The Marriage of Bisimulations and Kripke Logical Relations

Technical Appendix

Chung-Kil Hur   Derek Dreyer   Georg Neis   Viktor Vafeiadis
Max Planck Institute for Software Systems (MPI-SWS)
{gil,dreyer,neis,viktor}@mpi-sws.org

November 2011

Contents

Part I
Relation Transition Systems for the Full Language

1 Language

We define the language $\mathsf{F}^{\mu!}$.

1.1 Syntax

$$
\begin{array}{lll}
\ell \in \mathrm{Loc} & & \\
x \in \mathrm{Var} & & \\
\alpha \in \mathrm{TypeVar} & & \\
\sigma \in \mathrm{Typ} & ::= & \alpha \mid \mathsf{unit} \mid \mathsf{int} \mid \mathsf{bool} \mid \sigma_1 \times \sigma_2 \mid \sigma_1 + \sigma_2 \mid \sigma_1 \to \sigma_2 \mid \mu\alpha.\,\sigma \mid \forall\alpha.\,\sigma \mid \exists\alpha.\,\sigma \mid \mathsf{ref}\,\sigma \\
v \in \mathrm{Val} & ::= & x \mid \langle\rangle \mid n \mid \mathsf{tt} \mid \mathsf{ff} \mid \langle v_1, v_2\rangle \mid \mathsf{inj}^1\, v \mid \mathsf{inj}^2\, v \mid \mathsf{roll}\ v \mid \\
& & \mathsf{fix}\, f(x).\, e \mid \Lambda.\, e \mid \mathsf{pack}\ v \mid \ell \\
e \in \mathrm{Exp} & ::= & v \mid \mathsf{if}\ e_0\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 \mid \langle e_1, e_2\rangle \mid e.1 \mid e.2 \mid \mathsf{inj}^1\, e \mid \mathsf{inj}^2\, e \mid \\
& & (\mathsf{case}\, e\, \mathsf{of}\ \mathsf{inj}^1\, x \Rightarrow e_1 \,|\, \mathsf{inj}^2\, x \Rightarrow e_2) \mid \mathsf{roll}\ e \mid \mathsf{unroll}\ e \mid e_1\ e_2 \mid e[] \mid \mathsf{pack}\ e \mid \\
& & \mathsf{unpack}\ e_1\ \mathsf{as}\ x\ \mathsf{in}\ e_2 \mid \mathsf{ref}\ e \mid\ !e \mid e_1 := e_2 \mid e_1 == e_2 \\
K \in \mathrm{Cont} & ::= & \bullet \mid \mathsf{if}\ K\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 \mid \langle K, e\rangle \mid \langle v, K\rangle \mid K.1 \mid K.2 \mid \mathsf{inj}^1\, K \mid \mathsf{inj}^2\, K \mid \\
& & \mathsf{case}\, K\, \mathsf{of}\, [\mathsf{inj}^i\, x \Rightarrow e_i] \mid \mathsf{roll}\ K \mid \mathsf{unroll}\ K \mid K\ e \mid v\ K \mid K[] \mid \mathsf{pack}\ K \mid \\
& & \mathsf{unpack}\ K\ \mathsf{as}\ x\ \mathsf{in}\ e \mid \mathsf{ref}\ K \mid\ !K \mid K := e \mid v := K \mid K == e \mid v == K \\
p \in \mathrm{Prog} & ::= & x \mid \langle\rangle \mid n \mid \mathsf{tt} \mid \mathsf{ff} \mid \mathsf{if}\ p_0\ \mathsf{then}\ p_1\ \mathsf{else}\ p_2 \mid \langle p_1, p_2\rangle \mid p.1 \mid p.2 \mid \mathsf{inj}^1_\sigma\, p \mid \mathsf{inj}^2_\sigma\, p \mid \\
& & (\mathsf{case}\, p\, \mathsf{of}\ \mathsf{inj}^1\, x \Rightarrow p_1 \,|\, \mathsf{inj}^2\, x \Rightarrow p_2) \mid \mathsf{roll}_\sigma\ p \mid \mathsf{unroll}\ p \mid \mathsf{fix}\, f(x{:}\sigma_1){:}\sigma_2.\, p \mid p_1\ p_2 \mid \Lambda\alpha.\, p \mid \\
& & p[\sigma] \mid \mathsf{pack}\ \langle\sigma, p\rangle\ \mathsf{as}\ \exists\alpha.\,\sigma' \mid \mathsf{unpack}\ p_1\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ p_2 \mid \mathsf{ref}\ p \mid\ !p \mid p_1 := p_2 \mid p_1 == p_2 \\
h \in \mathrm{Heap} & := & \mathrm{Loc} \stackrel{\text{fin}}{\rightharpoonup} \mathrm{CVal}
\end{array}
$$

1.2 Dynamic Semantics

$$
\begin{array}{rcll}
h, \mathsf{if}\ \mathsf{tt}\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 & \hookrightarrow & h, e_1 & \\
h, \mathsf{if}\ \mathsf{ff}\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 & \hookrightarrow & h, e_2 & \\
h, \langle v_1, v_2\rangle.i & \hookrightarrow & h, v_i & \\
h, \mathsf{case}\, \mathsf{inj}^j\ v\, \mathsf{of}\, [\mathsf{inj}^i\, x \Rightarrow e_i] & \hookrightarrow & h, e_j[v/x] & \\
h, (\mathsf{fix}\, f(x).\, e)\ v & \hookrightarrow & h, e[(\mathsf{fix}\, f(x).\, e)/f, v/x] & \\
h, (\Lambda.\, e)[] & \hookrightarrow & h, e & \\
h, \mathsf{unpack}\ (\mathsf{pack}\ v)\ \mathsf{as}\ x\ \mathsf{in}\ e & \hookrightarrow & h, e[v/x] & \\
h, \mathsf{unroll}\ (\mathsf{roll}\ v) & \hookrightarrow & h, v & \\
h, \mathsf{ref}\ v & \hookrightarrow & h \uplus [\ell{\mapsto}v], \ell & \text{where } \ell \notin \mathrm{dom}(h) \\
h \uplus [\ell{\mapsto}v], !\ell & \hookrightarrow & h \uplus [\ell{\mapsto}v], v & \\
h \uplus [\ell{\mapsto}v], \ell := v' & \hookrightarrow & h \uplus [\ell{\mapsto}v'], \langle\rangle & \\
h, \ell == \ell & \hookrightarrow & h, \mathsf{tt} & \\
h, \ell == \ell' & \hookrightarrow & h, \mathsf{ff} & \text{where } \ell \neq \ell' \\
h, K[e] & \hookrightarrow & h', K[e'] & \text{where } h, e \hookrightarrow h', e'
\end{array}
$$

1.3 Static Semantics

$$
\begin{array}{lccl}
\text{Type environments} & \Delta & ::= & \cdot \mid \Delta, \alpha \\
\text{Term environments} & \Gamma & ::= & \cdot \mid \Gamma, x{:}\sigma
\end{array}
$$

$\boxed{\Delta \vdash \sigma}$

$$\frac{\mathrm{fv}(\sigma) \subseteq \Delta \quad \mathrm{names}(\sigma) = \emptyset}{\Delta \vdash \sigma}$$

$\boxed{\Delta \vdash \Gamma}$

$$\frac{\forall x{:}\sigma \in \Gamma.\ \Delta \vdash \sigma}{\Delta \vdash \Gamma}$$

