, \mathsf{K}_2[()])$$

where $\mathsf{H}'_{1g} : \mathit{GCHeap}$, $\mathsf{H}'_{2g} : \mathit{GCHeap}$, *then there exists some world* W' *such that* $\mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W'$ *and*

$$W \sqsubseteq_{(\mathit{dom}(\mathsf{H}_{1m}),\mathit{dom}(\mathsf{H}_{2m})),\mathit{rchgclocs}(W,L'_1,L'_2)} W' \tag{30}$$

Note: Remember that for all H, L, $L \subseteq \mathit{reachablelocs}(\mathsf{H}, L)$ *and* $\mathit{FL}(\mathit{cod}(\mathsf{H})) \subseteq \mathit{reachablelocs}(\mathsf{H}, L)$. *Ergo,* $\mathit{FL}(\mathit{cod}(\mathsf{H}_{im})) \cup \mathit{FL}(\mathsf{K}_\mathsf{j}[\cdot]) \cup L_j \subseteq L'_j$ *for* $j \in \{1, 2\}$, *which implies*

$$\mathit{rchgclocs}(W, \mathit{FL}(\mathit{cod}(\mathsf{H}_{1m})) \cup \mathit{FL}(\mathsf{K}_1[\cdot]) \cup L_1, \mathit{FL}(\mathit{cod}(\mathsf{H}_{2m})) \cup \mathit{FL}(\mathsf{K}_2[\cdot]) \cup L_2) \subseteq \mathit{rchgclocs}(W, L'_1, L'_2)$$

so by Lemma 4.5, it follows that

$$W \sqsubseteq_{(\mathit{dom}(\mathsf{H}_{1m}),\mathit{dom}(\mathsf{H}_{2m})),\mathit{rchgclocs}(W,\mathit{FL}(\mathit{cod}(\mathsf{H}_{1m}))\cup \mathit{FL}(\mathsf{K}_1[\cdot])\cup L_1,\mathit{FL}(\mathit{cod}(\mathsf{H}_{2m}))\cup \mathit{FL}(\mathsf{K}_2[\cdot])\cup L_2)} W'$$

Proof. Let $W' = (W.k, \Psi')$ where Ψ' is the subset of Ψ restricted to $\mathrm{rchgclocs}(W, L'_1, L'_2)$.

First, it is clear that $W'.k \leq W.k$.

Second, since $W'.\Psi \subseteq W.\Psi$, $\mathrm{dom}(\mathsf{H}_{1m})\#\mathrm{dom}(W.\Psi^1)$, and $\mathrm{dom}(\mathsf{H}_{2m})\#\mathrm{dom}(W.\Psi^2)$, we find that $\mathrm{dom}(\mathsf{H}_{1m})\#\mathrm{dom}(W'.\Psi^1)$ and $\mathrm{dom}(\mathsf{H}_{2m})\#\mathrm{dom}(W'.\Psi^2)$.

Finally, to finish showing (30), we need to show that for all $(\ell_1, \ell_2) \in \mathrm{rchgclocs}(W, L'_1, L'_2)$,

$$W'.\Psi(\ell_1, \ell_2) = \lfloor W.\Psi(\ell_1, \ell_2) \rfloor_{W'.k}$$

If $(\ell_1, \ell_2) \in \mathrm{rchgclocs}(W, L'_1, L'_2)$, then by the definition of Ψ' above, $W'.\Psi(\ell_1, \ell_2) = W.\Psi(\ell_1, \ell_2)$. Thus, since $W'.k = W.k$,

$$W'.\Psi(\ell_1, \ell_2) = W.\Psi(\ell_1, \ell_2) = \lfloor W.\Psi(\ell_1, \ell_2) \rfloor_{W.k} = \lfloor W.\Psi(\ell_1, \ell_2) \rfloor_{W'.k}$$

as was to be demonstrated.

Next, we must show that $\mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W'$. First, since $\mathsf{H}'_{1g} \subseteq \mathsf{H}_{1g}$ and $\mathsf{H}'_{2g} \subseteq \mathsf{H}_{2g}$, it follows that $\mathsf{H}'_{1g} : \mathit{GCHeap}$ and $\mathsf{H}'_{2g} : \mathit{GCHeap}$.

Next, we must show that for all $(\ell_1, \ell_2) \in \mathrm{dom}(W'.\Psi)$, we must show $\ell_1 \in \mathrm{dom}(\mathsf{H}'_{1g})$, $\ell_2 \in \mathrm{dom}(\mathsf{H}'_{2g})$, and

$$(\triangleright W', (\emptyset, \mathsf{H}'_{1g}(\ell_1)), (\emptyset, \mathsf{H}'_{2g}(\ell_2))) \in W'.\Psi(\ell_1, \ell_2) \tag{31}$$

By definition, $\mathrm{dom}(W'.\Psi) = \mathrm{rchgclocs}(W, L'_1, L'_2)$, so if $(\ell_1, \ell_2) \in \mathrm{dom}(W'.\Psi)$, then $(\ell_1, \ell_2) \in \mathrm{dom}(W.\Psi)$, $\ell_1 \in L'_1$ and $\ell_2 \in L'_2$. Since $(\ell_1, \ell_2) \in \mathrm{dom}(W.\Psi)$ and $\mathsf{H}_{1g}, \mathsf{H}_{2g} : W$, we find that $\ell_1 \in \mathrm{dom}(\mathsf{H}_{1g})$, $\ell_2 \in \mathrm{dom}(\mathsf{H}_{2g})$, and $(\triangleright W, (\emptyset, \mathsf{H}_{1g}(\ell_1)), (\emptyset, \mathsf{H}_{2g}(\ell_2))) \in W.\Psi(\ell_1, \ell_2)$.

Then, since $(\ell_1, \ell_2) \in \mathrm{dom}(W'.\Psi)$, $W'.\Psi(\ell_1, \ell_2) = W.\Psi(\ell_1, \ell_2)$. Moreover, by the operational semantics of callgc, $L'_1 \cap \mathrm{dom}(\mathsf{H}_{1g}) \subseteq \mathrm{dom}(\mathsf{H}'_{1g})$, so $\ell_1 \in \mathrm{dom}(\mathsf{H}'_{1g})$ and $\mathsf{H}'_{1g}(\ell_1) = \mathsf{H}_{1g}(\ell_1)$. By similar reasoning, $\ell_2 \in \mathrm{dom}(\mathsf{H}'_{2g})$ and $\mathsf{H}'_{2g}(\ell_2) = \mathsf{H}_{2g}(\ell_2)$. Thus, we deduce that

$$(\triangleright W, (\emptyset, \mathsf{H}'_{1g}(\ell_1)), (\emptyset, \mathsf{H}'_{2g}(\ell_2))) \in W'.\Psi(\ell_1, \ell_2) \tag{32}$$

Next, notice that, by the definition of reachablelocs, since $\ell_1 \in L'_1$, it follows that $\mathit{FL}(\mathsf{H}'_{1g}(\ell_1)) = \mathit{FL}(\mathsf{H}_{1g}(\ell_1)) \subseteq L'_1$. By similar reasoning, $\mathit{FL}(\mathsf{H}'_{2g}(\ell_2)) \subseteq L'_2$. Ergo,

$$\mathrm{rchgclocs}(W, \mathit{FL}(\mathsf{H}'_{1g}(\ell_1)), \mathit{FL}(\mathsf{H}'_{2g}(\ell_2))) \subseteq \mathrm{rchgclocs}(W, L'_1, L'_2)$$

By Lemma 4.5, we then have

$$W \sqsubseteq_{(\emptyset,\emptyset),\mathrm{rchgclocs}(W,\mathit{FL}(\mathsf{H}'_{1g}(\ell_1)),\mathit{FL}(\mathsf{H}'_{2g}(\ell_2)))} W'$$

so it follows that

$$\triangleright W \sqsubseteq_{(\emptyset,\emptyset),\mathrm{rchgclocs}(W,\mathit{FL}(\mathsf{H}'_{1g}(\ell_1)),\mathit{FL}(\mathsf{H}'_{2g}(\ell_2)))} \triangleright W'$$

In other words, $\triangleright W \sqsubseteq_{\emptyset,\emptyset,\mathsf{H}'_{1g}(\ell_1),\mathsf{H}'_{2g}(\ell_2)} \triangleright W'$. Ergo, by (32) and the fact that $W'.\Psi(\ell_1,\ell_2) \in \mathit{Typ}_{W.k}$ to deduce (31), as was to be proven. □

Lemma 4.9 (Compositionality). *If $\Delta \vdash \tau_1$ and $\Delta, \alpha \vdash \tau_2$ and $\rho \in \mathcal{D}[\![\Delta]\!]$, then*

$$\mathcal{V}[\![[\alpha \mapsto \tau_1]\tau_2]\!]_\rho = \mathcal{V}[\![\tau_2]\!]_{\rho[\mathsf{F}(\alpha)\mapsto\mathcal{V}[\![\tau_1]\!]_\rho]}$$

Proof. By induction on τ_2. We show the interesting cases:

Case $\tau_2 = \alpha$.

$$\begin{aligned}
\mathcal{V}[\![[\alpha \mapsto \tau_1]\alpha]\!]_\rho &= \mathcal{V}[\![\tau_1]\!]_\rho && \text{(by sub)}\\
&= \rho[\mathsf{F}(\alpha) \mapsto \mathcal{V}[\![\tau_1]\!]_\rho].\mathsf{F}(\alpha) && \text{(by lookup)}\\
&= \mathcal{V}[\![\alpha]\!]_{\rho[\mathsf{F}(\alpha)\mapsto\mathcal{V}[\![\tau_1]\!]_\rho]} && \text{(by def } \mathcal{V}[\![\cdot]\!]_\cdot\text{)}
\end{aligned}$$

Case $\tau_2 = \beta \neq \alpha$.

$$\begin{aligned}
\mathcal{V}[\![[\alpha \mapsto \tau_1]\beta]\!]_\rho &= \mathcal{V}[\![\beta]\!]_\rho && \text{(by sub)}\\
&= \rho.\mathsf{F}(\beta) && \text{(by def } \mathcal{V}[\![\cdot]\!]_\cdot\text{)}\\
&= \rho[\mathsf{F}(\alpha) \mapsto \mathcal{V}[\![\tau_1]\!]_\rho].\mathsf{F}(\beta) && \text{(by lookup)}\\
&= \mathcal{V}[\![\beta]\!]_{\rho[\mathsf{F}(\alpha)\mapsto\mathcal{V}[\![\tau_1]\!]_\rho]} && \text{(by def } \mathcal{V}[\![\cdot]\!]_\cdot\text{)}
\end{aligned}$$

The other cases are straightforward by expanding the definitions of $\mathcal{V}[\![\cdot]\!]_\cdot, \mathcal{E}[\![\cdot]\!]_\cdot$ and applying the induction hypotheses. □

Lemma 4.10 ($\mathbf{L}^3$ Compositionality). *If $\Delta, \zeta \vdash \tau$, $\rho \in \mathcal{D}[\![\Delta]\!]$, and $\rho(\zeta') = (\ell_1', \ell_2')$, then*

$$\mathcal{V}[\![[\zeta \mapsto \zeta']\tau]\!]_\rho = \mathcal{V}[\![\tau]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_1',\ell_2')]}$$

Proof. By induction on τ. We show the interesting cases:

Case $\tau = \mathrm{ptr}\,\zeta$.

$$\begin{aligned}
\mathcal{V}[\![[\zeta \mapsto \zeta']\mathrm{ptr}\,\zeta]\!]_\rho &= \mathcal{V}[\![\mathrm{ptr}\,\zeta']\!]_\rho && \text{(by sub)}\\
&= \{(W, (\emptyset, \ell_1), (\emptyset, \ell_2)) \mid \rho.\mathrm{L3}(\zeta') = (\ell_1, \ell_2)\} && \text{(by def)}\\
&= \{(W, (\emptyset, \ell_1), (\emptyset, \ell_2)) \mid (\ell_1', \ell_2') = (\ell_1, \ell_2)\} && \text{(by assumption)}\\
&= \{(W, (\emptyset, \ell_1), (\emptyset, \ell_2)) \mid \rho[\mathrm{L3}(\zeta) \mapsto (\ell_1', \ell_2')].\mathrm{L3}(\zeta) = (\ell_1, \ell_2)\} && \text{(by lookup)}\\
&= \mathcal{V}[\![\mathrm{ptr}\,\zeta]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_1',\ell_2')]} && \text{(by def)}
\end{aligned}$$

Case $\tau = \mathrm{ptr}\,\zeta_2$ where $\zeta_2 \neq \zeta$.

$$\begin{aligned}
\mathcal{V}[\![[\zeta \mapsto \zeta']\mathrm{ptr}\,\zeta_2]\!]_\rho &= \mathcal{V}[\![\mathrm{ptr}\,\zeta_2]\!]_\rho && \text{(by sub)}\\
&= \{(W, (\emptyset, \ell_1), (\emptyset, \ell_2)) \mid \rho.\mathrm{L3}(\zeta_2) = (\ell_1, \ell_2)\} && \text{(by def)}\\
&= \{(W, (\emptyset, \ell_1), (\emptyset, \ell_2)) \mid \rho[\mathrm{L3}(\zeta) \mapsto (\ell_1', \ell_2')].\mathrm{L3}(\zeta_2) = (\ell_1, \ell_2)\} && \text{(by lookup)}\\
&= \mathcal{V}[\![\mathrm{ptr}\,\zeta_2]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_1',\ell_2')]} && \text{(by def)}
\end{aligned}$$

Case $\tau = \text{cap}\ \zeta\ \tau_2$**.**

$$\begin{aligned}
\mathcal{V}[\![[\zeta \mapsto \zeta']\text{cap}\ \zeta\ \tau_2]\!]_\rho &= \mathcal{V}[\![\text{cap}\ \zeta'\ [\zeta \mapsto \zeta']\tau_2]\!]_\rho && \text{(by sub)}\\
&= \{(W, (\mathsf{H}_1 \uplus \{\ell_1 \mapsto \mathsf{v}_1\}, ()), (\mathsf{H}_2 \uplus \{\ell_2 \mapsto \mathsf{v}_2\}, ())) \mid \\
&\qquad \rho.\text{L3}(\zeta') = (\ell_1, \ell_2) \wedge (W, (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in \mathcal{V}[\![[\zeta \mapsto \zeta']\tau_2]\!]_\rho\} && \text{(by def)}\\
&= \{(W, (\mathsf{H}_1 \uplus \{\ell_1 \mapsto \mathsf{v}_1\}, ()), (\mathsf{H}_2 \uplus \{\ell_2 \mapsto \mathsf{v}_2\}, ())) \mid \\
&\qquad (\ell_1', \ell_2') = (\ell_1, \ell_2) \wedge (W, (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in \mathcal{V}[\![[\zeta \mapsto \zeta']\tau_2]\!]_\rho\} && \text{(by assumption)}\\
&= \{(W, (\mathsf{H}_1 \uplus \{\ell_1 \mapsto \mathsf{v}_1\}, ()), (\mathsf{H}_2 \uplus \{\ell_2 \mapsto \mathsf{v}_2\}, ())) \mid \\
&\qquad \rho[\text{L3}(\zeta) \mapsto (\ell_1', \ell_2')].\text{L3}(\zeta) = (\ell_1, \ell_2) \wedge \\
&\qquad (W, (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in \mathcal{V}[\![[\zeta \mapsto \zeta']\tau_2]\!]_\rho\} && \text{(by lookup)}\\
&= \{(W, (\mathsf{H}_1 \uplus \{\ell_1 \mapsto \mathsf{v}_1\}, ()), (\mathsf{H}_2 \uplus \{\ell_2 \mapsto \mathsf{v}_2\}, ())) \mid \\
&\qquad \rho[\text{L3}(\zeta) \mapsto (\ell_1', \ell_2')].\text{L3}(\zeta) = (\ell_1, \ell_2) \wedge \\
&\qquad (W, (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in \mathcal{V}[\![\tau_2]\!]_{\rho[\text{L3}(\zeta) \mapsto (\ell_1', \ell_2')]}\} && \text{(by induction)}\\
&= \mathcal{V}[\![\text{cap}\ \zeta\ \tau_2]\!]_{\rho[\text{L3}(\zeta) \mapsto (\ell_1', \ell_2')]} && \text{(by def)}
\end{aligned}$$

Case $\tau = \text{cap}\ \zeta_2\ \tau_2$ **where** $\zeta_2 \neq \zeta$**.**

$$\begin{aligned}
\mathcal{V}[\![[\zeta \mapsto \zeta']\text{cap}\ \zeta_2\ \tau_2]\!]_\rho &= \mathcal{V}[\![\text{cap}\ \zeta_2\ [\zeta \mapsto \zeta']\tau_2]\!]_\rho && \text{(by sub)}\\
&= \{(W, (\mathsf{H}_1 \uplus \{\ell_1 \mapsto \mathsf{v}_1\}, ()), (\mathsf{H}_2 \uplus \{\ell_2 \mapsto \mathsf{v}_2\}, ())) \mid \\
&\qquad \rho.\text{L3}(\zeta_2) = (\ell_1, \ell_2) \wedge (W, (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in \mathcal{V}[\![[\zeta \mapsto \zeta']\tau_2]\!]_\rho\} && \text{(by def)}\\
&= \{(W, (\mathsf{H}_1 \uplus \{\ell_1 \mapsto \mathsf{v}_1\}, ()), (\mathsf{H}_2 \uplus \{\ell_2 \mapsto \mathsf{v}_2\}, ())) \mid \\
&\qquad \rho[\text{L3}(\zeta) \mapsto (\ell_1', \ell_2')].\text{L3}(\zeta_2) = (\ell_1, \ell_2) \wedge \\
&\qquad (W, (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in \mathcal{V}[\![[\zeta \mapsto \zeta']\tau_2]\!]_\rho\} && \text{(by lookup)}\\
&= \{(W, (\mathsf{H}_1 \uplus \{\ell_1 \mapsto \mathsf{v}_1\}, ()), (\mathsf{H}_2 \uplus \{\ell_2 \mapsto \mathsf{v}_2\}, ())) \mid \\
&\qquad \rho[\text{L3}(\zeta) \mapsto (\ell_1', \ell_2')].\text{L3}(\zeta_2) = (\ell_1, \ell_2) \wedge \\
&\qquad (W, (\mathsf{H}_1, \mathsf{v}_1), (\mathsf{H}_2, \mathsf{v}_2)) \in \mathcal{V}[\![\tau_2]\!]_{\rho[\text{L3}(\zeta) \mapsto (\ell_1', \ell_2')]}\} && \text{(by induction)}\\
&= \mathcal{V}[\![\text{cap}\ \zeta\ \tau_2]\!]_{\rho[\text{L3}(\zeta) \mapsto (\ell_1', \ell_2')]} && \text{(by def)}
\end{aligned}$$

The other cases are straightforward by expanding the definitions of $\mathcal{V}[\![\cdot]\!]_\cdot$, $\mathcal{E}[\![\cdot]\!]_\cdot$ and applying the induction hypotheses. □

Lemma 4.11 (Irrelevant Location Variables in $\mathbf{L}^3$). *If* $\Delta \vdash \tau$, $\rho \in \mathcal{D}[\![\Delta]\!]$, *and* $\zeta \notin \Delta$, *then*

$$\mathcal{V}[\![\tau]\!]_\rho = \mathcal{V}[\![\tau]\!]_{\rho[\text{L3}(\zeta) \mapsto (\ell_1, \ell_2)]}$$

Proof. Since $\zeta \notin \Delta$ and $\Delta \vdash \tau$, it must be that ζ is not free in τ. Therefore, the definition of either $\mathcal{V}[\![\tau]\!]_\rho$ or $\mathcal{V}[\![\tau]\!]_{\rho[\text{L3}(\zeta) \mapsto (\ell_1, \ell_2)]}$ will never require looking up $\rho.\text{L3}(\zeta)$, so whether ζ is in the domain of $\rho.\text{L3}$ or not is irrelevant for the definition of the value relation. It then trivially follows that these two value relations are equal. □

Lemma 4.12 (Value Lifting). *If* $(W, (\mathsf{H}_1, \mathsf{e}_1), (\mathsf{H}_2, \mathsf{e}_2)) \in \mathcal{V}[\![\tau]\!]_\rho$ *and, if* τ *is a* `MiniML` *type,* $\mathsf{H}_1 = \mathsf{H}_2 = \emptyset$, *then*

$$(W, (\mathsf{H}_1, \mathsf{e}_1), (\mathsf{H}_2, \mathsf{e}_2)) \in \mathcal{E}[\![\tau]\!]_\rho$$

Proof. Since `MiniML` and $\mathbf{L}^3$ have different definitions of $\mathcal{E}[\![\cdot]\!]_\cdot$, we must show the claim for the two languages separately.

MiniML **Language.** Expanding the definition of $\mathcal{E}[\![\cdot]\!]$, we are to show that

$$\begin{array}{l}\exists W', \mathrm{H}'_{1g}, \mathrm{H}'_{2g}.\forall \mathrm{H}_{2+} : \mathit{MHeap}.\exists \mathrm{v}_2.\\ \mathrm{H}_{1*} = \mathrm{H}'_{1g} \uplus \mathrm{H}_{1+} \ \wedge \mathrm{H}'_{1g}, \mathrm{H}'_{2g} : W' \wedge \\ W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W' \wedge \\ (W', (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho \wedge \\ (\mathrm{H}_{2g+} \uplus \mathrm{H}_{2+}, \mathrm{e}_2) \xrightarrow{*}_{L_2} (\mathrm{H}'_{2g} \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \nrightarrow_{L_2}\end{array} \tag{33}$$

given arbitrary $L_1, L_2, \mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W, \mathrm{v}_1, \mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_{1+} : \mathit{MHeap}, \mathrm{H}_{1*}$, such that

$$(\mathrm{H}_{1g+} \uplus \mathrm{H}_{1+}, \mathrm{e}_1) \xrightarrow{*}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \nrightarrow$$

But if $(W, (\emptyset, \mathrm{e}_1), (\emptyset, \mathrm{e}_2)) \in \mathcal{V}[\![\tau]\!]_\rho$, then $\mathrm{e}_1, \mathrm{e}_2$ are values. Since configurations with values as programs do not step, $\mathrm{v}_1 = \mathrm{e}_1$ and we can choose $W' = W$, $\mathrm{H}'_{1g} = \mathrm{H}_{1g}$, $\mathrm{H}'_{2g} = \mathrm{H}_{2g}$, and $\mathrm{v}_2 = \mathrm{e}_2$. Then, by assumption, we have $(W, (\emptyset, \mathrm{e}_1), (\emptyset, \mathrm{e}_2)) \in \mathcal{V}[\![\tau]\!]_\rho$, which suffices to finish the proof.

$\mathbf{L^3}$ **Language** Expanding the definition of $\mathcal{E}[\![\cdot]\!]$., we are to show that

$$\begin{array}{l}\exists \mathrm{H}'_1, \mathrm{H}'_{1g}.\forall \mathrm{H}_{2+} : \mathit{MHeap}.\exists \mathrm{H}'_2, W', \mathrm{H}'_{2g}, \mathrm{v}_2.\\ \mathrm{H}_{1*} = \mathrm{H}'_{1g} \uplus \mathrm{H}'_1 \uplus \mathrm{H}_{1+} \ \wedge \mathrm{H}'_{1g}, \mathrm{H}_{2g'} : W' \wedge \\ W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W' \wedge \\ (W', (\mathrm{H}'_1, \mathrm{v}_1), (\mathrm{H}'_2, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho \wedge \\ (\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathrm{e}_2) \xrightarrow{*}_{L_2} (\mathrm{H}'_{2g} \uplus \mathrm{H}'_2 \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \nrightarrow\end{array} \tag{34}$$

given arbitrary $L_1, L_2, \mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W, \mathrm{v}_1, \mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_{1+} : \mathit{MHeap}, \mathrm{H}_{1*}$, such that

$$(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \mathrm{e}_1) \xrightarrow{*}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \nrightarrow$$

But if $(W, (\mathrm{H}_1, \mathrm{e}_1), (\mathrm{H}_2, \mathrm{e}_2)) \in \mathcal{V}[\![\tau]\!]_\rho$, then $\mathrm{e}_1, \mathrm{e}_2$ are values. Since configurations with values as programs do not step, $\mathrm{v}_1 = \mathrm{e}_1$ and we can choose $W' = W$, $\mathrm{H}'_{1g} = \mathrm{H}_{1g}$, $\mathrm{H}'_{2g} = \mathrm{H}_{2g}$, and $\mathrm{v}_2 = \mathrm{e}_2$. Then, by assumption, we have $(W, (\mathrm{H}_1, \mathrm{e}_1), (\mathrm{H}_2, \mathrm{e}_2)) \in \mathcal{V}[\![\tau]\!]_\rho$, which suffices to finish the proof.

□

Lemma 4.13 (Split Substitutions). *For any world W and substitution γ such that*

$$(W, \mathrm{H}_1, \mathrm{H}_2, \gamma) \in \mathcal{G}[\![\Gamma_1 \uplus \Gamma_2]\!]_\rho$$

there exist $\gamma_1, \gamma_2, \mathrm{H}_{1l}, \mathrm{H}_{1r}, \mathrm{H}_{2l}, \mathrm{H}_{2r}$ such that $\gamma = \gamma_1 \uplus \gamma_2$, $\mathrm{H}_1 = \mathrm{H}_{1l} \uplus \mathrm{H}_{1r}$, $\mathrm{H}_2 = \mathrm{H}_{2l} \uplus \mathrm{H}_{2r}$,

$$(W, \mathrm{H}_{1l}, \mathrm{H}_{1r}, \gamma_1) \in \mathcal{G}[\![\Gamma_1]\!]_\rho$$

and

$$(W, \mathrm{H}_{2l}, \mathrm{H}_{2r}, \gamma_2) \in \mathcal{G}[\![\Gamma_2]\!]_\rho$$

Moreover, for any $i, j \in \{1, 2\}$, for any $\Delta; \Gamma; \Delta; \Gamma_\mathrm{i} \vdash \mathrm{e}_\mathrm{i} : \tau$ and $\gamma_\Gamma \in \mathcal{G}[\![\Gamma]\!]_\rho$,

$$\gamma^j(\gamma^j_\Gamma(\mathrm{e_i}^+)) = \gamma^j_i(\gamma^j_\Gamma(\mathrm{e_i}^+))$$

Proof. First, we need to show that there exist substitutions γ_1 and γ_2. This follows from the inductive structure of $\mathcal{G}[\![\Gamma_1 \uplus \Gamma_2]\!]_\rho$, where we can separate the parts that came from $\mathcal{G}[\![\Gamma_1]\!]_\rho$ and $\mathcal{G}[\![\Gamma_2]\!]_\rho$. The second follows from the fact that the statics means that the rest of the substitution must not occur in the term. and thus $\gamma^j(\mathrm{e_1}^+) = \gamma^j_1(\gamma^j_2(\mathrm{e_1}^+)) = \gamma^j_1(\mathrm{e_1}^+)$ (for example). □

Lemma 4.14 (Bang Substitutions Own No Heap). *For any* $(W, \mathrm{H}_1, \mathrm{H}_2, \gamma_\Gamma) \in \mathcal{G}[\![!\Gamma]\!]_\rho$*, it must be the case that* $\mathrm{H}_1 = \mathrm{H}_2 = \emptyset$.

Proof. We will prove the lemma by induction on the size of $!\Gamma$. If $!\Gamma$ is empty, then the theorem is trivial. Otherwise, suppose that $!\Gamma = !\Gamma_2, \mathrm{x} :!\tau$. Then,

$$(W, \mathrm{H}_1, \mathrm{H}_2, \gamma_\Gamma) = (W, \mathrm{H}_1' \uplus \mathrm{H}_{1v}, \mathrm{H}_2' \uplus \mathrm{H}_{2v}, \gamma_\mathrm{L}.\Gamma'[\mathrm{x} \mapsto (\mathrm{v}_1, \mathrm{v}_2)])$$

where $(W, \mathrm{H}_1', \mathrm{H}_2', \gamma_\mathrm{L}.\Gamma) \in \mathcal{G}[\![!\Gamma_2]\!]_\rho$ and $(W, (\mathrm{H}_{1v}, \mathrm{v}_1), (\mathrm{H}_{2v}, \mathrm{v}_2)) \in \mathcal{V}[\![!\tau]\!]_\rho$. By induction, $\mathrm{H}_1' = \mathrm{H}_2' = \emptyset$ and by expanding the value relation, $\mathrm{H}_{1v} = \mathrm{H}_{2v} = \emptyset$. Thus, $\mathrm{H}_1 = \mathrm{H}_2 = \emptyset$, as was to be proven. □

Lemma 4.15 ($\mathbf{L}^3$ Values Compile to LCVM values). *If* $\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{v} : \tau$ *then given* $\rho, \gamma_\mathrm{L}, \gamma_\Gamma, W, \mathrm{H}_1, \mathrm{H}_2$ *such that*

$$\rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!], \rho.\mathrm{F} \in \mathcal{D}[\![\Delta]\!], (W, \mathrm{H}_1, \mathrm{H}_2, \gamma_\mathrm{L}) \in \mathcal{G}[\![\Gamma]\!]_\rho, \gamma_\Gamma \in \mathcal{G}[\![\Gamma]\!]_\rho$$

it holds that $\gamma_\mathrm{L}^1(\gamma_\Gamma^1(\mathrm{v}^+)))$ *and* $\gamma_\mathrm{L}^2(\gamma_\Gamma^2(\mathrm{v}^+)))$ *are both target values.*

Proof. We will prove the theorem by induction over v.

Case $\mathrm{v} = ()$**.**

If $\mathrm{v} = ()$, then $\mathrm{v}^+ = ()$, which is a target value.

Case $\mathrm{v} = \mathrm{b}$ **for some** $\mathrm{b} \in \mathbb{B}$**.**

If $\mathrm{v} = \mathrm{b}$, then $\mathrm{v}^+ = \mathrm{n}$ for some $\mathrm{n} \in \{0, 1\}$, which is a target value.

Case $\mathrm{v} = \lambda \mathrm{x} : \tau.\mathrm{e}$**.**

If $\mathrm{v} = \lambda \mathrm{x} : \tau.\mathrm{e}$, then $\mathrm{v}^+ = \lambda \mathrm{x}.\mathrm{e}^+$, which is a target value.

Case $\mathrm{v} = \Lambda\zeta.\mathrm{e}$**.**

If $\mathrm{v} = \Lambda\zeta.\mathrm{e}$, then $\mathrm{v}^+ = \lambda \mathrm{x}_\zeta.\mathrm{e}^+$, which is a target value.

Case $\mathrm{v} = \ulcorner\zeta,\ \mathrm{v}\urcorner$**.**

If $\mathrm{v} = \ulcorner\zeta,\ \mathrm{v}'\urcorner$, then $\mathrm{v}^+ = \mathrm{v}'^+$. Ergo, for any $i \in \{1, 2\}$, $\gamma_\mathrm{L}^i(\gamma_\Gamma^i(\mathrm{v}^+)) = \gamma_\mathrm{L}^i(\gamma_\Gamma^i(\mathrm{v}'^+))$, which is a target value by induction.

Case $\mathrm{v} = (\mathrm{v}_1, \mathrm{v}_2)$**.**

If $\mathrm{v} = (\mathrm{v}_1, \mathrm{v}_2)$, then $\mathrm{v}^+ = (\mathrm{v}_1{}^+, \mathrm{v}_2{}^+)$. Ergo, for any $i \in \{1, 2\}$, $\gamma_\mathrm{L}^i(\gamma_\Gamma^i(\mathrm{v}^+)) = (\gamma_\mathrm{L}^i(\gamma_\Gamma^i(\mathrm{v}_1{}^+)), \gamma_\mathrm{L}^i(\gamma_\Gamma^i(\mathrm{v}_2{}^+)))$ is a target value because it is a pair of values as, by induction, $\gamma_\mathrm{L}^i(\gamma_\Gamma^i(\mathrm{v}_1{}^+))$ and $\gamma_\mathrm{L}^i(\gamma_\Gamma^i(\mathrm{v}_2{}^+))$ are target values.

Case $\mathrm{v} = !\mathrm{v}'$**.**

If $\mathrm{v} = !\mathrm{v}'$, then $\mathrm{v}^+ = \mathrm{v}'^+$. Ergo, for any $i \in \{1, 2\}$, $\gamma_\mathrm{L}^i(\gamma_\Gamma^i(\mathrm{v}^+)) = \gamma_\mathrm{L}^i(\gamma_\Gamma^i(\mathrm{v}'^+))$, which is a target value by induction.

□

Lemma 4.16 (Fundamental Property). *If* $\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{e} : \tau$*, then* $\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \tau$ *and if* $\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{e} : \tau$*, then* $\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \tau$*.*

Proof. By induction on typing derivation, relying on the following compatibility lemmas, which have to exist for every typing rule in both source languages. □

Theorem 4.17 (Type Safety for MiniML). *If* $\cdot; \cdot; \cdot; \cdot \vdash \mathrm{e} : \tau$*, then for any heap* H*, if* $(\mathrm{H}, \mathrm{e}^+) \xrightarrow{*} (\mathrm{H}', \mathrm{e}')$*, either there exist* $\mathrm{H}'', \mathrm{e}''$ *such that* $(\mathrm{H}', \mathrm{e}') \longrightarrow (\mathrm{H}'', \mathrm{e}'')$ *or* e' *is a vlaue.*

Proof. By the fundamental property, since the environments under which e is typechecked are empty, $(\cdot, (\emptyset, \mathrm{e}^+), (\emptyset, \mathrm{e}^+)) \in \mathcal{E}[\![\tau]\!]_\cdot$.

Then, either $(\mathrm{H}', \mathrm{e}') \longrightarrow (\mathrm{H}'', \mathrm{e}'')$ or $(\mathrm{H}', \mathrm{e}')$ is irreducible. If $(\mathrm{H}, \mathrm{e}')$ is irreducible, we can apply the expression relation and find that there exists a world W and expression v_2 such that $(W, (\emptyset, \mathrm{e}'), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\cdot$. Since expressions in the value relation are target values, this suffices to show that e' is a value. □

Theorem 4.18 (Type Safety for $\mathbf{L^3}$). *If* $\cdot;\cdot;\cdot;\cdot \vdash \mathrm{e} : \tau$, *then for any heap* H, *if* $(\mathrm{H}, \mathrm{e}^+) \xrightarrow{*} (\mathrm{H}', \mathrm{e}')$, *either there exist* $\mathrm{H}'', \mathrm{e}''$ *such that* $(\mathrm{H}', \mathrm{e}') \longrightarrow (\mathrm{H}'', \mathrm{e}'')$ *or* e' *is a vlaue.*

Proof. By the fundamental property, since the environments under which e is typechecked are empty, $(\cdot, (\emptyset, \mathrm{e}^+), (\emptyset, \mathrm{e}^+)) \in \mathcal{E}\llbracket\tau\rrbracket_{\cdot}$.