$\boxed{\Delta; \Gamma \vdash p : \sigma}$

$$\frac{\Delta \vdash \Gamma \quad x{:}\sigma \in \Gamma}{\Delta; \Gamma \vdash x : \sigma} \qquad \frac{\Delta \vdash \Gamma}{\Delta; \Gamma \vdash c : \tau_{\mathrm{base}}}$$

$$\frac{\Delta; \Gamma \vdash p_1 : \sigma_1 \quad \Delta; \Gamma \vdash p_2 : \sigma_2}{\Delta; \Gamma \vdash \langle p_1, p_2 \rangle : \sigma_1 \times \sigma_2} \qquad \frac{\Delta; \Gamma \vdash p : \sigma_1 \times \sigma_2}{\Delta; \Gamma \vdash p.1 : \sigma_1} \qquad \frac{\Delta; \Gamma \vdash p : \sigma_1 \times \sigma_2}{\Delta; \Gamma \vdash p.2 : \sigma_2}$$

$$\frac{\Delta; \Gamma, x{:}\sigma_1 \vdash p : \sigma_2}{\Delta; \Gamma \vdash \lambda x{:}\sigma_1.\, p : \sigma_1 \to \sigma_2} \qquad \frac{\Delta; \Gamma \vdash p_1 : \sigma_1 \to \sigma_2 \quad \Delta; \Gamma \vdash p_2 : \sigma_1}{\Delta; \Gamma \vdash p_1\ p_2 : \sigma_2}$$

$$\frac{\Delta, \alpha; \Gamma \vdash p : \sigma}{\Delta; \Gamma \vdash \Lambda\alpha.\, p : \forall\alpha.\, \sigma} \qquad \frac{\Delta; \Gamma \vdash p : \forall\alpha.\, \sigma_1 \quad \Delta \vdash \sigma_2}{\Delta; \Gamma \vdash p[\sigma_2] : \sigma_1[\sigma_2/\alpha]}$$

$$\frac{\Delta \vdash \sigma_1 \quad \Delta; \Gamma \vdash p : \sigma_2[\sigma_1/\alpha]}{\Delta; \Gamma \vdash \mathsf{pack}\ \langle \sigma_1, p \rangle\ \mathsf{as}\ \exists\alpha.\, \sigma_2 : \exists\alpha.\, \sigma_2} \qquad \frac{\Delta; \Gamma \vdash p_1 : \exists\alpha.\, \sigma_1 \quad \Delta, \alpha; \Gamma, x{:}\sigma_1 \vdash p_2 : \sigma_2 \quad \Delta \vdash \sigma_2}{\Delta; \Gamma \vdash \mathsf{unpack}\ p_1\ \mathsf{as}\ \langle \alpha, x \rangle\ \mathsf{in}\ p_2 : \sigma_2}$$

$$\frac{\Delta; \Gamma \vdash p : \sigma[\mu\alpha.\, \sigma/\alpha]}{\Delta; \Gamma \vdash \mathsf{roll}_{\mu\alpha.\, \sigma}\ p : \mu\alpha.\, \sigma} \qquad \frac{\Delta; \Gamma \vdash p : \mu\alpha.\, \sigma}{\Delta; \Gamma \vdash \mathsf{unroll}\ p : \sigma[\mu\alpha.\, \sigma/\alpha]}$$

$$\frac{\Delta; \Gamma \vdash p : \sigma}{\Delta; \Gamma \vdash \mathsf{ref}\ p : \mathsf{ref}\ \sigma} \qquad \frac{\Delta; \Gamma \vdash p_1 : \mathsf{ref}\ \sigma \quad \Delta; \Gamma \vdash p_2 : \sigma}{\Delta; \Gamma \vdash p_1 := p_2 : \mathsf{unit}}$$

$$\frac{\Delta; \Gamma \vdash p : \mathsf{ref}\ \sigma}{\Delta; \Gamma \vdash {!p} : \sigma} \qquad \frac{\Delta; \Gamma \vdash p_1 : \mathsf{ref}\ \sigma \quad \Delta; \Gamma \vdash p_2 : \mathsf{ref}\ \sigma}{\Delta; \Gamma \vdash p_1 == p_2 : \mathsf{bool}}$$

$$\dots$$

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

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

$$\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1) \quad \Delta'; \Gamma' \vdash p_2 : \sigma_2}{\vdash \langle C, p_2 \rangle : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1 \times \sigma_2)}$$

$$\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1 \times \sigma_2)}{\vdash C.1 : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1)} \qquad \frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1 \times \sigma_2)}{\vdash C.2 : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_2)}$$

$$\frac{\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma', x{:}\sigma_1; \sigma_2)}{\vdash \lambda x{:}\sigma_1.\, C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma_1 \to \sigma_2)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1 \to \sigma_2) \quad \Delta';\Gamma' \vdash p_2 : \sigma_1}{\vdash C\ p_2 : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_2)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1) \quad \Delta';\Gamma' \vdash p_1 : \sigma_1 \to \sigma_2}{\vdash p_1\ C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_2)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta',\alpha;\Gamma';\sigma_1)}{\vdash \Lambda\alpha.\, C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\forall\alpha.\,\sigma_1)} \qquad \frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\forall\alpha.\,\sigma_1)}{\vdash C[\sigma_2] : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1[\sigma_2/\alpha])}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_2[\sigma_1/\alpha])}{\vdash \mathsf{pack}\ \langle\sigma_1, C\rangle\ \mathsf{as}\ \exists\alpha.\,\sigma_2 : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\exists\alpha.\,\sigma_2)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\exists\alpha.\,\sigma_1) \quad \Delta',\alpha;\Gamma',x{:}\sigma_1 \vdash p_2 : \sigma_2 \quad \Delta' \vdash \sigma_2}{\vdash \mathsf{unpack}\ C\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ p_2 : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_2)}$$

$$\frac{\Delta';\Gamma' \vdash p_1 : \exists\alpha.\,\sigma_1 \quad \vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta',\alpha;\Gamma',x{:}\sigma_1;\sigma_2) \quad \Delta' \vdash \sigma_2}{\vdash \mathsf{unpack}\ p_1\ \mathsf{as}\ \langle\alpha, x\rangle\ \mathsf{in}\ C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_2)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1[\mu\alpha.\,\sigma_1/\alpha])}{\vdash \mathsf{roll}_{\mu\alpha.\,\sigma_1}\ C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mu\alpha.\,\sigma_1)}$$
$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mu\alpha.\,\sigma_1)}{\vdash \mathsf{unroll}\ C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1[\mu\alpha.\,\sigma_1/\alpha])}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1)}{\vdash \mathsf{ref}\ C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{ref}\,\sigma_1)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{ref}\,\sigma_1) \quad \Delta';\Gamma' \vdash p_2 : \sigma_1}{\vdash C := p_2 : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{unit})}$$

$$\frac{\Delta';\Gamma' \vdash p_1 : \mathsf{ref}\,\sigma_1 \quad \vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1)}{\vdash p_1 := C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{unit})}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{ref}\,\sigma_1)}{\vdash\ !C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\sigma_1)}$$

$$\frac{\vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{ref}\,\sigma_1) \quad \Delta';\Gamma' \vdash p_2 : \mathsf{ref}\,\sigma_1}{\vdash C == p_2 : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{bool})}$$

$$\frac{\Delta';\Gamma' \vdash p_1 : \mathsf{ref}\,\sigma_1 \quad \vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{ref}\,\sigma_1)}{\vdash p_1 == C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\Delta';\Gamma';\mathsf{bool})}$$

$$\ldots$$

1.4 Contextual Equivalence

Definition 1 (Contextual equivalence)**.**
Let $\Delta;\Gamma \vdash p_1 : \sigma$ and $\Delta;\Gamma \vdash p_2 : \sigma$. Then:
$\Delta;\Gamma \vdash p_1 \sim_{\text{ctx}} p_2 : \sigma := \forall C, h, \tau.\ \vdash C : (\Delta;\Gamma;\sigma) \rightsquigarrow (\cdot;\cdot;\tau) \Longrightarrow (h, |C[p_1]| \uparrow \Longleftrightarrow\ h, |C[p_2]| \uparrow)$

2 Model

2.1 Definitions

Various Relations.

$$\begin{array}{lll} \mathit{beta}(e) & := & \begin{cases} e' & \text{if } \forall h.\ h, e \hookrightarrow^1 h, e' \\ \text{undef} & \text{otherwise} \end{cases} \\ \text{FunVal} & := & \{\, f \in \text{CVal} \mid \forall v.\ \mathit{beta}(f\ v) \text{ defined} \,\} \\ \text{TyFunVal} & := & \{\, v \in \text{CVal} \mid \mathit{beta}(v[]) \text{ defined} \,\} \end{array}$$

$$\begin{array}{lll} \mathbf{n} \in \text{TypeName} & & \\ \text{Names} & := & \{\, \mathcal{N} \in \mathbb{P}(\text{TypeName}) \mid \mathcal{N} \text{ is countably infinite} \,\} \\ \sigma \in \text{Type} & ::= & \mathbf{n} \mid \alpha \mid \mathsf{unit} \mid \mathsf{int} \mid \mathsf{bool} \mid \sigma_1 \times \sigma_2 \mid \sigma_1 + \sigma_2 \mid \sigma_1 \to \sigma_2 \mid \mu\alpha.\,\sigma \mid \forall\alpha.\,\sigma \mid \exists\alpha.\,\sigma \mid \mathsf{ref}\,\sigma \\ \text{CType} & := & \{\, \tau \in \text{Type} \mid \text{ftv}(\tau) = \emptyset \,\} \\ \text{CTypeF} & := & \{\, (\tau_1 \to \tau_2) \in \text{CType} \,\} \cup \{\, \mathsf{ref}\,\tau \in \text{CType} \,\} \cup \{\, (\forall\alpha.\,\sigma) \in \text{CType} \,\} \cup \text{TypeName} \\ \text{VRelF} & := & \text{CTypeF} \to \mathbb{P}(\text{CVal} \times \text{CVal}) \\ \text{VRel} & := & \text{CType} \to \mathbb{P}(\text{CVal} \times \text{CVal}) \\ \text{ERel} & := & \text{CType} \to \mathbb{P}(\text{CExp} \times \text{CExp}) \\ \text{KRel} & := & \text{CType} \times \text{CType} \to \mathbb{P}(\text{CCont} \times \text{CCont}) \\ \text{HRel} & := & \mathbb{P}(\text{Heap} \times \text{Heap}) \end{array}$$

Note that as a notational convention we use σ to range over possibly open types and τ over closed types.

Value Closure. We define the closure $\overline{R} \in \text{VRel}$ for $R \in \text{VRelF}$ as the least fixpoint of the following equation.

$$\begin{array}{lll} \overline{R}(\tau_{\text{base}}) & := & \text{ID}_{\tau_{\text{base}}} \\ \overline{R}(\tau_1 \times \tau_2) & := & \{\, ((v_1, v_1'), (v_2, v_2')) \mid (v_1, v_2) \in \overline{R}(\tau_1) \wedge (v_1', v_2') \in \overline{R}(\tau_2) \,\} \\ \overline{R}(\tau_1 + \tau_2) & := & \{\, (\mathsf{inj}^1\, v_1, \mathsf{inj}^1\, v_2) \mid (v_1, v_2) \in \overline{R}(\tau_1) \,\} \cup \{\, (\mathsf{inj}^2\, v_1, \mathsf{inj}^2\, v_2) \mid (v_1, v_2) \in \overline{R}(\tau_2) \,\} \\ \overline{R}(\mu\alpha.\,\sigma) & := & \{\, (\mathsf{roll}\, v_1, \mathsf{roll}\, v_2) \mid (v_1, v_2) \in \overline{R}(\sigma[\mu\alpha.\,\sigma/\alpha]) \,\} \\ \overline{R}(\exists\alpha.\,\sigma) & := & \{\, (\mathsf{pack}\, v_1, \mathsf{pack}\, v_2) \mid \exists\tau \in \text{CType}.\ (v_1, v_2) \in \overline{R}(\sigma[\tau/\alpha]) \,\} \\ \overline{R}(\tau_1 \to \tau_2) & := & R(\tau_1 \to \tau_2) \\ \overline{R}(\mathsf{ref}\,\tau) & := & R(\mathsf{ref}\,\tau) \\ \overline{R}(\mathbf{n}) & := & R(\mathbf{n}) \\ \overline{R}(\forall\alpha.\,\sigma) & := & R(\forall\alpha.\,\sigma) \end{array}$$

Dependent World. For a preordered set $P = (\mathsf{S}_P, \sqsubseteq_P)$ we define

$$\begin{array}{l} \text{DepWorld}(P) \ := \\ \quad \{\, (\mathsf{N}, \mathsf{S}, \sqsubseteq, \sqsubseteq_{\text{pub}}, \mathsf{L}, \mathsf{H}) \\ \qquad \in \mathbb{P}(\text{TypeName}) \times \text{Set} \times \mathbb{P}(\mathsf{S} \times \mathsf{S}) \times \mathbb{P}(\mathsf{S} \times \mathsf{S}) \times \\ \qquad\quad (\mathsf{S}_P \to \mathsf{S} \to \text{VRelF} \to \text{VRelF}) \times (\mathsf{S}_P \to \mathsf{S} \to \text{VRelF} \to \text{HRel}) \mid \\ \quad \sqsubseteq, \sqsubseteq_{\text{pub}} \text{ are preorders } \wedge \\ \quad \sqsubseteq_{\text{pub}} \text{ is a subset of } \sqsubseteq \wedge \\ \quad \mathsf{L} \text{ is monotone in the first argument w.r.t. } \sqsubseteq_P\text{, in the second w.r.t. } \sqsubseteq\text{, in the third w.r.t. } \leq \wedge \\ \quad \mathsf{H} \text{ is monotone in the third argument w.r.t. } \leq \wedge \\ \quad (\forall s_1, s_2.\ \forall R.\ \forall \mathbf{n} \notin \mathsf{N}.\ \mathsf{L}(s_1)(s_2)(R)(\mathbf{n}) = \emptyset) \wedge \\ \quad (\forall s_1, s_2.\ \forall R.\ \forall (\tau_1 \to \tau_2, f_1, f_2) \in \mathsf{L}(s_1)(s_2)(R).\ f_1, f_2 \in \text{FunVal}) \wedge \\ \quad (\forall s_1, s_2.\ \forall R.\ \forall (\forall\alpha.\,\sigma, v_1, v_2) \in \mathsf{L}(s_1)(s_2)(R).\ v_1, v_2 \in \text{TyFunVal}) \quad \} \end{array}$$

Here we write $\leq$ for the pointwise lifting of the usual subset ordering $\subseteq$ to function spaces.