Then, either $(\mathrm{H}', \mathrm{e}') \longrightarrow (\mathrm{H}'', \mathrm{e}'')$ or $(\mathrm{H}', \mathrm{e}')$ is irreducible. If $(\mathrm{H}, \mathrm{e}')$ is irreducible, we can apply the expression relation and find that there exists a world W, heaps $\mathrm{H}_1', \mathrm{H}_2'$, and an expression v_2 such that $(W, (\mathrm{H}_1', \mathrm{e}'), (\mathrm{H}_2', \mathrm{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_{\cdot}$. Since expressions in the value relation are target values, this suffices to show that e' is a value. □

4.6.2 MiniML Compatibility Lemmas.

Lemma 4.19 (Compat x).

$$\Delta; !\Gamma; \Delta; \Gamma, \mathrm{x} : \tau \vdash \mathrm{x} \preceq \mathrm{x} : \tau$$

Proof. Expanding the definition of $\preceq$, $\cdot^+$, and $\mathcal{E}\llbracket\cdot\rrbracket_{\cdot}$ (noting via Lemma 4.14 that $\mathrm{H}_1 = \mathrm{H}_2 = \emptyset$), we are to show that

$$\begin{aligned}
&\exists W'\ \mathrm{H}_{1g}'\ \mathrm{H}_{2g}'\ \mathrm{v}_2.\mathrm{H}_{1*} = \mathrm{H}_{1g}' \uplus \mathrm{H}_{1+} \wedge \mathrm{H}_{1g}', \mathrm{H}_{2g}' : W' \wedge \\
&\quad W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W' \wedge (W', (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho \wedge \\
&\qquad (\mathrm{H}_{2g+} \uplus \mathrm{H}_{2+}, \gamma_{\mathrm{L}}^2(\gamma_{\Gamma,\mathrm{x}:\tau}^2(\mathrm{x}))) \xrightarrow{*}_{L_2} (\mathrm{H}_{2g+}' \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \not\twoheadrightarrow_{L_2}
\end{aligned} \tag{35}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_{\Gamma,\mathrm{x}:\tau}, W, \mathrm{H}_{1g+}, \mathrm{H}_{2g+}, \mathrm{H}_{1+}, \mathrm{H}_{1*}, \mathrm{H}_{2+}, \mathrm{v}_1, L_1, L_2$ such that $\rho.\mathrm{L3} \in \mathcal{D}\llbracket\Delta\rrbracket$, $\rho.\mathrm{F} \in \mathcal{D}\llbracket\Delta\rrbracket$, $(W, \emptyset, \emptyset, \gamma_{\mathrm{L}}) \in \mathcal{G}\llbracket!\Gamma\rrbracket_\rho$,
$\gamma_{\Gamma,\mathrm{x}:\tau} \in \mathcal{G}\llbracket\Gamma, \mathrm{x} : \tau\rrbracket_\rho$,
$\mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W$ and

$$(\mathrm{H}_{1g+} \uplus \mathrm{H}_{1+}, \gamma_{\mathrm{L}}^1(\gamma_{\Gamma,\mathrm{x}:\tau}^1(\mathrm{x}))) \xrightarrow{*}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \not\twoheadrightarrow_{L_1}$$

Expanding the definition of $\mathcal{G}\llbracket\cdot\rrbracket_{\cdot}$, we have that

$$\gamma_{\Gamma,\mathrm{x}:\tau} = \gamma[\mathrm{x} \mapsto (\mathrm{v}_1, \mathrm{v}_2)] \wedge \gamma \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho \wedge (W, (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho$$

so $\gamma_{\mathrm{L}}^i(\gamma_{\Gamma,\mathrm{x}:\tau}^i(\mathrm{x})) = \mathrm{v}_\mathrm{i}$. Then we have (35) by taking $W' = W$, $\mathrm{H}_{1g}' = \mathrm{H}_{1g+}$ and $\mathrm{H}_{2g}' = \mathrm{H}_{2g+}$ noting that configurations with values as programs do not step. □

Lemma 4.20 (Compat $()$).

$$\Delta; !\Gamma; \Delta; \Gamma \vdash () \preceq () : \mathtt{unit}$$

Proof. Expanding the definition of $\preceq$, $\cdot^+$, and $\mathcal{E}\llbracket\cdot\rrbracket_{\cdot}$ (noting via Lemma 4.14 that $\mathrm{H}_1 = \mathrm{H}_2 = \emptyset$), we are to show that

$$\begin{aligned}
&\exists W'\ \mathrm{H}_{1g}'\ \mathrm{H}_{2g}'\ \mathrm{v}_2.\mathrm{H}_{1*} = \mathrm{H}_{1g}' \uplus \mathrm{H}_{1+} \wedge \mathrm{H}_{1g}', \mathrm{H}_{2g}' : W' \wedge \\
&\quad W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W' \wedge (W', (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho \wedge \\
&\qquad (\mathrm{H}_{2g+} \uplus \mathrm{H}_{2+}, \gamma_{\mathrm{L}}^2(\gamma_{\Gamma}^2(()))) \xrightarrow{*}_{L_2} (\mathrm{H}_{2g+}' \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \not\twoheadrightarrow_{L_2}
\end{aligned} \tag{36}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_{\Gamma}, W, \mathrm{H}_{1g+}, \mathrm{H}_{2g+}, \mathrm{H}_{1+}, \mathrm{H}_{1*}, \mathrm{H}_{2+}, \mathrm{v}_1, L_1, L_2$ such that $\rho.\mathrm{L3} \in \mathcal{D}\llbracket\Delta\rrbracket$, $\rho.\mathrm{F} \in \mathcal{D}\llbracket\Delta\rrbracket$, $(W, \emptyset, \emptyset, \gamma_{\mathrm{L}}) \in \mathcal{G}\llbracket!\Gamma\rrbracket_\rho$,
$\gamma_{\Gamma} \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho$,
$\mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W$ and

$$(\mathrm{H}_{1g+} \uplus \mathrm{H}_{1+}, \gamma_{\mathrm{L}}^1(\gamma_{\Gamma}^1(()))) \xrightarrow{*}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \not\twoheadrightarrow_{L_1}$$

We can simplify the substitutions away, and note that the configuration $(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1+}, ())$ does not step because $()$ is a value. Thus, we have (36) by taking $W' = W$, $\mathsf{H}'_{1g} = \mathsf{H}_{1g+}$ and $\mathsf{H}'_{2g} = \mathsf{H}_{2g+}$. □

Lemma 4.21 (Compat $\lambda\mathsf{x} : \tau.\mathsf{e}$). *If* $\Delta; !\Gamma; \Delta; \Gamma, \mathsf{x} : \tau_1 \vdash \mathsf{e} \preceq \mathsf{e} : \tau_2$, *then*

$$\Delta; !\Gamma; \Delta; \Gamma, \mathsf{x} : \tau_1 \vdash \lambda\mathsf{x} : \tau_1.\mathsf{e} \preceq \lambda\mathsf{x} : \tau_1.\mathsf{e} : \tau_1 \longrightarrow \tau_2$$

Proof. Expanding the definition of $\preceq$, $\cdot^+$, and $\mathcal{E}\llbracket\cdot\rrbracket$. (noting via Lemma 4.14 that $\mathsf{H}_1 = \mathsf{H}_2 = \emptyset$), we are to show that

$$\begin{aligned}&\exists W'\ \mathsf{H}'_{1g}\ \mathsf{H}'_{2g}\ \mathsf{v}_2.\mathsf{H}_{1*} = \mathsf{H}'_{1g} \uplus \mathsf{H}_{1+} \wedge \mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W' \wedge \\ &\quad W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W' \wedge (W', (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho \wedge \\ &\qquad (\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, \lambda\mathsf{x}.\gamma^2_{\mathrm{L}}(\gamma^2_\Gamma(\mathsf{e}^+))) \xrightarrow{*} (\mathsf{H}'_{2g+} \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \not\rightarrow\end{aligned} \tag{37}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_\Gamma, W, \mathsf{H}_{1g+}, \mathsf{H}_{2g+}, \mathsf{H}_{1+}, \mathsf{H}_{1*}, \mathsf{H}_{2+}, \mathsf{v}_1, L_1, L_2$ such that $\rho.\mathsf{L3} \in \mathcal{D}\llbracket\Delta\rrbracket$, $\rho.\mathsf{F} \in \mathcal{D}\llbracket\Delta\rrbracket$,
$(W, \emptyset, \emptyset, \gamma_{\mathrm{L}}) \in \mathcal{G}\llbracket!\Gamma\rrbracket_\rho$,
$\gamma_\Gamma \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho$,
$\mathsf{H}_{1g+}, \mathsf{H}_{2g+} : W$ and

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1+}, \lambda\mathsf{x}.\gamma^1_{\mathrm{L}}(\gamma^1_\Gamma(\mathsf{e_1}^+))) \xrightarrow{*}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \not\rightarrow$$

We show (37) by taking $W' = W$, $\mathsf{H}'_{1g} = \mathsf{H}_{1g+}$ and $\mathsf{H}'_{2g} = \mathsf{H}_{2g+}$, noting that configurations with values as programs do not step. It thus suffices to show:

$$(W, (\emptyset, \lambda\mathsf{x}.\gamma^1_{\mathrm{L}}(\gamma^1_\Gamma(\mathsf{e}^+))), (\emptyset, \lambda\mathsf{x}.\gamma^2_{\mathrm{L}}(\gamma^2_\Gamma(\mathsf{e}^+)))) \in \mathcal{V}\llbracket\tau_1 \longrightarrow \tau_2\rrbracket_\rho$$

Expanding the definition of $\mathcal{V}\llbracket\tau_1 \longrightarrow \tau_2\rrbracket_\rho$ and pushing substitutions inside γ_Γ, we are to show that

$$(W^*, (\emptyset, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma,\mathsf{x}:\tau}[\mathsf{x} \mapsto (\mathsf{v}_{1a}, \mathsf{v}_{2a})](\mathsf{e}^+))), (\emptyset, \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma,\mathsf{x}:\tau}[\mathsf{x} \mapsto (\mathsf{v}_{1a}, \mathsf{v}_{2a})](\mathsf{e}^+)))) \in \mathcal{E}\llbracket\tau_2\rrbracket_\rho$$

given arbitrary $\mathsf{v}_{1a}, \mathsf{v}_{2a}$ such that $W \sqsubseteq_{\emptyset,\emptyset,\gamma^1_{\mathrm{L}}(\gamma^1_\Gamma(\mathsf{e}^+)),\gamma^2_{\mathrm{L}}(\gamma^2_\Gamma(\mathsf{e}^+))} W^*$ and $(W^*, (\emptyset, \mathsf{v}_{1a}), (\emptyset, \mathsf{v}_{2a})) \in \mathcal{V}\llbracket\tau_1\rrbracket_\rho$ We have this by expanding the definition of $\preceq$ in the premise and specializing where appropriate. □

Lemma 4.22 (Compat $\mathsf{e}_1\ \mathsf{e}_2$). *If* $\Delta; !\Gamma; \Delta; \Gamma \vdash \mathsf{e}_1 \preceq \mathsf{e}_1 : \tau_1 \longrightarrow \tau_2$ *and* $\Delta; !\Gamma; \Delta; \Gamma \vdash \mathsf{e}_2 \preceq \mathsf{e}_2 : \tau_1$, *then*

$$\Delta; !\Gamma; \Delta; \Gamma \vdash \mathsf{e}_1\ \mathsf{e}_2 \preceq \mathsf{e}_1\ \mathsf{e}_2 : \tau_2$$

Proof. Expanding the definition of $\preceq$, $\cdot^+$, and $\mathcal{E}\llbracket\cdot\rrbracket$. (noting via Lemma 4.14 that $\mathsf{H}_1 = \mathsf{H}_2 = \emptyset$), we are to show that

$$\begin{aligned}&\exists W'\ \mathsf{H}'_{1g}\ \mathsf{H}'_{2g}\ \mathsf{v}_2.\mathsf{H}_{1*} = \mathsf{H}'_{1g} \uplus \mathsf{H}_{1+} \wedge \mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W' \wedge \\ &\quad W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W' \wedge (W', (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}\llbracket\tau_2\rrbracket_\rho \wedge \\ &\qquad (\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, (\gamma^2_{\mathrm{L}}\ (\gamma^2_\Gamma\ (\mathsf{e_1}^+))\ \ \gamma^2_{\mathrm{L}}\ (\gamma^2_\Gamma\ (\mathsf{e_2}^+)))) \xrightarrow{*}_{L_2} (\mathsf{H}'_{2g+} \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \not\rightarrow\end{aligned} \tag{38}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_\Gamma, W, \mathsf{H}_{1g+}, \mathsf{H}_{2g+}, \mathsf{H}_{1+}, \mathsf{H}_{1*}, \mathsf{H}_{2+}, \mathsf{v}_1, L_1, L_2$ such that $\rho.\mathsf{L3} \in \mathcal{D}\llbracket\Delta\rrbracket$, $\rho.\mathsf{F} \in \mathcal{D}\llbracket\Delta\rrbracket$,
$(W, \emptyset, \emptyset, \gamma_{\mathrm{L}}) \in \mathcal{G}\llbracket!\Gamma\rrbracket_\rho$,
$\gamma_\Gamma \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho$,
$\mathsf{H}_{1g+}, \mathsf{H}_{2g+} : W$ and

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1+}, (\gamma^1_{\mathrm{L}}\ (\gamma^1_\Gamma\ (\mathsf{e_1}^+))\ \ \gamma^1_{\mathrm{L}}\ (\gamma^1_\Gamma\ (\mathsf{e_2}^+)))) \xrightarrow{*}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \not\rightarrow$$

By Lemma 4.3, we have that $\left(\mathrm{H}_{1g+} \uplus \mathrm{H}_{1+}, \gamma^1_{\mathrm{L}}\left(\gamma^1_{\Gamma}\left(\mathrm{e}_1{}^{+}\right)\right)\right) \overset{*}{\longrightarrow}_{L_1 \cup FL\left(\gamma^1_{\mathrm{L}}\left(\gamma^1_{\Gamma}(\mathrm{e}_2{}^{+})\right)\right)} (\mathrm{H}^1_{1*}, \mathrm{v}^1_1) \not\twoheadrightarrow$ for some $\mathrm{H}^1_{1*}, \mathrm{v}^1_1$. Then expanding the definition of $\preceq$ and $\mathcal{E}[\![\cdot]\!]$. in the first premise and specializing where appropriate, we have that

$$\begin{aligned}
&\exists W^1\ \mathrm{H}^1_{1g}\ \mathrm{H}^1_{2g}\ \mathrm{v}_2{}^1.\mathrm{H}^1_{1*} = \mathrm{H}^1_{1g} \uplus \mathrm{H}_{1+} \wedge \mathrm{H}^1_{1g}, \mathrm{H}^1_{2g} : W^1 \wedge \\
&\quad W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W, FL(\mathrm{cod}(\mathrm{H}_{1+}))\cup FL(\gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathrm{e}_2{}^{+})))\cup L_1, FL(\mathrm{cod}(\mathrm{H}_{2+}))\cup FL(\gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathrm{e}_2{}^{+})))\cup L_2)} W^1 \wedge \\
&\qquad (W^1, (\emptyset, \mathrm{v}^1_1), (\emptyset, \mathrm{v}^1_2)) \in \mathcal{V}[\![\tau_1 \longrightarrow \tau_2]\!]_\rho \wedge \\
&\qquad \forall \mathrm{H}_{2+}.\ \left(\mathrm{H}_{2g+} \uplus \mathrm{H}_{2+}, \gamma^2_{\mathrm{L}}\left(\gamma^2_{\Gamma}\left(\mathrm{e}_1{}^{+}\right)\right)\right) \overset{*}{\longrightarrow}_{L_2 \cup FL\left(\gamma^2_{\mathrm{L}}\left(\gamma^2_{\Gamma}(\mathrm{e}_2{}^{+})\right)\right)} (\mathrm{H}^1_{2g} \uplus \mathrm{H}_{2+}, \mathrm{v}^1_2) \not\twoheadrightarrow
\end{aligned} \tag{39}$$

Expanding the definition of $\mathcal{V}[\![\tau_1 \longrightarrow \tau_2]\!]_\rho$, we have that

$$\begin{aligned}
&\mathrm{v}^1_1 = \lambda \mathrm{x}_1.\mathrm{e}_{1\mathrm{b}} \wedge \mathrm{v}^1_2 = \lambda \mathrm{x}_2.\mathrm{e}_{2\mathrm{b}} \wedge \\
&\forall (W^{1*}, (\emptyset, \mathrm{v}_{1\mathrm{a}}), (\emptyset, \mathrm{v}_{2\mathrm{a}})) \in \mathcal{V}[\![\tau_1]\!]_\rho . W^1 \sqsubseteq_{\emptyset,\emptyset,\mathrm{e}_{1\mathrm{b}},\mathrm{e}_{2\mathrm{b}}} W^{1*} \wedge (W^{1*}, (\emptyset, [\mathrm{x}_1 \mapsto \mathrm{v}_{1\mathrm{a}}]\mathrm{e}_{1\mathrm{b}}, \emptyset, [\mathrm{x}_2 \mapsto \mathrm{v}_{2\mathrm{a}}]\mathrm{e}_{2\mathrm{b}}) \in \mathcal{E}[\![\tau_2]\!]_\rho
\end{aligned} \tag{40}$$

Proceeding to work on our second premise, by Lemma 4.3, we have that

$$\left(\mathrm{H}^1_{1g} \uplus \mathrm{H}_{1+}, \gamma^1_{\mathrm{L}}\left(\gamma^1_{\Gamma}\left(\mathrm{e}_2{}^{+}\right)\right)\right) \overset{*}{\longrightarrow}_{L_1 \cup FL(\mathrm{e}_{1\mathrm{b}})} (\mathrm{H}^2_{1*}, \mathrm{v}^2_1) \not\twoheadrightarrow$$

for some $\mathrm{H}^2_{1*}, \mathrm{v}^2_1$.

Then expanding the definition of $\preceq$ and $\mathcal{E}[\![\cdot]\!]$. in the second premise, noting due to Lemma 4.7 that we can use W^1, and specializing where appropriate, we have that

$$\begin{aligned}
&\exists W^2\ \mathrm{H}^2_{1g}\ \mathrm{H}^2_{2g}\ \mathrm{v}_2{}^2.\mathrm{H}^2_{1*} = \mathrm{H}^2_{1g} \uplus \mathrm{H}_{1+} \wedge \mathrm{H}^2_{1g}, \mathrm{H}^2_{2g} : W^2 \wedge \\
&\quad W^1 \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W^1, L_1 \cup FL(\mathrm{e}_{1\mathrm{b}})\cup FL(\mathrm{cod}(\mathrm{H}_{1+})), L_2 \cup FL(\mathrm{e}_{2\mathrm{b}})\cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W^2 \wedge \\
&\qquad (W^2, (\emptyset, \mathrm{v}^2_1), (\emptyset, \mathrm{v}^2_2)) \in \mathcal{V}[\![\tau_1]\!]_\rho \wedge \\
&\qquad \forall \mathrm{H}_{2+}.\ \left(\mathrm{H}^1_{2g} \uplus \mathrm{H}_{2+}, \gamma^2_{\mathrm{L}}\left(\gamma^2_{\Gamma}\left(\mathrm{e}_2{}^{+}\right)\right)\right) \overset{*}{\longrightarrow}_{L_2 \cup FL(\mathrm{e}_{2\mathrm{b}})} (\mathrm{H}^2_{2g} \uplus \mathrm{H}_{2+}, \mathrm{v}^2_2) \not\twoheadrightarrow
\end{aligned} \tag{41}$$

Now, we want to start putting things together. We appeal to (40), instantiating it with the values found in (45), taking W^{1*} to be W^2. Thus we have $(W^2, (\emptyset, [\mathrm{x}_1 \mapsto \mathrm{v}^2_1]\mathrm{e}_{1\mathrm{b}}), (\emptyset, [\mathrm{x}_2 \mapsto \mathrm{v}^2_2]\mathrm{e}_{2\mathrm{b}})) \in \mathcal{E}[\![\tau_2]\!]_\rho$.

Then, expanding the definition of $\mathcal{E}[\![\cdot]\!]$ and specializing where appropriate, we have that

$$\begin{aligned}
&\exists W^3 \mathrm{H}^3_{1g}\ \mathrm{H}^3_{2g}\ \mathrm{v}_2{}^3.\mathrm{H}^3_{1*} = \mathrm{H}^3_{1g} \uplus \mathrm{H}_{1+} \wedge \mathrm{H}^3_{1g}, \mathrm{H}^3_{2g} : W^3 \wedge \\
&\quad W^2 \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W^2, L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})), L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W^3 \wedge (W^3, (\emptyset, \mathrm{v}^3_1), (\emptyset, \mathrm{v}^3_2)) \in \mathcal{V}[\![\tau_2]\!]_\rho \wedge \\
&\quad \forall \mathrm{H}_{2+}.\ \left(\mathrm{H}^2_{2g} \uplus \mathrm{H}_{2+}, [\mathrm{x}_2 \mapsto \mathrm{v}^2_2]\mathrm{e}_{2\mathrm{b}}\right) \overset{*}{\longrightarrow}_{L_2} (\mathrm{H}^2_{2g} \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \not\twoheadrightarrow
\end{aligned} \tag{42}$$

Then we show (38) by taking $\mathrm{H}_{1*} = \mathrm{H}^3_{1g} \uplus \mathrm{H}_{1+}$ and $\mathrm{v}_2 = \mathrm{v}_2$. All that remains is to show that

$$\exists \mathrm{H}'_{2g}.\ \left(\mathrm{H}'_{2g} \uplus \mathrm{H}_{2+}, \left(\gamma^2_{\mathrm{L}}\left(\gamma^2_{\Gamma}\left(\mathrm{e}_1{}^{+}\right)\right)\ \gamma^2_{\mathrm{L}}\left(\gamma^2_{\Gamma}\left(\mathrm{e}_2{}^{+}\right)\right)\right)\right) \overset{*}{\longrightarrow}_{L_2} (\mathrm{H}'_{2g} \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \not\twoheadrightarrow$$

Specializing where appropriate, we have that

$$
\begin{aligned}
&\left(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, \left(\gamma_{\mathrm{L}}^{2}\left(\gamma_{\Gamma}^{2}\left(\mathsf{e}_{1}{}^{+}\right)\right)\ \gamma_{\mathrm{L}}^{2}\left(\gamma_{\Gamma}^{2}\left(\mathsf{e}_{2}{}^{+}\right)\right)\right)\right) && \\
&\overset{*}{\longrightarrow}_{L_2 \cup FL(\gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_2{}^{+})))} \left(\mathsf{H}_{2g}^{2} \uplus \mathsf{H}_{2+}, (\lambda \mathsf{x}_2.\mathsf{e}_{2b})\ \gamma_{\mathrm{L}}^{2}\left(\gamma_{\Gamma}^{2}\left(\mathsf{e}_{2}{}^{+}\right)\right)\right) && \text{(by 45)} \\
&\overset{*}{\longrightarrow}_{L_2 \cup FL(\mathsf{e}_{2b})} \left(\mathsf{H}_{2g}^{3} \uplus \mathsf{H}_{2+}, (\lambda \mathsf{x}_2.\mathsf{e}_{2b})\ \mathsf{v}_2^2\right) && \text{(by 41)} \\
&\overset{1}{\longrightarrow}_{L_2} \left(\mathsf{H}_{2g}^{2} \uplus \mathsf{H}_{2+}, [\mathsf{x}_2 \mapsto \mathsf{v}_2^2]\mathsf{e}_{2b}\right) && \text{(by LCVM)} \\
&\overset{*}{\longrightarrow}_{L_2} \left(\mathsf{H}_{2g}^{3} \uplus \mathsf{H}_{2+}, \mathsf{v}_2\right) && \text{(by 42)} \\
&\not\rightarrow && \text{(values don't step)}
\end{aligned}
$$

□

Lemma 4.23 (Compat $\Lambda\alpha.\mathsf{e}$). *If* $\Delta; !\Gamma; \Delta, \alpha; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau$, *then*

$$\Delta; !\Gamma; \Delta; \Gamma \vdash \Lambda\alpha.\mathsf{e} \preceq \Lambda\alpha.\mathsf{e} : \forall\alpha.\tau$$

Proof. Expanding the definition of $\preceq$, $\cdot^{+}$, $\mathcal{E}[\![\cdot]\!]_{\cdot}$ and pushing substitutions in the goal (noting via Lemma 4.14 that $\mathsf{H}_1 = \mathsf{H}_2 = \emptyset$), we are to show that

$$
\begin{aligned}
&\exists W', \mathsf{H}'_{1g}, \mathsf{H}'_{2g}.\forall \mathsf{H}_{2+}.\exists \mathsf{v}_2. \\
&\mathsf{H}_{1*} = \mathsf{H}'_{1g} \uplus \mathsf{H}_{1+}\ \wedge \mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W' \wedge \\
&W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W, L_1 \cup FL(\mathrm{cod}(\mathsf{H}_{1+})), L_2 \cup FL(\mathrm{cod}(\mathsf{H}_{2+})))}\ W' \wedge \\
&(W', (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}[\![\forall\alpha.\ \tau]\!]_\rho \wedge \\
&(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, \lambda\_.\ \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}^{+}))) \overset{*}{\longrightarrow}_{L_2} (\mathsf{H}'_{2g} \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \not\rightarrow
\end{aligned}
$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_{\Gamma}, W, L_1, L_2, \mathsf{H}_{1g+}, \mathsf{H}_{2g+} : W, \mathsf{v}_1, \mathsf{H}_{1+}, \mathsf{H}_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!], \rho.\mathsf{F} \in \mathcal{D}[\![\Delta]\!], (W, \emptyset, \emptyset, \gamma_{\mathrm{L}}) \in \mathcal{G}[\![!\Gamma]\!]_\rho, (W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]_\rho$$

and

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1+}, \lambda\_.\ \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}^{+}))) \overset{*}{\longrightarrow}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \not\rightarrow$$

We show the goal by taking $W' = W$, $\mathsf{H}'_{1g} = \mathsf{H}_{1g+}$, and $\mathsf{H}'_{2g} = \mathsf{H}_{2g+}$, noting that configurations with values as programs do not step. Thus, it suffices to show that

$$(W, (\emptyset, \lambda\_.\gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}^{+}))), (\emptyset, \lambda\_.\gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}^{+})))) \in \mathcal{V}[\![\forall\alpha.\tau]\!]_\rho$$

Expanding the definition of $\mathcal{V}[\![\forall\alpha.\tau]\!]_\rho$, we are to show that

$$(W', (\emptyset, \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}^{+}))), (\emptyset, \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}^{+})))) \in \mathcal{E}[\![\tau_2]\!]_{\rho[\mathsf{F}(\alpha) \mapsto R]}$$

given arbitrary $R \in RelT$ and W' such that $W \sqsubset_{\emptyset,\emptyset,\gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}^{+})),\gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}^{+}))}\ W'$.

We have this by expanding the definition of $\preceq$ and then $\mathcal{D}[\![\cdot]\!]$ in the premise and specializing where appropriate. □

Lemma 4.24 (Compat $\mathsf{e}\ [\tau]$). *If* $\Delta; !\Gamma; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \forall\alpha.\tau_2$, *then*

$$\Delta; !\Gamma; \Delta; \Gamma \vdash \mathsf{e}\ [\tau_1] \preceq \mathsf{e}\ [\tau_1] : [\alpha \mapsto \tau_1]\tau_2$$

Proof. Expanding the definition of $\preceq$, $\cdot^{+}$, $\mathcal{E}[\![\cdot]\!]_{\cdot}$ and pushing substitutions in the goal, we are to show that

$$\begin{array}{l}
\exists W', \mathrm{H}'_{1g}, \mathrm{H}'_{2g}.\forall \mathrm{H}_{2+}.\exists \mathrm{v}_2. \\
\mathrm{H}_{1*} = \mathrm{H}'_{1g} \uplus \mathrm{H}_{1+} \ \wedge \mathrm{H}'_{1g}, \mathrm{H}'_{2g} : W' \wedge \\
W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W' \wedge \\
(W', (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}\llbracket [\alpha \mapsto \tau_1]\tau_2 \rrbracket_\rho \wedge \\
(\mathrm{H}_{2g+} \uplus \mathrm{H}_{2+}, \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathrm{e}^+))\ ()\ \overset{*}{\longrightarrow}_{L_2} (\mathrm{H}'_{2g} \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \not\twoheadrightarrow
\end{array}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_{\Gamma}, W, L_1, L_2, \mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W, \mathrm{v}_1, \mathrm{H}_{1+}, \mathrm{H}_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}\llbracket \Delta \rrbracket, \rho.\mathsf{F} \in \mathcal{D}\llbracket \Delta \rrbracket, (W, \emptyset, \emptyset, \gamma_{\mathrm{L}}) \in \mathcal{G}\llbracket \Gamma_1 \uplus \Gamma_2 \rrbracket_\rho, (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho$$

and

$$(\mathrm{H}_{1g+} \uplus \mathrm{H}_{1+}, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathrm{e}^+))\ ())\ \overset{*}{\longrightarrow}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \not\twoheadrightarrow$$

By Lemma 4.3, we have that $\left(\mathrm{H}_{1g+} \uplus \mathrm{H}_{1+}, \gamma^1_{\mathrm{L}}\left(\gamma^1_{\Gamma}\left(\mathrm{e}^+\right)\right)\right) \overset{*}{\longrightarrow}_{L_1} (\mathrm{H}^1_{1*}, \mathrm{v}^1_1) \not\twoheadrightarrow$ for some $\mathrm{H}^1_{1*}, \mathrm{v}^1_1$. Then expanding the definition of $\preceq$ and $\mathcal{E}\llbracket \cdot \rrbracket$. in the premise and specializing where appropriate, we have that

$$\begin{array}{l}
\exists W', \mathrm{H}'_{1g}, \mathrm{H}'_{2g}.\forall \mathrm{H}_{2+}.\exists \mathrm{v}_2. \\
\mathrm{H}^1_{1*} = \mathrm{H}'_{1g} \uplus \mathrm{H}_{1+} \ \wedge \mathrm{H}'_{1g}, \mathrm{H}'_{2g} : W' \wedge \\
W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W' \wedge \\
(W', (\emptyset, \mathrm{v}^1_1), (\emptyset, \mathrm{v}^1_2)) \in \mathcal{V}\llbracket \forall \alpha.\tau_2 \rrbracket_\rho \wedge \\
(\mathrm{H}_{2g+} \uplus \mathrm{H}_{2+}, \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathrm{e}^+)))\ \overset{*}{\longrightarrow}_{L_2} (\mathrm{H}'_{2g} \uplus \mathrm{H}_{2+}, \mathrm{v}_2{}^1) \not\twoheadrightarrow
\end{array}$$

Expanding the definition of $\mathcal{V}\llbracket \forall \alpha.\tau_2 \rrbracket_\rho$, we have that

$$\begin{array}{l}
\mathrm{v}^1_1 = \lambda\_.\mathrm{e}_{1\mathrm{b}} \wedge \mathrm{v}^1_2 = \lambda\_.\mathrm{e}_{2\mathrm{b}} \wedge \\
\forall R \in \mathit{RelT}.(W', (\emptyset, \mathrm{e}_{1\mathrm{b}}), (\emptyset, \mathrm{e}_{2\mathrm{b}})) \in \mathcal{E}\llbracket \tau_2 \rrbracket_{\rho[\mathsf{F}(\alpha) \mapsto R]}
\end{array}$$

By Lemma 4.3, we now have that

$$\begin{array}{rl}
\left(\mathrm{H}'_{1g} \uplus \mathrm{H}_{1+}, (\lambda\_.\mathrm{e}_{1\mathrm{b}})\ \ ()\right) & \overset{1}{\longrightarrow}_{L_1} \left(\mathrm{H}'_{1g} \uplus \mathrm{H}_{1+}, \mathrm{e}_{1\mathrm{b}}\right) \\
& \overset{*}{\longrightarrow}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \\
& \not\twoheadrightarrow
\end{array}$$

Recall that $(W', (\emptyset, \mathrm{e}_{1\mathrm{b}}), (\emptyset, \mathrm{e}_{2\mathrm{b}})) \in \mathcal{E}\llbracket \tau_2 \rrbracket_{\rho[\mathsf{F}(\alpha) \mapsto R]}$ given arbitrary $R \in \mathit{RelT}$. Then take $R = \mathcal{V}\llbracket \tau_1 \rrbracket_\rho$. Expanding the definition of $\mathcal{E}\llbracket \cdot \rrbracket$, specializing where appropriate, and applying Lemma 4.9, we have that

$$\begin{array}{l}
\exists W'', \mathrm{H}''_{1g}, \mathrm{H}''_{2g}.\forall \mathrm{H}_{2+}.\exists \mathrm{v}_2. \\
\mathrm{H}^1_{1*} = \mathrm{H}''_{1g} \uplus \mathrm{H}_{1+} \ \wedge \mathrm{H}''_{1g}, \mathrm{H}''_{2g} : W'' \wedge \\
W' \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W'' \wedge \\
(W'', (\emptyset, \mathrm{v}_1), (\emptyset, \mathrm{v}_2)) \in \mathcal{V}\llbracket [\alpha \mapsto \tau]\tau_2 \rrbracket_\rho \wedge \\
(\mathrm{H}_{2g+} \uplus \mathrm{H}_{2+}, \mathrm{e}_{2\mathrm{b}})\ \overset{*}{\longrightarrow}_{L_2} (\mathrm{H}''_{2g} \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \not\twoheadrightarrow
\end{array}$$

Then all that remains is to show that

$$\left(\mathrm{H}_{2g+} \uplus \mathrm{H}_{2+}, \left(\gamma^2_{\mathrm{L}}\left(\gamma^2_{\Gamma}\left(\mathrm{e}^+\right)\right)\ \ ()\right)\right) \overset{*}{\longrightarrow}_{L_2} (\mathrm{H}_{2g''} \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \not\twoheadrightarrow$$

Specializing where appropriate, the above gives us that

$$\begin{aligned}
\left(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, \left(\gamma_{\mathrm{L}}^{2}\left(\gamma_{\Gamma}^{2}\left(\mathsf{e}^{+}\right)\right)\ ()\right)\right) &\xrightarrow{*}_{L_2} \left(\mathsf{H}'_{2g} \uplus \mathsf{H}_{2+}, (\lambda\_.\mathsf{e}_{2\mathrm{b}})\ ()\right) \\
&\xrightarrow{1}_{L_2} \left(\mathsf{H}'_{2g} \uplus \mathsf{H}_{2+}, \mathsf{e}_{2\mathrm{b}}\right) && \text{(by MiniML)} \\
&\xrightarrow{*}_{L_2} \left(\mathsf{H}''_{2g} \uplus \mathsf{H}_{2+}, \mathsf{v}_2\right) \\
&\not\rightarrow && \text{(values don't step)}
\end{aligned}$$

□

Lemma 4.25 (Compat `ref e`). *If* $\Delta; !\Gamma; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau$*, then*

$$\Delta; !\Gamma; \Delta; \Gamma \vdash \mathtt{ref\ e} \preceq \mathtt{ref\ e} : \mathtt{ref}\ \tau$$

Proof. Expanding the definition of $\preceq$ and $\cdot^{+}$ and pushing substitutions in the goal, we are to show that

$$\begin{aligned}
&\exists W', \mathsf{H}'_{1g}, \mathsf{H}'_{2g}.\forall \mathsf{H}_{2+}.\exists \mathsf{v}_2. \\
&\mathsf{H}_{1*} = \mathsf{H}'_{1g} \uplus \mathsf{H}_{1+} \ \wedge \mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W' \wedge \\
&W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W' \wedge \\
&(W', (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}[\![\mathtt{ref}\ \tau]\!]_\rho \wedge \\
&(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, \mathsf{let}\ \_ = \mathsf{callgc\ in\ ref}\ \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}^{+}))) \xrightarrow{*}_{L_2} (\mathsf{H}'_{2g} \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \not\rightarrow
\end{aligned}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_{\Gamma}, W, L_1, L_2, \mathsf{H}_{1g+}, \mathsf{H}_{2g+} : W, \mathsf{v}_1, \mathsf{H}_{1+}, \mathsf{H}_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!], \rho.\mathsf{F} \in \mathcal{D}[\![\Delta]\!], (W, \emptyset, \emptyset, \gamma_{\mathrm{L}}) \in \mathcal{G}[\![!\Gamma]\!]_\rho, (W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]_\rho$$

and

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = \mathsf{callgc\ in\ ref}\ \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}^{+}))) \xrightarrow{*}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \not\rightarrow$$

First, notice that

$$\begin{aligned}
&(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = \mathsf{callgc\ in\ ref}\ \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}^{+}))) \rightarrow_{L_1} \\
&(\mathsf{H}_{1ga} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = ()\ \mathsf{in\ ref}\ \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}^{+}))) \rightarrow_{L_1} \\
&(\mathsf{H}_{1ga} \uplus \mathsf{H}_{1+}, \mathsf{ref}\ \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}^{+})))
\end{aligned}$$

and

$$\begin{aligned}
&(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, \mathsf{let}\ \_ = \mathsf{callgc\ in\ ref}\ \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}^{+}))) \xrightarrow{*}_{L_2} \\
&(\mathsf{H}_{2ga} \uplus \mathsf{H}_{2+}, \mathsf{ref}\ \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}^{+})))
\end{aligned}$$

for some heaps $\mathsf{H}_{1ga} : \mathit{GCHeap}, \mathsf{H}_{2ga} : \mathit{GCHeap}$. By Lemma 4.8, there exists a world

$$W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,FL(\mathrm{cod}(\mathsf{H}_{1+}))\cup FL(\gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}^{+})))\cup L_1,FL(\mathrm{cod}(\mathsf{H}_{2+}))\cup FL(\gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}^{+})))\cup L_2)} W_a$$

such that $\mathsf{H}_{1ga}, \mathsf{H}_{2ga} : W_a$.