Full World. We define

$$\text{World} := \{\, W \in \text{DepWorld}(\{*\}, \{(*,*)\}) \,\}$$

and for $W \in \text{World}$ and $s \in W.\mathsf{S}$ often write just $W.\mathsf{H}(s)$ for $W.\mathsf{H}(*)(s)$ (and similar for the L component).

World for Mutable References. We define the reference world $W_{\text{ref}} \in \text{World}$ as follows.

$$\begin{array}{lll}
W_{\text{ref}}.\mathsf{N} & := & \emptyset \\
W_{\text{ref}}.\mathsf{S} & := & \{\, s_{\text{ref}} \in \mathbb{P}_{\text{fin}}(\text{CType} \times \text{Loc} \times \text{Loc}) \mid \\
& & \quad \forall (\tau, \ell_1, \ell_2), (\tau', \ell_1', \ell_2') \in s_{\text{ref}}. \\
& & \quad (\ell_1 = \ell_1' \implies \tau = \tau' \wedge \ell_2 = \ell_2') \wedge (\ell_2 = \ell_2' \implies \tau = \tau' \wedge \ell_1 = \ell_1') \,\} \\
s_{\text{ref}}' \sqsupseteq s_{\text{ref}} & \text{iff} & s_{\text{ref}}' \supseteq s_{\text{ref}} \\
s_{\text{ref}}' \sqsupseteq_{\text{pub}} s_{\text{ref}} & \text{iff} & s_{\text{ref}}' \supseteq s_{\text{ref}} \\
W_{\text{ref}}.\mathsf{L}(s_{\text{ref}})(R) & := & \{\, (\mathsf{ref}\,\tau, \ell_1, \ell_2) \mid (\tau, \ell_1, \ell_2) \in s_{\text{ref}} \,\} \\
W_{\text{ref}}.\mathsf{H}(s_{\text{ref}})(R) & := & \{\, (h_1, h_2) \mid \text{dom}(h_1) = s_{\text{ref}\,[1]} \wedge \text{dom}(h_2) = s_{\text{ref}\,[2]} \wedge \\
& & \qquad \forall (\tau, \ell_1, \ell_2) \in s_{\text{ref}}.\ (\tau, h_1(\ell_1), h_2(\ell_2)) \in \overline{R} \,\}
\end{array}$$

where

$$\begin{array}{lll}
s_{[1]} & := & \{\, \ell_1 \mid \exists \tau, \ell_2.\ (\tau, \ell_1, \ell_2) \in s \,\}\ , \\
s_{[2]} & := & \{\, \ell_2 \mid \exists \tau, \ell_1.\ (\tau, \ell_1, \ell_2) \in s \,\}\ .
\end{array}$$

Local World. We define

$$\text{LWorld} := \{\, w \in \text{DepWorld}(W_{\text{ref}}.\mathsf{S}, W_{\text{ref}}.\sqsubseteq) \mid \forall s_{\text{ref}}, s, R, \tau.\ w.\mathsf{L}(s_{\text{ref}})(s)(R)(\mathsf{ref}\,\tau) = \emptyset \,\}$$

Product World. For $w_1, w_2 \in \text{LWorld}$, we define $w_1 \otimes w_2 \in \text{LWorld}$ as follows.

$$\begin{array}{lll}
\mathsf{N} & := & w_1.\mathsf{N} \uplus w_2.\mathsf{N} \\
\mathsf{S} & := & w_1.\mathsf{S} \times w_2.\mathsf{S} \\
(s_1', s_2') \sqsupseteq (s_1, s_2) & \text{iff} & s_1' \sqsupseteq s_1 \wedge s_2' \sqsupseteq s_2 \\
(s_1', s_2') \sqsupseteq_{\text{pub}} (s_1, s_2) & \text{iff} & s_1' \sqsupseteq_{\text{pub}} s_1 \wedge s_2' \sqsupseteq_{\text{pub}} s_2 \\
\mathsf{L}(s_{\text{ref}})(s_1, s_2)(R) & := & w_1.\mathsf{L}(s_{\text{ref}})(s_1)(R) \cup w_2.\mathsf{L}(s_{\text{ref}})(s_2)(R) \\
\mathsf{H}(s_{\text{ref}})(s_1, s_2)(R) & := & w_1.\mathsf{H}(s_{\text{ref}})(s_1)(R) \otimes w_2.\mathsf{H}(s_{\text{ref}})(s_2)(R)
\end{array}$$

where

$$H_1 \otimes H_2 \quad := \quad \{\, (h_1 \uplus h_1', h_2 \uplus h_2') \mid (h_1, h_2) \in H_1 \wedge (h_1', h_2') \in H_2 \,\}$$

Note that $w_1 \otimes w_2$ is undefined iff $w_1.\mathsf{N}$ and $w_2.\mathsf{N}$ is not disjoint.

Lifting of a Local World. For $w \in \text{LWorld}$, we define $w\!\uparrow\, \in \text{World}$ as follows.

$$\begin{array}{lll}
\mathsf{N} & := & w.\mathsf{N} \\
\mathsf{S} & := & W_{\text{ref}}.\mathsf{S} \times w.\mathsf{S} \\
(s_{\text{ref}}', s') \sqsupseteq (s_{\text{ref}}, s) & \text{iff} & s_{\text{ref}}' \sqsupseteq s_{\text{ref}} \wedge s' \sqsupseteq s \\
(s_{\text{ref}}', s') \sqsupseteq_{\text{pub}} (s_{\text{ref}}, s) & \text{iff} & s_{\text{ref}}' \sqsupseteq_{\text{pub}} s_{\text{ref}} \wedge s' \sqsupseteq_{\text{pub}} s \\
\mathsf{L}(s_{\text{ref}}, s)(R) & := & W_{\text{ref}}.\mathsf{L}(s_{\text{ref}})(R) \cup w.\mathsf{L}(s_{\text{ref}})(s)(R) \\
\mathsf{H}(s_{\text{ref}}, s)(R) & := & W_{\text{ref}}.\mathsf{H}(s_{\text{ref}})(R) \otimes w.\mathsf{H}(s_{\text{ref}})(s)(R)
\end{array}$$

Single-State Worlds. Given a local knowledge $L \in \text{VRelF} \xrightarrow{\text{mon}} \text{VRelF}$ and a heap relation $H \in \text{VRelF} \xrightarrow{\text{mon}} \text{HRel}$ such that

$$\begin{array}{l} \forall R.\ \forall(\tau_1 \to \tau_2, f_1, f_2) \in L(R).\ f_1, f_2 \in \text{FunVal} \land \\ \forall R.\ \forall(\forall\alpha.\,\tau, f_1, f_2) \in L(R).\ f_1, f_2 \in \text{TyFunVal} \end{array}$$

we define the single-state local world $w_{\text{single}}(L, H) \in \text{LWorld}$ as follows.

$$\begin{array}{lcl} w_{\text{single}}(L,H).\mathsf{N} & := & \emptyset \\ w_{\text{single}}(L,H).\mathsf{S} & := & \{\,*\,\} \\ * \sqsupseteq * & & \\ * \sqsupseteq_{\text{pub}} * & & \\ w_{\text{single}}(L,H).\mathsf{L}(s_{\text{ref}})(*)(R) & := & \{\, (\tau' \to \tau, f_1, f_2) \in L(R) \,\} \cup \{\, (\forall\alpha.\,\tau, f_1, f_2) \in L(R) \,\} \\ w_{\text{single}}(L,H).\mathsf{H}(s_{\text{ref}})(*)(R) & := & H(R) \end{array}$$

Global Knowledge. We define the ref-name-preserving order $\geq^{\mathcal{N}}_{\text{ref}}$ between $R, R' \in \text{VRelF}$ as follows.

$$R' \geq^{\mathcal{N}}_{\text{ref}} R \quad \text{iff} \quad \begin{array}{l} \forall \tau.\ R'(\tau) \supseteq R(\tau) \land \\ \forall \tau.\ R'(\mathsf{ref}\,\tau) = R(\mathsf{ref}\,\tau) \land \\ \forall \mathbf{n} \in \mathcal{N}.\ R'(\mathbf{n}) = R(\mathbf{n}) \end{array}$$

Note that $R' \geq^{\mathcal{N}}_{\text{ref}} R \implies R' \geq R$.