Then, since $\mathcal{G}[\![\,`\,]\!]_\rho, \mathcal{G}[\![!\Gamma]\!]_\rho$ are closed under world extension by Lemma 4.7, we can instantiate the induction hypothesis with $\rho, \gamma_{\Gamma}, \gamma_{\mathrm{L}}, W_a$ and then expanding the expression relation, so we find that:

$$(W_a, (\emptyset, \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}^{+}))), (\emptyset, \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}^{+})))) \in \mathcal{E}[\![\tau]\!]_\rho$$

Then, by applying Lemma 2.1 and expanding the expression relation, we find that

$$(\mathsf{H}_{1ga} \uplus \mathsf{H}_{1+}, \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}^{+}))) \xrightarrow{*}_{L_1} (\mathsf{H}'_{1g} \uplus \mathsf{H}_{1+}, \mathsf{v}_1^{*}) \not\rightarrow$$

and

$$(\mathsf{H}_{2ga} \uplus \mathsf{H}_{2+}, \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}^{+}))) \xrightarrow{*}_{L_2} (\mathsf{H}'_{2g} \uplus \mathsf{H}_{2+}, \mathsf{v}_2^{*}) \not\rightarrow$$

where $\mathrm{H}'_{1g}, \mathrm{H}'_{2g} : W'$ for some

$$W_a \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,FL(\mathrm{cod}(\mathrm{H}_{1+}))\cup L_1,FL(\mathrm{cod}(\mathrm{H}_{2+}))\cup L_2)} W'$$

where

$$(W', (\emptyset, \mathrm{v}_1^*), (\emptyset, \mathrm{v}_2^*)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho$$

Thus, we find that

$$\begin{aligned}
&(\mathrm{H}_{1g+} \uplus \mathrm{H}_{1+}, \mathsf{let}\ \_ = \mathsf{callgc}\ \mathsf{in}\ \mathsf{ref}\ \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathrm{e}^+))) \xrightarrow{*}_{L_1}\\
&(\mathrm{H}_{1ga} \uplus \mathrm{H}_{1+}, \mathsf{ref}\ \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathrm{e}^+))) \xrightarrow{*}_{L_1}\\
&(\mathrm{H}'_{1g} \uplus \mathrm{H}_{1+}, \mathsf{ref}\ \mathrm{v}_1^*) \xrightarrow{*}_{L_1}\\
&(\mathrm{H}'_{1g}[\ell_1 \overset{gc}{\mapsto} \mathrm{v}_1^*] \uplus \mathrm{H}_{1+}, \ell_1)
\end{aligned}$$

and

$$\begin{aligned}
&(\mathrm{H}_{2g+} \uplus \mathrm{H}_{1+}, \mathsf{let}\ \_ = \mathsf{callgc}\ \mathsf{in}\ \mathsf{ref}\ \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathrm{e}^+))) \xrightarrow{*}_{L_2}\\
&(\mathrm{H}_{2ga} \uplus \mathrm{H}_{2+}, \mathsf{ref}\ \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathrm{e}^+))) \xrightarrow{*}_{L_2}\\
&(\mathrm{H}'_{2g} \uplus \mathrm{H}_{2+}, \mathsf{ref}\ \mathrm{v}_2^*) \xrightarrow{*}_{L_2}\\
&(\mathrm{H}'_{2g}[\ell_2 \overset{gc}{\mapsto} \mathrm{v}_2^*] \uplus \mathrm{H}_{2+}, \ell_2)
\end{aligned}$$

for some $\ell_1 \notin \mathrm{dom}(\mathrm{H}'_{1g+} \uplus \mathrm{H}_{1+})$ and $\ell_2 \notin \mathrm{dom}(\mathrm{H}'_{2g+} \uplus \mathrm{H}_{2+})$.

Since $\mathrm{H}'_{1g+}, \mathrm{H}'_{2g+} : W'$, $\ell_1 \notin \mathrm{dom}(\mathrm{H}'_{1g+})$, and $\ell_2 \notin \mathrm{dom}(\mathrm{H}'_{2g+})$, it follows that $(\ell_1, \ell_2) \notin \mathrm{dom}(W'.\Psi)$. Then, let

$$W'' = (W'.k, \lfloor W'.\Psi \rfloor_{W'.k}[(\ell_1, \ell_2) \mapsto \lfloor \mathcal{V}\llbracket\tau\rrbracket_\rho \rfloor_{W'.k}])$$

Notice that $W''.k \leq W'.k$. Moreover, since $W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\cdot} W'$, we have $\mathrm{dom}(\mathrm{H}_{1+})\#W'.\Psi$ and $\mathrm{dom}(\mathrm{H}_{2+})\#W'.\Psi$. Since $\ell_1 \notin \mathrm{dom}(\mathrm{H}_{1+})$ and $\ell_2 \notin \mathrm{dom}(\mathrm{H}_{2+})$, it follows that $\mathrm{dom}(\mathrm{H}_{1+})\#W''.\Psi$ and $\mathrm{dom}(\mathrm{H}_{2+})\#W''.\Psi$. Finally, for all $(\ell_1', \ell_2') \in \mathrm{dom}(W'.\Psi)$, $W''.\Psi(\ell_1', \ell_2') = \lfloor W'.\Psi \rfloor_{W'.k}(\ell_1', \ell_2') = \lfloor W'.\Psi(\ell_1, \ell_2) \rfloor_{W''.k}$. This suffices to show that $W' \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+}),\mathrm{dom}(W'.\Psi)} W''$. Then, by Lemma 4.6, $W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,FL(\mathrm{cod}(\mathrm{H}_{1+}))\cup L_1,FL(\mathrm{cod}(\mathrm{H}_{2+}))\cup L_2)} W''$.

Then, choose $\mathrm{H}'_{1g} = \mathrm{H}'_{1g+}[\ell_1 \overset{gc}{\mapsto} \mathrm{v}_1^*]$, $\mathrm{H}'_{2g} = \mathrm{H}'_{2g+}[\ell_1 \overset{gc}{\mapsto} \mathrm{v}_2^*]$, and $W' = W''$. One can see that

$$(W'', (\emptyset, \ell_1), (\emptyset, \ell_2)) \in \mathcal{V}\llbracket\mathtt{ref}\ \tau\rrbracket_\rho$$

because by definition of W'', $W''(\ell_1, \ell_2) = \lfloor \mathcal{V}\llbracket\tau\rrbracket_\rho \rfloor_{W''.k}$. To finish the proof, we must show

$$\mathrm{H}'_{1g+}[\ell_1 \overset{gc}{\mapsto} \mathrm{v}_1^*], \mathrm{H}'_{2g+}[\ell_1 \overset{gc}{\mapsto} \mathrm{v}_2^*] : W''$$

For any $(\ell_1', \ell_2') \mapsto R \in W''.\Psi$, there are two cases: **(1)** $(\ell_1, \ell_2) = (\ell_1', \ell_2')$, in which case $W''.\Psi(\ell_1, \ell_2) = \lfloor \mathcal{V}\llbracket\tau\rrbracket_\rho \rfloor_{W'.k}$. Then, since $(W', (\emptyset, \mathrm{v}_1^*), (\emptyset, \mathrm{v}_2^*)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho$, by Lemma 4.6, we have $(W'', (\emptyset, \mathrm{v}_1^*), (\emptyset, \mathrm{v}_2^*)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho$ and thus $(\triangleright W'', (\emptyset, \mathrm{v}_1^*), (\emptyset, \mathrm{v}_2^*)) \in \lfloor \mathcal{V}\llbracket\tau\rrbracket_\rho \rfloor_{W'.k}$ **(2)** $(\ell_1', \ell_2') \in \mathrm{dom}(W'.\Psi)$, in which case we must show $(\triangleright W'', (\emptyset, \mathrm{H}_1'(\ell_1')), (\emptyset, \mathrm{H}_2'(\ell_2'))) \in W''.\Psi(\ell_1', \ell_2') = \lfloor W'.\Psi(\ell_1', \ell_2') \rfloor_{W'.k}$. First, since $\mathrm{H}_1', \mathrm{H}_2' : W'$, we have $(\triangleright W', (\emptyset, \mathrm{H}_1'(\ell_1')), (\emptyset, \mathrm{H}_2'(\ell_2'))) \in W'.\Psi(\ell_1', \ell_2')$. Then, since $\triangleright W'.k < W'.k$, it follows that $(\triangleright W', (\emptyset, \mathrm{H}_1'(\ell_1')), (\emptyset, \mathrm{H}_2'(\ell_2'))) \in \lfloor W'.\Psi(\ell_1', \ell_2') \rfloor_{W'.k}$. Finally, since $W' \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{dom}(W'.\Psi)} W''$, it follows that $\triangleright W' \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{dom}(W'.\Psi)} \triangleright W''$, so by Lemma 4.7, we have

$$(\triangleright W'', (\emptyset, \mathrm{H}_1'(\ell_1')), (\emptyset, \mathrm{H}_2'(\ell_2'))) \in \lfloor W'.\Psi(\ell_1', \ell_2') \rfloor_{W'.k}$$

as was to be proven. □

LEMMA 4.26 (COMPAT $!\mathrm{e}$). *If* $\Delta; !\Gamma; \Delta; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \mathtt{ref}\ \tau$ *then*

$$\Delta; !\Gamma; \Delta; \Gamma \vdash !\mathrm{e} \preceq !\mathrm{e} : \tau$$

Proof. Expanding the definition of $\preceq$ and $\cdot^+$ and pushing substitutions in the goal, we are to show that

$$\begin{array}{l}
\exists W', \mathsf{H}'_{1g}, \mathsf{H}'_{2g}.\forall \mathsf{H}_{2+}.\exists \mathsf{v}_2. \\
\mathsf{H}_{1*} = \mathsf{H}'_{1g} \uplus \mathsf{H}_{1+} \ \wedge \mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W' \wedge \\
W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,FL(\mathrm{cod}(\mathsf{H}_{1+}))\cup L_1,FL(\mathrm{cod}(\mathsf{H}_{2+}))\cup L_2)} W' \wedge \\
(W', (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho \wedge \\
(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, !\gamma^2_{\mathsf{L}}(\gamma^2_\Gamma(\mathsf{e}^+))) \xrightarrow{*}_{L_2} (\mathsf{H}'_{2g} \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \nrightarrow
\end{array}$$

given arbitrary $\rho, \gamma_{\mathsf{L}}, \gamma_\Gamma, W, L_1, L_2, \mathsf{H}_{1g+}, \mathsf{H}_{2g+} : W, \mathsf{v}_1, \mathsf{H}_{1+}, \mathsf{H}_{1*}$, such that

$$\rho.\mathsf{L3} \in \mathcal{D}\llbracket\Delta\rrbracket, \rho.\mathsf{F} \in \mathcal{D}\llbracket\Delta\rrbracket, (W, \emptyset, \emptyset, \gamma_{\mathsf{L}}) \in \mathcal{G}\llbracket!\Gamma\rrbracket_\rho, (W, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho$$

and

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1+}, !\gamma^1_{\mathsf{L}}(\gamma^1_\Gamma(\mathsf{e}^+))) \xrightarrow{*}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \nrightarrow$$

By Lemma 4.3, we have that $\left(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1+}, \gamma^1_{\mathsf{L}}\left(\gamma^1_\Gamma\left(\mathsf{e}^+\right)\right)\right) \xrightarrow{*}_{L_1} (\mathsf{H}^1_{1*}, \mathsf{v}^1_1) \nrightarrow$ for some $\mathsf{H}^1_{1*}, \mathsf{v}^1_1$. Then expanding the definition of $\preceq$ and $\mathcal{E}\llbracket\cdot\rrbracket.$ in the first premise and specializing where appropriate, we have that

$$\begin{array}{l}
\exists W^1\ \mathsf{H}^1_{1g}\ \mathsf{H}^1_{2g}\ \mathsf{v}_2{}^1.\mathsf{H}^1_{1*} = \mathsf{H}^1_{1g} \uplus \mathsf{H}_{1+} \wedge \mathsf{H}^1_{1g}, \mathsf{H}^1_{2g} : W^1 \wedge \\
\quad W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,FL(\mathrm{cod}(\mathsf{H}_{1+}))\cup L_1,FL(\mathrm{cod}(\mathsf{H}_{2+}))\cup L_2)} W^1 \wedge (W^1, (\emptyset, \mathsf{v}^1_1), (\emptyset, \mathsf{v}^1_2)) \in \mathcal{V}\llbracket\mathsf{ref}\ \tau\rrbracket_\rho \wedge \\
\qquad \forall \mathsf{H}_{2+}. \left(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, \gamma^2_{\mathsf{L}}\left(\gamma^2_\Gamma\left(\mathsf{e}^+\right)\right)\right) \xrightarrow{*}_{L_2} (\mathsf{H}^1_{2g} \uplus \mathsf{H}_{2+}, \mathsf{v}^1_2) \nrightarrow
\end{array} \tag{43}$$

From the definition of $\mathcal{V}\llbracket\mathsf{ref}\ \tau\rrbracket_\rho$, we know that v^1_1 and v^1_2 are both locations (call them ℓ_1 and ℓ_2) and that $W^1.\Psi(\ell_1, \ell_2) = \lfloor\mathcal{V}\llbracket\tau\rrbracket_\rho\rfloor_{W^1.k}$. Since $\mathsf{H}^1_{1g}, \mathsf{H}^1_{2g} : W^1$, this means that

$$(\mathsf{H}^1_{1g} \uplus \mathsf{H}_{1+}, !\ell_1) \xrightarrow{*}_{L_1} (\mathsf{H}^1_{1g} \uplus \mathsf{H}_{1+}, \mathsf{v}_1)$$

and

$$(\mathsf{H}^1_{2g} \uplus \mathsf{H}_{2+}, !\ell_2) \xrightarrow{*}_{L_2} (\mathsf{H}^1_{2g} \uplus \mathsf{H}_{2+}, \mathsf{v}_2)$$

Further, we know that $(\triangleright W^1, (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_\rho$.

By Lemma 4.7, we know that

$$\begin{array}{l}
W \sqsubseteq_{\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+}),\mathrm{rchgclocs}(W,FL(\mathrm{cod}(\mathsf{H}_{1+}))\cup L_1,FL(\mathrm{cod}(\mathsf{H}_{2+}))\cup L_2)} W^1 \\
\quad \sqsubseteq_{\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+}),\mathrm{rchgclocs}(W,FL(\mathrm{cod}(\mathsf{H}_{1+}))\cup L_1,FL(\mathrm{cod}(\mathsf{H}_{2+}))\cup L_2)} \triangleright W^1
\end{array}$$

which, with $\mathsf{H}_{1*} = \mathsf{H}^1_{1g} \uplus \mathsf{H}_{1+}$ and $\mathsf{H}_{2g+} = \mathsf{H}^1_{2g}$, is enough to prove our goal.

□

Lemma 4.27 (Compat $\mathsf{e} := \mathsf{e}$). *If* $\Delta; !\Gamma; \Delta; \Gamma \vdash \mathsf{e}_1 \preceq \mathsf{e}_1 : \mathsf{ref}\ \tau$ *and* $\Delta; !\Gamma; \Delta; \Gamma \vdash \mathsf{e}_2 \preceq \mathsf{e}_2 : \tau$ *then*

$$\Delta; !\Gamma; \Delta; \Gamma \vdash \mathsf{e}_1 := \mathsf{e}_2 \preceq \mathsf{e}_1 := \mathsf{e2} : \mathsf{unit}$$

Proof. Expanding the definition of $\preceq$ and $\cdot^+$ and pushing substitutions in the goal, we are to show that

$$\begin{array}{l}
\exists W', \mathsf{H}'_{1g}, \mathsf{H}'_{2g}.\forall \mathsf{H}_{2+}.\exists \mathsf{v}_2. \\
\mathsf{H}_{1*} = \mathsf{H}'_{1g} \uplus \mathsf{H}_{1+} \ \wedge \mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W' \wedge \\
W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,FL(\mathrm{cod}(\mathsf{H}_{1+}))\cup L_1,FL(\mathrm{cod}(\mathsf{H}_{2+}))\cup L_2)} W' \wedge \\
(W', (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}\llbracket\mathsf{unit}\rrbracket_\rho \wedge \\
(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, \gamma^2_{\mathsf{L}}(\gamma^2_\Gamma(\mathsf{e}_1{}^+)) := \gamma^2_{\mathsf{L}}(\gamma^2_\Gamma(\mathsf{e}_2{}^+))) \xrightarrow{*}_{L_2} (\mathsf{H}'_{2g} \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \nrightarrow
\end{array}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_{\Gamma}, W, L_1, L_2, \mathsf{H}_{1g+}, \mathsf{H}_{2g+} : W, \mathsf{v}_1, \mathsf{H}_{1+}, \mathsf{H}_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}\llbracket\Delta\rrbracket, \rho.\mathsf{F} \in \mathcal{D}\llbracket\Delta\rrbracket, (W, \emptyset, \emptyset, \gamma_{\mathrm{L}}) \in \mathcal{G}\llbracket !\Gamma\rrbracket_\rho, (W, \gamma_{\Gamma}) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho$$

and

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1+}, \gamma_{\mathrm{L}}^1(\gamma_{\Gamma}^1(\mathsf{e_1}^+)) := \gamma_{\mathrm{L}}^1(\gamma_{\Gamma}^1(\mathsf{e_2}^+))) \xrightarrow{*}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \nrightarrow$$

By Lemma 4.3, we have that $\left(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1+}, \gamma_{\mathrm{L}}^1\left(\gamma_{\Gamma}^1\left(\mathsf{e_1}^+\right)\right)\right) \xrightarrow{*}_{L_1 \cup FL\gamma_{\mathrm{L}}^2(\gamma_{\Gamma}^2(\mathsf{e_2}^+))} (\mathsf{H}_{1*}^1, \mathsf{v}_1^1) \nrightarrow$ for some $\mathsf{H}_{1*}^1, \mathsf{v}_1^1$.

Then expanding the definition of $\preceq$ and $\mathcal{E}\llbracket\cdot\rrbracket.$ in the first premise and specializing where appropriate, we have that

$$\begin{aligned}
&\exists W^1\ \mathsf{H}_{1g}^1\ \mathsf{H}_{2g}^1\ \mathsf{v_2}^1.\mathsf{H}_{1*}^1 = \mathsf{H}_{1g}^1 \uplus \mathsf{H}_{1+} \wedge \mathsf{H}_{1g}^1, \mathsf{H}_{2g}^1 : W^1 \wedge \\
&\quad W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W, FL(\mathrm{cod}(\mathsf{H}_{1+})) \cup FL(\gamma_{\mathrm{L}}^1(\gamma_{\Gamma}^1(\mathsf{e_2}^+))) \cup L_1, FL(\mathrm{cod}(\mathsf{H}_{2+})) \cup FL(\gamma_{\mathrm{L}}^2(\gamma_{\Gamma}^2(\mathsf{e_2}^+))) \cup L_2)} W^1 \wedge \\
&\quad\ (W^1, (\emptyset, \mathsf{v}_1^1), (\emptyset, \mathsf{v}_2^1)) \in \mathcal{V}\llbracket \mathtt{ref}\ \tau\rrbracket_\rho \wedge \\
&\quad\ \forall \mathsf{H}_{2+}. \left(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, \gamma_{\mathrm{L}}^2\left(\gamma_{\Gamma}^2\left(\mathsf{e_1}^+\right)\right)\right) \xrightarrow{*}_{L_2 \cup FL\gamma_{\mathrm{L}}^1(\gamma_{\Gamma}^1(\mathsf{e_2}^+))} (\mathsf{H}_{2g}^1 \uplus \mathsf{H}_{2+}, \mathsf{v}_2^1) \nrightarrow
\end{aligned} \tag{44}$$

From the definition of $\mathcal{V}\llbracket \mathtt{ref}\ \tau\rrbracket_\rho$, we know that v_1^1 and v_2^1 are both locations (call them ℓ_1 and ℓ_2) and that $W^1.\Psi(\ell_1, \ell_2) = \lfloor \mathcal{V}\llbracket\tau\rrbracket_\rho \rfloor_{W^1.k}$.

Now, we again appeal to Lemma 4.3, this time with the context $\ell_i := [\cdot]$. This means, in particular, that we have that:

$\left(\mathsf{H}_{1g}^1 \uplus \mathsf{H}_{1+}, \gamma_{\mathrm{L}}^1\left(\gamma_{\Gamma}^1\left(\mathsf{e_2}^+\right)\right)\right) \xrightarrow{*}_{L_1 \cup FL(\ell_1)} (\mathsf{H}_{1*}^2, \mathsf{v}_1^2) \nrightarrow$ for some $\mathsf{H}_{1*}^2, \mathsf{v}_1^2$.

Now we expand the definition of $\preceq$ and $\mathcal{E}\llbracket\cdot\rrbracket.$ in the second premise and specialize where appropriate to get that

$$\begin{aligned}
&\exists W^2\ \mathsf{H}_{1g}^2\ \mathsf{H}_{2g}^2\ \mathsf{v_2}^2.\mathsf{H}_{1*}^2 = \mathsf{H}_{1g}^2 \uplus \mathsf{H}_{1+} \wedge \mathsf{H}_{1g}^2, \mathsf{H}_{2g}^2 : W^2 \wedge \\
&\quad W^1 \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W^1, FL(\ell_1) \cup FL(\mathrm{cod}(\mathsf{H}_{1+})) \cup L_1, FL(\ell_2) \cup FL(\mathrm{cod}(\mathsf{H}_{2+})) \cup L_2)} W^2 \wedge \\
&\quad\ (W^2, (\emptyset, \mathsf{v}_1^2), (\emptyset, \mathsf{v}_2^2)) \in \mathcal{V}\llbracket \mathtt{unit}\rrbracket_\rho \wedge \\
&\quad\ \forall \mathsf{H}_{2+}. \left(\mathsf{H}_{2g}^1 \uplus \mathsf{H}_{2+}, \gamma_{\mathrm{L}}^2\left(\gamma_{\Gamma}^2\left(\mathsf{e_2}^+\right)\right)\right) \xrightarrow{*}_{L_2 \cup FL(\ell_2)} (\mathsf{H}_{2g}^2 \uplus \mathsf{H}_{2+}, \mathsf{v}_2^2) \nrightarrow
\end{aligned} \tag{45}$$

Now we can assemble the pieces that we need to complete the proof. First, we stitch together our reductions (we reduced analogously on the left side):

$$\begin{aligned}
&(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, \gamma_{\mathrm{L}}^2(\gamma_{\Gamma}^2(\mathsf{e_1}^+)) := \gamma_{\mathrm{L}}^2(\gamma_{\Gamma}^2(\mathsf{e_2}^+))) \\
&\xrightarrow{*}_{L_2 \cup FL(\gamma_{\mathrm{L}}^1(\gamma_{\Gamma}^1(\mathsf{e_2}^+)))} (\mathsf{H}_{2g}^1 \uplus \mathsf{H}_{2+}, \ell_2\ := \gamma_{\mathrm{L}}^2(\gamma_{\Gamma}^2(\mathsf{e_2}^+))) \\
&\xrightarrow{*}_{L_2 \cup FL(\ell_1)} (\mathsf{H}_{2g}^2 \uplus \mathsf{H}_{2+}, \ell_2\ := \mathsf{v}_2^2) \\
&\rightarrow_{L_2 \cup FL(\ell_1)} (\mathsf{H}_{2g}^2[\ell_2 := \mathsf{v}_2^2] \uplus \mathsf{H}_{2+}, ())
\end{aligned}$$

Next, we need to show a W' such that $W \sqsubseteq_{\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+}),\mathrm{rchgclocs}(W, FL(\mathrm{cod}(\mathsf{H}_{1+})) \cup L_1, FL(\mathrm{cod}(\mathsf{H}_{2+})) \cup L_2)} W'$ and $\mathsf{H}_{1g}^2[\ell_1 := \mathsf{v}_1^2], \mathsf{H}_{2g}^2[\ell_2 := \mathsf{v}_2^2] : W'$. We can choose W^2, as we know that at W^1, ℓ_1, ℓ_2 mapped to $\mathcal{V}\llbracket\tau\rrbracket_\rho$, and W^2 is an extension of W^2 that protected those locations, and thus the above worlds satisfy this world. Since otherwise, membership in $\mathcal{V}\llbracket\mathtt{unit}\rrbracket_\rho$ is trivial, this suffices to finish the proof.

□

Lemma 4.28 (Compat $(\!|\mathsf{e}|\!)_\tau$). *If* $\Delta; \Gamma; \Delta; !\Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau$ *and* $\tau \sim \tau$*, then*

$$\Delta; !\Gamma; \Delta; \Gamma \vdash (\!|\mathsf{e}|\!)_\tau \preceq (\!|\mathsf{e}|\!)_\tau : \tau$$

Proof. Expanding the definition of $\preceq$ and $\cdot^{+}$ and pushing substitutions in the goal, we are to show that

$$(W, (\mathrm{H}_1, \mathrm{C}_{\tau \mapsto \tau}\left(\gamma_{\Gamma}^{1}\left(\gamma_{\mathrm{L}}^{1}\left(\mathrm{e}^{+}\right)\right)\right),), (\mathrm{H}_2, \mathrm{C}_{\tau \mapsto \tau}\left(\gamma_{\Gamma}^{2}\left(\gamma_{\mathrm{L}}^{2}\left(\mathrm{e}^{+}\right)\right)\right))) \in \mathcal{E}[\![\tau]\!]_{\rho} \tag{46}$$

given arbitrary $\rho, \gamma_{\Gamma}, \gamma_{\mathrm{L}}$ such that $\rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!]$, $\rho.\mathrm{F} \in \mathcal{D}[\![\Delta]\!]$, $(W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}[\![\Gamma]\!]_{\rho}$, $\gamma_{\Gamma} \in \mathcal{G}[\![\Gamma]\!]_{\rho}$. Expanding the definition of $\approx$ in the premise, specializing where appropriate, and commuting substitutions, we have that

$$(W, \left(\mathrm{H}_1, \gamma_{\Gamma}^{1}\left(\gamma_{\mathrm{L}}^{1}\left(\mathrm{e}^{+}\right)\right)\right), \left(\mathrm{H}_2, \gamma_{\Gamma}^{2}\left(\gamma_{\mathrm{L}}^{2}\left(\mathrm{e}^{+}\right)\right)\right)) \in \mathcal{E}[\![\tau]\!]_{\rho}$$

Then since $\tau \sim \tau$, we have (46) by Lemma 4.4. □

4.6.3 L^3 Compatibility Lemmas.

Lemma 4.29 (Compat x).

$$\Delta; \Gamma; \Delta; \mathrm{x} : \tau \vdash \mathrm{x} \preceq \mathrm{x} : \tau$$

Proof. Expanding the conclusion, we must show that given

$$\forall \rho, \gamma_{\Gamma}, \gamma_{\mathrm{L}}, W, \mathrm{H}_1, \mathrm{H}_2.$$
$$\rho.\mathrm{F} \in \mathcal{D}[\![\Delta]\!] \wedge \rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!] \wedge (W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]_{\rho} \wedge (W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}[\![\mathrm{x} : \tau]\!]_{\rho}$$

it holds that:

$$(W, (\mathrm{H}_1, \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{x}^{+}))), (\mathrm{H}_2, \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{x}^{+})))) \in \mathcal{E}[\![\tau]\!]_{\rho}$$

By Lemma 4.12, it suffices to show that:

$$(W, (\mathrm{H}_1, \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{x}^{+}))), (\mathrm{H}_2, \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{x}^{+})))) \in \mathcal{V}[\![\tau]\!]_{\rho}$$

Because $(W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}[\![\mathrm{x} : \tau]\!]_{\rho}$, we must have $\gamma_{\mathrm{L}}(\mathrm{x}) = (\mathrm{v}_1, \mathrm{v}_2)$ and $(W, (\mathrm{H}_1, \mathrm{v}_1), (\mathrm{H}_2, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_{\rho}$. Thus,

$$\gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{x}^{+})) = \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{x})) = \gamma_{\mathrm{L}}^{1}(\mathrm{x}) = \mathrm{v}_1$$
$$\gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{x}^{+})) = \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{x})) = \gamma_{\mathrm{L}}^{2}(\mathrm{x}) = \mathrm{v}_2$$

Finally, noting that $(W, (\mathrm{H}_1, \mathrm{v}_1), (\mathrm{H}_2, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_{\rho}$ by assumption suffices to finish the proof. □

Lemma 4.30 (Compat $\lambda \mathrm{x} : \tau.\mathrm{e}$). *If* $\Delta; \Gamma; \Delta; \Gamma, \mathrm{x} : \tau_1 \vdash \mathrm{e} \preceq \mathrm{e} : \tau_2$*, then*

$$\Delta; \Gamma; \Delta; \Gamma \vdash \lambda \mathrm{x} : \tau.\mathrm{e} \preceq \lambda \mathrm{x} : \tau.\mathrm{e} : \tau_1 \multimap \tau_2$$

Proof. Expanding the conclusion, we must show that given

$$\forall \rho, \gamma_{\Gamma}, \gamma_{\mathrm{L}}, W, \mathrm{H}_1, \mathrm{H}_2.$$
$$\rho.\mathrm{F} \in \mathcal{D}[\![\Delta]\!] \wedge \rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!] \wedge (W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]_{\rho} \wedge (W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}[\![\Gamma]\!]_{\rho}$$

it holds that:

$$(W, (\mathrm{H}_1, \lambda \mathrm{x}.\gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e}^{+}))), (\mathrm{H}_2, \lambda \mathrm{x}.\gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e}^{+})))) \in \mathcal{E}[\![\tau_1 \multimap \tau_2]\!]_{\rho}$$

By Lemma 4.12, it suffices to show that:

$$(W, (\mathrm{H}_1, \lambda \mathrm{x}.\gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e}^{+}))), (\mathrm{H}_2, \lambda \mathrm{x}.\gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e}^{+})))) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!]_{\rho}$$

Thus, consider some arbitrary $W', \mathrm{H}_{1v}, \mathrm{v}_1, \mathrm{H}_{2v}, \mathrm{v}_2$ such that $W \sqsubseteq_{\mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e}^{+})), \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e}^{+}))} W'$ and $(W', (\mathrm{H}_{1v}, \mathrm{v}_1), (\mathrm{H}_{2v}, \mathrm{v}_2)) \in \mathcal{V}[\![\tau_1]\!]_{\rho}$. We must show

$$(W', (\mathrm{H}_1 \uplus \mathrm{H}_{1v}, [\mathrm{x} \mapsto \mathrm{v}_1]\gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e}^{+}))), (\mathrm{H}_2 \uplus \mathrm{H}_{2v}, [\mathrm{x} \mapsto \mathrm{v}_2]\gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e}^{+})))) \in \mathcal{E}[\![\tau_2]\!]_{\rho}$$

Let $\gamma_{\mathrm{L}}' = \gamma_{\mathrm{L}}[\mathrm{x} \mapsto (\mathrm{v}_1, \mathrm{v}_2)]$. Next, notice that $(W', \mathrm{H}_1 \uplus \mathrm{H}_{1v}, \mathrm{H}_2 \uplus \mathrm{H}_{2v}, \gamma_{\mathrm{L}}') \in \mathcal{G}[\![\Gamma, \mathrm{x} : \tau_1]\!]_{\rho}$ because $(W', \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}[\![\Gamma]\!]_{\rho}$ (by Lemma 4.7) and $(W', (\mathrm{H}_{1v}, \mathrm{v}_1), (\mathrm{H}_{2v}, \mathrm{v}_2)) \in \mathcal{V}[\![\tau_1]\!]_{\rho}$. Thus, we can instantiate the first induction hypothesis with $\rho, \gamma_{\Gamma}, \gamma_{\mathrm{L}}', W', \mathrm{H}_1 \uplus \mathrm{H}_{1v}, \mathrm{H}_2 \uplus \mathrm{H}_{2v}$, which suffices to prove the above statement. □

Lemma 4.31 (Compat $e_1\ e_2$). *If* $\Delta;\Gamma;\Delta;\Gamma_1 \vdash e_1 \preceq e_1 : \tau_1 \multimap \tau_2$ *and* $\Delta;\Gamma;\Delta;\Gamma_2 \vdash e_2 \preceq e_2 : \tau_1$ *, then*

$$\Delta;\Gamma;\Delta;\Gamma_1 \uplus \Gamma_2 \vdash e_1\ e_2 \preceq e_1\ e_2 : \tau_2$$

Proof. Expanding the definition of $\preceq$, $\cdot^+$, $\mathcal{E}[\![\cdot]\!]_\cdot$ and pushing substitutions in the goal, we are to show that

$$\begin{array}{l}
\exists H_1', H_{1g}'.\forall H_{2+} : \mathit{MHeap}.\exists H_2', W', H_{2g}', v_2. \\
H_{1*} = H_{1g}' \uplus H_1' \uplus H_{1+} \ \wedge H_{1g}', H_{2g}' : W' \wedge \\
W \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(H_{1+})),L_2\cup FL(\mathrm{cod}(H_{2+})))} W' \wedge \\
(W', (H_1', v_1), (H_2', v_2)) \in \mathcal{V}[\![\tau_2]\!]_\rho \wedge \\
(H_{2g+} \uplus H_2 \uplus H_{2+}, \gamma_L^2(\gamma_\Gamma^2(e_1{}^+))\ \gamma_L^2(\gamma_\Gamma^2(e_2{}^+))) \xrightarrow{*}_{L_2} (H_{2g}' \uplus H_2' \uplus H_{2+}, v_2) \not\twoheadrightarrow
\end{array}$$

given arbitrary $\rho, \gamma_L, \gamma_\Gamma, W, L_1, L_2, H_{1g+}, H_{2g+} : W, v_1, H_1, H_2, H_{1+} : \mathit{MHeap}, H_{1*}$, such that

$$\rho.L3 \in \mathcal{D}[\![\Delta]\!], \rho.F \in \mathcal{D}[\![\Delta]\!], (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho, (W, H_1, H_2, \gamma_L) \in \mathcal{G}[\![\Gamma]\!]_\rho$$

and

$$(H_{1g+} \uplus H_1 \uplus H_{1+}, \gamma_L^1(\gamma_\Gamma^1(e_1{}^+))\ \gamma_L^1(\gamma_\Gamma^1(e_2{}^+))) \xrightarrow{*}_{L_1} (H_{1*}, v_1) \not\twoheadrightarrow$$

Then, by Lemma 4.13, there exist $\gamma_{L1}, \gamma_{L2}, H_{1l}, H_{1r}, H_{2l}, H_{2r}$ such that $\gamma_L = \gamma_{L1} \uplus \gamma_{L2}$, $H_1 = H_{1l} \uplus H_{1r}$, $H_2 = H_{2l} \uplus H_{2r}$,

$$\begin{array}{c}
(W, H_{1l}, H_{2l}, \gamma_{L1}) \in \mathcal{G}[\![\Gamma_1]\!]_\rho \\
(W, H_{1r}, H_{2r}, \gamma_{L2}) \in \mathcal{G}[\![\Gamma_2]\!]_\rho
\end{array}$$

and for all $j \in \{1, 2\}$,

$$\begin{array}{c}
\gamma_L^j(\gamma_\Gamma^j(e_1{}^+)) = \gamma_{L1}^j(\gamma_\Gamma^j(e_1{}^+)) \\
\gamma_L^j(\gamma_\Gamma^j(e_2{}^+)) = \gamma_{L2}^j(\gamma_\Gamma^j(e_2{}^+))
\end{array}$$

Then, by instantiating the first induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{L1}, W, H_{1l}, H_{2l}$, we find

$$(W, (H_{1l}, \gamma_{L1}^1(\gamma_\Gamma^1(e_1{}^+))), (H_{2l}, \gamma_{L1}^2(\gamma_\Gamma^2(e_1{}^+)))) \in \mathcal{E}[\![\tau_1 \multimap \tau_2]\!]_\rho$$

Thus, by Lemma 4.3, we have

$$(H_{1g+} \uplus H_{1l} \uplus H_{1r} \uplus H_{1+}, \gamma_{L1}^1(\gamma_\Gamma^1(e_1{}^+))) \xrightarrow{*}_{L_1\cup FL(\gamma_{L2}^1(\gamma_\Gamma^1(e_2{}^+)))} (H_{1g}' \uplus H_{1r} \uplus H_{1+} \uplus H_{1l}^*, v_{1l}) \not\twoheadrightarrow$$

and, for any H_{2+},

$$(H_{2g+} \uplus H_{2l} \uplus H_{2r} \uplus H_{2+}, \gamma_{L1}^2(\gamma_\Gamma^2(e_1{}^+))) \xrightarrow{*}_{L_2\cup FL(\gamma_{L2}^2(\gamma_\Gamma^2(e_2{}^+)))} (H_{2g}' \uplus H_{2r} \uplus H_{2+} \uplus H_{2l}^*, v_{2l}) \not\twoheadrightarrow$$

where $H_{1g}', H_{2g}' : W'$ for some

$$W \sqsubseteq_{(\mathrm{dom}(H_{1r}\uplus H_{1+}),\mathrm{dom}(H_{2r}\uplus H_{2+})),\mathrm{rchgclocs}(W,FL(\mathrm{cod}(H_{1r}))\cup FL(\mathrm{cod}(H_{1+}))\cup FL(\gamma_{L2}^1(\gamma_\Gamma^1(e_2{}^+)))\cup L_1,FL(\mathrm{cod}(H_{2r}))\cup FL(\mathrm{cod}(H_{2+}))\cup FL(\gamma_{L2}^2(\gamma_\Gamma^2(} W'$$

and

$$(W', (H_{1l}^*, v_{1l}), (H_{2l}^*, v_{2l})) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!]_\rho$$

By expanding the value relation, we find that there exist expressions e_{1l}, e_{2l} such that $v_{1l} = \lambda x.e_{1l}$ and $v_{2l} = \lambda x.e_{2l}$.

Then, since $\mathcal{G}[\![\Gamma]\!]_\rho, \mathcal{G}[\![\Gamma_1 \uplus \Gamma_2]\!]_\rho$ are closed under world extension by Lemma 4.7, we can instantiate the second induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{L2}, W', H_{1r}, H_{2r}$ to find

$$(W', (H_{1r}, \gamma_{L2}^1(\gamma_\Gamma^1(e_2{}^+))), (H_{2r}, \gamma_{L2}^2(\gamma_\Gamma^2(e_2{}^+)))) \in \mathcal{E}[\![\tau_1]\!]_\rho$$

Thus, by Lemma 4.3, we have

$$(H_{1g}' \uplus H_{1r} \uplus H_{1+} \uplus H_{1l}^*, \gamma_{L2}^1(\gamma_\Gamma^1(e_2{}^+))) \xrightarrow{*}_{L_1\cup FL(e_{1l})} (H_{1g}'' \uplus H_{1+} \uplus H_{1l}^* \uplus H_{1r}^*, v_{1r})$$

and

$$(\mathrm{H}'_{2g} \uplus \mathrm{H}_{1r} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}^*_{2l}, \gamma_{\mathrm{L}}{}^2_2(\gamma^2_\Gamma(\mathrm{e}_2{}^+))) \xrightarrow{*}_{L_2 \cup FL(\mathrm{e}_{2\mathrm{l}})} (\mathrm{H}''_{2g} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}^*_{2l} \uplus \mathrm{H}^*_{2r}, \mathrm{v}_{2\mathrm{r}})$$

where $\mathrm{H}''_{1g}, \mathrm{H}''_{2g} : W''$ for some

$W' \sqsubseteq_{(\mathrm{dom}(\mathrm{H}^*_{1l} \uplus \mathrm{H}_{1+}), \mathrm{dom}(\mathrm{H}^*_{2l} \uplus \mathrm{H}_{2+})), \mathrm{rchgclocs}(W', FL(\mathrm{cod}(\mathrm{H}^*_{1l})) \cup FL(\mathrm{cod}(\mathrm{H}_{1+})) \cup FL(\mathrm{e}_{1\mathrm{l}}) \cup L_1, FL(\mathrm{cod}(\mathrm{H}^*_{2l})) \cup FL(\mathrm{cod}(\mathrm{H}_{2+})) \cup FL(\mathrm{e}_{2\mathrm{l}}) \cup L_2)} W''$

and

$$(W'', (\mathrm{H}^*_{1r}, \mathrm{v}_{1\mathrm{r}}), (\mathrm{H}^*_{2r}, \mathrm{v}_{2\mathrm{r}})) \in \mathcal{V}[\![\tau_2]\!]_\rho$$

Thus, the original configurations step as follows:

$$\begin{array}{l}
(\mathrm{H}_{1g} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \gamma_{\mathrm{L}}{}^1_1(\gamma^1_\Gamma(\mathrm{e}_1{}^+))\ \gamma_{\mathrm{L}}{}^1_2(\gamma^1_\Gamma(\mathrm{e}_2{}^+))) \xrightarrow{*}_{L_1} \\
(\mathrm{H}'_{1g} \uplus \mathrm{H}_{1r} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}^*_{1l}, \lambda \mathrm{x}.\mathrm{e}_{1\mathrm{l}}\ \gamma_{\mathrm{L}}{}^1_2(\gamma^1_\Gamma(\mathrm{e}_2{}^+))) \xrightarrow{*}_{L_1} \\
(\mathrm{H}''_{1g} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}^*_{1l} \uplus \mathrm{H}^*_{1r}, \lambda \mathrm{x}.\mathrm{e}_{1\mathrm{l}}\ \mathrm{v}_{1\mathrm{r}}) \xrightarrow{*}_{L_1} \\
(\mathrm{H}''_{1g} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}^*_{1l} \uplus \mathrm{H}^*_{1r}, [\mathrm{x} \mapsto \mathrm{v}_{1\mathrm{r}}]\mathrm{e}_{1\mathrm{l}})
\end{array}$$

and similarly on the other side, the configuration steps to

$$(\mathrm{H}''_{2g} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}^*_{2l} \uplus \mathrm{H}^*_{2r}, [\mathrm{x} \mapsto \mathrm{v}_{2\mathrm{r}}]\mathrm{e}_{2\mathrm{l}})$$

Since $(W', (\mathrm{H}^*_{1l}, \lambda \mathrm{x}.\mathrm{e}_{1\mathrm{l}}), (\mathrm{H}^*_{2l}, \lambda \mathrm{x}.\mathrm{e}_{2\mathrm{l}})) \in \mathcal{V}[\![\tau_1 \multimap \tau_2]\!]_\rho$, $W' \sqsubseteq_{\mathrm{H}^*_{1l}, \mathrm{H}^*_{2l}, \mathrm{e}_{1\mathrm{l}}, \mathrm{e}_{2\mathrm{l}}} W''$ (by Lemma 4.5), and $(W'', (\mathrm{H}^*_{1r}, \mathrm{v}_{1\mathrm{r}}), (\mathrm{H}^*_{2r}, \mathrm{v}_{2\mathrm{r}})) \in \mathcal{V}[\![\tau_2]\!]_\rho$, we have

$$(W'', (\mathrm{H}^*_{1l} \uplus \mathrm{H}^*_{1r}, [\mathrm{x} \mapsto \mathrm{v}_{1\mathrm{r}}]\mathrm{e}_{1\mathrm{l}}), (\mathrm{H}^*_{2l} \uplus \mathrm{H}^*_{2r}, [\mathrm{x} \mapsto \mathrm{v}_{2\mathrm{r}}]\mathrm{e}_{2\mathrm{l}})) \in \mathcal{E}[\![\tau_2]\!]_\rho \tag{47}$$

Next, by the assumption that the configuration on the left-hand side terminates, we have

$$(\mathrm{H}''_{1g} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}^*_{1l} \uplus \mathrm{H}^*_{1r}, [\mathrm{x} \mapsto \mathrm{v}_{1\mathrm{r}}]\mathrm{e}_{1\mathrm{l}}) \xrightarrow{*}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \nrightarrow_{L_1}$$

Then, by applying (47), we find

$$(\mathrm{H}_{1*}, \mathrm{v}_1) = (\mathrm{H}'''_{1g} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}_{1f}, \mathrm{v}_{1\mathrm{f}})$$

and

$$(\mathrm{H}''_{2g} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}^*_{2l} \uplus \mathrm{H}^*_{2r}, [\mathrm{x} \mapsto \mathrm{v}_{2\mathrm{r}}]\mathrm{e}_{2\mathrm{l}}) \xrightarrow{*}_{L_2} (\mathrm{H}'''_{2g} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}_{2f}, \mathrm{v}_{2\mathrm{f}})$$

where $\mathrm{H}'''_{1g}, \mathrm{H}'''_{2g} : W'''$ for some $W'' \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}), \mathrm{dom}(\mathrm{H}_{2+})), \mathrm{rchgclocs}(W'', L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})), L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W'''$ and

$$(W''', (\mathrm{H}_{1f}, \mathrm{v}_{1\mathrm{f}}), (\mathrm{H}_{2f}, \mathrm{v}_{2\mathrm{f}})) \in \mathcal{V}[\![\tau_2]\!]_\rho$$

Then, choose $\mathrm{H}'_1 = \mathrm{H}_{1f}$, $\mathrm{H}'_2 = \mathrm{H}_{2f}$, $W' = W'''$, $\mathrm{H}'_{1g} = \mathrm{H}'''_{1g}$, and $\mathrm{H}'_{2g} = \mathrm{H}'''_{2g}$. Notice that $W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}), \mathrm{dom}(\mathrm{H}_{2+})), \mathrm{rchgclocs}(W'', L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})), L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W'''$ by Lemma 4.6. This suffices to finish the proof. □

Lemma 4.32 (Compat ()).

$$\Delta; \Gamma; \Delta; \emptyset \vdash () \preceq () : \mathrm{Unit}$$

Proof. Expanding the conclusion, we must show that given

$$\begin{array}{l}
\forall \rho, \gamma_\Gamma, \gamma_{\mathrm{L}}, W, \mathrm{H}_1, \mathrm{H}_2. \\
\rho.\mathrm{F} \in \mathcal{D}[\![\Delta]\!] \wedge \rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!] \wedge (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \wedge (W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}.\Gamma) \in \mathcal{G}[\![\emptyset]\!]_\rho \\
\wedge\ \gamma_{\mathrm{L}}.\Delta = \gamma_{\mathrm{locs}}(\rho.\mathrm{L3})
\end{array}$$

it holds that:

$$(W, (\mathrm{H}_1, ()), (\mathrm{H}_2, ())) \in \mathcal{E}[\![\mathrm{Unit}]\!]_\rho$$

By Lemma 4.12, it suffices to show that:

$$(W, (\mathrm{H}_1, ()), (\mathrm{H}_2, ())) \in \mathcal{V}[\![\mathrm{Unit}]\!]_\rho$$

Notice that, since $(W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}.\Gamma) \in \mathcal{G}[\![\emptyset]\!]_\rho$, it must be the case that $\mathrm{H}_1 = \mathrm{H}_2 = \emptyset$. Thus, one can easily see by definition that $(W, (\emptyset, ()), (\emptyset, ())) \in \mathcal{V}[\![\mathrm{Unit}]\!]_\rho$, which suffices to finish the proof. □

Lemma 4.33 (Compat $\mathbb{B}$). *If* $\mathrm{b} \in \mathbb{B}$*, then*

$$\Delta; \Gamma; \Delta; \emptyset \vdash \mathrm{b} \preceq \mathrm{b} : \mathrm{Bool}$$

Proof. By a simple case analysis, one can see that, for all $\mathrm{b} \in \mathbb{B}$, there exists a $\mathrm{b} \in \{0, 1\}$ such that $\mathrm{b}^+ = \mathrm{b}$. Expanding the conclusion, we must show that given

$$\begin{array}{l}\forall \rho, \gamma_\Gamma, \gamma_{\mathrm{L}}, W, \mathrm{H}_1, \mathrm{H}_2. \\ \rho.\mathrm{F} \in \mathcal{D}[\![\Delta]\!] \land \rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!] \land (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \land (W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}.\Gamma) \in \mathcal{G}[\![\emptyset]\!]_\rho \\ \land\ \gamma_{\mathrm{L}}.\Delta = \gamma_{\mathrm{locs}}(\rho.\mathrm{L3})\end{array}$$

it holds that:

$$(W, (\mathrm{H}_1, \mathrm{b}), (\mathrm{H}_2, \mathrm{b})) \in \mathcal{E}[\![\mathrm{Bool}]\!]_\rho$$

By Lemma 4.12, it suffices to show that:

$$(W, (\mathrm{H}_1, \mathrm{b}), (\mathrm{H}_2, \mathrm{b})) \in \mathcal{V}[\![\mathrm{Bool}]\!]_\rho$$

Notice that, since $(W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}.\Gamma) \in \mathcal{G}[\![\emptyset]\!]_\rho$, it must be the case that $\mathrm{H}_1 = \mathrm{H}_2 = \emptyset$. Thus, since $\mathrm{b} \in \{0, 1\}$, one can easily see by definition that $(W, (\emptyset, \mathrm{b}), (\emptyset, \mathrm{b})) \in \mathcal{V}[\![\mathrm{Bool}]\!]_\rho$, which suffices to finish the proof. □

Lemma 4.34 (Compat let ()). *If* $\Delta; \Gamma; \Delta; \Gamma_1 \vdash \mathrm{e}_1 \preceq \mathrm{e}_1 : \mathrm{Unit}$ *and* $\Delta; \Gamma; \Delta; \Gamma_2 \vdash \mathrm{e}_2 \preceq \mathrm{e}_2 : \tau$*, then*

$$\Delta; \Gamma; \Delta; \Gamma_1 \uplus \Gamma_2 \vdash \mathrm{let}\ () = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 \preceq \mathrm{let}\ () = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 : \tau$$

Proof. Expanding the definition of $\preceq$, $\cdot^+$, $\mathcal{E}[\![\cdot]\!]$. and pushing substitutions in the goal, we are to show that

$$\begin{array}{l}\exists \mathrm{H}_1', \mathrm{H}_{1g}'.\forall \mathrm{H}_{2+} : \mathit{MHeap}.\exists \mathrm{H}_2', W', \mathrm{H}_{2g}', \mathrm{v}_2. \\ \mathrm{H}_{1*} = \mathrm{H}_{1g}' \uplus \mathrm{H}_1' \uplus \mathrm{H}_{1+}\ \land \mathrm{H}_{1g}', \mathrm{H}_{2g}' : W' \land \\ W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W'',L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))}\ W' \land \\ (W', (\mathrm{H}_1', \mathrm{v}_1), (\mathrm{H}_2', \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho \land \\ (\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathrm{let}\ \_ = \gamma_{\mathrm{L}}^2(\gamma_\Gamma^2(\mathrm{e}_1{}^+))\ \mathrm{in}\ \gamma_{\mathrm{L}}^2(\gamma_\Gamma^2(\mathrm{e}_2{}^+))) \overset{*}{\rightarrow}_{L_2} (\mathrm{H}_{2g}' \uplus \mathrm{H}_2' \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \nrightarrow\end{array}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_\Gamma, W, L_1, L_2, \mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W, \mathrm{v}_1, \mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_{1+} : \mathit{MHeap}, \mathrm{H}_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!], \rho.\mathrm{F} \in \mathcal{D}[\![\Delta]\!], (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho, (W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}[\![\Gamma_1 \uplus \Gamma_2]\!]_\rho$$

and

$$(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \mathrm{let}\ \_ = \gamma_{\mathrm{L}}^1(\gamma_\Gamma^1(\mathrm{e}_1{}^+))\ \mathrm{in}\ \gamma_{\mathrm{L}}^1(\gamma_\Gamma^1(\mathrm{e}_2{}^+))) \overset{*}{\rightarrow}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \nrightarrow$$

Then, by Lemma 4.13, there exist $\gamma_{\mathrm{L}1}, \gamma_{\mathrm{L}2}, \mathrm{H}_{1l}, \mathrm{H}_{1r}, \mathrm{H}_{2l}, \mathrm{H}_{2r}$ such that $\gamma_{\mathrm{L}} = \gamma_{\mathrm{L}1} \uplus \gamma_{\mathrm{L}2}$, $\mathrm{H}_1 = \mathrm{H}_{1l} \uplus \mathrm{H}_{1r}$, $\mathrm{H}_2 = \mathrm{H}_{2l} \uplus \mathrm{H}_{2r}$,

$$\begin{array}{c}(W, \mathrm{H}_{1l}, \mathrm{H}_{2l}, \gamma_{\mathrm{L}1}) \in \mathcal{G}[\![\Gamma_1]\!]_\rho \\ (W, \mathrm{H}_{1r}, \mathrm{H}_{2r}, \gamma_{\mathrm{L}2}) \in \mathcal{G}[\![\Gamma_2]\!]_\rho\end{array}$$

and for all $j \in \{1, 2\}$,

$$\begin{array}{c}\gamma_{\mathrm{L}}^j(\gamma_\Gamma^j(\mathrm{e}_1{}^+)) = \gamma_{\mathrm{L}1}^j(\gamma_\Gamma^j(\mathrm{e}_1{}^+)) \\ \gamma_{\mathrm{L}}^j(\gamma_\Gamma^j(\mathrm{e}_2{}^+)) = \gamma_{\mathrm{L}2}^j(\gamma_\Gamma^j(\mathrm{e}_2{}^+))\end{array}$$

Then, by instantiating the first induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{\mathrm{L}1}, W, \mathrm{H}_{1l}, \mathrm{H}_{2l}$, we find

$$(W, (\mathrm{H}_{1l}, \gamma_{\mathrm{L}1}^1(\gamma_\Gamma^1(\mathrm{e}_1{}^+))), (\mathrm{H}_{2l}, \gamma_{\mathrm{L}1}^2(\gamma_\Gamma^2(\mathrm{e}_1{}^+)))) \in \mathcal{E}[\![\mathrm{Unit}]\!]_\rho$$

Thus, by Lemma 4.3, we have

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1l} \uplus \mathsf{H}_{1r} \uplus \mathsf{H}_{1+}, \gamma_{\mathrm{L}_1}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_1{}^{+}))) \xrightarrow{*}_{L_1 \cup FL(\gamma_{\mathrm{L}_2}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_2{}^{+})))} (\mathsf{H}'_{1g} \uplus \mathsf{H}_{1r} \uplus \mathsf{H}_{1+} \uplus \mathsf{H}^{*}_{1l}, \mathsf{v}_{1\mathsf{l}}) \nrightarrow$$

and, for any H_{2+},

$$(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2l} \uplus \mathsf{H}_{2r} \uplus \mathsf{H}_{2+}, \gamma_{\mathrm{L}_1}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_1{}^{+}))) \xrightarrow{*}_{L_2 \cup FL(\gamma_{\mathrm{L}_2}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_2{}^{+})))} (\mathsf{H}'_{2g} \uplus \mathsf{H}_{2r} \uplus \mathsf{H}_{2+} \uplus \mathsf{H}^{*}_{2l}, \mathsf{v}_{2\mathsf{l}}) \nrightarrow$$

where $\mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W'$ for some

$$W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1r} \uplus \mathsf{H}_{1+}), \mathrm{dom}(\mathsf{H}_{2r} \uplus \mathsf{H}_{2+})), \mathrm{rchgclocs}(W, FL(\mathrm{cod}(\mathsf{H}_{1r})) \cup FL(\mathrm{cod}(\mathsf{H}_{1+})) \cup FL(\gamma_{\mathrm{L}_2}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_2{}^{+}))) \cup L_1, FL(\mathrm{cod}(\mathsf{H}_{2r})) \cup FL(\mathrm{cod}(\mathsf{H}_{2+})) \cup FL(\gamma_{\mathrm{L}_2}^{2}(\gamma_{\Gamma}^{2}(} W'$$

and

$$(W', (\mathsf{H}^{*}_{1l}, \mathsf{v}_{1\mathsf{l}}), (\mathsf{H}^{*}_{2l}, \mathsf{v}_{2\mathsf{l}})) \in \mathcal{V}[\![\mathsf{Unit}]\!]_{\rho}$$

By expanding the value relation, we find $\mathsf{H}^{*}_{1l} = \mathsf{H}^{*}_{2l} = \emptyset$ and $\mathsf{v}_1 = \mathsf{v}_2 = ()$.

Thus, the original configuration steps as follows:

$$\begin{aligned}
&(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = \gamma_{\mathrm{L}_1}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_1{}^{+}))\ \mathsf{in}\ \gamma_{\mathrm{L}_2}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_2{}^{+}))) \xrightarrow{*}\\
&(\mathsf{H}'_{1g} \uplus \mathsf{H}_{1r} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = ()\ \mathsf{in}\ \gamma_{\mathrm{L}_2}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_2{}^{+}))) \rightarrow\\
&(\mathsf{H}'_{1g} \uplus \mathsf{H}_{1r} \uplus \mathsf{H}_{1+}, \gamma_{\mathrm{L}_2}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_2{}^{+})))
\end{aligned}$$

and

$$\begin{aligned}
&(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \mathsf{let}\ \_ = \gamma_{\mathrm{L}_1}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_1{}^{+}))\ \mathsf{in}\ \gamma_{\mathrm{L}_2}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_2{}^{+}))) \xrightarrow{*}\\
&(\mathsf{H}'_{2g} \uplus \mathsf{H}_{2r} \uplus \mathsf{H}_{2+}, \mathsf{let}\ \_ = ()\ \mathsf{in}\ \gamma_{\mathrm{L}_2}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_2{}^{+}))) \rightarrow\\
&(\mathsf{H}'_{2g} \uplus \mathsf{H}_{2t} \uplus \mathsf{H}_{2+}, \gamma_{\mathrm{L}_2}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_2{}^{+})))
\end{aligned}$$

Then, since $\mathcal{G}[\![\Gamma]\!]_{\rho}, \mathcal{G}[\![\Gamma_1 \uplus \Gamma_2]\!]_{\rho}$ are closed under world extension by Lemma 4.7, we can instantiate the second induction hypothesis with $\rho, \gamma_{\Gamma}, \gamma_{\mathrm{L}_2}, W', \mathsf{H}_{1r}, \mathsf{H}_{2r}$:

$$(W', (\mathsf{H}_{1r}, \gamma_{\mathrm{L}_2}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_2{}^{+}))), (\mathsf{H}_{2r}, \gamma_{\mathrm{L}_2}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_2{}^{+})))) \in \mathcal{E}[\![\tau]\!]_{\rho} \tag{48}$$

Next, by the assumption that the configuration on the left-hand side terminates, we have

$$(\mathsf{H}'_{1g} \uplus \mathsf{H}_{1r} \uplus \mathsf{H}_{1+}, \gamma_{\mathrm{L}_2}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_2{}^{+}))) \xrightarrow{*}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \nrightarrow_{L_1}$$

Then, by applying (48), we find

$$(\mathsf{H}_{1*}, \mathsf{v}_1) = (\mathsf{H}''_{1g} \uplus \mathsf{H}^{*}_{1r} \uplus \mathsf{H}_{1+}, \mathsf{v}'_1)$$

and

$$(\mathsf{H}'_{2g} \uplus \mathsf{H}_{2r} \uplus \mathsf{H}_{2+}, \gamma_{\mathrm{L}_2}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_2{}^{+}))) \xrightarrow{*}_{L_2} (\mathsf{H}''_{2g} \uplus \mathsf{H}^{*}_{2r} \uplus \mathsf{H}_{2+}, \mathsf{v}'_2)$$

where $\mathsf{H}''_{1g}, \mathsf{H}''_{2g} : W''$, $W' \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}), \mathrm{dom}(\mathsf{H}_{2+})), \mathrm{rchgclocs}(W', L_1 \cup FL(\mathrm{cod}(\mathsf{H}_{1+})), L_2 \cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W''$, and $(W'', (\mathsf{H}^{*}_{1r}, \mathsf{v}'_1), (\mathsf{H}^{*}_{2r}, \mathsf{v}_2{}')) \in \mathcal{V}[\![\tau]\!]_{\rho}$. By Lemma 4.7, we find that $W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}), \mathrm{dom}(\mathsf{H}_{2+})), \mathrm{rchgclocs}(W, L_1 \cup FL(\mathrm{cod}(\mathsf{H}_{1+})), L_2 \cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W''$. Finally, we can take $\mathsf{H}'_{1g} = \mathsf{H}''_{1g}$, $\mathsf{H}'_1 = \mathsf{H}^{*}_{1r}$, $\mathsf{H}'_{2g} = \mathsf{H}''_{2g}$, and $\mathsf{H}'_2 = \mathsf{H}^{*}_{2r}$, which suffices to finish the proof. □

Lemma 4.35 (Compat if). *If* $\Delta; \Gamma; \Delta; \Gamma_1 \vdash \mathsf{e}_1 \preceq \mathsf{e}_1 : \mathsf{Bool}$ *and* $\Delta; \Gamma; \Delta; \Gamma_2 \vdash \mathsf{e}_2 \preceq \mathsf{e}_2 : \tau$ *and* $\Delta; \Gamma; \Delta; \Gamma_2 \vdash \mathsf{e}_3 \preceq \mathsf{e}_3 : \tau$ *, then*

$$\Delta; \Gamma; \Delta; \Gamma_1 \uplus \Gamma_2 \vdash \mathsf{if}\ \mathsf{e}_1\ \mathsf{e}_2\ \mathsf{e}_3 \preceq \mathsf{if}\ \mathsf{e}_1\ \mathsf{e}_2\ \mathsf{e}_3 : \tau$$

Proof. Expanding the definition of $\preceq$, $\cdot^{+}$, $\mathcal{E}[\![\cdot]\!]$. and pushing substitutions in the goal, we are to show that

$$\begin{array}{l}
\exists H_1', H_{1g}'.\forall H_{2+} : \mathit{MHeap}.\exists H_2', W', H_{2g}', v_2. \\
H_{1*} = H_{1g}' \uplus H_1' \uplus H_{1+} \ \wedge H_{1g}', H_{2g}' : W' \wedge \\
W \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(H_{1+})),L_2\cup FL(\mathrm{cod}(H_{2+})))} W' \wedge \\
(W', (H_1', v_1), (H_2', v_2)) \in \mathcal{V}[\![\tau]\!]_\rho \wedge \\
(H_{2g+} \uplus H_2 \uplus H_{2+}, \text{if } \gamma_L^2(\gamma_\Gamma^2({e_1}^+))\ \gamma_L^2(\gamma_\Gamma^2({e_2}^+))\ \gamma_L^2(\gamma_\Gamma^2({e_3}^+))) \xrightarrow{*}_{L_2} (H_{2g}' \uplus H_2' \uplus H_{2+}, v_2) \not\twoheadrightarrow
\end{array}$$

given arbitrary $\rho, \gamma_L, \gamma_\Gamma, W, L_1, L_2, H_{1g+}, H_{2g+} : W, v_1, H_1, H_2, H_{1+} : \mathit{MHeap}, H_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!], \rho.\mathrm{F} \in \mathcal{D}[\![\Delta]\!], (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho, (W, H_1, H_2, \gamma_L) \in \mathcal{G}[\![\Gamma_1 \uplus \Gamma_2]\!]_\rho$$

and

$$(H_{1g+} \uplus H_1 \uplus H_{1+}, \text{if } \gamma_L^1(\gamma_\Gamma^1({e_1}^+))\ \gamma_L^1(\gamma_\Gamma^1({e_2}^+))\ \gamma_L^1(\gamma_\Gamma^1({e_3}^+))) \xrightarrow{*}_{L_1} (H_{1*}, v_1) \not\twoheadrightarrow$$

Then, by Lemma 4.13, there exist $\gamma_{L_1}, \gamma_{L_2}, H_{1l}, H_{1r}, H_{2l}, H_{2r}$ such that $\gamma_L = \gamma_{L_1} \uplus \gamma_{L_2}$, $H_1 = H_{1l} \uplus H_{1r}$, $H_2 = H_{2l} \uplus H_{2r}$,

$$(W, H_{1l}, H_{2l}, \gamma_{L_1}) \in \mathcal{G}[\![\Gamma_1]\!]_\rho$$
$$(W, H_{1r}, H_{2r}, \gamma_{L_2}) \in \mathcal{G}[\![\Gamma_2]\!]_\rho$$

and for all $j \in \{1, 2\}$,

$$\gamma_L^j(\gamma_\Gamma^j({e_1}^+)) = {\gamma_{L}}_1^j(\gamma_\Gamma^j({e_1}^+))$$
$$\gamma_L^j(\gamma_\Gamma^j({e_2}^+)) = {\gamma_{L}}_2^j(\gamma_\Gamma^j({e_2}^+))$$

Then, by instantiating the first induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{L_1}, W, H_{1l}, H_{2l}$, we find

$$(W, (H_{1l}, {\gamma_{L}}_1^1(\gamma_\Gamma^1({e_1}^+))), (H_{2l}, {\gamma_{L}}_1^2(\gamma_\Gamma^2({e_1}^+)))) \in \mathcal{E}[\![\mathrm{Bool}]\!]_\rho$$

Thus, by Lemma 4.3, we have

$$(H_{1g+} \uplus H_{1l} \uplus H_{1r} \uplus H_{1+}, {\gamma_{L}}_1^1(\gamma_\Gamma^1({e_1}^+))) \xrightarrow{*}_{L_1 \cup FL({\gamma_{L}}_2^1(\gamma_\Gamma^1({e_2}^+))) \cup FL({\gamma_{L}}_2^1(\gamma_\Gamma^1({e_3}^+)))} (H_{1g}' \uplus H_{1r} \uplus H_{1+} \uplus H_{1l}^*, v_{1l}) \not\twoheadrightarrow$$

and, for any H_{2+},

$$(H_{2g+} \uplus H_{2l} \uplus H_{2r} \uplus H_{2+}, {\gamma_{L}}_1^2(\gamma_\Gamma^2({e_1}^+))) \xrightarrow{*}_{L_2 \cup FL({\gamma_{L}}_2^2(\gamma_\Gamma^2({e_2}^+))) \cup FL({\gamma_{L}}_2^1(\gamma_\Gamma^1({e_3}^+)))} (H_{2g}' \uplus H_{2r} \uplus H_{2+} \uplus H_{2l}^*, v_{2l}) \not\twoheadrightarrow$$

where $H_{1g}', H_{2g}' : W'$ for some

$$W \sqsubseteq_{\substack{(\mathrm{dom}(H_{1r} \uplus H_{1+}),\mathrm{dom}(H_{2r} \uplus H_{2+})),\mathrm{rchgclocs}(W,FL(\mathrm{cod}(H_{1r}))\cup FL(\mathrm{cod}(H_{1+}))\cup FL({\gamma_{L}}_2^1(\gamma_\Gamma^1({e_2}^+)))\cup FL({\gamma_{L}}_2^1(\gamma_\Gamma^1({e_3}^+)))\cup L_1, \\ FL(\mathrm{cod}(H_{2r}))\cup FL(\mathrm{cod}(H_{2+}))\cup FL({\gamma_{L}}_2^2(\gamma_\Gamma^2({e_2}^+)))\cup FL({\gamma_{L}}_2^2(\gamma_\Gamma^2({e_3}^+)))\cup L_2)}} W'$$

and

$$(W', (H_{1l}^*, v_{1l}), (H_{2l}^*, v_{2l})) \in \mathcal{V}[\![\mathrm{Bool}]\!]_\rho$$

By expanding the value relation, we find $H_{1l}^* = H_{2l}^* = \emptyset$ and either $v_{1l} = v_{2l} = 0$ or $v_1 = v_2 = 1$. Both cases are trivially similar to each other, so we only prove the case where $v_{1l} = v_{2l} = 0$.