We define $\text{GK}(W)$ for $W \in \text{World}$ as follows.

$$\text{GK}(W) \quad := \quad \{\, G \in W.\mathsf{S} \to \text{VRelF} \mid G \text{ is monotone w.r.t. } \sqsubseteq\ \land \forall s.\ G(s) \geq^{W.\mathsf{N}}_{\text{ref}} W.\mathsf{L}(s)(G(s)) \,\}$$

Expression and Continuation Equivalence. We define the following notation.

$$s' \sqsupseteq [s_0, s] \quad \text{iff} \quad s' \sqsupseteq_{\text{pub}} s_0 \land s' \sqsupseteq s$$

For $W \in \text{World}$, we coinductively define $\mathbf{E}_W \in \text{GK}(W) \to W.\mathsf{S} \times W.\mathsf{S} \to \text{ERel}$ and $\mathbf{K}_W \in \text{GK}(W) \to W.\mathsf{S} \times W.\mathsf{S} \to \text{KRel}$ as follows.

$$\begin{array}{lcl} \mathbf{E}_W(G)(s_0,s)(\tau) & := & \{\, (e_1, e_2) \mid \forall (h_1,h_2) \in W.\mathsf{H}(s)(G(s)).\ \forall h^{\text{F}}_1, h^{\text{F}}_2. \\ & & \quad ((h_1, h^{\text{F}}_1, e_1), (h_2, h^{\text{F}}_2, e_2)) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s_0,s)(\tau) \,\} \\ \mathbf{K}_W(G)(s_0,s)(\tau_1,\tau_2) & := & \{\, (K_1, K_2) \mid \forall (v_1,v_2) \in \overline{G(s)}(\tau_1).\ (K_1[v_1], K_2[v_2]) \in \mathbf{E}_W(G)(s_0,s)(\tau_2) \,\} \\ \mathbf{O}_W(R^{\mathbf{K}})(G)(s_0,s)(\tau) & := & \{\, ((h_1, h^{\text{F}}_1, e_1), (h_2, h^{\text{F}}_2, e_2)) \mid h_1 \uplus h^{\text{F}}_1 \text{ defined} \land h_2 \uplus h^{\text{F}}_2 \text{ defined} \implies \\ & & \quad (h_1 \uplus h^{\text{F}}_1, e_1 \uparrow \land h_2 \uplus h^{\text{F}}_2, e_2 \uparrow) \\ & & \quad \lor (\exists h'_1, h'_2, v_1, v_2.\ h_1 \uplus h^{\text{F}}_1, e_1 \hookrightarrow^* h'_1 \uplus h^{\text{F}}_1, v_1 \land h_2 \uplus h^{\text{F}}_2, e_2 \hookrightarrow^* h'_2 \uplus h^{\text{F}}_2, v_2 \land \\ & & \quad\quad \exists s' \sqsupseteq [s_0, s].\ (h'_1, h'_2) \in W.\mathsf{H}(s')(G(s')) \land (v_1, v_2) \in \overline{G(s')}(\tau)) \\ & & \quad \lor (\exists h'_1, h'_2, \tau', K_1, K_2, e'_1, e'_2. \\ & & \quad\quad h_1 \uplus h^{\text{F}}_1, e_1 \hookrightarrow^* h'_1 \uplus h^{\text{F}}_1, K_1[e'_1] \land h_2 \uplus h^{\text{F}}_2, e_2 \hookrightarrow^* h'_2 \uplus h^{\text{F}}_2, K_2[e'_2] \land \\ & & \quad\quad \exists s' \sqsupseteq s.\ (h'_1, h'_2) \in W.\mathsf{H}(s')(G(s')) \land (\tau', e'_1, e'_2) \in \mathbf{S}(G(s'), G(s')) \land \\ & & \quad\quad \forall s'' \sqsupseteq_{\text{pub}} s'.\ \forall G' \geq G.\ (K_1, K_2) \in R^{\mathbf{K}}(G')(s_0, s'')(\tau', \tau)) \,\} \\ \mathbf{S}(R_f, R_v) & := & \{\, (\tau, f_1\ v_1, f_2\ v_2) \mid \exists \tau'.\ (f_1, f_2) \in R_f(\tau' \to \tau) \land (v_1, v_2) \in \overline{R_v}(\tau') \,\} \\ & & \cup \{\, (\sigma[\tau/\alpha], f_1[], f_2[]) \mid \tau \in \text{CType} \land (f_1, f_2) \in R_f(\forall\alpha.\,\sigma) \,\} \end{array}$$

Program Equivalence.

For $w \in \text{LWorld}$, we define:

$$\begin{array}{lcl} \mathit{stable}(w) & := & \forall G \in \text{GK}(w\uparrow).\ \forall s_{\text{ref}}, s.\ \forall (h_1, h_2) \in w.\mathsf{H}(s_{\text{ref}})(s)(G(s_{\text{ref}}, s)). \\ & & \forall s'_{\text{ref}} \sqsupseteq s_{\text{ref}}.\ \forall (h^1_{\text{ref}}, h^2_{\text{ref}}) \in W_{\text{ref}}.\mathsf{H}(s'_{\text{ref}})(G(s'_{\text{ref}}, s)).\ h^1_{\text{ref}} \uplus h_1 \text{ defined} \land h^2_{\text{ref}} \uplus h_2 \text{ defined} \implies \\ & & \exists s' \sqsupseteq_{\text{pub}} s.\ (h_1, h_2) \in w.\mathsf{H}(s'_{\text{ref}})(s')(G(s'_{\text{ref}}, s')) \end{array}$$

For $W \in$ World, we define:

$$\begin{array}{lcl} \mathit{inhabited}(W) & := & \forall G \in \mathrm{GK}(W).\ \exists s_0.\ (\emptyset, \emptyset) \in W.\mathsf{H}(s_0)(G(s_0)) \\ \mathit{consistent}(W) & := & \forall G \in \mathrm{GK}(W).\ \forall s.\ \forall (\tau, e_1, e_2) \in \mathbf{S}(W.\mathsf{L}(s)(G(s)), G(s)). \\ & & \quad (\tau, \mathit{beta}(e_1), \mathit{beta}(e_2)) \in \mathbf{E}_W(G)(s, s) \end{array}$$

We define program equivalence $\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma$.