Then, the original configuration steps as follows:

$$\begin{array}{l}
(H_{1g+} \uplus H_1 \uplus H_{1+}, \text{if } {\gamma_{L}}_1^1(\gamma_\Gamma^1({e_1}^+))\ {\gamma_{L}}_2^1(\gamma_\Gamma^1({e_2}^+))\ \gamma_2^1(\gamma_\Gamma^1({e_3}^+))) \xrightarrow{*}_{L_1} \\
(H_{1g}' \uplus H_{1r} \uplus H_{1+}, \text{if } 0\ {\gamma_{L}}_2^1(\gamma_\Gamma^1({e_2}^+))\ {\gamma_{L}}_2^1(\gamma_\Gamma^1({e_3}^+))) \xrightarrow{*}_{L_1} \\
(H_{1g}' \uplus H_{1r} \uplus H_{1+}, {\gamma_{L}}_2^1(\gamma_\Gamma^1({e_2}^+)))
\end{array}$$

and

$$\begin{array}{l}
(H_{2g+} \uplus H_2 \uplus H_{2+}, \text{if } {\gamma_{L}}_1^2(\gamma_\Gamma^2({e_1}^+))\ {\gamma_{L}}_2^2(\gamma_\Gamma^2({e_2}^+))\ {\gamma_{L}}_2^2(\gamma_\Gamma^2({e_3}^+))) \xrightarrow{*}_{L_2} \\
(H_{2g}' \uplus H_{2r} \uplus H_{2+}, \text{if } 0\ {\gamma_{L}}_2^2(\gamma_\Gamma^2({e_2}^+))\ {\gamma_{L}}_2^2(\gamma_\Gamma^2({e_3}^+))) \xrightarrow{*}_{L_2} \\
(H_{2g}' \uplus H_{2r} \uplus H_{2+}, {\gamma_{L}}_2^2(\gamma_\Gamma^2({e_2}^+)))
\end{array}$$

Then, since $\mathcal{G}\llbracket\Gamma\rrbracket_\rho, \mathcal{G}\llbracket\Gamma_1 \uplus \Gamma_2\rrbracket_\rho$ are closed under world extension by Lemma 4.7, we can instantiate the second induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{L2}, W', H_{1r}, H_{2r}$:

$$(W', (H_{1r}, \gamma_{L2}^{1}(\gamma_\Gamma^1(e_2{}^+))), (H_{2r}, \gamma_{L2}^{2}(\gamma_\Gamma^2(e_2{}^+)))) \in \mathcal{E}\llbracket\tau\rrbracket_\rho \tag{49}$$

Next, by the assumption that the configuration on the left-hand side terminates, we have

$$(H'_{1g} \uplus H_{1r} \uplus H_{1+}, \gamma_{L2}^{1}(\gamma_\Gamma^1(e_2{}^+))) \xrightarrow{*}_{L_1} (H_{1*}, v_1)$$

Then, by applying (49), we find

$$(H_{1*}, v_1) = (H''_{1g} \uplus H^*_{1r} \uplus H_{1+}, v'_1)$$

and

$$(H'_{2g} \uplus H_{2r} \uplus H_{2+}, \gamma_{L2}^{2}(\gamma_\Gamma^2(e_2{}^+))) \xrightarrow{*}_{L_2} (H''_{2g} \uplus H^*_{2r} \uplus H_{2+}, v'_2)$$

where $H''_{1g}, H''_{2g} : W''$, $W' \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(H_{1+})),L_2\cup FL(\mathrm{cod}(H_{2+})))} W''$, and $(W'', (H^*_{1r}, v'_1), (H^*_{2r}, v_2{}')) \in \mathcal{V}\llbracket\tau\rrbracket_\rho$. By Lemma 4.7, we find that $W \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(H_{1+})),L_2\cup FL(\mathrm{cod}(H_{2+})))} W''$. Finally, we can take $H'_{1g} = H''_{1g}$, $H'_1 = H^*_{1r}$, $H'_{2g} = H''_{2g}$, and $H'_2 = H^*_{2r}$, which suffices to finish the proof. □

Lemma 4.36 (Compat $(e_1,\ e_2)$). *If* $\Delta; \Gamma; \Delta; \Gamma_1 \vdash e_1 \preceq e_1 : \tau_1$ *and* $\Delta; \Gamma; \Delta; \Gamma_2 \vdash e_2 \preceq e_2 : \tau_2$ *, then*

$$\Delta; \Gamma; \Delta; \Gamma_1 \uplus \Gamma_2 \vdash (e_1,\ e_2) \preceq (e_1,\ e_2) : \tau_1 \otimes \tau_2$$

Proof. Expanding the definition of $\preceq$, $\cdot^+$, $\mathcal{E}\llbracket\cdot\rrbracket_\cdot$ and pushing substitutions in the goal, we are to show that

$$\begin{aligned}
&\exists H'_1, H'_{1g}.\forall H_{2+} : \mathit{MHeap}.\exists H'_2, W', H'_{2g}, v_2.\\
&H_{1*} = H'_{1g} \uplus H'_1 \uplus H_{1+} \ \wedge H'_{1g}, H'_{2g} : W' \wedge\\
&W \sqsubseteq_{(\mathrm{dom}(H_{1+}),\mathrm{dom}(H_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(H_{1+})),L_2\cup FL(\mathrm{cod}(H_{2+})))} W' \wedge\\
&(W', (H'_1, v_1), (H'_2, v_2)) \in \mathcal{V}\llbracket\tau_1 \otimes \tau_2\rrbracket_\rho \wedge\\
&(H_{2g+} \uplus H_2 \uplus H_{2+}, (\gamma_L^2(\gamma_\Gamma^2(e_1{}^+)),\ \gamma_L^2(\gamma_\Gamma^2(e_2{}^+)))) \xrightarrow{*}_{L_2} (H'_{2g} \uplus H'_2 \uplus H_{2+}, v_2) \not\twoheadrightarrow
\end{aligned}$$

given arbitrary $\rho, \gamma_L, \gamma_\Gamma, W, L_1, L_2, H_{1g+}, H_{2g+} : W, v_1, H_1, H_2, H_{1+} : \mathit{MHeap}, H_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}\llbracket\Delta\rrbracket, \rho.\mathrm{F} \in \mathcal{D}\llbracket\Delta\rrbracket, (W, \gamma_\Gamma) \in \mathcal{G}\llbracket\Gamma\rrbracket_\rho, (W, H_1, H_2, \gamma_L) \in \mathcal{G}\llbracket\Gamma_1 \uplus \Gamma_2\rrbracket_\rho$$

and

$$(H_{1g+} \uplus H_1 \uplus H_{1+}, (\gamma_L^1(\gamma_\Gamma^1(e_1{}^+)),\ \gamma_L^1(\gamma_\Gamma^1(e_2{}^+)))) \xrightarrow{*}_{L_1} (H_{1*}, v_1) \not\twoheadrightarrow$$

Then, by Lemma 4.13, there exist $\gamma_{L1}, \gamma_{L2}, H_{1l}, H_{1r}, H_{2l}, H_{2r}$ such that $\gamma_L = \gamma_{L1} \uplus \gamma_{L2}$, $H_1 = H_{1l} \uplus H_{1r}$, $H_2 = H_{2l} \uplus H_{2r}$,

$$(W, H_{1l}, H_{2l}, \gamma_{L1}) \in \mathcal{G}\llbracket\Gamma_1\rrbracket_\rho$$
$$(W, H_{1r}, H_{2r}, \gamma_{L2}) \in \mathcal{G}\llbracket\Gamma_2\rrbracket_\rho$$

and for all $j \in \{1, 2\}$,

$$\gamma_L^j(\gamma_\Gamma^j(e_1{}^+)) = \gamma_{L1}^{j}(\gamma_\Gamma^j(e_1{}^+))$$
$$\gamma_L^j(\gamma_\Gamma^j(e_2{}^+)) = \gamma_{L2}^{j}(\gamma_\Gamma^j(e_2{}^+))$$

Then, by instantiating the first induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{L1}, W, H_{1l}, H_{2l}$, we find

$$(W, (H_{1l}, \gamma_{L1}^{1}(\gamma_\Gamma^1(e_1{}^+))), (H_{2l}, \gamma_{L1}^{2}(\gamma_\Gamma^2(e_1{}^+)))) \in \mathcal{E}\llbracket\tau_1\rrbracket_\rho$$

Thus, by Lemma 4.3, we have

$$(H_{1g+} \uplus H_{1l} \uplus H_{1r} \uplus H_{1+}, \gamma_{L1}^{1}(\gamma_\Gamma^1(e_1{}^+))) \xrightarrow{*}_{L_1\cup FL(\gamma_{L2}^{1}(\gamma_\Gamma^1(e_2{}^+)))} (H'_{1g} \uplus H_{1r} \uplus H_{1+} \uplus H^*_{1l}, v_{1l}) \not\twoheadrightarrow$$

and, for any H_{2+},

$$(\mathrm{H}_{2g+} \uplus \mathrm{H}_{2l} \uplus \mathrm{H}_{2r} \uplus \mathrm{H}_{2+}, \gamma_{\mathrm{L}_1}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e}_1{}^{+}))) \xrightarrow{*}_{L_2 \cup FL(\gamma_{\mathrm{L}_2}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e}_2{}^{+})))} (\mathrm{H}'_{2g} \uplus \mathrm{H}_{2r} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}^*_{2l}, \mathrm{v}_{2\mathrm{l}}) \not\rightarrow$$

where $\mathrm{H}'_{1g}, \mathrm{H}'_{2g} : W'$ for some

$$W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1r} \uplus \mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2r} \uplus \mathrm{H}_{2+})),\mathrm{rchgclocs}(W, FL(\mathrm{cod}(\mathrm{H}_{1r})) \cup FL(\mathrm{cod}(\mathrm{H}_{1+})) \cup FL(\gamma_{\mathrm{L}_2}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e}_2{}^{+}))) \cup L_1, FL(\mathrm{cod}(\mathrm{H}_{2r})) \cup FL(\mathrm{cod}(\mathrm{H}_{2+})) \cup FL(\gamma_{\mathrm{L}_2}^{2}(\gamma_{\Gamma}^{2}(} W'$$

and

$$(W', (\mathrm{H}^*_{1l}, \mathrm{v}_{1\mathrm{l}}), (\mathrm{H}^*_{2l}, \mathrm{v}_{2\mathrm{l}})) \in \mathcal{V}[\![\tau_1]\!]_\rho$$

Thus, since $\mathrm{v}_{1\mathrm{l}}, \mathrm{v}_{2\mathrm{l}}$ are values as they are in the value relation, the original configuration will continue reducing on the second component of the pair. Then, since $\mathcal{G}[\![\Gamma]\!]_\rho, \mathcal{G}[\![\Gamma_1 \uplus \Gamma_2]\!]_\rho$ are closed under world extension by Lemma 4.7, we can instantiate the second induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{\mathrm{L}_2}, W', \mathrm{H}_{1r}, \mathrm{H}_{2r}$ to find

$$(W', (\mathrm{H}_{1r}, \gamma_{\mathrm{L}_2}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e}_2{}^{+}))), (\mathrm{H}_{2r}, \gamma_{\mathrm{L}_2}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e}_2{}^{+})))) \in \mathcal{E}[\![\tau_2]\!]_\rho$$

Thus, by Lemma 4.3, we have

$$(\mathrm{H}'_{1g} \uplus \mathrm{H}_{1r} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}^*_{1l}, \gamma_{\mathrm{L}_2}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e}_2{}^{+}))) \xrightarrow{*}_{L_1 \cup FL(\mathrm{v}_{1\mathrm{l}})} (\mathrm{H}''_{1g} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}^*_{1l} \uplus \mathrm{H}^*_{1r}, \mathrm{v}_{1\mathrm{r}}) \not\rightarrow$$

and

$$(\mathrm{H}'_{2g} \uplus \mathrm{H}_{1r} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}^*_{2l}, \gamma_{\mathrm{L}_2}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e}_2{}^{+}))) \xrightarrow{*}_{L_2 \cup FL(\mathrm{v}_{2\mathrm{l}})} (\mathrm{H}''_{2g} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}^*_{2l} \uplus \mathrm{H}^*_{2r}, \mathrm{v}_{2\mathrm{r}}) \not\rightarrow$$

where $\mathrm{H}''_{1g}, \mathrm{H}''_{2g} : W''$ for some

$$W' \sqsubseteq_{(\mathrm{dom}(\mathrm{H}^*_{1l} \uplus \mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}^*_{2l} \uplus \mathrm{H}_{2+})),\mathrm{rchgclocs}(W', FL(\mathrm{cod}(\mathrm{H}^*_{1l})) \cup FL(\mathrm{cod}(\mathrm{H}_{1+})) \cup FL(\mathrm{v}_{1\mathrm{l}}) \cup L_1, FL(\mathrm{cod}(\mathrm{H}^*_{2l})) \cup FL(\mathrm{cod}(\mathrm{H}_{2+})) \cup FL(\mathrm{v}_{2\mathrm{l}}) \cup L_2)} W''$$

and

$$(W'', (\mathrm{H}^*_{1r}, \mathrm{v}_{1\mathrm{r}}), (\mathrm{H}^*_{2r}, \mathrm{v}_{2\mathrm{r}})) \in \mathcal{V}[\![\tau_2]\!]_\rho$$

Thus, the original configurations step as follows:

$$\begin{aligned}
&(\mathrm{H}_{1g} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, (\gamma_{\mathrm{L}_1}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e}_1{}^{+})),\ \gamma_{\mathrm{L}_2}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e}_2{}^{+})))) \xrightarrow{*}_{L_1} \\
&(\mathrm{H}'_{1g} \uplus \mathrm{H}_{1r} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}^*_{1l}, (\mathrm{v}_{1\mathrm{l}},\ \gamma_{\mathrm{L}_2}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e}_2{}^{+})))) \xrightarrow{*}_{L_1} \\
&(\mathrm{H}''_{1g} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}^*_{1l} \uplus \mathrm{H}^*_{1r}, (\mathrm{v}_{1\mathrm{l}},\ \mathrm{v}_{2\mathrm{l}})) \not\rightarrow
\end{aligned}$$

and similarly on the other side, the configuration steps to

$$(\mathrm{H}''_{2g} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}^*_{2l} \uplus \mathrm{H}^*_{2r}, (\mathrm{v}_{1\mathrm{r}},\ \mathrm{v}_{2\mathrm{r}}))$$

Then, choose $\mathrm{H}'_1 = \mathrm{H}^*_{1l} \uplus \mathrm{H}^*_{1r}$, $\mathrm{H}'_2 = \mathrm{H}^*_{2l} \uplus \mathrm{H}^*_{2r}$, $W' = W''$, $\mathrm{H}'_{1g} = \mathrm{H}''_{1g}$, and $\mathrm{H}'_{2g} = \mathrm{H}''_{2g}$. First, notice that

$$W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W, FL(\mathrm{cod}(\mathrm{H}_{1+})) \cup L_1, FL(\mathrm{cod}(\mathrm{H}_{2+})) \cup L_2)} W''$$

by Lemma 4.6. One can see

$$(W'', (\mathrm{H}^*_{1l} \uplus \mathrm{H}^*_{1r}, (\mathrm{v}_{1\mathrm{l}}, \mathrm{v}_{1\mathrm{r}})), (\mathrm{H}^*_{2l} \uplus \mathrm{H}^*_{2r}, (\mathrm{v}_{2\mathrm{l}}, \mathrm{v}_{2\mathrm{r}}))) \in \mathcal{V}[\![\tau_1 \otimes \tau_2]\!]_\rho$$

because we have $(W'', (\mathrm{H}^*_{1l}, \mathrm{v}_{1\mathrm{l}}), (\mathrm{H}^*_{2l}, \mathrm{v}_{2\mathrm{l}})) \in \mathcal{V}[\![\tau_1]\!]_\rho$ (by Lemma 4.7) and $(W'', (\mathrm{H}^*_{1r}, \mathrm{v}_{1\mathrm{r}}), (\mathrm{H}^*_{2r}, \mathrm{v}_{2\mathrm{r}})) \in \mathcal{V}[\![\tau_2]\!]_\rho$. This suffices to finish the proof. □

Lemma 4.37 (Compat let $(\mathrm{x}_1,\ \mathrm{x}_2)$). *If* $\Delta; \Gamma; \Delta; \Gamma_1 \vdash \mathrm{e}_1 \preceq \mathrm{e}_1 : \tau_1 \otimes \tau_2$ *and* $\Delta; \Gamma; \Delta; \Gamma_2, \mathrm{x}_1 : \tau_1, \mathrm{x}_2 : \tau_2 \vdash \mathrm{e}_2 \preceq \mathrm{e}_2 : \tau$ *, then*

$$\Delta; \Gamma; \Delta; \Gamma_1 \uplus \Gamma_2 \vdash \mathrm{let}\ (\mathrm{x}_1,\ \mathrm{x}_2) = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 \preceq \mathrm{let}\ (\mathrm{x}_1,\ \mathrm{x}_2) = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 : \tau$$

Proof. Expanding the definition of $\preceq$, $\cdot^{+}$, $\mathcal{E}[\![\cdot]\!]_{.}$ and pushing substitutions in the goal, we are to show that

$$\begin{array}{l}\exists \mathrm{H}_1', \mathrm{H}_{1g}'.\forall \mathrm{H}_{2+} : \mathit{MHeap}.\exists \mathrm{H}_2', W', \mathrm{H}_{2g}', \mathrm{v}_2.\\ \mathrm{H}_{1*} = \mathrm{H}_{1g}' \uplus \mathrm{H}_1' \uplus \mathrm{H}_{1+} \ \wedge \mathrm{H}_{1g}', \mathrm{H}_{2g}' : W' \wedge\\ W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,\mathit{FL}(\mathrm{cod}(\mathrm{H}_{1+}))\cup L_1,\mathit{FL}(\mathrm{cod}(\mathrm{H}_{2+}))\cup L_2)} W' \wedge\\ (W', (\mathrm{H}_1', \mathrm{v}_1), (\mathrm{H}_2', \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho \wedge\\ (\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathsf{let}\ \mathrm{p} = \gamma_{\mathrm{L}}^2(\gamma_\Gamma^2(\mathrm{e}_1{}^{+}))\ \mathsf{in}\ \mathsf{let}\ \mathrm{x}_1 = \mathsf{fst}\ \mathrm{p}\ \mathsf{in}\ \mathsf{let}\ \mathrm{x}_2 = \mathsf{snd}\ \mathrm{p}\ \mathsf{in}\ \gamma_{\mathrm{L}}^2(\gamma_\Gamma^2(\mathrm{e}_2{}^{+}))) \xrightarrow{*}_{L_2}\\ (\mathrm{H}_{2g}' \uplus \mathrm{H}_2' \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \nrightarrow\end{array}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_\Gamma, W, L_1, L_2, \mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W, \mathrm{v}_1, \mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_{1+} : \mathit{MHeap}, \mathrm{H}_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!], \rho.\mathrm{F} \in \mathcal{D}[\![\Delta]\!], (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho, (W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}[\![\Gamma_1 \uplus \Gamma_2]\!]_\rho$$

and

$$(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \mathsf{let}\ \mathrm{p} = \gamma_{\mathrm{L}}^1(\gamma_\Gamma^1(\mathrm{e}_1{}^{+}))\ \mathsf{in}\ \mathsf{let}\ \mathrm{x}_1 = \mathsf{fst}\ \mathrm{p}\ \mathsf{in}\ \mathsf{let}\ \mathrm{x}_2 = \mathsf{snd}\ \mathrm{p}\ \mathsf{in}\ \gamma_{\mathrm{L}}^1(\gamma_\Gamma^1(\mathrm{e}_2{}^{+}))) \xrightarrow{*}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \nrightarrow$$

Then, by Lemma 4.13, there exist $\gamma_{\mathrm{L}1}, \gamma_{\mathrm{L}2}, \mathrm{H}_{1l}, \mathrm{H}_{1r}, \mathrm{H}_{2l}, \mathrm{H}_{2r}$ such that $\gamma_{\mathrm{L}} = \gamma_{\mathrm{L}1} \uplus \gamma_{\mathrm{L}2}$, $\mathrm{H}_1 = \mathrm{H}_{1l} \uplus \mathrm{H}_{1r}$, $\mathrm{H}_2 = \mathrm{H}_{2l} \uplus \mathrm{H}_{2r}$,

$$(W, \mathrm{H}_{1l}, \mathrm{H}_{2l}, \gamma_{\mathrm{L}1}) \in \mathcal{G}[\![\Gamma_1]\!]_\rho$$
$$(W, \mathrm{H}_{1r}, \mathrm{H}_{2r}, \gamma_{\mathrm{L}2}) \in \mathcal{G}[\![\Gamma_2]\!]_\rho$$

and for all $j \in \{1, 2\}$,

$$\gamma_{\mathrm{L}}^j(\gamma_\Gamma^j(\mathrm{e}_1{}^{+})) = \gamma_{\mathrm{L}1}^{\,j}(\gamma_\Gamma^j(\mathrm{e}_1{}^{+}))$$
$$\gamma_{\mathrm{L}}^j(\gamma_\Gamma^j(\mathrm{e}_2{}^{+})) = \gamma_{\mathrm{L}2}^{\,j}(\gamma_\Gamma^j(\mathrm{e}_2{}^{+}))$$

Then, by instantiating the first induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{\mathrm{L}1}, W, \mathrm{H}_{1l}, \mathrm{H}_{2l}$, we find

$$(W, (\mathrm{H}_{1l}, \gamma_{\mathrm{L}1}^{\,1}(\gamma_\Gamma^1(\mathrm{e}_1{}^{+}))), (\mathrm{H}_{2l}, \gamma_{\mathrm{L}1}^{\,2}(\gamma_\Gamma^2(\mathrm{e}_1{}^{+})))) \in \mathcal{E}[\![\tau_1 \otimes \tau_2]\!]_\rho$$

Thus, by Lemma 4.3, we have

$$(\mathrm{H}_{1g} \uplus \mathrm{H}_{1l} \uplus \mathrm{H}_{1r} \uplus \mathrm{H}_{1+}, \gamma_{\mathrm{L}1}^{\,1}(\gamma_\Gamma^1(\mathrm{e}_1{}^{+}))) \xrightarrow{*}_{L_1 \cup \mathit{FL}(\gamma_{\mathrm{L}2}^{\,1}(\gamma_\Gamma^1(\mathrm{e}_2{}^{+})))} (\mathrm{H}_{1g}' \uplus \mathrm{H}_{1r} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}_{1l}^*, \mathrm{v}_1) \nrightarrow$$

and, for any H_{2+},

$$(\mathrm{H}_{2g} \uplus \mathrm{H}_{2l} \uplus \mathrm{H}_{2r} \uplus \mathrm{H}_{2+}, \gamma_{\mathrm{L}1}^{\,2}(\gamma_\Gamma^2(\mathrm{e}_1{}^{+}))) \xrightarrow{*}_{L_2 \cup \mathit{FL}(\gamma_{\mathrm{L}2}^{\,2}(\gamma_\Gamma^2(\mathrm{e}_2{}^{+})))} (\mathrm{H}_{2g}' \uplus \mathrm{H}_{2r} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}_{2l}^*, \mathrm{v}_2) \nrightarrow$$

where $\mathrm{H}_{1g}', \mathrm{H}_{2g}' : W'$ for some

$$W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+} \uplus \mathrm{H}_{1r}),\mathrm{dom}(\mathrm{H}_{2+} \uplus \mathrm{H}_{2r})),\mathrm{rchgclocs}(W,\mathit{FL}(\mathrm{cod}(\mathrm{H}_{1r}))\cup\mathit{FL}(\mathrm{cod}(\mathrm{H}_{1+}))\cup\mathit{FL}(\gamma_{\mathrm{L}2}^{\,1}(\gamma_\Gamma^1(\mathrm{e}_2{}^{+})))\cup L_1,\mathit{FL}(\mathrm{cod}(\mathrm{H}_{2r}))\cup\mathit{FL}(\mathrm{cod}(\mathrm{H}_{2+}))\cup\mathit{FL}(\gamma_{\mathrm{L}2}^{\,2}(\gamma_\Gamma^2(} W'$$

and

$$(W', (\mathrm{H}_{1l}^*, \mathrm{v}_1), (\mathrm{H}_{2l}^*, \mathrm{v}_2)) \in \mathcal{V}[\![\tau_1 \otimes \tau_2]\!]_\rho$$

By expanding the value relation, we find $\mathrm{H}_{1l}^* = \mathrm{H}_{1ll} \uplus \mathrm{H}_{1lr}$, $\mathrm{H}_{2l}^* = \mathrm{H}_{2ll} \uplus \mathrm{H}_{2lr}$, $\mathrm{v}_1 = (\mathrm{v}_{1\mathrm{l}}, \mathrm{v}_{1\mathrm{r}})$, and $\mathrm{v}_2 = (\mathrm{v}_{2\mathrm{l}}, \mathrm{v}_{2\mathrm{r}})$ where $(W', (\mathrm{H}_{1ll}, \mathrm{v}_{1\mathrm{l}}), (\mathrm{H}_{2ll}, \mathrm{v}_{2\mathrm{l}})) \in \mathcal{V}[\![\tau_1]\!]_\rho$ and $(W', (\mathrm{H}_{1lr}, \mathrm{v}_{1\mathrm{r}}), (\mathrm{H}_{2lr}, \mathrm{v}_{2\mathrm{r}})) \in \mathcal{V}[\![\tau_2]\!]_\rho$.

Thus, the original configuration steps as follows:

$$\begin{array}{l}(\mathrm{H}_{1g} \uplus \mathrm{H}_{1l} \uplus \mathrm{H}_{1r} \uplus \mathrm{H}_{1+}, \mathsf{let}\ \mathrm{p} = \gamma_{\mathrm{L}1}^{\,1}(\gamma_\Gamma^1(\mathrm{e}_1{}^{+}))\ \mathsf{in}\ \mathsf{let}\ \mathrm{x}_1 = \mathsf{fst}\ \mathrm{p}\ \mathsf{in}\ \mathsf{let}\ \mathrm{x}_2 = \mathsf{snd}\ \mathrm{p}\ \mathsf{in}\ \gamma_{\mathrm{L}2}^{\,1}(\gamma_\Gamma^1(\mathrm{e}_2{}^{+}))) \xrightarrow{*}_{L_1}\\ (\mathrm{H}_{1g}' \uplus \mathrm{H}_{1r} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}_{1ll} \uplus \mathrm{H}_{1lr}, \mathsf{let}\ \mathrm{p} = \ (\mathrm{v}_{1\mathrm{l}}, \mathrm{v}_{1\mathrm{r}})\ \mathsf{in}\ \mathsf{let}\ \mathrm{x}_1 = \mathsf{fst}\ \mathrm{p}\ \mathsf{in}\ \mathsf{let}\ \mathrm{x}_2 = \mathsf{snd}\ \mathrm{p}\ \mathsf{in}\ \gamma_{\mathrm{L}2}^{\,1}(\gamma_\Gamma^1(\mathrm{e}_2{}^{+}))) \xrightarrow{*}_{L_1}\\ (\mathrm{H}_{1g}' \uplus \mathrm{H}_{1r} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}_{1ll} \uplus \mathrm{H}_{1lr}, [\mathrm{x}_1 \mapsto \mathrm{v}_{1\mathrm{l}}, \mathrm{x}_2 \mapsto \mathrm{v}_{1\mathrm{r}}]\gamma_{\mathrm{L}2}^{\,1}(\gamma_\Gamma^1(\mathrm{e}_2{}^{+})))\end{array}$$

and the original configuration on the other side steps to:

$$(\mathrm{H}_{2g}' \uplus \mathrm{H}_{2r} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}_{2ll} \uplus \mathrm{H}_{2lr}, [\mathrm{x}_1 \mapsto \mathrm{v}_{2\mathrm{l}}, \mathrm{x}_2 \mapsto \mathrm{v}_{2\mathrm{r}}]\gamma_{\mathrm{L}2}^{\,2}(\gamma_\Gamma^2(\mathrm{e}_2{}^{+})))$$

Next, notice that

$(W', \mathrm{H}_{1ll} \uplus \mathrm{H}_{1lr} \uplus \mathrm{H}_{1r}, \mathrm{H}_{2ll} \uplus \mathrm{H}_{2lr} \uplus \mathrm{H}_{2r}, \gamma_{\mathrm{L}2}[\mathrm{x}_1 \mapsto (\mathrm{v}_{1l}, \mathrm{v}_{2l}), \mathrm{x}_2 \mapsto (\mathrm{v}_{1r}, \mathrm{v}_{2r})]) \in \mathcal{G}\llbracket \Gamma_2, \mathrm{x}_1 : \tau_1, \mathrm{x}_2 : \tau_2 \rrbracket_\rho$
because $(W', (\mathrm{H}_{1ll}, \mathrm{v}_{1l}), (\mathrm{H}_{2ll}, \mathrm{v}_{2l})) \in \mathcal{V}\llbracket \tau_1 \rrbracket_\rho$, $(W', (\mathrm{H}_{1lr}, \mathrm{v}_{1r}), (\mathrm{H}_{2lr}, \mathrm{v}_{2r})) \in \mathcal{V}\llbracket \tau_2 \rrbracket_\rho$, and $(W', \mathrm{H}_{1r}, \mathrm{H}_{2r}, \gamma_{\mathrm{L}2}) \in \mathcal{G}\llbracket \Gamma_2 \rrbracket_\rho$ (by Lemma 4.7).

Let $\gamma_{\mathrm{L}2}' = \gamma_{\mathrm{L}2}[\mathrm{x}_1 \mapsto (\mathrm{v}_{1l}, \mathrm{v}_{2l}), \mathrm{x}_2 \mapsto (\mathrm{v}_{1r}, \mathrm{v}_{2r})]$.

Thus, we can instantiate the second induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{\mathrm{L}2}', \mathrm{H}_{1ll} \uplus \mathrm{H}_{1lr} \uplus \mathrm{H}_{1r}, \mathrm{H}_{2ll} \uplus \mathrm{H}_{2lr} \uplus \mathrm{H}_{2r}$ to find that

$$\begin{gathered}(W', (\mathrm{H}_{1ll} \uplus \mathrm{H}_{1lr} \uplus \mathrm{H}_{1r}, [\mathrm{x}_1 \mapsto \mathrm{v}_{1l}, \mathrm{x}_2 \mapsto \mathrm{v}_{1r}]\gamma_{\mathrm{L}2}^{1}(\gamma_\Gamma^1(\mathrm{e}_2{}^+))), \\ (\mathrm{H}_{2ll} \uplus \mathrm{H}_{2lr} \uplus \mathrm{H}_{2r}, [\mathrm{x}_1 \mapsto \mathrm{v}_{2l}, \mathrm{x}_2 \mapsto \mathrm{v}_{2r}]\gamma_{\mathrm{L}2}^{2}(\gamma_\Gamma^2(\mathrm{e}_2{}^+)))) \in \mathcal{E}\llbracket \tau \rrbracket_\rho\end{gathered} \tag{50}$$

Next, by the assumption that the configuration on the left-hand side terminates, we have

$$(\mathrm{H}_{1g}' \uplus \mathrm{H}_{1+} \uplus \mathrm{H}_{1r} \uplus \mathrm{H}_{1ll} \uplus \mathrm{H}_{1lr}, [\mathrm{x}_1 \mapsto \mathrm{v}_{1l}, \mathrm{x}_2 \mapsto \mathrm{v}_{1r}]\gamma_{\mathrm{L}2}^{1}(\gamma_\Gamma^1(\mathrm{e}_2{}^+))) \overset{*}{\rightarrow}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1)$$

Then, by applying (50), we find

$$(\mathrm{H}_{1*}, \mathrm{v}_1) = (\mathrm{H}_{1g}'' \uplus \mathrm{H}_{1+} \uplus \mathrm{H}_{1f}^*, \mathrm{v}_{1f})$$

and

$$(\mathrm{H}_{2g}' \uplus \mathrm{H}_{2+} \uplus \mathrm{H}_{2r} \uplus \mathrm{H}_{2ll} \uplus \mathrm{H}_{2lr}, [\mathrm{x}_1 \mapsto \mathrm{v}_{2l}, \mathrm{x}_2 \mapsto \mathrm{v}_{2r}]\gamma_{\mathrm{L}2}^{2}(\gamma_\Gamma^2(\mathrm{e}_2{}^+))) \overset{*}{\rightarrow}_{L_2} (\mathrm{H}_{2g}'' \uplus \mathrm{H}_{2+} \uplus \mathrm{H}_{2f}^*, \mathrm{v}_{2f})$$

where $\mathrm{H}_{1g}'', \mathrm{H}_{2g}'' : W''$ for some $W' \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W, FL(\mathrm{cod}(\mathrm{H}_{1+}))\cup L_1, FL(\mathrm{cod}(\mathrm{H}_{2+}))\cup L_2)} W''$ and

$$(W'', (\mathrm{H}_{1f}^*, \mathrm{v}_{1f}), (\mathrm{H}_{2f}^*, \mathrm{v}_{2f})) \in \mathcal{V}\llbracket \tau \rrbracket_\rho$$

Then, choose $\mathrm{H}_1' = \mathrm{H}_{1f}^*$, $\mathrm{H}_2' = \mathrm{H}_{2f}^*$, $W' = W''$, $\mathrm{H}_{1g}' = \mathrm{H}_{1g}''$, and $\mathrm{H}_{2g}' = \mathrm{H}_{2g}''$. Notice that

$$W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W, FL(\mathrm{cod}(\mathrm{H}_{1+}))\cup L_1, FL(\mathrm{cod}(\mathrm{H}_{2+}))\cup L_2)} W''$$

by Lemma 4.6. This suffices to finish the proof. □

Lemma 4.38 (Compat !v). *If* $\Delta; \Gamma; \Delta; !\Gamma \vdash \mathrm{v} \preceq \mathrm{v} : \tau$, *then*

$$\Delta; \Gamma; \Delta; !\Gamma \vdash !\mathrm{v} \preceq !\mathrm{v} : !\tau$$

Proof. Expanding the definition of $\preceq$, $\cdot^+$, $\mathcal{E}\llbracket \cdot \rrbracket_\cdot$ and pushing substitutions in the goal, we are to show that

$$\begin{aligned}&\exists \mathrm{H}_1', \mathrm{H}_{1g}'.\forall \mathrm{H}_{2+} : \mathit{MHeap}.\exists \mathrm{H}_2', W', \mathrm{H}_{2g}', \mathrm{v}_2. \\ &\mathrm{H}_{1*} = \mathrm{H}_{1g}' \uplus \mathrm{H}_1' \uplus \mathrm{H}_{1+} \ \wedge \mathrm{H}_{1g}', \mathrm{H}_{2g}' : W' \wedge \\ &W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W, L_1\cup FL(\mathrm{cod}(\mathrm{H}_{1+})), L_2\cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W' \wedge \\ &(W', (\mathrm{H}_1', \mathrm{v}_1), (\mathrm{H}_2', \mathrm{v}_2)) \in \mathcal{V}\llbracket !\tau \rrbracket_\rho \wedge \\ &(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \gamma_{\mathrm{L}}^2(\gamma_\Gamma^2(\mathrm{v}^+))) \overset{*}{\rightarrow}_{L_2} (\mathrm{H}_{2g}' \uplus \mathrm{H}_2' \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \nrightarrow\end{aligned}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_\Gamma, W, L_1, L_2, \mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W, \mathrm{v}_1, \mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_{1+} : \mathit{MHeap}, \mathrm{H}_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}\llbracket \Delta \rrbracket, \rho.\mathrm{F} \in \mathcal{D}\llbracket \Delta \rrbracket, (W, \gamma_\Gamma) \in \mathcal{G}\llbracket \Gamma \rrbracket_\rho, (W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}\llbracket !\Gamma \rrbracket_\rho$$

and

$$(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \gamma_{\mathrm{L}}^1(\gamma_\Gamma^1(\mathrm{v}^+))) \overset{*}{\rightarrow}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \nrightarrow$$

By Lemma 4.14, $(W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}\llbracket !\Gamma \rrbracket_\rho$ implies $\mathrm{H}_1 = \mathrm{H}_2 = \emptyset$. Then, by instantiating the first induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{\mathrm{L}}, W, \emptyset, \emptyset$, we find

$$(W, (\emptyset, \gamma_{\mathrm{L}}^1(\gamma_\Gamma^1(\mathrm{v}^+))), (\emptyset, \gamma_{\mathrm{L}}^2(\gamma_\Gamma^2(\mathrm{v}^+)))) \in \mathcal{E}\llbracket \tau \rrbracket_\rho$$

Therefore,

$$(\mathrm{H}_{1*}, \mathrm{v}_1) = (\mathrm{H}_{1g}' \uplus \mathrm{H}_{1f} \uplus \mathrm{H}_{1+}, \mathrm{v}_1)$$

and

$$(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{v}^{+}))) \xrightarrow{*}_{L_2} (\mathsf{H}'_{2g} \uplus \mathsf{H}_{2f} \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \not\twoheadrightarrow_{L_2}$$

where $\mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W'$ for some $W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W'$ and

$$(W', (\mathsf{H}_{1f}, \mathsf{v}_1), (\mathsf{H}_{2f}, \mathsf{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_{\rho}$$

However, by Lemma 4.15, $\gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{v}^{+}))$ and $\gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{v}^{+}))$ are target values, so the original configurations $(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1+}, \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{v}^{+})))$ and $(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2+}, \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{v}^{+})))$ must be irreducible. Ergo, the heaps that these configurations step to must be the initial configurations, so $\mathsf{H}_{1g+} = \mathsf{H}'_{1g} \uplus \mathsf{H}_{1f}$ and $\mathsf{H}_{2g+} = \mathsf{H}'_{2g} \uplus \mathsf{H}_{2f}$.

Now, notice that, by the definition of $Atom_n$, $\mathsf{H}_{1f} : MHeap$ and $\mathsf{H}_{2f} : MHeap$. However, since $\mathsf{H}_{1g+}, \mathsf{H}_{2g+} : W$, we also have $\mathsf{H}_{1g+} : GCHeap$ and $\mathsf{H}_{2g+} : GCHeap$. Thus, H_{1f} and H_{2f} has only manually mapped locations while H_{1g+} and H_{2g+} have only garbage collectable locations. However, the observation above implies $\mathsf{H}_{1f} \subseteq \mathsf{H}_{1g+}$ and $\mathsf{H}_{2f} \subseteq \mathsf{H}_{2g+}$, so this must imply $\mathsf{H}_{1f} = \mathsf{H}_{2f} = \emptyset$.

Ergo, $(W', (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}\llbracket \tau \rrbracket_{\rho}$. From here, it follows that $(W', (\emptyset, \mathsf{v}_1), (\emptyset, \mathsf{v}_2)) \in \mathcal{V}\llbracket !\tau \rrbracket_{\rho}$, which suffices to finish the proof. □

Lemma 4.39 (Compat let !x). *If* $\Delta; \Gamma; \Delta; \Gamma_1 \vdash \mathrm{e}_1 \preceq \mathrm{e}_1 : !\tau_1$ *and* $\Delta; \Gamma; \Delta; \Gamma_2, \mathrm{x} : \tau_1 \vdash \mathrm{e}_2 \preceq \mathrm{e}_2 : \tau_2$ *, then*

$$\Delta; \Gamma; \Delta; \Gamma_1 \uplus \Gamma_2 \vdash \mathrm{let}\ !\mathrm{x} = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 \preceq \mathrm{let}\ !\mathrm{x} = \mathrm{e}_1\ \mathrm{in}\ \mathrm{e}_2 : \tau_2$$

Proof. Expanding the definition of $\preceq$, $\cdot^{+}$, $\mathcal{E}\llbracket \cdot \rrbracket_{\cdot}$ and pushing substitutions in the goal, we are to show that

$$\begin{array}{l}
\exists \mathsf{H}'_1, \mathsf{H}'_{1g}. \forall \mathsf{H}_{2+} : MHeap. \exists \mathsf{H}'_2, W', \mathsf{H}'_{2g}, \mathsf{v}_2. \\
\mathsf{H}_{1*} = \mathsf{H}'_{1g} \uplus \mathsf{H}'_1 \uplus \mathsf{H}_{1+} \ \wedge \mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W' \wedge \\
W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W' \wedge \\
(W', (\mathsf{H}'_1, \mathsf{v}_1), (\mathsf{H}'_2, \mathsf{v}_2)) \in \mathcal{V}\llbracket \tau_2 \rrbracket_{\rho} \wedge \\
(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \mathsf{let}\ \mathsf{x} = \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e}_1{}^{+}))\ \mathsf{in}\ \gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e}_2{}^{+}))) \xrightarrow{*}_{L_2} \\
(\mathsf{H}'_{2g} \uplus \mathsf{H}'_2 \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \not\twoheadrightarrow
\end{array}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_{\Gamma}, W, L_1, L_2, \mathsf{H}_{1g+}, \mathsf{H}_{2g+} : W, \mathsf{v}_1, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_{1+} : MHeap, \mathsf{H}_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}\llbracket \Delta \rrbracket, \rho.\mathsf{F} \in \mathcal{D}\llbracket \Delta \rrbracket, (W, \gamma_{\Gamma}) \in \mathcal{G}\llbracket \Gamma \rrbracket_{\rho}, (W, \mathsf{H}_1, \mathsf{H}_2, \gamma_{\mathrm{L}}.\Gamma) \in \mathcal{G}\llbracket \Gamma_1 \uplus \Gamma_2 \rrbracket_{\rho}, \gamma_{\mathrm{L}}.\Delta = \gamma_{\mathrm{locs}}(\rho.\mathrm{L3})$$

and

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x} = \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e}_1{}^{+}))\ \mathsf{in}\ \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e}_2{}^{+}))) \xrightarrow{*}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \not\twoheadrightarrow$$

Then, by Lemma 4.13, there exist $\gamma_{\mathrm{L}1}, \gamma_{\mathrm{L}2}, \mathsf{H}_{1l}, \mathsf{H}_{1r}, \mathsf{H}_{2l}, \mathsf{H}_{2r}$ such that $\gamma_{\mathrm{L}} = \gamma_{\mathrm{L}1} \uplus \gamma_{\mathrm{L}2}$, $\mathsf{H}_1 = \mathsf{H}_{1l} \uplus \mathsf{H}_{1r}$, $\mathsf{H}_2 = \mathsf{H}_{2l} \uplus \mathsf{H}_{2r}$,

$$(W, \mathsf{H}_{1l}, \mathsf{H}_{2l}, \gamma_{\mathrm{L}1}) \in \mathcal{G}\llbracket \Gamma_1 \rrbracket_{\rho}$$
$$(W, \mathsf{H}_{1r}, \mathsf{H}_{2r}, \gamma_{\mathrm{L}2}) \in \mathcal{G}\llbracket \Gamma_2 \rrbracket_{\rho}$$

and for all $j \in \{1, 2\}$,

$$\gamma_{\mathrm{L}}^{j}(\gamma_{\Gamma}^{j}(\mathrm{e}_1{}^{+})) = \gamma_{\mathrm{L}1}^{\ j}(\gamma_{\Gamma}^{j}(\mathrm{e}_1{}^{+}))$$
$$\gamma_{\mathrm{L}}^{j}(\gamma_{\Gamma}^{j}(\mathrm{e}_2{}^{+})) = \gamma_{\mathrm{L}2}^{\ j}(\gamma_{\Gamma}^{j}(\mathrm{e}_2{}^{+}))$$

Then, by instantiating the first induction hypothesis with $\rho, \gamma_{\Gamma}, \gamma_{\mathrm{L}1}, W, \mathsf{H}_{1l}, \mathsf{H}_{2l}$, we find

$$(W, (\mathsf{H}_{1l}, \gamma_{\mathrm{L}1}^{\ 1}(\gamma_{\Gamma}^{1}(\mathrm{e}_1{}^{+}))), (\mathsf{H}_{2l}, \gamma_{\mathrm{L}1}^{\ 2}(\gamma_{\Gamma}^{2}(\mathrm{e}_1{}^{+})))) \in \mathcal{E}\llbracket !\tau_1 \rrbracket_{\rho}$$

Thus, by Lemma 4.3, we have

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1l} \uplus \mathsf{H}_{1r} \uplus \mathsf{H}_{1+}, \gamma_{\mathrm{L}1}^{\ 1}(\gamma_{\Gamma}^{1}(\mathrm{e}_1{}^{+}))) \xrightarrow{*}_{L_1 \cup FL(\gamma_{\mathrm{L}2}^{\ 1}(\gamma_{\Gamma}^{1}(\mathrm{e}_2{}^{+})))} (\mathsf{H}'_{1g} \uplus \mathsf{H}_{1r} \uplus \mathsf{H}_{1+} \uplus \mathsf{H}^{*}_{1l}, \mathsf{v}_{1l}) \not\twoheadrightarrow$$

and, for any H_{2+},

$$(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2l} \uplus \mathsf{H}_{2r} \uplus \mathsf{H}_{2+}, \gamma_{L_1}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_1{}^{+}))) \xrightarrow{*}_{L_2 \cup FL(\gamma_{L_2}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_2{}^{+})))} (\mathsf{H}'_{2g} \uplus \mathsf{H}_{2r} \uplus \mathsf{H}_{2+} \uplus \mathsf{H}^{*}_{2l}, \mathsf{v}_{2l}) \nrightarrow$$

where $\mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W'$ for some

W
$\sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1r} \uplus \mathsf{H}_{1+}), \mathrm{dom}(\mathsf{H}_{2r} \uplus \mathsf{H}_{2+})), \mathrm{rchgclocs}(W, FL(\mathrm{cod}(\mathsf{H}_{1r})) \cup FL(\mathrm{cod}(\mathsf{H}_{1+})) \cup FL(\gamma_{L_2}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_2{}^{+}))) \cup L_1, FL(\mathrm{cod}(\mathsf{H}_{2r})) \cup FL(\mathrm{cod}(\mathsf{H}_{2+})) \cup FL(\gamma_{L_2}^{2}(\gamma_{\Gamma}^{2}(}$
W'

and

$$(W', (\mathsf{H}^{*}_{1l}, \mathsf{v}_{1l}), (\mathsf{H}^{*}_{2l}, \mathsf{v}_{2l})) \in \mathcal{V}[\![!\tau_1]\!]_{\rho}$$

By expanding the value relation, we find $\mathsf{H}^{*}_{1l} = \mathsf{H}^{*}_{2l} = \emptyset$ and $(W', (\emptyset, \mathsf{v}^{*}_{1}), (\emptyset, \mathsf{v}^{*}_{2})) \in \mathcal{V}[\![\tau_1]\!]_{\rho}$.

Thus, the original configuration steps as follows:

$$\begin{aligned}
&(\mathsf{H}_{1g+} \uplus \mathsf{H}_{1l} \uplus \mathsf{H}_{1r} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x} = \gamma_{L_1}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_1{}^{+}))\ \mathsf{in}\ \gamma_{L_2}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_2{}^{+}))) \xrightarrow{*}_{L_1}\\
&(\mathsf{H}'_{1g} \uplus \mathsf{H}_{1r} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x} = \mathsf{v}^{*}_{1}\ \mathsf{in}\ \gamma_{L_2}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_2{}^{+}))) \rightarrow_{L_1}\\
&(\mathsf{H}'_{1g} \uplus \mathsf{H}_{1r} \uplus \mathsf{H}_{1+}, [\mathsf{x} \mapsto \mathsf{v}^{*}_{1}]\gamma_{L_2}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_2{}^{+})))
\end{aligned}$$

and

$$\begin{aligned}
&(\mathsf{H}_{2g+} \uplus \mathsf{H}_{2l} \uplus \mathsf{H}_{2r} \uplus \mathsf{H}_{2+}, \mathsf{let}\ \mathsf{x} = \gamma_{L_1}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_1{}^{+}))\ \mathsf{in}\ \gamma_{L_2}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_2{}^{+}))) \xrightarrow{*}_{L_2}\\
&(\mathsf{H}'_{2g} \uplus \mathsf{H}_{2r} \uplus \mathsf{H}_{2+}, \mathsf{let}\ \mathsf{x} = \mathsf{v}^{*}_{2}\ \mathsf{in}\ \gamma_{L_2}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_2{}^{+}))) \rightarrow_{L_2}\\
&(\mathsf{H}'_{2g} \uplus \mathsf{H}_{2r} \uplus \mathsf{H}_{2+}, [\mathsf{x} \mapsto \mathsf{v}^{*}_{2}]\gamma_{L_2}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_2{}^{+})))
\end{aligned}$$

Then, notice that

$$(W', \mathsf{H}_{1r}, \mathsf{H}_{2r}, \gamma_{L_2}[\mathsf{x} \mapsto (\mathsf{v}^{*}_{1}, \mathsf{v}^{*}_{2})]) \in \mathcal{G}[\![\Gamma, \mathsf{x} : \tau_1]\!]_{\rho}$$

because, by Lemma 4.7, $(W', \mathsf{H}_{1r}, \mathsf{H}_{2r}, \gamma_{L_2}) \in \mathcal{G}[\![\Gamma, \mathsf{x} : \tau_1]\!]_{\rho}$ and $(W', (\emptyset, \mathsf{v}^{*}_{1}), (\emptyset, \mathsf{v}^{*}_{2})) \in \mathcal{V}[\![\tau_1]\!]_{\rho}$.

Let $\gamma_{L_2}' = \gamma_{L_2}[\mathsf{x} \mapsto (\mathsf{v}^{*}_{1}, \mathsf{v}^{*}_{2})]$.

Ergo, we instantiate the second induction hypothesis with $\rho, \gamma_{\Gamma}, \gamma_{L_2}', \mathsf{H}_{1r}, \mathsf{H}_{2r}$ to find that:

$$(W', (\mathsf{H}_{1r}, [\mathsf{x} \mapsto \mathsf{v}^{*}_{1}]\gamma_{L_2}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_2{}^{+}))), (\mathsf{H}_{2r}, [\mathsf{x} \mapsto \mathsf{v}^{*}_{2}]\gamma_{L_2}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_2{}^{+})))) \in \mathcal{E}[\![\tau_2]\!]_{\rho} \tag{51}$$

Next, by the assumption that the configuration on the left-hand side terminates, we have

$$(\mathsf{H}'_{1g} \uplus \mathsf{H}_{1r} \uplus \mathsf{H}_{1+}, [\mathsf{x} \mapsto \mathsf{v}^{*}_{1}]\gamma_{L_2}^{1}(\gamma_{\Gamma}^{1}(\mathsf{e}_2{}^{+}))) \xrightarrow{*}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \nrightarrow_{L_1}$$

Then, by applying (51), we find

$$(\mathsf{H}_{1*}, \mathsf{v}_1) = (\mathsf{H}''_{1g} \uplus \mathsf{H}_{1+} \uplus \mathsf{H}^{*}_{1f}, \mathsf{v}_{1f})$$

and

$$(\mathsf{H}'_{2g} \uplus \mathsf{H}_{2r} \uplus \mathsf{H}_{2+}, [\mathsf{x} \mapsto \mathsf{v}^{*}_{2}]\gamma_{L_2}^{2}(\gamma_{\Gamma}^{2}(\mathsf{e}_2{}^{+}))) \xrightarrow{*}_{L_2} (\mathsf{H}''_{2g} \uplus \mathsf{H}_{2+} \uplus \mathsf{H}^{*}_{2f}, \mathsf{v}_{2f})$$

where $\mathsf{H}''_{1g}, \mathsf{H}''_{2g} : W''$ for some $W' \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}), \mathrm{dom}(\mathsf{H}_{2+})), \mathrm{rchgclocs}(W, L_1 \cup FL(\mathrm{cod}(\mathsf{H}_{1+})), L_2 \cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W''$ and and

$$(W'', (\mathsf{H}^{*}_{1f}, \mathsf{v}_{1f}), (\mathsf{H}^{*}_{2f}, \mathsf{v}_{2f})) \in \mathcal{V}[\![\tau_2]\!]_{\rho}$$

Then, choose $\mathsf{H}'_1 = \mathsf{H}^{*}_{1f}$, $\mathsf{H}'_2 = \mathsf{H}^{*}_{2f}$, $W' = W''$, $\mathsf{H}'_{1g} = \mathsf{H}''_{1g}$, and $\mathsf{H}'_{2g} = \mathsf{H}''_{2g}$. Notice that $W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}), \mathrm{dom}(\mathsf{H}_{2+})), \mathrm{rchgclocs}(W, L_1 \cup FL(\mathrm{cod}(\mathsf{H}_{1+})), L_2 \cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W''$ by Lemma 4.6. This suffices to finish the proof. □

Lemma 4.40 (Compat $\mathsf{dupl\ e}$). *If* $\Delta; \Gamma; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : !\tau$ *, then*

$$\Delta; \Gamma; \Delta; \Gamma \vdash \mathsf{dupl\ e} \preceq \mathsf{dupl\ e} : !\tau \otimes !\tau$$

Proof. Expanding the definition of $\preceq$, $\cdot^{+}$, $\mathcal{E}[\![\cdot]\!]_{\cdot}$ and pushing substitutions in the goal, we are to show that

$$\begin{aligned}&\exists \mathsf{H}_1', \mathsf{H}_{1g}'.\forall \mathsf{H}_{2+} : \mathit{MHeap}.\exists \mathsf{H}_2', W', \mathsf{H}_{2g}', \mathsf{v}_2.\\ &\mathsf{H}_{1*} = \mathsf{H}_{1g}' \uplus \mathsf{H}_1' \uplus \mathsf{H}_{1+} \ \wedge \mathsf{H}_{1g}', \mathsf{H}_{2g}' : W' \wedge\\ &W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W' \wedge\\ &(W', (\mathsf{H}_1', \mathsf{v}_1), (\mathsf{H}_2', \mathsf{v}_2)) \in \mathcal{V}[\![!\tau \otimes !\tau]\!]_\rho \wedge\\ &(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \mathsf{let}\ \mathsf{x} = \gamma_{\mathrm{L}}^2(\gamma_{\Gamma}^2(\mathrm{e}^{+}))\ \mathsf{in}\ (\mathsf{x},\mathsf{x})) \overset{*}{\longrightarrow}_{L_2}\\ &(\mathsf{H}_{2g}' \uplus \mathsf{H}_2' \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \not\twoheadrightarrow\end{aligned}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_{\Gamma}, W, L_1, L_2, \mathsf{H}_{1g+}, \mathsf{H}_{2g+} : W, \mathsf{v}_1, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_{1+} : \mathit{MHeap}, \mathsf{H}_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!], \rho.\mathsf{F} \in \mathcal{D}[\![\Delta]\!], (W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]_\rho, (W, \mathsf{H}_1, \mathsf{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}[\![\Gamma]\!]_\rho$$

and

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x} = \gamma_{\mathrm{L}}^1(\gamma_{\Gamma}^1(\mathrm{e_1}^{+}))\ \mathsf{in}\ (\mathsf{x},\mathsf{x})) \overset{*}{\longrightarrow}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \not\twoheadrightarrow$$

We can instantiate the first induction hypothesis with $\rho, \gamma_{\Gamma}, \gamma_{\mathrm{L}}, \mathsf{H}_1, \mathsf{H}_2$ to find

$$(W, (\mathsf{H}_1, \gamma_{\mathrm{L}}^1(\gamma_{\Gamma}^1(\mathrm{e}^{+}))), (\mathsf{H}_2, \gamma_{\mathrm{L}}^2(\gamma_{\Gamma}^2(\mathrm{e}^{+})))) \in \mathcal{E}[\![!\tau]\!]_\rho$$

Thus, we find

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \gamma_{\mathrm{L}}^1(\gamma_{\Gamma}^1(\mathrm{e}^{+}))) \overset{*}{\longrightarrow}_{L_1} (\mathsf{H}_{1g}' \uplus \mathsf{H}_1^* \uplus \mathsf{H}_{1+}, \mathsf{v}_1^*) \not\twoheadrightarrow_{L_1}$$

and

$$(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \gamma_{\mathrm{L}}^2(\gamma_{\Gamma}^2(\mathrm{e}^{+}))) \overset{*}{\longrightarrow}_{L_2} (\mathsf{H}_{2g}' \uplus \mathsf{H}_2^* \uplus \mathsf{H}_{2+}, \mathsf{v}_2^*) \not\twoheadrightarrow_{L_2}$$

where $\mathsf{H}_{1g}', \mathsf{H}_{2g}' : W'$ for some $W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W'$ and

$$(W', (\mathsf{H}_1^*, \mathsf{v}_1^*), (\mathsf{H}_2^*, \mathsf{v}_2^*)) \in \mathcal{V}[\![!\tau]\!]_\rho$$

By expanding the value relation, we find $\mathsf{H}_1^* = \mathsf{H}_2^* = \emptyset$.

Thus, the original configuration steps as follows:

$$\begin{aligned}&(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x} = \gamma_{\mathrm{L}}^1(\gamma_{\Gamma}^1(\mathrm{e}^{+}))\ \mathsf{in}\ (\mathsf{x},\ \mathsf{x})) \overset{*}{\longrightarrow}_{L_1}\\ &(\mathsf{H}_{1g}' \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x} =\ \mathsf{v}_1^*\ \mathsf{in}\ (\mathsf{x},\ \mathsf{x})) \overset{*}{\longrightarrow}_{L_1}\\ &(\mathsf{H}_{1g}' \uplus \mathsf{H}_{1+}, (\mathsf{v}_1^*,\ \mathsf{v}_1^*))\end{aligned}$$

and

$$\begin{aligned}&(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \mathsf{let}\ \mathsf{x} = \gamma_{\mathrm{L}}^2(\gamma_{\Gamma}^2(\mathrm{e}^{+}))\ \mathsf{in}\ (\mathsf{x},\ \mathsf{x})) \overset{*}{\longrightarrow}_{L_2}\\ &(\mathsf{H}_{2g}' \uplus \mathsf{H}_{2+}, \mathsf{let}\ \mathsf{x} =\ \mathsf{v}_2^*\ \mathsf{in}\ (\mathsf{x},\ \mathsf{x})) \overset{*}{\longrightarrow}_{L_2}\\ &(\mathsf{H}_{2g}' \uplus \mathsf{H}_{2+}, (\mathsf{v}_2^*,\ \mathsf{v}_2^*))\end{aligned}$$

Notice that both of these configurations are irreducible because $(\mathsf{v}_1^*, \mathsf{v}_1^*)$ and $(\mathsf{v}_2^*, \mathsf{v}_2^*)$ are both values. Next, choose $\mathsf{H}_1' = \emptyset, \mathsf{H}_{1g}' = \mathsf{H}_{1g}', \mathsf{H}_2' = \emptyset$, and $\mathsf{H}_{2g}' = \mathsf{H}_{2g}'$. Finally, we find $(W', (\emptyset, (\mathsf{v}_1^*, \mathsf{v}_1^*)), (\emptyset, (\mathsf{v}_2^*, \mathsf{v}_2^*))) \in \mathcal{V}[\![!\tau \otimes !\tau]\!]_\rho$ because $(W', (\emptyset, \mathsf{v}_1^*), (\emptyset, \mathsf{v}_2^*)) \in \mathcal{V}[\![!\tau]\!]_\rho$, which suffices to finish the proof. □

Lemma 4.41 (Compat drop e). *If* $\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : !\tau$ *, then*

$$\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{drop\ e} \preceq \mathrm{drop\ e} : \mathrm{Unit}$$

Proof. Expanding the definition of $\preceq$, $\cdot^{+}$, $\mathcal{E}[\![\cdot]\!].$ and pushing substitutions in the goal, we are to show that

$$\begin{array}{l}
\exists \mathsf{H}_1', \mathsf{H}_{1g}'.\forall \mathsf{H}_{2+} : \mathit{MHeap}.\exists \mathsf{H}_2', W', \mathsf{H}_{2g}', \mathsf{v}_2. \\
\mathsf{H}_{1*} = \mathsf{H}_{1g}' \uplus \mathsf{H}_1' \uplus \mathsf{H}_{1+} \ \wedge \mathsf{H}_{1g}', \mathsf{H}_{2g}' : W' \wedge \\
W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W' \wedge \\
(W', (\mathsf{H}_1', \mathsf{v}_1), (\mathsf{H}_2', \mathsf{v}_2)) \in \mathcal{V}[\![\mathsf{Unit}]\!]_\rho \wedge \\
(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \mathsf{let}\ \_ = \gamma_{\mathsf{L}}^2(\gamma_{\Gamma}^2(\mathsf{e}^+))\ \mathsf{in}\ ()) \xrightarrow{*}_{L_2} \\
(\mathsf{H}_{2g}' \uplus \mathsf{H}_2' \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \nrightarrow
\end{array}$$

given arbitrary $\rho, \gamma_{\mathsf{L}}, \gamma_{\Gamma}, W, L_1, L_2, \mathsf{H}_{1g+}, \mathsf{H}_{2g+} : W, \mathsf{v}_1, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_{1+} : \mathit{MHeap}, \mathsf{H}_{1*}$, such that

$$\rho.\mathsf{L3} \in \mathcal{D}[\![\Delta]\!], \rho.\mathsf{F} \in \mathcal{D}[\![\Delta]\!], (W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]_\rho, (W, \mathsf{H}_1, \mathsf{H}_2, \gamma_{\mathsf{L}}.\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho, \gamma_{\mathsf{L}}.\Delta = \gamma_{\mathrm{locs}}(\rho.\mathsf{L3})$$

and

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = \gamma_{\mathsf{L}}^1(\gamma_{\Gamma}^1(\mathsf{e}^+))\ \mathsf{in}\ ()) \xrightarrow{*}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \nrightarrow_{L_1}$$

We can instantiate the first induction hypothesis with $\rho, \gamma_{\Gamma}, \gamma_{\mathsf{L}}, \mathsf{H}_1, \mathsf{H}_2$ to find

$$(W, (\mathsf{H}_1, \gamma_{\mathsf{L}}^1(\gamma_{\Gamma}^1(\mathsf{e}^+))), (\mathsf{H}_2, \gamma_{\mathsf{L}}^2(\gamma_{\Gamma}^2(\mathsf{e}^+)))) \in \mathcal{E}[\![!\tau]\!]_\rho$$

Thus, we find

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \gamma_{\mathsf{L}}^1(\gamma_{\Gamma}^1(\mathsf{e}^+))) \xrightarrow{*}_{L_1} (\mathsf{H}_{1g}' \uplus \mathsf{H}_{1+} \uplus \mathsf{H}_1^*, \mathsf{v}_1^*) \nrightarrow_{L_1}$$

and

$$(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \gamma_{\mathsf{L}}^2(\gamma_{\Gamma}^2(\mathsf{e}^+))) \xrightarrow{*}_{L_2} (\mathsf{H}_{2g}' \uplus \mathsf{H}_{2+} \uplus \mathsf{H}_2^*, \mathsf{v}_2^*) \nrightarrow_{L_2}$$

where $\mathsf{H}_{1g}', \mathsf{H}_{2g}' : W'$ for some $W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W'$ and

$$(W', (\mathsf{H}_1^*, \mathsf{v}_1^*), (\mathsf{H}_2^*, \mathsf{v}_2^*)) \in \mathcal{V}[\![!\tau]\!]_\rho$$

By expanding the value relation, we find $\mathsf{H}_1^* = \mathsf{H}_2^* = \emptyset$.

Thus, the original configuration steps as follows:

$$\begin{array}{l}
(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = \gamma_{\mathsf{L}}^1(\gamma_{\Gamma}^1(\mathsf{e}^+))\ \mathsf{in}\ ()) \xrightarrow{*}_{L_1} \\
(\mathsf{H}_{1g}' \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ =\ \mathsf{v}_1^*\ \mathsf{in}\ ()) \xrightarrow{*}_{L_1} \\
(\mathsf{H}_{1g}' \uplus \mathsf{H}_{1+}, ())
\end{array}$$

and

$$\begin{array}{l}
(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \mathsf{let}\ \_ = \gamma_{\mathsf{L}}^2(\gamma_{\Gamma}^2(\mathsf{e}^+))\ \mathsf{in}\ ()) \xrightarrow{*}_{L_2} \\
(\mathsf{H}_{2g}' \uplus \mathsf{H}_{2+} \uplus \mathsf{H}_{2+}^*, \mathsf{let}\ \_ =\ \mathsf{v}_2^*\ \mathsf{in}\ ()) \xrightarrow{*}_{L_2} \\
(\mathsf{H}_{2g}' \uplus \mathsf{H}_{2+} \uplus \mathsf{H}_{2+}^*, ())
\end{array}$$

Next, choose $\mathsf{H}_1' = \emptyset$, $\mathsf{H}_{1g}' = \mathsf{H}_{1g}'$, $\mathsf{H}_2' = \emptyset$, and $\mathsf{H}_{2g}' = \mathsf{H}_{2g}'$. Then, we find $(W'.(\emptyset, ()), (\emptyset, ())) \in \mathcal{V}[\![\mathsf{Unit}]\!]_\rho$ by definition, which suffices to finish the proof. □

Lemma 4.42 (Compat new e). *If* $\Delta; \Gamma; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \tau$ *, then*

$$\Delta; \Gamma; \Delta; \Gamma \vdash \mathsf{new}\ \mathsf{e} \preceq \mathsf{new}\ \mathsf{e} : \exists\zeta.\mathsf{cap}\ \zeta\ \tau \otimes !\mathsf{ptr}\ \zeta$$

Proof. Expanding the definition of $\preceq$, $\cdot^{+}$, $\mathcal{E}[\![\cdot]\!]$. and pushing substitutions in the goal, we are to show that

$$\begin{array}{l}
\exists \mathsf{H}'_1, \mathsf{H}'_{1g}. \forall \mathsf{H}_{2+} : \mathit{MHeap}. \exists \mathsf{H}'_2, W', \mathsf{H}'_{2g}, \mathsf{v}_2. \\
\mathsf{H}_{1*} = \mathsf{H}'_{1g} \uplus \mathsf{H}'_1 \uplus \mathsf{H}_{1+} \ \wedge \mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W' \wedge \\
W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W, L_1 \cup FL(\mathrm{cod}(\mathsf{H}_{1+})), L_2 \cup FL(\mathrm{cod}(\mathsf{H}_{2+})))} W' \wedge \\
(W', (\mathsf{H}'_1, \mathsf{v}_1), (\mathsf{H}'_2, \mathsf{v}_2)) \in \mathcal{V}[\![\exists \zeta.\mathsf{cap}\, \zeta\, \tau \otimes !\mathsf{ptr}\, \zeta]\!]_{\rho} \wedge \\
(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \mathsf{let}\ \_ = \mathsf{callgc}\ \mathsf{in}\ \mathsf{let}\ \mathsf{x}_{\ell} = \mathsf{ref}\ \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathsf{e}^{+}))\ \mathsf{in}\ ((),\ \mathsf{x}_{\ell})) \xrightarrow{*}_{L_2} \\
(\mathsf{H}'_{2g} \uplus \mathsf{H}'_2 \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \nrightarrow
\end{array}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_{\Gamma}, W, L_1, L_2, \mathsf{H}_{1g+}, \mathsf{H}_{2g+} : W, \mathsf{v}_1, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_{1+} : \mathit{MHeap}, \mathsf{H}_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!], \rho.\mathsf{F} \in \mathcal{D}[\![\Delta]\!], (W, \gamma_{\Gamma}) \in \mathcal{G}[\![\Gamma]\!]_{\rho}, (W, \mathsf{H}_1, \mathsf{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}[\![\Gamma]\!]_{\rho}$$

and

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = \mathsf{callgc}\ \mathsf{in}\ \mathsf{let}\ \mathsf{x}_{\ell} = \mathsf{ref}\ \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}^{+}))\ \mathsf{in}\ ((),\ \mathsf{x}_{\ell})) \xrightarrow{*}_{L_1} (\mathsf{H}_{1*}, \mathsf{v}_1) \nrightarrow_{L_1}$$

First, notice that

$$\begin{array}{l}
(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = \mathsf{callgc}\ \mathsf{in}\ \mathsf{let}\ \mathsf{x}_{\ell} = \mathsf{ref}\ \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}^{+}))\ \mathsf{in}\ ((),\ \mathsf{x}_{\ell})) \rightarrow_{L_1} \\
(\mathsf{H}_{1ga} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = ()\ \mathsf{in}\ \mathsf{let}\ \mathsf{x}_{\ell} = \mathsf{ref}\ \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}^{+}))\ \mathsf{in}\ ((),\ \mathsf{x}_{\ell})) \rightarrow_{L_1} \\
(\mathsf{H}_{1ga} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x}_{\ell} = \mathsf{ref}\ \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}^{+}))\ \mathsf{in}\ ((),\ \mathsf{x}_{\ell}))
\end{array}$$

and similarly,

$$\begin{array}{l}
(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \mathsf{let}\ \_ = \mathsf{callgc}\ \mathsf{in}\ \mathsf{let}\ \mathsf{x}_{\ell} = \mathsf{ref}\ \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathsf{e}^{+}))\ \mathsf{in}\ ((),\ \mathsf{x}_{\ell})) \xrightarrow{*}_{L_2} \\
(\mathsf{H}_{2ga} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \mathsf{let}\ \mathsf{x}_{\ell} = \mathsf{ref}\ \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathsf{e}^{+}))\ \mathsf{in}\ ((),\ \mathsf{x}_{\ell}))
\end{array}$$

for some heaps $\mathsf{H}_{1ga} : \mathit{GCHeap}, \mathsf{H}_{2ga} : \mathit{GCHeap}$. By Lemma 4.8, there exists a world

$$W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_1) \uplus \mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_2) \uplus \mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W, FL(\mathrm{cod}(\mathsf{H}_{1+})) \cup FL(\gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}))) \cup L_1, FL(\mathrm{cod}(\mathsf{H}_{2+})) \cup FL(\gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathsf{e}))) \cup L_2)} W_a$$

such that $\mathsf{H}_{1ga}, \mathsf{H}_{2ga} : W_a$.

Then, since $\mathcal{G}[\![\grave{}\,]\!]_{\rho}, \mathcal{G}[\![\Gamma]\!]_{\rho}$ are closed under world extension by Lemma 4.7, we can instantiate the first induction hypothesis with $\rho, \gamma_{\Gamma}, \gamma_{\mathrm{L}}, W_a, \mathsf{H}_1, \mathsf{H}_2$, so we find

$$(W_a, (\mathsf{H}_1, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}^{+}))), (\mathsf{H}_2, \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathsf{e}^{+})))) \in \mathcal{E}[\![\tau]\!]_{\rho}$$

Ergo,

$$(\mathsf{H}_{1ga} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}^{+}))) \xrightarrow{*}_{L_1} (\mathsf{H}'_{1g} \uplus \mathsf{H}^*_1 \uplus \mathsf{H}_{1+}, \mathsf{v}_1)$$

and

$$(\mathsf{H}_{2ga} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathsf{e}^{+}))) \xrightarrow{*}_{L_2} (\mathsf{H}'_{2g} \uplus \mathsf{H}^*_2 \uplus \mathsf{H}_{2+}, \mathsf{v}_2)$$

where $\mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W'$ for some $W_a \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W, FL(\mathrm{cod}(\mathsf{H}_{1+})) \cup L_1, FL(\mathrm{cod}(\mathsf{H}_{2+})) \cup L_2)} W'$ and

$$(W', (\mathsf{H}^*_1, \mathsf{v}_1), (\mathsf{H}^*_2, \mathsf{v}_2)) \in \mathcal{V}[\![\tau]\!]_{\rho}$$

Thus, the original configuration steps as follows:

$$\begin{array}{l}
(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = \mathsf{callgc}\ \mathsf{in}\ \mathsf{let}\ \mathsf{x}_{\ell} = \mathsf{ref}\ \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}^{+}))\ \mathsf{in}\ ((),\ \mathsf{x}_{\ell})) \xrightarrow{*}_{L_1} \\
(\mathsf{H}_{1ga} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x}_{\ell} = \mathsf{ref}\ \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}^{+}))\ \mathsf{in}\ ((),\ \mathsf{x}_{\ell})) \xrightarrow{*}_{L_1} \\
(\mathsf{H}'_{1g} \uplus \mathsf{H}^*_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x}_{\ell} = \mathsf{ref}\ \mathsf{v}_1\ \mathsf{in}\ ((),\ \mathsf{x}_{\ell})) \xrightarrow{*}_{L_1} \\
(\mathsf{H}'_{1g} \uplus \mathsf{H}^*_1[\ell_1 \overset{m}{\mapsto} \mathsf{v}_1] \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x}_{\ell} = \ell_1\ \mathsf{in}\ ((),\ \mathsf{x}_{\ell})) \xrightarrow{*}_{L_1} \\
(\mathsf{H}'_{1g} \uplus \mathsf{H}^*_1[\ell_1 \overset{m}{\mapsto} \mathsf{v}_1] \uplus \mathsf{H}_{1+}, ((),\ \ell_1))
\end{array}$$

and, by similar logic,

$$(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathrm{let}\ \mathrm{x}_\ell = \mathrm{ref}\ \gamma_{\mathrm{L}}^2(\gamma_{\Gamma}^2(\mathrm{e}^+))\ \mathrm{in}\ ((),\ \mathrm{x}_\ell)) \xrightarrow{*}_{L_2} (\mathrm{H}'_{2g} \uplus \mathrm{H}^*_2[\ell_2 \mapsto \mathrm{v}_2] \uplus \mathrm{H}_{2+}, ((),\ \ell_2))$$

for some locations $\ell_1 \notin \mathrm{dom}(\mathrm{H}'_{1g} \uplus \mathrm{H}^*_1 \uplus \mathrm{H}_{1+})$ and $\ell_2 \notin \mathrm{dom}(\mathrm{H}'_{2g} \uplus \mathrm{H}^*_2 \uplus \mathrm{H}_{2+})$.