$$\begin{array}{lcl} \mathrm{TyEnv}(\Delta) & := & \{\, \delta \mid \delta \in \Delta \to \mathrm{CType} \,\} \\ \mathrm{Env}(\Gamma, R) & := & \{\, (\gamma_1, \gamma_2) \mid \gamma_1, \gamma_2 \in \mathrm{dom}(\Gamma) \to \mathrm{CVal} \wedge \forall x.\ (\Gamma(x), \gamma_1(x), \gamma_2(x)) \in \overline{R} \,\} \\ \Delta; \Gamma \vdash e_1 \sim_W e_2 : \sigma & := & \mathit{inhabited}(W) \wedge \mathit{consistent}(W) \wedge \\ & & \forall G \in \mathrm{GK}(W).\ \forall s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s)). \\ & & (\delta\sigma, \gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_W(G)(s, s) \\ \Delta; \Gamma \vdash e_1 \sim_w e_2 : \sigma & := & \mathit{stable}(w) \wedge \Delta; \Gamma \vdash e_1 \sim_{w\uparrow} e_2 : \sigma \\ \Delta; \Gamma \vdash e_1 \sim e_2 : \sigma & := & \forall \mathcal{N} \in \mathrm{Names}.\ \exists w \in \mathrm{LWorld}.\ w.\mathsf{N} \subseteq \mathcal{N} \wedge \Delta; \Gamma \vdash e_1 \sim_w e_2 : \sigma \end{array}$$

2.2 Basic Properties

Notation. For a monotone function $F \in \text{VRelF} \to \text{VRelF}$ and $R \in \text{VRelF}$, we define $R^{[F]}$ as the least fixpoint of the monotone function $F(-) \cup R$:

$$R^{[F]} := \mu X.\ F(X) \cup R\ .$$

For $W \in \text{World}$, we define $[W] \in W.\mathsf{S} \to \text{VRelF}$ as follows:

$$[W](s) := \emptyset^{[W.\mathsf{L}(s)]}\ .$$

Lemma 1. If $G' \geq G$ and $s' \sqsupseteq s$, then:

1. $G'(s') \geq G(s)$
2. $\text{Env}(\Gamma, G'(s')) \supseteq \text{Env}(\Gamma, G(s))$

Proof.

1. By definition of GK we know $G'(s') \geq G'(s)$. And since $G' \geq G$ we also know $G'(s) \geq G(s)$.
2. Follows immediately from (1).

□

Lemma 2. $\forall W \in \text{World}.\ [W] \in \text{GK}(W)$

Proof. We must establish four properties:

a) To show: $[W]$ is monotone w.r.t. $\sqsubseteq$.
Follows from monotonicity of $W.\mathsf{L}$.

b) To show: $\forall s, \tau.\ [W](s)(\tau) \supseteq W.\mathsf{L}(s)([W](s))(\tau)$.
Immediate after unrolling fixpoint once.

c) To show: $\forall s, \tau.\ [W](s)(\mathsf{ref}\,\tau) = W.\mathsf{L}(s)([W](s))(\mathsf{ref}\,\tau)$.
Easy fixpoint induction.

d) To show: $\forall s, \mathbf{n} \in W.\mathsf{N}.\ [W](s)(\mathbf{n}) = W.\mathsf{L}(s)([W](s))(\mathbf{n})$.
Easy fixpoint induction.

□

Lemma 3. $\forall W \in \text{World}, G \in \text{GK}(W).\ [W] \leq G$

Proof. Easy fixpoint induction. □

Lemma 4. If

- $h_1 \uplus h_1^f, e_1 \hookrightarrow^* h_1' \uplus h_1^f, e_1'$,
- $h_2 \uplus h_2^f, e_2 \hookrightarrow^* h_2' \uplus h_2^f, e_2'$,
- $s' \sqsupseteq s$, and
- $(\tau, (h_1', h_1^f, e_1'), (h_2', h_2^f, e_2')) \in \mathbf{O}_W(R^{\mathbf{K}})(s_0, s')$,

then $(\tau, (h_1, h_1^f, e_1), (h_2, h_2^f, e_2)) \in \mathbf{O}_W(R^{\mathbf{K}})(s_0, s)$.

Proof. Follows easily from the definition of $\mathbf{O}_W$. □

Lemma 5. $G(s) \leq \overline{G(s)} \leq \mathbf{E}_W(G)(s,s)$

Proof. The first inclusion holds immediately by definition; the second by choosing the final state to be s. □

Lemma 6. $(\tau, \tau, \bullet, \bullet) \in \mathbf{K}_W(G)(s,s)$

Proof. We need to show $(\tau, v_1, v_2) \in \mathbf{E}_W(G)(s,s)$ for $(\tau, v_1, v_2) \in \overline{G(s)}$, which holds by Lemma 5. □

Lemma 7. If $s_0' \sqsupseteq_{\text{pub}} s_0$, then:

1. $\mathbf{E}_W(G)(s_0', s) \leq \mathbf{E}_W(G)(s_0, s)$
2. $\mathbf{K}_W(G)(s_0', s) \leq \mathbf{K}_W(G)(s_0, s)$

Proof. We define $\mathbf{E}_W'$ and $\mathbf{K}_W'$ as follows:

$$\mathbf{E}_W'(G)(s_0, s) = \{ (\tau, e_1, e_2) \mid \exists s_0'.\ s_0' \sqsupseteq_{\text{pub}} s_0 \land (\tau, e_1, e_2) \in \mathbf{E}_W(G)(s_0', s) \}$$
$$\mathbf{K}_W'(G)(s_0, s) = \{ (\tau_1, \tau_2, K_1, K_2) \mid \exists s_0'.\ s_0' \sqsupseteq_{\text{pub}} s_0 \land (\tau_1, \tau_2, K_1, K_2) \in \mathbf{K}_W(G)(s_0', s) \}$$

If $\mathbf{E}_W' \leq \mathbf{E}_W$ and $\mathbf{K}_W' \leq \mathbf{K}_W$, then for $s_0' \sqsupseteq_{\text{pub}} s_0$ we have

$$\mathbf{E}_W(G)(s_0', s) \leq \mathbf{E}_W'(G)(s_0, s) \leq \mathbf{E}_W(G)(s_0, s)$$

(and similar for $\mathbf{K}_W$).

We now prove $\mathbf{E}_W' \leq \mathbf{E}_W$ and $\mathbf{K}_W' \leq \mathbf{K}_W$ by coinduction. Concretely, we have to show:

1. $\forall e_1, e_2, G, s_0, s, \tau.$
   $(e_1, e_2) \in \mathbf{E}_W'(G)(s_0, s)(\tau) \implies$
   $\forall (h_1, h_2) \in W.\mathsf{H}(s)(G(s)). \forall h_1^{\text{F}}, h_2^{\text{F}}.\ ((h_1, h_1^{\text{F}}, e_1), (h_2, h_2^{\text{F}}, e_2)) \in \mathbf{O}_W(\mathbf{K}_W')(G)(s_0, s)(\tau)$
2. $\forall K_1, K_2, G, s_0, s, \tau', \tau.$
   $(K_1, K_2) \in \mathbf{K}_W'(G)(s_0, s)(\tau', \tau) \implies$
   $\forall (v_1, v_2) \in \overline{G(s)}(\tau').\ (K_1[v_1], K_2[v_2]) \in \mathbf{E}_W'(G)(s_0, s)(\tau)$

For (1):

- Suppose $(e_1, e_2) \in \mathbf{E}_W'(G)(s_0, s)(\tau)$ and $(h_1, h_2) \in W.\mathsf{H}(s)(G(s))$.
- We must show $((h_1, h_1^{\text{F}}, e_1), (h_2, h_2^{\text{F}}, e_2)) \in \mathbf{O}_W(\mathbf{K}_W')(G)(s_0, s)(\tau)$.
- By definition of $\mathbf{E}_W'$ we know $(e_1, e_2) \in \mathbf{E}_W(G)(s_0', s)(\tau)$ for some $s_0' \sqsupseteq_{\text{pub}} s_0$.
- Hence $((h_1, h_1^{\text{F}}, e_1), (h_2, h_2^{\text{F}}, e_2)) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s_0', s)(\tau)$.
- It is easy to see that this implies $((h_1, h_1^{\text{F}}, e_1), (h_2, h_2^{\text{F}}, e_2)) \in \mathbf{O}_W(\mathbf{K}_W')(G)(s_0, s)(\tau)$.