Now, we can choose $\mathrm{H}'_1 = \mathrm{H}^*_1[\ell_1 \mapsto \mathrm{v}_1]$, $\mathrm{H}'_2 = \mathrm{H}^*_2[\ell_2 \mapsto \mathrm{v}_2]$, $W' = W'$, $\mathrm{H}'_{1g} = \mathrm{H}'_{1g}$, and $\mathrm{H}'_{2g} = \mathrm{H}'_{2g}$. Thus, it suffices to show:

$$(W', (\mathrm{H}^*_1[\ell_1 \mapsto \mathrm{v}_1], ((), \ell_1)), (\mathrm{H}^*_2[\ell_2 \mapsto \mathrm{v}_2], ((), \ell_2))) \in \mathcal{V}[\![\exists\zeta.\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta]\!]_\rho$$

By expanding the value relation, it suffices to show:

$$(W', (\mathrm{H}^*_1[\ell_1 \mapsto \mathrm{v}_1], ((), \ell_1)), (\mathrm{H}^*_2[\ell_2 \mapsto \mathrm{v}_2], ((), \ell_2))) \in \mathcal{V}[\![\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_1,\ell_2)]}$$

By expanding the value relation and splitting the heaps appropriately, it suffices to show

$$(W', (\mathrm{H}^*_1[\ell_1 \mapsto \mathrm{v}_1], ()), (\mathrm{H}^*_2[\ell_2 \mapsto \mathrm{v}_2], ())) \in \mathcal{V}[\![\mathrm{cap}\ \zeta\ \tau]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_1,\ell_2)]} \tag{52}$$

and

$$(W', (\emptyset, \ell_1), (\emptyset, \ell_2)) \in \mathcal{V}[\![!\mathrm{ptr}\ \zeta]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_1,\ell_2)]} \tag{53}$$

We first prove (53). By expanding the value relation, it suffices to show:

$$(W', (\emptyset, \ell_1), (\emptyset, \ell_2)) \in \mathcal{V}[\![\mathrm{ptr}\ \zeta]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_1,\ell_2)]}$$

Then, since ζ clearly maps to (ℓ_1, ℓ_2) in the environment in the above value relation, we are done.

Next, we prove (52). By expanding the value relation, since ζ clearly maps to (ℓ_1, ℓ_2) in the environment in the value relation, it suffices to show

$$(W', (\mathrm{H}^*_1, \mathrm{v}_1), (\mathrm{H}_2, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_1,\ell_2)]}$$

However, we have $(W', (\mathrm{H}^*_1, \mathrm{v}_1), (\mathrm{H}^*_2, \mathrm{v}_2)) \in \mathcal{V}[\![\tau]\!]_\rho$, and extending ρ does not remove any atoms from the value relation, so this suffices to finish the proof. □

Lemma 4.43 (Compat free e). *If* $\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \exists\zeta.\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta$ *, then*

$$\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{free}\ \mathrm{e} \preceq \mathrm{free}\ \mathrm{e} : \exists\zeta.\tau$$

Proof. Expanding the definition of $\preceq$, $\cdot^+$, $\mathcal{E}[\![\cdot]\!]$. and pushing substitutions in the goal, we are to show that

$$\begin{array}{l}
\exists \mathrm{H}'_1, \mathrm{H}'_{1g}.\forall \mathrm{H}_{2+} : \mathit{MHeap}.\exists \mathrm{H}'_2, W', \mathrm{H}'_{2g}, \mathrm{v}_2.\\
\mathrm{H}_{1*} = \mathrm{H}'_{1g} \uplus \mathrm{H}'_1 \uplus \mathrm{H}_{1+}\ \wedge \mathrm{H}'_{1g}, \mathrm{H}'_{2g} : W' \wedge\\
W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W, \mathit{FL}(\mathrm{cod}(\mathrm{H}_{1+}))\cup L_1, \mathit{FL}(\mathrm{cod}(\mathrm{H}_{2+}))\cup L_2)} W' \wedge\\
(W', (\mathrm{H}'_1, \mathrm{v}_1), (\mathrm{H}'_2, \mathrm{v}_2)) \in \mathcal{V}[\![\exists\zeta.\tau]\!]_\rho \wedge\\
(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \mathrm{let}\ \mathrm{x} = \gamma_{\mathrm{L}}^2(\gamma^2_{`}(\mathrm{e}^+))\ \mathrm{in}\ \mathrm{let}\ \mathrm{x_r} =!(\mathrm{snd}\ \mathrm{x})\ \mathrm{in}\ \mathrm{let}\ \_ = \mathrm{free}\ (\mathrm{snd}\ \mathrm{x})\ \mathrm{in}\ \mathrm{x_r}) \xrightarrow{*}_{L_2}\\
(\mathrm{H}'_{2g} \uplus \mathrm{H}'_2 \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \not\rightarrow
\end{array}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_{\Gamma}, W, L_1, L_2, \mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W, \mathrm{v}_1, \mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_{1+} : \mathit{MHeap}, \mathrm{H}_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!], \rho.\mathrm{F} \in \mathcal{D}[\![\Delta]\!], (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho, (W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}[\![\Gamma]\!]_\rho$$

and

$$\begin{array}{l}
(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \mathrm{let}\ \mathrm{x} = \gamma_{\mathrm{L}}^1(\gamma^1_{`}(\mathrm{e}^+))\ \mathrm{in}\ \mathrm{let}\ \mathrm{x_r} =!(\mathrm{snd}\ \mathrm{x})\ \mathrm{in}\ \mathrm{let}\ \_ = \mathrm{free}\ (\mathrm{snd}\ \mathrm{x})\ \mathrm{in}\ \mathrm{x_r}) \xrightarrow{*}_{L_1}\\
(\mathrm{H}_{1*}, \mathrm{v}_1) \not\rightarrow_{L_1}
\end{array}$$

By instantiating the first induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{\mathrm{L}}, \mathrm{H}_1, \mathrm{H}_2$, we find

$$(W, (\mathrm{H}_1, \gamma_{\mathrm{L}}^1(\gamma_\Gamma^1(\mathrm{e}^+))), (\mathrm{H}_2, \gamma_{\mathrm{L}}^2(\gamma_\Gamma^2(\mathrm{e}^+)))) \in \mathcal{E}[\![\exists\zeta.\mathrm{cap}\ \zeta\ \tau \otimes !\mathrm{ptr}\ \zeta]\!]_\rho$$

Ergo, by Lemma 4.3,

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathrm{e}^+))) \xrightarrow{*}_{L_1} (\mathsf{H}'_{1g} \uplus \mathsf{H}^*_1 \uplus \mathsf{H}_{1+}, \mathsf{v}_1) \twoheadrightarrow_{L_1}$$

and

$$(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathrm{e}^+))) \xrightarrow{*}_{L_2} (\mathsf{H}'_{2g} \uplus \mathsf{H}^*_2 \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \twoheadrightarrow_{L_2}$$

where $\mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W'$ for some $W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,FL(\mathrm{cod}(\mathsf{H}_{1+}))\cup L_1,FL(\mathrm{cod}(\mathsf{H}_{2+}))\cup L_2)} W'$ and

$$(W', (\mathsf{H}^*_1, \mathsf{v}_1), (\mathsf{H}^*_2, \mathsf{v}_2)) \in \mathcal{V}[\![\exists\zeta.\mathrm{cap}\,\zeta\,\tau \otimes !\mathrm{ptr}\,\zeta]\!]_\rho$$

By expanding the value relation, there exist some locations ℓ_1, ℓ_2 and, for any $i \in \{1, 2\}$,

$$\mathsf{v}_{\mathsf{i}} = ((), \ell_i)$$

and

$$\mathsf{H}^*_i = \mathsf{H}^v_i \uplus \{\ell_i \mapsto \mathsf{v}_{\mathsf{h}i}\}$$

where

$$(W', (\mathsf{H}^v_1, \mathsf{v}_{\mathsf{h}1}), (\mathsf{H}^v_2, \mathsf{v}_{\mathsf{h}2})) \in \mathcal{V}[\![\tau]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_1,\ell_2)]}$$

Thus, the original configuration steps as follows:

$$\begin{array}{l}
(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x} = \gamma^1_{\mathrm{L}}(\gamma^1(\mathrm{e}^+))\ \mathsf{in}\ \mathsf{let}\ \mathsf{x_r} = !(\mathsf{snd}\ \mathsf{x})\ \mathsf{in}\ \mathsf{let}\ \_ = \mathsf{free}\ (\mathsf{snd}\ \mathsf{x})\ \mathsf{in}\ \mathsf{x_r}) \xrightarrow{*}_{L_1} \\
(\mathsf{H}'_{1g} \uplus \mathsf{H}^v_1 \uplus \{\ell_1 \mapsto \mathsf{v}_{\mathsf{h}1}\} \uplus \mathsf{H}_{1+}, \\
\quad \mathsf{let}\ \mathsf{x} = ((), \ell_1)\ \mathsf{in}\ \mathsf{let}\ \mathsf{x_r} = !(\mathsf{snd}\ \mathsf{x})\ \mathsf{in}\ \mathsf{let}\ \_ = \mathsf{free}\ (\mathsf{snd}\ \mathsf{x})\ \mathsf{in}\ \mathsf{x_r}) \xrightarrow{*}_{L_1} \\
(\mathsf{H}'_{1g} \uplus \mathsf{H}^v_1 \uplus \{\ell_1 \mapsto \mathsf{v}_{\mathsf{h}1}\} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x_r} = !\ell_1\ \mathsf{in}\ \mathsf{let}\ \_ = \mathsf{free}\ \ell_1\ \mathsf{in}\ \mathsf{x_r}) \xrightarrow{*}_{L_1} \\
(\mathsf{H}'_{1g} \uplus \mathsf{H}^v_1 \uplus \{\ell_1 \mapsto \mathsf{v}_{\mathsf{h}1}\} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \mathsf{x_r} = \mathsf{v}_{\mathsf{h}1}\ \mathsf{in}\ \mathsf{let}\ \_ = \mathsf{free}\ \ell_1\ \mathsf{in}\ \mathsf{x_r}) \xrightarrow{*}_{L_1} \\
(\mathsf{H}'_{1g} \uplus \mathsf{H}^v_1 \uplus \{\ell_1 \mapsto \mathsf{v}_{\mathsf{h}1}\} \uplus \mathsf{H}_{1+}, \mathsf{let}\ \_ = \mathsf{free}\ \ell_1\ \mathsf{in}\ \mathsf{v}_{\mathsf{h}1}) \xrightarrow{*}_{L_1} \\
(\mathsf{H}'_{1g} \uplus \mathsf{H}^v_1 \uplus \mathsf{H}_{1+}, \mathsf{v}_{\mathsf{h}1})
\end{array}$$

and by similar logic,

$$\begin{array}{l}
(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \mathsf{let}\ \mathsf{x} = \gamma^2_{\mathrm{L}}(\gamma^2(\mathrm{e}^+))\ \mathsf{in}\ \mathsf{let}\ \mathsf{x_r} = !(\mathsf{snd}\ \mathsf{x})\ \mathsf{in}\ \mathsf{let}\ \_ = \mathsf{free}\ (\mathsf{snd}\ \mathsf{x})\ \mathsf{in}\ \mathsf{x_r}) \xrightarrow{*}_{L_2} \\
(\mathsf{H}'_{2g} \uplus \mathsf{H}^v_2 \uplus \mathsf{H}_{2+}, \mathsf{v}_{\mathsf{h}2})
\end{array}$$

Then, we can take $W' = W'$, $\mathsf{H}'_1 = \mathsf{H}^v_1$, $\mathsf{H}'_2 = \mathsf{H}^v_2$, $\mathsf{H}'_{1g} = \mathsf{H}'_{1g}$, and $\mathsf{H}'_{2+} = \mathsf{H}'_{2g}$. Thus, it suffices to show

$$(W', (\mathsf{H}^v_1, \mathsf{v}_{\mathsf{h}1}), (\mathsf{H}^v_2, \mathsf{v}_{\mathsf{h}2})) \in \mathcal{V}[\![\exists\zeta.\tau]\!]_\rho$$

Because we have $(W', (\mathsf{H}^v_1, \mathsf{v}_{\mathsf{h}1}), (\mathsf{H}^v_2, \mathsf{v}_{\mathsf{h}2})) \in \mathcal{V}[\![\tau]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_1,\ell_2)]}$, the above statement clearly follows, which suffices to finish the proof. □

Lemma 4.44 (Compat swap). *If* $\Delta; \Gamma; \Delta; \Gamma_1 \vdash \mathrm{e}_1 \preceq \mathrm{e}_1 : \mathrm{cap}\,\zeta\,\tau_1$, $\Delta; \Gamma; \Delta; \Gamma_2 \vdash \mathrm{e}_2 \preceq \mathrm{e}_2 : \mathrm{ptr}\,\zeta$, *and* $\Delta; \Gamma; \Delta; \Gamma_3 \vdash \mathrm{e}_3 \preceq \mathrm{e}_3 : \tau_3$ *, then*

$$\Delta; \Gamma; \Delta; \Gamma \vdash \mathrm{swap}\ \mathrm{e}_1\ \mathrm{e}_2\ \mathrm{e}_3 \preceq \mathrm{swap}\ \mathrm{e}_1\ \mathrm{e}_2\ \mathrm{e}_3 : \mathrm{cap}\,\zeta\,\tau_3\ \otimes\ \tau_1$$

Proof. Expanding the definition of $\preceq$, $\cdot^{+}$, $\mathcal{E}[\![\cdot]\!].$ and pushing substitutions in the goal, we are to show that

$$\begin{array}{l}
\exists \mathrm{H}'_1, \mathrm{H}'_{1g}.\forall \mathrm{H}_{2+} : \mathit{MHeap}.\exists \mathrm{H}'_2, W', \mathrm{H}'_{2g}, \mathrm{v}_2. \\
\mathrm{H}_{1*} = \mathrm{H}'_{1g} \uplus \mathrm{H}'_1 \uplus \mathrm{H}_{1+} \ \wedge \mathrm{H}'_{1g}, \mathrm{H}'_{2g} : W' \wedge \\
W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W' \wedge \\
(W', (\mathrm{H}'_1, \mathrm{v}_1), (\mathrm{H}'_2, \mathrm{v}_2)) \in \mathcal{V}[\![\mathrm{cap}\ \zeta\ \tau_3\ \otimes\ \tau_1]\!]_\rho \wedge \\
(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \\
\ \mathrm{let}\ \mathrm{x_p} = \gamma^2_{\mathrm{L}}(\gamma^2_{\cdot}(\mathrm{e}_2{}^{+}))\ \mathrm{in}\ \mathrm{let}\ \_ = \gamma^2_{\mathrm{L}}(\gamma^2_{\cdot}(\mathrm{e}_1))\ \mathrm{in}\ \mathrm{let}\ \mathrm{x_{v'}} = !\mathrm{x_p}\ \mathrm{in}\ \mathrm{let}\ \_ = (\mathrm{x_p} := \gamma^2_{\mathrm{L}}(\gamma^2_{\cdot}(\mathrm{e}_3+)))\ \mathrm{in}\ ((), \mathrm{x_{v'}})) \xrightarrow{*}_{L_2} \\
(\mathrm{H}'_{2g} \uplus \mathrm{H}'_2 \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \nrightarrow
\end{array}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_{\Gamma}, W, L_1, L_2, \mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W, \mathrm{v}_1, \mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_{1+} : \mathit{MHeap}, \mathrm{H}_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!], \rho.\mathrm{F} \in \mathcal{D}[\![\Delta]\!], (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho, (W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}[\![\Gamma_1 \uplus \Gamma_2 \uplus \Gamma_3]\!]_\rho$$

and

$$\begin{array}{l}
(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \\
\ \mathrm{let}\ \mathrm{x_p} = \gamma^1_{\mathrm{L}}(\gamma^1_{\cdot}(\mathrm{e}_2{}^{+}))\ \mathrm{in}\ \mathrm{let}\ \_ = \gamma^1_{\mathrm{L}}(\gamma^1_{\cdot}(\mathrm{e}_1))\ \mathrm{in}\ \mathrm{let}\ \mathrm{x_{v'}} = !\mathrm{x_p}\ \mathrm{in}\ \mathrm{let}\ \_ = (\mathrm{x_p} := \gamma^1_{\mathrm{L}}(\gamma^1_{\cdot}(\mathrm{e}_3+)))\ \mathrm{in}\ ((), \mathrm{x_{v'}})) \xrightarrow{*}_{L_1} \\
(\mathrm{H}_{1*}, \mathrm{v}_1) \nrightarrow_{L_1}
\end{array}$$

Then, by applying Lemma 4.13 twice, there exist $\gamma_{\mathrm{L}1}, \gamma_{\mathrm{L}2}, \gamma_{\mathrm{L}3}, \mathrm{H}_{1a}, \mathrm{H}_{1b}, \mathrm{H}_{1c}, \mathrm{H}_{2a}, \mathrm{H}_{2b}, \mathrm{H}_{2c}$ such that $\gamma_{\mathrm{L}}.\Gamma = \gamma_{\mathrm{L}1} \uplus \gamma_{\mathrm{L}2} \uplus \gamma_{\mathrm{L}3}$, $\mathrm{H}_1 = \mathrm{H}_{1a} \uplus \mathrm{H}_{1b} \uplus \mathrm{H}_{1c}$, $\mathrm{H}_2 = \mathrm{H}_{2a} \uplus \mathrm{H}_{2b} \uplus \mathrm{H}_{2c}$,

$$(W, \mathrm{H}_{1a}, \mathrm{H}_{2a}, \gamma_{\mathrm{L}1}) \in \mathcal{G}[\![\Gamma_1]\!]_\rho$$
$$(W, \mathrm{H}_{1b}, \mathrm{H}_{2b}, \gamma_{\mathrm{L}2}) \in \mathcal{G}[\![\Gamma_2]\!]_\rho$$
$$(W, \mathrm{H}_{1c}, \mathrm{H}_{2c}, \gamma_{\mathrm{L}3}) \in \mathcal{G}[\![\Gamma_3]\!]_\rho$$

and for all $j \in \{1, 2\}$,

$$\gamma^j_{\mathrm{L}}(\gamma^j_{\Gamma}(\mathrm{e}_1{}^{+})) = \gamma_{\mathrm{L}}{}^j_1(\gamma^j_{\Gamma}(\mathrm{e}_1{}^{+}))$$
$$\gamma^j_{\mathrm{L}}(\gamma^j_{\Gamma}(\mathrm{e}_2{}^{+})) = \gamma_{\mathrm{L}}{}^j_2(\gamma^j_{\Gamma}(\mathrm{e}_2{}^{+}))$$
$$\gamma^j_{\mathrm{L}}(\gamma^j_{\Gamma}(\mathrm{e}_3{}^{+})) = \gamma_{\mathrm{L}}{}^j_3(\gamma^j_{\Gamma}(\mathrm{e}_3{}^{+}))$$

Then, by instantiating the second induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{\mathrm{L}2}, W, \mathrm{H}_{1b}, \mathrm{H}_{2b}$, we find

$$(W, (\mathrm{H}_{1b}, \gamma_{\mathrm{L}}{}^1_2(\gamma^1_{\Gamma}(\mathrm{e}_2{}^{+}))), (\mathrm{H}_{2b}, \gamma_{\mathrm{L}}{}^2_2(\gamma^2_{\Gamma}(\mathrm{e}_2{}^{+})))) \in \mathcal{E}[\![\mathrm{ptr}\ \zeta]\!]_\rho$$

Thus, by Lemma 4.3, we have

$$\begin{array}{l}
(\mathrm{H}_{1g+} \uplus \mathrm{H}_{1a} \uplus \mathrm{H}_{1b} \uplus \mathrm{H}_{1c} \uplus \mathrm{H}_{1+}, \gamma_{\mathrm{L}}{}^1_2(\gamma^1_{\Gamma}(\mathrm{e}_2{}^{+}))) \xrightarrow{*}_{L_1\cup FL(\gamma_{\mathrm{L}}{}^1_1(\gamma^1_{\Gamma}(\mathrm{e}_1{}^{+})))\cup FL(\gamma_{\mathrm{L}}{}^1_3(\gamma^1_{\Gamma}(\mathrm{e}_3{}^{+}))} \\
(\mathrm{H}'_{1g} \uplus \mathrm{H}_{1a} \uplus \mathrm{H}_{1c} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}^*_{1b}, \mathrm{v}_{1\mathrm{b}}) \nrightarrow
\end{array}$$

and, for any H_{2+},

$$\begin{array}{l}
(\mathrm{H}_{2g+} \uplus \mathrm{H}_{2a} \uplus \mathrm{H}_{2b} \uplus \mathrm{H}_{2c} \uplus \mathrm{H}_{2+}, \gamma_{\mathrm{L}}{}^2_2(\gamma^2_{\Gamma}(\mathrm{e}_2{}^{+}))) \xrightarrow{*}_{L_2\cup FL(\gamma_{\mathrm{L}}{}^2_1(\gamma^2_{\Gamma}(\mathrm{e}_1{}^{+})))\cup FL(\gamma_{\mathrm{L}}{}^2_3(\gamma^2_{\Gamma}(\mathrm{e}_3{}^{+})))} \\
(\mathrm{H}'_{2g} \uplus \mathrm{H}_{2a} \uplus \mathrm{H}_{2c} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}^*_{2b}, \mathrm{v}_{2\mathrm{b}}) \nrightarrow
\end{array}$$

where $\mathrm{H}'_{1g}, \mathrm{H}'_{2g} : W'$ for some

$$W \sqsubseteq_{\substack{(\mathrm{dom}(\mathrm{H}_{1a}\uplus\mathrm{H}_{1c}\uplus\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2a}\uplus\mathrm{H}_{2c}\uplus\mathrm{H}_{2+})), \\ \mathrm{rchgclocs}(W,FL(\mathrm{cod}(\mathrm{H}_{1a}))\cup FL(\mathrm{cod}(\mathrm{H}_{1c}))\cup FL(\mathrm{cod}(\mathrm{H}_{1+}))\cup FL(\gamma_{\mathrm{L}}{}^1_1(\gamma^1_{\Gamma}(\mathrm{e}_1{}^{+})))\cup FL(\gamma_{\mathrm{L}}{}^1_3(\gamma^1_{\Gamma}(\mathrm{e}_3{}^{+})))\cup L_1, \\ FL(\mathrm{cod}(\mathrm{H}_{2a}))\cup FL(\mathrm{cod}(\mathrm{H}_{2c}))\cup FL(\mathrm{cod}(\mathrm{H}_{2+}))\cup FL(\gamma_{\mathrm{L}}{}^2_1(\gamma^2_{\Gamma}(\mathrm{e}_1{}^{+})))\cup FL(\gamma_{\mathrm{L}}{}^2_3(\gamma^2_{\Gamma}(\mathrm{e}_3{}^{+})))\cup L_2)}} W'$$

and

$$(W', (\mathrm{H}^*_{1b}, \mathrm{v}_{1\mathrm{b}}), (\mathrm{H}^*_{2b}, \mathrm{v}_{2\mathrm{b}})) \in \mathcal{V}[\![\mathrm{ptr}\ \zeta]\!]_\rho$$

Expanding the value relation, we find that $\mathrm{H}^*_{1b} = \mathrm{H}^*_{2b} = \emptyset$ and there exist locations ℓ_1, ℓ_2 such that $\rho.\mathrm{L3}(\zeta) = (\ell_1, \ell_2) = (\mathrm{v}_{1\mathrm{b}}, \mathrm{v}_{2\mathrm{b}})$.

Then, since $\mathcal{G}[\![\Gamma]\!]_\rho, \mathcal{G}[\![\Gamma_1 \uplus \Gamma_2 \uplus \Gamma_3]\!]_\rho$ are closed under world extension by Lemma 4.7, we can instantiate the first induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{\mathrm{L}1}, W', \mathrm{H}_{1a}, \mathrm{H}_{2a}$:

$$(W', (\mathrm{H}_{1a}, \gamma_{\mathrm{L}1}^{\,1}(\gamma_\Gamma^1(\mathrm{e}_1{}^+))), (\mathrm{H}_{2a}, \gamma_{\mathrm{L}1}^{\,2}(\gamma_\Gamma^2(\mathrm{e}_1{}^+)))) \in \mathcal{E}[\![\mathrm{cap}\,\zeta\,\tau_1]\!]_\rho$$

Thus, by Lemma 4.3, we have

$$\begin{array}{l}(\mathrm{H}'_{1g} \uplus \mathrm{H}_{1a} \uplus \mathrm{H}_{1c} \uplus \mathrm{H}_{1+}, \gamma_{\mathrm{L}1}^{\,1}(\gamma_\Gamma^1(\mathrm{e}_1{}^+))) \xrightarrow{*}_{L_1 \cup FL(\gamma_{\mathrm{L}3}^{\,1}(\gamma_\Gamma^1(\mathrm{e}_3{}^+))} \\ (\mathrm{H}''_{1g} \uplus \mathrm{H}_{1c} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}^*_{1a}, \mathrm{v}_{1\mathrm{a}}) \nrightarrow\end{array}$$

and, for any H_{2+},

$$\begin{array}{l}(\mathrm{H}'_{2g} \uplus \mathrm{H}_{2a} \uplus \mathrm{H}_{2c} \uplus \mathrm{H}_{2+}, \gamma_{\mathrm{L}1}^{\,2}(\gamma_\Gamma^2(\mathrm{e}_1{}^+))) \xrightarrow{*}_{L_2 \cup FL(\gamma_{\mathrm{L}3}^{\,2}(\gamma_\Gamma^2(\mathrm{e}_3{}^+)))} \\ (\mathrm{H}''_{2g} \uplus \mathrm{H}_{2c} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}^*_{2a}, \mathrm{v}_{2\mathrm{a}}) \nrightarrow\end{array}$$

where $\mathrm{H}''_{1g}, \mathrm{H}''_{2g} : W''$ for some

$$W' \sqsubseteq_{\substack{(\mathrm{dom}(\mathrm{H}_{1c} \uplus \mathrm{H}_{1+}), \mathrm{dom}(\mathrm{H}_{2c} \uplus \mathrm{H}_{2+})), \\ \mathrm{rchgclocs}(W, FL(\mathrm{cod}(\mathrm{H}_{1c})) \cup FL(\mathrm{cod}(\mathrm{H}_{1+})) \cup FL(\gamma_{\mathrm{L}3}^{\,1}(\gamma_\Gamma^1(\mathrm{e}_3{}^+))) \cup L_1, FL(\mathrm{cod}(\mathrm{H}_{2c})) \cup FL(\mathrm{cod}(\mathrm{H}_{2+})) \cup FL(\gamma_{\mathrm{L}3}^{\,2}(\gamma_\Gamma^2(\mathrm{e}_3{}^+))) \cup L_2)}} W''$$

and

$$(W'', (\mathrm{H}^*_{1a}, \mathrm{v}_{1\mathrm{a}}), (\mathrm{H}^*_{2a}, \mathrm{v}_{2\mathrm{a}})) \in \mathcal{V}[\![\mathrm{cap}\,\zeta\,\tau_1]\!]_\rho$$

Expanding the value relation, we find that $\mathrm{v}_{1\mathrm{a}} = \mathrm{v}_{2\mathrm{a}} = ()$ and there exist values $\mathrm{v}_1, \mathrm{v}_2$ such that $\mathrm{H}^*_{1a} = \mathrm{H}_{1av} \uplus \{\ell_1 \overset{m}{\mapsto} \mathrm{v}_1\}$, $\mathrm{H}^*_{2a} = \mathrm{H}_{2av} \uplus \{\ell_2 \overset{m}{\mapsto} \mathrm{v}_2\}$, and

$$(W'', (\mathrm{H}_{1av}, \mathrm{v}_1), (\mathrm{H}_{2av}, \mathrm{v}_2)) \in \mathcal{V}[\![\tau_1]\!]_\rho$$

Then, since $\mathcal{G}[\![\Gamma]\!]_\rho, \mathcal{G}[\![\Gamma_1 \uplus \Gamma_2 \uplus \Gamma_3]\!]_\rho$ are closed under world extension by Lemma 4.7, we can instantiate the third induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{\mathrm{L}3}, W'', \mathrm{H}_{1c}, \mathrm{H}_{2c}$:

$$(W', (\mathrm{H}_{1c}, \gamma_{\mathrm{L}3}^{\,1}(\gamma_\Gamma^1(\mathrm{e}_3{}^+))), (\mathrm{H}_{2c}, \gamma_{\mathrm{L}3}^{\,2}(\gamma_\Gamma^2(\mathrm{e}_3{}^+)))) \in \mathcal{E}[\![\tau_3]\!]_\rho$$

Thus, by Lemma 4.3, we have

$$\begin{array}{l}(\mathrm{H}''_{1g} \uplus \mathrm{H}_{1av} \uplus \{\ell_1 \overset{m}{\mapsto} \mathrm{v}_1\} \uplus \mathrm{H}_{1c} \uplus \mathrm{H}_{1+}, \gamma_{\mathrm{L}3}^{\,1}(\gamma_\Gamma^1(\mathrm{e}_3{}^+))) \xrightarrow{*}_{L_1} \\ (\mathrm{H}'''_{1g} \uplus \mathrm{H}_{1av} \uplus \{\ell_1 \overset{m}{\mapsto} \mathrm{v}_1\} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}^*_{1c}, \mathrm{v}_{1\mathrm{c}}) \nrightarrow\end{array}$$

and, for any H_{2+},

$$\begin{array}{l}(\mathrm{H}''_{2g} \uplus \mathrm{H}_{2av} \uplus \{\ell_2 \overset{m}{\mapsto} \mathrm{v}_2\} \uplus \mathrm{H}_{2c} \uplus \mathrm{H}_{2+}, \gamma_{\mathrm{L}3}^{\,2}(\gamma_\Gamma^2(\mathrm{e}_3{}^+))) \xrightarrow{*}_{L_2} \\ (\mathrm{H}'''_{2g} \uplus \mathrm{H}_{2av} \uplus \{\ell_2 \overset{m}{\mapsto} \mathrm{v}_2\} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}^*_{2c}, \mathrm{v}_{2\mathrm{c}}) \nrightarrow\end{array}$$

where $\mathrm{H}'''_{1g}, \mathrm{H}'''_{2g} : W'''$ for some

$$W'' \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1av} \uplus \mathrm{H}_{1+}), \mathrm{dom}(\mathrm{H}_{2av} \uplus \mathrm{H}_{2+})), \mathrm{rchgclocs}(W'', L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})) \cup FL(\mathrm{cod}(\mathrm{H}_{1av})) \cup FL(\mathrm{v}_1), L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})) \cup FL(\mathrm{cod}(\mathrm{H}_{2av})) \cup FL(\mathrm{v}_2))}$$

and

$$(W''', (\mathrm{H}^*_{1c}, \mathrm{v}_{1\mathrm{c}}), (\mathrm{H}^*_{2c}, \mathrm{v}_{2\mathrm{c}})) \in \mathcal{V}[\![\tau_3]\!]_\rho$$

Thus, the original configuration steps as follows:

$$
\begin{array}{l}
(\mathrm{H}_{1g+} \uplus \mathrm{H}_{1a} \uplus \mathrm{H}_{1b} \uplus \mathrm{H}_{1c} \uplus \mathrm{H}_{1+},\\
\ \mathrm{let}\ \mathrm{x_p} = \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e_2}^{+}))\ \mathrm{in\ let}\ \_ = \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e_1}))\ \mathrm{in\ let}\ \mathrm{x_{v'}} = !\mathrm{x_p}\ \mathrm{in\ let}\ \_ = (\mathrm{x_p} := \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e_3}+)))\ \mathrm{in}\ ((), \mathrm{x_{v'}}) \xrightarrow{*}_{L_1}\\
(\mathrm{H}'_{1g} \uplus \mathrm{H}_{1a} \uplus \mathrm{H}_{1c} \uplus \mathrm{H}_{1+},\\
\ \mathrm{let}\ \mathrm{x_p} = \ell_1\ \mathrm{in\ let}\ \_ = \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e_1}))\ \mathrm{in\ let}\ \mathrm{x_{v'}} = !\mathrm{x_p}\ \mathrm{in\ let}\ \_ = (\mathrm{x_p} := \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e_3}+)))\ \mathrm{in}\ ((), \mathrm{x_{v'}})) \xrightarrow{*}_{L_1}\\
(\mathrm{H}'_{1g} \uplus \mathrm{H}_{1a} \uplus \mathrm{H}_{1c} \uplus \mathrm{H}_{1+},\\
\ \mathrm{let}\ \_ = \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e_1}))\ \mathrm{in\ let}\ \mathrm{x_{v'}} = !\ell_1\ \mathrm{in\ let}\ \_ = (\ell_1 := \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e_3}+)))\ \mathrm{in}\ ((), \mathrm{x_{v'}})) \xrightarrow{*}_{L_1}\\
(\mathrm{H}''_{1g} \uplus \mathrm{H}_{1av} \uplus \{\ell_1 \overset{m}{\mapsto} \mathrm{v_1}\} \uplus \mathrm{H}_{1c} \uplus \mathrm{H}_{1+},\\
\ \mathrm{let}\ \_ = ()\ \mathrm{in\ let}\ \mathrm{x_{v'}} = !\ell_1\ \mathrm{in\ let}\ \_ = (\ell_1 := \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e_3}+)))\ \mathrm{in}\ ((), \mathrm{x_{v'}})) \xrightarrow{*}_{L_1}\\
(\mathrm{H}''_{1g} \uplus \mathrm{H}_{1av} \uplus \{\ell_1 \overset{m}{\mapsto} \mathrm{v_1}\} \uplus \mathrm{H}_{1c} \uplus \mathrm{H}_{1+},\\
\ \mathrm{let}\ \mathrm{x_{v'}} = !\ell_1\ \mathrm{in\ let}\ \_ = (\ell_1 := \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e_3}+)))\ \mathrm{in}\ ((), \mathrm{x_{v'}})) \xrightarrow{*}_{L_1}\\
(\mathrm{H}''_{1g} \uplus \mathrm{H}_{1av} \uplus \{\ell_1 \overset{m}{\mapsto} \mathrm{v_1}\} \uplus \mathrm{H}_{1c} \uplus \mathrm{H}_{1+},\\
\ \mathrm{let}\ \mathrm{x_{v'}} = \ \mathrm{v_1}\ \mathrm{in\ let}\ \_ = (\ell_1 := \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e_3}+)))\ \mathrm{in}\ ((), \mathrm{x_{v'}})) \xrightarrow{*}_{L_1}\\
(\mathrm{H}''_{1g} \uplus \mathrm{H}_{1av} \uplus \{\ell_1 \overset{m}{\mapsto} \mathrm{v_1}\} \uplus \mathrm{H}_{1c} \uplus \mathrm{H}_{1+}, \mathrm{let}\ \_ = (\ell_1 := \gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e_3}+)))\ \mathrm{in}\ ((), \mathrm{v_1})) \xrightarrow{*}_{L_1}\\
(\mathrm{H}'''_{1g} \uplus \mathrm{H}_{1av} \uplus \{\ell_1 \overset{m}{\mapsto} \mathrm{v_1}\} \uplus \mathrm{H}^{*}_{1c} \uplus \mathrm{H}_{1+}, \mathrm{let}\ \_ = (\ell_1 := \mathrm{v_{1c}})\ \mathrm{in}\ ((), \mathrm{v_1})) \xrightarrow{*}_{L_1}\\
(\mathrm{H}'''_{1g} \uplus \mathrm{H}_{1av} \uplus \{\ell_1 \overset{m}{\mapsto} \mathrm{v_{1c}}\} \uplus \mathrm{H}^{*}_{1c} \uplus \mathrm{H}_{1+}, \mathrm{let}\ \_ = ()\ \mathrm{in}\ ((), \mathrm{v_1})) \xrightarrow{*}_{L_1}\\
(\mathrm{H}'''_{1g} \uplus \mathrm{H}_{1av} \uplus \{\ell_1 \overset{m}{\mapsto} \mathrm{v_{1c}}\} \uplus \mathrm{H}^{*}_{1c} \uplus \mathrm{H}_{1+}, ((), \mathrm{v_1})) \nrightarrow
\end{array}
$$

and similarly, on the other side, the configuration steps to:

$$(\mathrm{H}'''_{2g} \uplus \mathrm{H}_{2av} \uplus \{\ell_2 \overset{m}{\mapsto} \mathrm{v_{2c}}\} \uplus \mathrm{H}^{*}_{2c} \uplus \mathrm{H}_{2+}, ((), \mathrm{v_2}))$$