For (2):

- Suppose $(K_1, K_2) \in \mathbf{K}_W'(G)(s_0, s)(\tau', \tau)$ and $(v_1, v_2) \in \overline{G(s)}(\tau')$.
- We must show $(K_1[v_1], K_2[v_2]) \in \mathbf{E}_W'(G)(s_0, s)(\tau)$.
- By definition of $\mathbf{K}_W'$ we know $(K_1, K_2) \in \mathbf{K}_W(G)(s_0', s)(\tau', \tau)$ for some $s_0' \sqsupseteq_{\text{pub}} s_0$.
- Hence $(K_1[v_1], K_2[v_2]) \in \mathbf{E}_W(G)(s_0', s)(\tau) \subseteq \mathbf{E}_W'(G)(s_0, s)(\tau)$.

□

Lemma 8. If $w_1, w_2 \in \text{LWorld}$, then $\forall G \in \text{GK}((w_1 \otimes w_2)\uparrow).\ \forall s_2 \in w_2.\mathsf{S}.\ G(-,-,s_2) \in \text{GK}(w_1\uparrow)$.

Proof. We must establish four properties:

a) To show: $G(-,-,s_2)$ is monotone w.r.t. $\sqsubseteq$.
This follows directly from the definition of $\uparrow, \otimes$ and the monotonicity of G.

b) To show: $\forall s_{\text{ref}}, s_1, \tau.\ G(s_{\text{ref}}, s_1, s_2)(\tau) \supseteq w_1{\uparrow}.\mathsf{L}(s_{\text{ref}}, s_1)(G(s_{\text{ref}}, s_1, s_2))(\tau)$.
We know $G(s_{\text{ref}}, s_1, s_2)(\tau) \supseteq (w_1 \otimes w_2){\uparrow}.\mathsf{L}(s_{\text{ref}}, s_1, s_2)(G(s_{\text{ref}}, s_1, s_2))(\tau)$.
By definition, the latter equals $w_1{\uparrow}.\mathsf{L}(s_{\text{ref}}, s_1)(G(s_{\text{ref}}, s_1, s_2))(\tau) \cup w_2.\mathsf{L}(s_{\text{ref}})(s_2)(G(s_{\text{ref}}, s_1, s_2))(\tau)$.

c) To show: $\forall s_{\text{ref}}, s_1, \tau.\ G(s_{\text{ref}}, s_1, s_2)(\mathsf{ref}\,\tau) = w_1{\uparrow}.\mathsf{L}(s_{\text{ref}}, s_1)(G(s_{\text{ref}}, s_1, s_2))(\mathsf{ref}\,\tau)$.
We know $G(s_{\text{ref}}, s_1, s_2)(\mathsf{ref}\,\tau) = (w_1 \otimes w_2){\uparrow}.\mathsf{L}(s_{\text{ref}}, s_1, s_2)(G(s_{\text{ref}}, s_1, s_2))(\mathsf{ref}\,\tau)$.
By definition, the latter equals $w_1{\uparrow}.\mathsf{L}(s_{\text{ref}}, s_1)(G(s_{\text{ref}}, s_1, s_2))(\mathsf{ref}\,\tau) \cup w_2.\mathsf{L}(s_{\text{ref}})(s_2)(G(s_{\text{ref}}, s_1, s_2))(\mathsf{ref}\,\tau)$.
Since $w_2 \in \text{LWorld}$, we are done.

d) To show: $\forall s_{\text{ref}}, s_1, \mathbf{n} \in w_1{\uparrow}.\mathsf{N}.\ G(s_{\text{ref}}, s_1, s_2)(\mathbf{n}) = w_1{\uparrow}.\mathsf{L}(s_{\text{ref}}, s_1)(G(s_{\text{ref}}, s_1, s_2))(\mathbf{n})$.
We know $G(s_{\text{ref}}, s_1, s_2)(\mathbf{n}) = (w_1 \otimes w_2){\uparrow}.\mathsf{L}(s_{\text{ref}}, s_1, s_2)(G(s_{\text{ref}}, s_1, s_2))(\mathbf{n})$.
By definition, the latter equals $w_1{\uparrow}.\mathsf{L}(s_{\text{ref}}, s_1)(G(s_{\text{ref}}, s_1, s_2))(\mathbf{n}) \cup w_2.\mathsf{L}(s_{\text{ref}})(s_2)(G(s_{\text{ref}}, s_1, s_2))(\mathbf{n})$.
Since $\mathbf{n} \notin w_2.\mathsf{N}$ by definition of $\uparrow, \otimes$, we are done.

□

Lemma 9. If $w_1, w_2 \in \text{LWorld}$, then $\forall G \in \text{GK}((w_1 \otimes w_2){\uparrow}).\ \forall s_1 \in w_1.\mathsf{S}.\ G(-, s_1, -) \in \text{GK}(w_2{\uparrow})$.

Proof. Similar to Lemma 8. □

Lemma 10. If $w = w_1 \otimes w_2$ with $w_1, w_2 \in \text{LWorld}$ and *stable*(w_2), then for all $G \in \text{GK}(w{\uparrow})$ and for all $s^0_{\text{ref}}, s_{\text{ref}} \in W_{\text{ref}}.\mathsf{S}$, $s^0_1, s_1 \in w_1.\mathsf{S}$, $s^0_2, s_2 \in w_2.\mathsf{S}$ with $s_2 \sqsupseteq_{\text{pub}} s^0_2$:

1. $\mathbf{E}_{w_1\uparrow}(G(-,-,s_2))((s^0_{\text{ref}}, s^0_1), (s_{\text{ref}}, s_1)) \leq \mathbf{E}_{w\uparrow}(G)((s^0_{\text{ref}}, s^0_1, s^0_2), (s_{\text{ref}}, s_1, s_2))$
2. $\mathbf{K}_{w_1\uparrow}(G(-,-,s_2))((s^0_{\text{ref}}, s^0_1), (s_{\text{ref}}, s_1) \leq \mathbf{K}_{w\uparrow}(G)((s^0_{\text{ref}}, s^0_1, s^0_2), (s_{\text{ref}}, s_1, s_2))$

Proof. We define $\mathbf{E}'_{w\uparrow}$ and $\mathbf{K}'_{w\uparrow}$ as follows:

$$\begin{aligned}\mathbf{E}'_{w\uparrow}(G)((s^0_{\text{ref}}, s^0_1, s^0_2), (s_{\text{ref}}, s_1, s_2)) = \{\, (\tau, e_1, e_2) \mid \\ s_2 \sqsupseteq_{\text{pub}} s^0_2 \wedge (\tau, e_1, e_2) \in \mathbf{E}_{w_1\uparrow}(G(-,-,s_2))((s^0_{\text{ref}}, s^0_1), (s_{\text{ref}}, s_1)) \,\}\end{aligned}$$

$$\begin{aligned}\mathbf{K}'_{w\uparrow}(G)((s^0_{\text{ref}}, s^0_1, s^0_2), (s_{\text{ref}}, s_1, s_2)) = \{\, (\tau', \tau, K_1, K_2) \mid \\ s_2 \sqsupseteq_{\text{pub}} s^0_2 \wedge (\tau', \tau, K_1, K_2) \in \mathbf{K}_{w_1\uparrow}(G(-,-,s_2))((s^0_{\text{ref}}, s^0_1), (s_{\text{ref}}, s_1)) \,\}\end{aligned}$$