Then, choose $\mathrm{H}_{1'} = \mathrm{H}_{1av} \uplus \{\ell_1 \overset{m}{\mapsto} \mathrm{v_{1c}}\} \uplus \mathrm{H}^{*}_{1c}$, $\mathrm{H}_{2'} = \mathrm{H}_{2av} \uplus \{\ell_2 \overset{m}{\mapsto} \mathrm{v_{2c}}\} \uplus \mathrm{H}^{*}_{2c}$, $W' = W'''$, $\mathrm{H}'_{1g} = \mathrm{H}'''_{1g}$, and $\mathrm{H}'_{2g} = \mathrm{H}'''_{2g}$. First, notice that $W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W'''$ by Lemma 4.6. Then, to finish the proof, we must show that

$$(W''', (\mathrm{H}_{1av} \uplus \{\ell_1 \overset{m}{\mapsto} \mathrm{v_{1c}}\} \uplus \mathrm{H}^{*}_{1c}, ((), \mathrm{v_1})), (\mathrm{H}_{2av} \uplus \{\ell_2 \overset{m}{\mapsto} \mathrm{v_{2c}}\} \uplus \mathrm{H}^{*}_{2c}, ((), \mathrm{v_2}))) \in \mathcal{V}[\![\mathrm{cap}\ \zeta\ \tau_3\ \otimes\ \tau_1]\!]_\rho$$

First, we have $(W''', (\mathrm{H}_{1av}, \mathrm{v_1}), (\mathrm{H}_{2av}, \mathrm{v_2})) \in \mathcal{V}[\![\tau_1]\!]_\rho$ by Lemma 4.7. Thus, it suffices to show:

$$(W''', (\{\ell_1 \overset{m}{\mapsto} \mathrm{v_{1c}}\} \uplus \mathrm{H}^{*}_{1c}, ()), (\{\ell_2 \overset{m}{\mapsto} \mathrm{v_{2c}}\} \uplus \mathrm{H}^{*}_{2c}, \mathrm{v_2})) \in \mathcal{V}[\![\mathrm{cap}\ \zeta\ \tau_3]\!]_\rho$$

This follows from the fact that $\rho.\mathrm{L3}(\zeta) = (\ell_1, \ell_2)$ and that $(W''', (\mathrm{H}^{*}_{1c}, \mathrm{v_{1c}}), (\mathrm{H}^{*}_{2c}, \mathrm{v_{2c}})) \in \mathcal{V}[\![\tau_3]\!]_\rho$, which suffices to finish the proof. □

Lemma 4.45 (Compat $\Lambda\zeta.\mathrm{e}$). *If* $\Delta; \Gamma; \Delta, \zeta; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \tau$, *then*

$$\Delta; \Gamma; \Delta; \Gamma \vdash \Lambda\zeta.\mathrm{e} \preceq \Lambda\zeta.\mathrm{e} : \forall\zeta.\tau$$

Proof. Expanding the conclusion, we must show that given

$$
\begin{array}{l}
\forall \rho, \gamma_\Gamma, \gamma_{\mathrm{L}}, W, \mathrm{H}_1, \mathrm{H}_2.\\
\rho.\mathrm{F} \in \mathcal{D}[\![\Delta]\!] \land \rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!] \land (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho \land (W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}.\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho\\
\land\ \gamma_{\mathrm{L}}.\Delta = \gamma_{\mathrm{locs}}(\rho.\mathrm{L3})
\end{array}
$$

it holds that:

$$(W, (\mathrm{H}_1, \lambda \mathrm{x}_\zeta.\gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e}^{+}))), (\mathrm{H}_2, \lambda \mathrm{x}_\zeta.\gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e}^{+})))) \in \mathcal{E}[\![\forall\zeta.\tau]\!]_\rho$$

By Lemma 4.12, it suffices to show that:

$$(W, (\mathrm{H}_1, \lambda \mathrm{x}_\zeta.\gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e}^{+}))), (\mathrm{H}_2, \lambda \mathrm{x}_\zeta.\gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e}^{+})))) \in \mathcal{V}[\![\forall\zeta.\tau]\!]_\rho$$

By expanding the value relation, for any locations ℓ_1, ℓ_2, we must show

$$(W, (\mathsf{H}_1, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}^+))), (\mathsf{H}_2, \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathsf{e}^+)))) \in \mathcal{E}[\![\tau]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_1,\ell_2)]}$$

Let ρ' be a record such that $\rho'.\mathsf{F} = \rho.\mathsf{F}$ and $\rho'.\mathrm{L3} = \rho.\mathrm{L3}[\zeta \mapsto (\ell_1, \ell_2)]$. It is easy to see $\rho'.\mathrm{L3} \in \mathcal{D}[\![\Delta, \zeta]\!]$, given that $\rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!]$. Thus, we can instantiate the first induction hypothesis with $\rho', \gamma_\Gamma, \gamma_{\mathrm{L}}, W, \mathsf{H}_1, \mathsf{H}_2$, which suffices to show the above statement. □

Lemma 4.46 (Compat $\mathsf{e}\ [\zeta']$). *If* $\Delta; \Gamma; \Delta; \Gamma \vdash \mathsf{e} \preceq \mathsf{e} : \forall\zeta.\tau$ *and* $\zeta' \in \Delta$, *then*

$$\Delta; \Gamma; \Delta; \Gamma \vdash \mathsf{e}\ [\zeta'] \preceq \mathsf{e}\ [\zeta'] : [\zeta \mapsto \zeta']\tau$$

Proof. Expanding the definition of $\preceq$, $\cdot^+$, $\mathcal{E}[\![\cdot]\!]$. and pushing substitutions in the goal, we are to show that

$$\begin{array}{l}
\exists \mathsf{H}'_1, \mathsf{H}'_{1g}.\forall \mathsf{H}_{2+} : \mathit{MHeap}.\exists \mathsf{H}'_2, W', \mathsf{H}'_{2g}, \mathsf{v}_2. \\
\mathsf{H}_{1*} = \mathsf{H}'_{1g} \uplus \mathsf{H}'_1 \uplus \mathsf{H}_{1+}\ \wedge \mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W' \wedge \\
W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathsf{H}_{2+})))}\ W' \wedge \\
(W', (\mathsf{H}'_1, \mathsf{v}_1), (\mathsf{H}'_2, \mathsf{v}_2)) \in \mathcal{V}[\![[\zeta \mapsto \zeta']\tau]\!]_\rho \wedge \\
(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}^+))\ ())\ \overset{*}{\longrightarrow}_{L_2} \\
(\mathsf{H}'_{2g} \uplus \mathsf{H}'_2 \uplus \mathsf{H}_{2+}, \mathsf{v}_2) \not\twoheadrightarrow
\end{array}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_\Gamma, W, L_1, L_2, \mathsf{H}_{1g+}, \mathsf{H}_{2g+} : W, \mathsf{v}_1, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_{1+} : \mathit{MHeap}, \mathsf{H}_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}[\![\Delta]\!], \rho.\mathsf{F} \in \mathcal{D}[\![\Delta]\!], (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho, (W, \mathsf{H}_1, \mathsf{H}_2, \gamma_{\mathrm{L}}.\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho, \gamma_{\mathrm{L}}.\Delta = \gamma_{\mathrm{locs}}(\rho.\mathrm{L3})$$

and

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}^+))\ ())\ \overset{*}{\longrightarrow}_{L_1}\ (\mathsf{H}_{1*}, \mathsf{v}_1) \not\twoheadrightarrow_{L_1}$$

First, we can instantiate the first induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{\mathrm{L}}, \mathsf{H}_1, \mathsf{H}_2$ to find that:

$$(W, (\mathsf{H}_1, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}^+))), (\mathsf{H}_2, \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathsf{e}^+)))) \in \mathcal{E}[\![\forall\zeta.\tau]\!]_\rho$$

Thus, we find

$$(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}^+)))\ \overset{*}{\longrightarrow}_{L_1}\ (\mathsf{H}'_{1g} \uplus \mathsf{H}^*_1 \uplus \mathsf{H}_{1+}, \mathsf{v}^*_1) \not\twoheadrightarrow_{L_1}$$

and

$$(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathsf{e}^+)))\ \overset{*}{\longrightarrow}_{L_2}\ (\mathsf{H}'_{2g} \uplus \mathsf{H}^*_2 \uplus \mathsf{H}_{2+}, \mathsf{v}^*_2) \not\twoheadrightarrow_{L_2}$$

where $\mathsf{H}'_{1g}, \mathsf{H}'_{2g} : W'$ for some $W \sqsubseteq_{(\mathrm{dom}(\mathsf{H}_{1+}),\mathrm{dom}(\mathsf{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathsf{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathsf{H}_{2+})))}\ W'$ and

$$(W', (\mathsf{H}^*_1, \mathsf{v}^*_1), (\mathsf{H}^*_2, \mathsf{v}^*_2)) \in \mathcal{V}[\![\forall\zeta.\tau]\!]_\rho$$

By expanding the value relation, we find $\mathsf{v}^*_1 = \lambda\_.\mathsf{e}^*_{\mathrm{b}}$ and $\mathsf{v}^*_2 = \lambda\_.\mathsf{e}^\dagger_{\mathrm{b}}$ where

$$(W', (\mathsf{H}^*_1, \mathsf{e}^*_{\mathrm{b}}), (\mathsf{H}^*_2, \mathsf{e}^\dagger_{\mathrm{b}})) \in \mathcal{E}[\![\tau]\!]_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_1,\ell_2)]} \tag{54}$$

Ergo, the original configuration steps as follows:

$$\begin{array}{l}
(\mathsf{H}_{1g+} \uplus \mathsf{H}_1 \uplus \mathsf{H}_{1+}, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathsf{e}^+))\ ())\ \overset{*}{\longrightarrow}_{L_1} \\
(\mathsf{H}'_{1g} \uplus \mathsf{H}^*_1 \uplus \mathsf{H}_{1+}, \lambda\_.\mathsf{e}^*_{\mathrm{b}}\ ())\ \overset{*}{\longrightarrow}_{L_1} \\
(\mathsf{H}'_{1g} \uplus \mathsf{H}^*_1 \uplus \mathsf{H}_{1+}, \mathsf{e}^*_{\mathrm{b}})
\end{array}$$

and

$$\begin{array}{l}
(\mathsf{H}_{2g+} \uplus \mathsf{H}_2 \uplus \mathsf{H}_{2+}, \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathsf{e}^+))\ ())\ \overset{*}{\longrightarrow}_{L_2} \\
(\mathsf{H}'_{2g} \uplus \mathsf{H}^*_2 \uplus \mathsf{H}_{2+}, \mathsf{e}^\dagger_{\mathrm{b}})
\end{array}$$

Next, by the fact that the configuration on the left-hand side terminates, we have

$$(\mathsf{H}'_{1g} \uplus \mathsf{H}^*_1 \uplus \mathsf{H}_{1+}, \mathsf{e}^*_{\mathrm{b}})\ \overset{*}{\longrightarrow}_{L_1}\ (\mathsf{H}_{1*}, \mathsf{v}_1) \not\twoheadrightarrow_{L_1}$$

Then, by applying (54), we find that

$$(\mathrm{H}_{1*}, \mathrm{v}_1) = (\mathrm{H}''_{1g} \uplus \mathrm{H}^{**}_1 \uplus \mathrm{H}_{1+}, \mathrm{v}^{\mathrm{f}}_1)$$

and

$$(\mathrm{H}'_{2g} \uplus \mathrm{H}^*_2 \uplus \mathrm{H}_{2+}, \mathrm{e}^{\dagger}_{\mathrm{b}}) \overset{*}{\rightarrow}_{L_2} (\mathrm{H}''_{2g} \uplus \mathrm{H}^{**}_2 \uplus \mathrm{H}_{2+}, \mathrm{v}^{\mathrm{f}}_2) \not\twoheadrightarrow_{L_2}$$

where $\mathrm{H}''_{1g}, \mathrm{H}''_{2g} : W''$ for some $W' \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W',L_1\cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W''$ and

$$(W'', (\mathrm{H}^{**}_1, \mathrm{v}^{\mathrm{f}}_1), (\mathrm{H}^{**}_2, \mathrm{v}^{\mathrm{f}}_2)) \in \mathcal{V}\llbracket\tau\rrbracket_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_1,\ell_2)]}$$

Then, by Lemma 4.10, we find

$$(W'', (\mathrm{H}^{**}_1, \mathrm{v}^{\mathrm{f}}_1), (\mathrm{H}^{**}_2, \mathrm{v}^{\mathrm{f}}_2)) \in \mathcal{V}\llbracket[\zeta \mapsto \zeta']\tau\rrbracket_{\rho}$$

Finally, we can take $\mathrm{H}'_1 = \mathrm{H}^{**}_1$, $\mathrm{H}'_2 = \mathrm{H}^{**}_2$, $W' = W''$, $\mathrm{H}'_{1g} = \mathrm{H}''_{1g}$, and $\mathrm{H}'_{2g} = \mathrm{H}''_{2g}$. Notice that $W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W''$ by Lemma 4.6. This suffices to finish the proof. □

Lemma 4.47 (Compat $\ulcorner\zeta,\ \mathrm{e}\urcorner$). *If* $\Delta;\Gamma;\Delta;\Gamma \vdash \mathrm{e} \preceq \mathrm{e} : [\zeta \mapsto \zeta']\tau$ *, then*

$$\Delta;\Gamma;\Delta;\Gamma \vdash \ulcorner\zeta',\ \mathrm{e}\urcorner \preceq \ulcorner\zeta',\ \mathrm{e}\urcorner : \exists\zeta.\tau$$

Proof. Expanding the definition of $\preceq$, $\cdot^+$, $\mathcal{E}\llbracket\cdot\rrbracket_{\cdot}$ and pushing substitutions in the goal, we are to show that

$$\begin{aligned}
&\exists \mathrm{H}'_1, \mathrm{H}'_{1g}.\forall \mathrm{H}_{2+} : \mathit{MHeap}.\exists \mathrm{H}'_2, W', \mathrm{H}'_{2g}, \mathrm{v}_2.\\
&\mathrm{H}_{1*} = \mathrm{H}'_{1g} \uplus \mathrm{H}'_1 \uplus \mathrm{H}_{1+}\ \wedge \mathrm{H}'_{1g}, \mathrm{H}'_{2g} : W' \wedge\\
&W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W' \wedge\\
&(W', (\mathrm{H}'_1, \mathrm{v}_1), (\mathrm{H}'_2, \mathrm{v}_2)) \in \mathcal{V}\llbracket[\zeta \mapsto \zeta']\tau\rrbracket_{\rho} \wedge\\
&(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathrm{e}^+))) \overset{*}{\rightarrow}_{L_2}\\
&(\mathrm{H}'_{2g} \uplus \mathrm{H}'_2 \uplus \mathrm{H}_{2+}, \mathrm{v}_2) \not\twoheadrightarrow
\end{aligned}$$

given arbitrary $\rho, \gamma_{\mathrm{L}}, \gamma_{\Gamma}, W, L_1, L_2, \mathrm{H}_{1g+}, \mathrm{H}_{2g+} : W, \mathrm{v}_1, \mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_{1+} : \mathit{MHeap}, \mathrm{H}_{1*}$, such that

$$\rho.\mathrm{L3} \in \mathcal{D}\llbracket\Delta\rrbracket, \rho.\mathrm{F} \in \mathcal{D}\llbracket\Delta\rrbracket, (W, \gamma_{\Gamma}) \in \mathcal{G}\llbracket\Gamma\rrbracket_{\rho}, (W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}) \in \mathcal{G}\llbracket\Gamma\rrbracket_{\rho}$$

and

$$(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathrm{e}^+))) \overset{*}{\rightarrow}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \not\twoheadrightarrow_{L_1}$$

First, we can instantiate the first induction hypothesis with $\rho, \gamma_{\Gamma}, \gamma_{\mathrm{L}}, W, \mathrm{H}_1, \mathrm{H}_2$ to find that:

$$(W, (\mathrm{H}_1, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathrm{e}^+))), (\mathrm{H}_2, \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathrm{e}^+)))) \in \mathcal{E}\llbracket[\zeta \mapsto \zeta']\tau\rrbracket_{\rho}$$

Thus, by Lemma 4.3, we find

$$(\mathrm{H}_{1g+} \uplus \mathrm{H}_1 \uplus \mathrm{H}_{1+}, \gamma^1_{\mathrm{L}}(\gamma^1_{\Gamma}(\mathrm{e}^+))) \overset{*}{\rightarrow}_{L_1} (\mathrm{H}'_{1g} \uplus \mathrm{H}^*_1 \uplus \mathrm{H}_{1+}, \mathrm{v}^*_1) \not\twoheadrightarrow_{L_1}$$

and

$$(\mathrm{H}_{2g+} \uplus \mathrm{H}_2 \uplus \mathrm{H}_{2+}, \gamma^2_{\mathrm{L}}(\gamma^2_{\Gamma}(\mathrm{e}^+))) \overset{*}{\rightarrow}_{L_2} (\mathrm{H}'_{2g} \uplus \mathrm{H}^*_2 \uplus \mathrm{H}_{2+}, \mathrm{v}^*_2) \not\twoheadrightarrow_{L_2}$$

where $\mathrm{H}'_{1g}, \mathrm{H}'_{2g} : W'$ for some $W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1\cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2\cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W'$ and

$$(W', (\mathrm{H}^*_1, \mathrm{v}^*_1), (\mathrm{H}^*_2, \mathrm{v}^*_2)) \in \mathcal{V}\llbracket[\zeta \mapsto \zeta']\tau\rrbracket_{\rho}$$

Then, we can take $\mathrm{H}'_1 = \mathrm{H}^*_1$, $\mathrm{H}'_2 = \mathrm{H}^*_2$, $W' = W'$, $\mathrm{H}'_{1g} = \mathrm{H}'_{1g}$, and $\mathrm{H}'_{2g} = \mathrm{H}'_{2g}$. Thus, it suffices to show:

$$(W', (\mathrm{H}^*_1, \mathrm{v}^*_1), (\mathrm{H}^*_2, \mathrm{v}^*_2)) \in \mathcal{V}\llbracket\exists\zeta.\tau\rrbracket_{\rho}$$

By expanding the value relation, it suffices to show:

$$(W', (\mathrm{H}^*_1, \mathrm{v}^*_1), (\mathrm{H}^*_2, \mathrm{v}^*_2)) \in \mathcal{V}\llbracket\tau\rrbracket_{\rho[\mathrm{L3}(\zeta)\mapsto(\ell_1,\ell_2)]}$$

The above statement must hold by Lemma 4.10 because we have that $(W', (H_1^*, v_1^*), (H_2^*, v_2^*)) \in \mathcal{V}[\![[\zeta \mapsto \zeta']\tau]\!]_\rho$ from earlier, which suffices to finish the proof. □

LEMMA 4.48 (COMPAT let $\ulcorner\zeta,\ x\urcorner$). *If* $\Delta; \Gamma; \Delta; \Gamma_1 \vdash e_1 \preceq e_1 : \exists\zeta.\tau_1$, $\Delta; \Gamma; \Delta, \zeta; \Gamma_2, x : \tau_1 \vdash e_2 \preceq e_2 : \tau_2$ *and* $FLV(\tau_2) \subseteq \Delta$, *then*

$$\Delta; \Gamma; \Delta; \Gamma_1 \uplus \Gamma_2 \vdash \text{let } \ulcorner\zeta,\ x\urcorner = e_1 \text{ in } e_2 \preceq \text{let } \ulcorner\zeta,\ x\urcorner = e_1 \text{ in } e_2 : \tau_2$$

PROOF. Expanding the definition of $\preceq$, $\cdot^+$, $\mathcal{E}[\![\cdot]\!]_\cdot$ and pushing substitutions in the goal, we are to show that

$$\begin{array}{l}
\exists H_1', H_{1g}'.\forall H_{2+} : \mathit{MHeap}.\exists H_2', W', H_{2g}', v_2. \\
H_{1*} = H_{1g}' \uplus H_1' \uplus H_{1+} \ \wedge H_{1g}', H_{2g}' : W' \wedge \\
W \sqsubseteq_{(\mathrm{dom}(H_{1+}), \mathrm{dom}(H_{2+})), \mathrm{rchgclocs}(W, L_1 \cup FL(\mathrm{cod}(H_{1+})), L_2 \cup FL(\mathrm{cod}(H_{2+})))} W' \wedge \\
(W', (H_1', v_1), (H_2', v_2)) \in \mathcal{V}[\![\tau_2]\!]_\rho \wedge \\
(H_{2g+} \uplus H_2 \uplus H_{2+}, \text{let } x = \gamma_L^2(\gamma_{`}^2(e_1{}^+)) \text{ in } \gamma_L^2(\gamma_{`}^2(e_2{}^+))) \overset{*}{\longrightarrow}_{L_2} \\
(H_{2g}' \uplus H_2' \uplus H_{2+}, v_2) \nrightarrow
\end{array}$$

given arbitrary $\rho, \gamma_L, \gamma_\Gamma, W, L_1, L_2, H_{1g+}, H_{2g+} : W, v_1, H_1, H_2, H_{1+} : \mathit{MHeap}, H_{1*}$, such that

$$\rho.L3 \in \mathcal{D}[\![\Delta]\!], \rho.F \in \mathcal{D}[\![\Delta]\!], (W, \gamma_\Gamma) \in \mathcal{G}[\![\Gamma]\!]_\rho, (W, H_1, H_2, \gamma_L) \in \mathcal{G}[\![\Gamma_1 \uplus \Gamma_2]\!]_\rho$$

and

$$(H_{1g+} \uplus H_1 \uplus H_{1+}, \text{let } x = \gamma_L^1(\gamma_{`}^1(e_1{}^+)) \text{ in } \gamma_L^1(\gamma_{`}^1(e_2{}^+))) \overset{*}{\longrightarrow}_{L_1} (H_{1*}, v_1) \nrightarrow_{L_1}$$

Then, by Lemma 4.13, there exist $\gamma_{L_1}, \gamma_{L_2}, H_{1l}, H_{1r}, H_{2l}, H_{2r}$ such that $\gamma_L = \gamma_{L_1} \uplus \gamma_{L_2}$, $H_1 = H_{1l} \uplus H_{1r}$, $H_2 = H_{2l} \uplus H_{2r}$,

$$\begin{array}{c}
(W, H_{1l}, H_{2l}, \gamma_{L_1}) \in \mathcal{G}[\![\Gamma_1]\!]_\rho \\
(W, H_{1r}, H_{2r}, \gamma_{L_2}) \in \mathcal{G}[\![\Gamma_2]\!]_\rho
\end{array}$$

and for all $j \in \{1, 2\}$,

$$\begin{array}{c}
\gamma_L^j(\gamma_\Gamma^j(e_1{}^+)) = \gamma_{L_1}^{\ j}(\gamma_\Gamma^j(e_1{}^+)) \\
\gamma_L^j(\gamma_\Gamma^j(e_2{}^+)) = \gamma_{L_2}^{\ j}(\gamma_\Gamma^j(e_2{}^+))
\end{array}$$

Then, by instantiating the first induction hypothesis with $\rho, \gamma_\Gamma, \gamma_{L_1}, W, H_{1l}, H_{2l}$, we find

$$(W, (H_{1l}, \gamma_{L_1}^{\ 1}(\gamma_\Gamma^1(e_1{}^+))), (H_{2l}, \gamma_{L_1}^{\ 2}(\gamma_\Gamma^2(e_1{}^+)))) \in \mathcal{E}[\![\exists\zeta.\tau_1]\!]_\rho$$

Thus, by Lemma 4.3, we have

$$(H_{1g+} \uplus H_{1l} \uplus H_{1r} \uplus H_{1+}, \gamma_{L_1}^{\ 1}(\gamma_\Gamma^1(e_1{}^+))) \overset{*}{\longrightarrow}_{L_1 \cup FL(\gamma_{L_2}^{\ 1}(\gamma_\Gamma^1(e_2{}^+)))} (H_{1g}' \uplus H_{1r} \uplus H_{1l}^* \uplus H_{1+}, v_1^*) \nrightarrow$$

and, for any H_{2+},

$$(H_{1g+} \uplus H_{2l} \uplus H_{2r} \uplus H_{2+}, \gamma_{L_1}^{\ 2}(\gamma_\Gamma^2(e_1{}^+))) \overset{*}{\longrightarrow}_{L_2 \cup FL(\gamma_{L_2}^{\ 2}(\gamma_\Gamma^2(e_2{}^+)))} (H_{1g}' \uplus H_{2r} \uplus H_{2l}^* \uplus H_{2+}, v_2^*) \nrightarrow$$

where $H_{1g}', H_{2g}' : W'$ for some

$$W \sqsubseteq_{\substack{(\mathrm{dom}(H_{1r} \uplus H_{1+}), \mathrm{dom}(H_{2r} \uplus H_{2+})), \mathrm{rchgclocs}(W, FL(\mathrm{cod}(H_{1r})) \cup FL(\mathrm{cod}(H_{1+})) \cup FL(\gamma_{L_2}^{\ 1}(\gamma_\Gamma^1(e_2{}^+))) \cup L_1, \\ FL(\mathrm{cod}(H_{2r})) \cup FL(\mathrm{cod}(H_{2+})) \cup FL(\gamma_{L_2}^{\ 2}(\gamma_\Gamma^2(e_2{}^+))) \cup L_2)}} W'$$

and

$$(W', (H_{1l}^*, v_1^*), (H_{2l}^*, v_2^*)) \in \mathcal{V}[\![\exists\zeta.\tau_1]\!]_\rho$$

By expanding the value relation, we find there exist locations ℓ_1, ℓ_2 such that, for any $i \in \{1, 2\}$,

$$(W', (H_{1l}^*, v_1^*), (H_{2l}^*, v_2^*)) \in \mathcal{V}[\![\tau_1]\!]_{\rho[L3(\zeta) \mapsto (\ell_1, \ell_2)]}$$

Thus, the original configuration steps as follows:

$$\begin{aligned}&(\mathrm{H}_{1g+} \uplus \mathrm{H}_{1l} \uplus \mathrm{H}_{1r} \uplus \mathrm{H}_{1+}, \mathsf{let}\ \mathrm{x} = \gamma_{\mathrm{L}}^{1}(\gamma_{\cdot}^{1}(\mathrm{e_1}^{+}))\ \mathsf{in}\ \gamma_{\mathrm{L}}^{1}(\gamma_{\cdot}^{1}(\mathrm{e_2}^{+}))) \xrightarrow{*}_{L_1}\\ &(\mathrm{H}'_{1g} \uplus \mathrm{H}_{1r} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}^{*}_{1l}, \mathsf{let}\ \mathrm{x} = \mathrm{v}_1^{*}\ \mathsf{in}\ \gamma_{\mathrm{L}}^{1}(\gamma_{\cdot}^{1}(\mathrm{e_2}^{+}))) \xrightarrow{*}_{L_1}\\ &(\mathrm{H}'_{1g} \uplus \mathrm{H}_{1r} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}^{*}_{1l}, [\mathrm{x} \mapsto \mathrm{v}_1^{*}]\gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e_2}^{+})))\end{aligned}$$

and similarly

$$\begin{aligned}&(\mathrm{H}_{1g+} \uplus \mathrm{H}_{2l} \uplus \mathrm{H}_{2r} \uplus \mathrm{H}_{2+}, \mathsf{let}\ \mathrm{x} = \gamma_{\mathrm{L}}^{2}(\gamma_{\cdot}^{2}(\mathrm{e_1}^{+}))\ \mathsf{in}\ \gamma_{\mathrm{L}}^{2}(\gamma_{\cdot}^{2}(\mathrm{e_2}^{+}))) \xrightarrow{*}_{L_2}\\ &(\mathrm{H}'_{1g} \uplus \mathrm{H}_{2r} \uplus \mathrm{H}_{2+} \uplus \mathrm{H}^{*}_{2l}, [\mathrm{x} \mapsto \mathrm{v}_2^{*}]\gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e_2}^{+})))\end{aligned}$$

Let $\gamma_{\mathrm{L}2}' = \gamma_{\mathrm{L}2}[\mathrm{x} \mapsto (\mathrm{v}_1^{*}, \mathrm{v}_2^{*})]$.

First, one can see that

$$(W', \mathrm{H}_{1r} \uplus \mathrm{H}^{*}_{1l}, \mathrm{H}_{2r} \uplus \mathrm{H}^{*}_{2l}, \gamma_{\mathrm{L}2}') \in \mathcal{G}\llbracket \Gamma_1, \mathrm{x} : \tau_1 \rrbracket_{\rho[\mathrm{L3}(\zeta) \mapsto (\ell_1, \ell_2)]}$$

because $(W', (\mathrm{H}^{*}_{1l}, \mathrm{v}_1^{*}), (\mathrm{H}^{*}_{2l}, \mathrm{v}_2^{*})) \in \mathcal{V}\llbracket \tau_1 \rrbracket_{\rho[\mathrm{L3}(\zeta) \mapsto (\ell_1, \ell_2)]}$ and $(W', \mathrm{H}_{1r}, \mathrm{H}_{2r}, \gamma_{\mathrm{L}2}) \in \mathcal{G}\llbracket \Gamma_2 \rrbracket_{\rho}$ (by Lemma 4.7, and extending ρ with ζ does not invalidate any atoms in the substitution).

Thus, since $\mathcal{G}\llbracket \Gamma \rrbracket_{\rho}, \mathcal{G}\llbracket \Gamma_1 \uplus \Gamma_2 \rrbracket_{\rho}$ are closed under world extension by Lemma 4.7, we can instantiate the second induction hypothesis with $\rho[\mathrm{L3}(\zeta) \mapsto (\ell_1, \ell_2)], \gamma_{\Gamma}, \gamma_{\mathrm{L}2}', W', \mathrm{H}_{1r} \uplus \mathrm{H}^{*}_{1l}, \mathrm{H}_{2r} \uplus \mathrm{H}^{*}_{2l}$ to find

$$(W', (\mathrm{H}_{1r} \uplus \mathrm{H}^{*}_{1l}, [\mathrm{x} \mapsto \mathrm{v}_1^{*}]\gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e_2}^{+}))), (\mathrm{H}_{2r} \uplus \mathrm{H}^{*}_{2l}, [\mathrm{x} \mapsto \mathrm{v}_2^{*}]\gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e_2}^{+})))) \in \mathcal{E}\llbracket \tau_2 \rrbracket_{\rho[\mathrm{L3}(\zeta) \mapsto (\ell_1, \ell_2)]} \tag{55}$$

Next, by the assumption that the configuration on the left-hand side terminates, we have

$$(\mathrm{H}'_{1g} \uplus \mathrm{H}_{1+} \uplus \mathrm{H}_{1r} \uplus \mathrm{H}^{*}_{1l}, [\mathrm{x} \mapsto \mathrm{v}_1^{*}]\gamma_{\mathrm{L}}^{1}(\gamma_{\Gamma}^{1}(\mathrm{e_2}^{+}))) \xrightarrow{*}_{L_1} (\mathrm{H}_{1*}, \mathrm{v}_1) \not\twoheadrightarrow_{L_1}$$

Ergo, by applying (55), we have

$$(\mathrm{H}_{1*}, \mathrm{v}_1) = (\mathrm{H}''_{1g} \uplus \mathrm{H}_{1f} \uplus \mathrm{H}_{1+}, \mathrm{v}_1^{\mathrm{f}})$$

and

$$(\mathrm{H}'_{2g} \uplus \mathrm{H}_{2r} \uplus \mathrm{H}^{*}_{2l} \uplus \mathrm{H}_{2+}, [\mathrm{x} \mapsto \mathrm{v}_2^{*}]\gamma_{\mathrm{L}}^{2}(\gamma_{\Gamma}^{2}(\mathrm{e_2}^{+}))) \xrightarrow{*}_{L_2} (\mathrm{H}''_{2g} \uplus \mathrm{H}_{2f} \uplus \mathrm{H}_{2+}, \mathrm{v}_2^{\mathrm{f}}) \not\twoheadrightarrow_{L_2}$$

where $\mathrm{H}''_{1g}, \mathrm{H}''_{2g} : W''$ for some $W' \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W',L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W''$ and

$$(W'', (\mathrm{H}_{1f}, \mathrm{v}_1^{\mathrm{f}}), (\mathrm{H}_{2f}, \mathrm{v}_2^{\mathrm{f}}) {\in} \mathcal{V}\llbracket \tau_2 \rrbracket_{\rho[\mathrm{L3}(\zeta) \mapsto (\ell_1, \ell_2)]}$$

Then, by Lemma 4.11, since $FLV(\tau_2) \subseteq \Delta$,

$$(W'', (\mathrm{H}_{1f}, \mathrm{v}_1^{\mathrm{f}}), (\mathrm{H}_{2f}, \mathrm{v}_2^{\mathrm{f}})) \in \mathcal{V}\llbracket \tau_2 \rrbracket_{\rho}$$

Finally, we can take $\mathrm{H}'_1 = \mathrm{H}_{1f}$, $\mathrm{H}'_2 = \mathrm{H}_{2f}$, $W' = W''$, $\mathrm{H}'_{1g} = \mathrm{H}''_{1g}$, and $\mathrm{H}'_{2g} = \mathrm{H}''_{2g}$. Notice that $W \sqsubseteq_{(\mathrm{dom}(\mathrm{H}_{1+}),\mathrm{dom}(\mathrm{H}_{2+})),\mathrm{rchgclocs}(W,L_1 \cup FL(\mathrm{cod}(\mathrm{H}_{1+})),L_2 \cup FL(\mathrm{cod}(\mathrm{H}_{2+})))} W''$ by Lemma 4.6. This suffices to finish the proof. □

Lemma 4.49 (Compat $\llparenthesis \mathrm{e} \rrparenthesis_{\tau}$). *If* $\Delta; !\Gamma; \Delta; \Gamma \vdash \mathrm{e} \preceq \mathrm{e} : \tau$ *and* $\tau \sim \tau$ *, then*

$$\Delta; \Gamma; \Delta; !\Gamma \vdash \llparenthesis \mathrm{e} \rrparenthesis_{\tau} \preceq \llparenthesis \mathrm{e} \rrparenthesis_{\tau} : \tau$$

Proof. Expanding the definition of $\preceq$ and $\cdot^{+}$ and pushing substitutions in the goal, we are to show that

$$(W, (\mathrm{H}_1, C_{\tau \mapsto \tau}(\gamma_{\Gamma}^{1}(\gamma_{\mathrm{L}}^{1}(\mathrm{e}^{+})))), (\mathrm{H}_2, C_{\tau \mapsto \tau}(\gamma_{\Gamma}^{2}(\gamma_{\mathrm{L}}^{2}(\mathrm{e}^{+}))))) \in \mathcal{E}\llbracket \tau \rrbracket_{\rho} \tag{56}$$

given $\rho, \gamma_{\Gamma}, \gamma_{\mathrm{L}}, W, \mathrm{H}_1, \mathrm{H}_2$ such that

$$\rho.\mathrm{F} \in \mathcal{D}\llbracket \Delta \rrbracket, \rho.\mathrm{L3} \in \mathcal{D}\llbracket \Delta \rrbracket, (W, \gamma_{\Gamma}) \in \mathcal{G}\llbracket \Gamma \rrbracket_{\rho}, (W, \mathrm{H}_1, \mathrm{H}_2, \gamma_{\mathrm{L}}.\Gamma) \in \mathcal{G}\llbracket !\Gamma \rrbracket_{\rho}, \gamma_{\mathrm{L}}.\Delta = \gamma_{\mathrm{locs}}(\rho.\mathrm{L3})$$

Our first induction hypothesis, appropriately instantiated, tells us that:

$$(W, (\mathsf{H}_1, \gamma_{\Gamma}^{1}(\gamma_{\mathrm{L}}^{1}(\mathsf{e}^{+}))), (\mathsf{H}_2, \gamma_{\Gamma}^{2}(\gamma_{\mathrm{L}}^{2}(\mathsf{e}^{+})))) \in \mathcal{E}[\![\tau]\!]_{\rho}$$

Since $\tau \sim \tau$, we have (56) by Theorem 4.4. □