We now prove $\mathbf{E}'_{w\uparrow} \leq \mathbf{E}_{w\uparrow}$ and $\mathbf{K}'_{w\uparrow} \leq \mathbf{K}_{w\uparrow}$ by coinduction. Concretely, we have to show:

1. $\forall e_1, e_2, G, s^0_{\text{ref}}, s_{\text{ref}}, s^0_1, s^0_2, s_1, s_2, \tau.$
   $(e_1, e_2) \in \mathbf{E}'_{w\uparrow}(G)((s^0_{\text{ref}}, s^0_1, s^0_2), (s_{\text{ref}}, s_1, s_2))(\tau) \implies$
   $\forall (h_1, h_2) \in w{\uparrow}.\mathsf{H}(s_{\text{ref}}, s_1, s_2)(G(s_{\text{ref}}, s_1, s_2)).\forall h^{\text{F}}_1, h^{\text{F}}_2.$
   $((h_1, h^{\text{F}}_1, e_1), (h_2, h^{\text{F}}_2, e_2)) \in \mathbf{O}_{w\uparrow}(\mathbf{K}'_{w\uparrow})(G)((s^0_{\text{ref}}, s^0_1, s^0_2), (s_{\text{ref}}, s_1, s_2))(\tau)$
2. $\forall K_1, K_2, G, s^0_{\text{ref}}, s_{\text{ref}}, s^0_1, s^0_2, s_1, s_2, \tau', \tau.$
   $(K_1, K_2) \in \mathbf{K}'_{w\uparrow}(G)((s^0_{\text{ref}}, s^0_1, s^0_2), (s_{\text{ref}}, s_1, s_2))(\tau', \tau) \implies$
   $\forall (v_1, v_2) \in \overline{G(s_{\text{ref}}, s_1, s_2)}(\tau').\ (K_1[v_1], K_2[v_2]) \in \mathbf{E}'_{w\uparrow}(G)((s^0_{\text{ref}}, s^0_1, s^0_2), (s_{\text{ref}}, s_1, s_2))(\tau)$

For (1):

- Suppose $(e_1, e_2) \in \mathbf{E}'_{w\uparrow}(G)((s^0_{\text{ref}}, s^0_1, s^0_2), (s_{\text{ref}}, s_1, s_2))(\tau)$ and $(h_1, h_2) \in w{\uparrow}.\mathsf{H}(s_{\text{ref}}, s_1, s_2)(G(s_{\text{ref}}, s_1, s_2))$.
- By definition of $\mathbf{E}'_{w\uparrow}$ we know $s_2 \sqsupseteq_{\text{pub}} s^0_2$ and $(e_1, e_2) \in \mathbf{E}_{w_1\uparrow}(G(-,-,s_2))((s^0_{\text{ref}}, s^0_1), (s_{\text{ref}}, s_1))(\tau)$.
- We must show $((h_1, h^{\text{F}}_1, e_1), (h_2, h^{\text{F}}_2, e_2)) \in \mathbf{O}_{w\uparrow}(\mathbf{K}'_{w\uparrow})(G)((s^0_{\text{ref}}, s^0_1, s^0_2), (s_{\text{ref}}, s_1, s_2))(\tau)$.

- So suppose defined($h_1 \uplus h_1^{\mathrm{F}}$) and defined($h_2 \uplus h_2^{\mathrm{F}}$).
- From $(h_1, h_2) \in w{\uparrow}.\mathsf{H}(s_{\mathrm{ref}}, s_1, s_2)(G(s_{\mathrm{ref}}, s_1, s_2))$ and the definition of $\uparrow, \otimes$, we know $h_1 = h_1' \uplus h_1''$ and $h_2 = h_2' \uplus h_2''$ with $(h_1', h_2') \in w_1{\uparrow}.\mathsf{H}(s_{\mathrm{ref}}, s_1)(G(s_{\mathrm{ref}}, s_1, s_2))$ and $(h_1'', h_2'') \in w_2.\mathsf{H}(s_{\mathrm{ref}})(s_2)(G(s_{\mathrm{ref}}, s_1, s_2))$.
- Hence $((h_1', h_1'' \uplus h_1^{\mathrm{F}}, e_1), (h_2', h_2'' \uplus h_2^{\mathrm{F}}, e_2)) \in \mathbf{O}_{w_1\uparrow}(\mathbf{K}_{w_1\uparrow})(G(-,-,s_2))((s_{\mathrm{ref}}^0, s_1^0), (s_{\mathrm{ref}}, s_1))(\tau)$.
- Consequently at least one of the following three properties holds:

  A) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \uparrow$ and $h_2 \uplus h_2^{\mathrm{F}}, e_2 \uparrow$

  B) (a) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* \widetilde{h_1'} \uplus h_1'' \uplus h_1^{\mathrm{F}}, v_1$ and $h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* \widetilde{h_2'} \uplus h_2'' \uplus h_2^{\mathrm{F}}, v_2$
     (b) $(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}) \sqsupseteq [(s_{\mathrm{ref}}^0, s_1^0), (s_{\mathrm{ref}}, s_1)]$
     (c) $(\widetilde{h_1'}, \widetilde{h_2'}) \in w_1{\uparrow}.\mathsf{H}(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1})(G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, s_2))$
     (d) $(v_1, v_2) \in \overline{G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, s_2)}(\tau)$

  C) (a) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* \widetilde{h_1'} \uplus h_1'' \uplus h_1^{\mathrm{F}}, K_1[e_1']$ and $h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* \widetilde{h_2'} \uplus h_2'' \uplus h_2^{\mathrm{F}}, K_2[e_2']$
     (b) $(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}) \sqsupseteq (s_{\mathrm{ref}}, s_1)$
     (c) $(\widetilde{h_1'}, \widetilde{h_2'}) \in w_1{\uparrow}.\mathsf{H}(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1})(G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, s_2))$
     (d) $(e_1', e_2') \in \mathbf{S}(G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s}, s_2), G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s}, s_2))(\widetilde{\tau})$
     (e) $\forall(\widehat{s_{\mathrm{ref}}}, \widehat{s_1}) \sqsupseteq_{\mathrm{pub}} (\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}).\ \forall G' \geq G(-,-,s_2).\ (K_1, K_2) \in \mathbf{K}_{w_1\uparrow}(G')((s_{\mathrm{ref}}^0, s_1^0), (\widehat{s_{\mathrm{ref}}}, \widehat{s_1}))(\widetilde{\tau}, \tau)$

- If (A) holds, then we are done.
- If (B) holds:
  - By *stable*(w_2) there is $\widetilde{s_2} \sqsupseteq_{\mathrm{pub}} s_2$ such that
    $$(h_1'', h_2'') \in w_2.\mathsf{H}(\widetilde{s_{\mathrm{ref}}})(\widetilde{s_2})(G(s_{\mathrm{ref}}, s_1, s_2)) \ .$$
  - By monotonicity of $w_2.\mathsf{H}$, from $G(s_{\mathrm{ref}}, s_1, s_2) \subseteq G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, \widetilde{st_2})$, we have
    $$(h_1'', h_2'') \in w_2.\mathsf{H}(\widetilde{s_{\mathrm{ref}}})(\widetilde{s_2})(G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, \widetilde{st_2})) \ .$$
  - From (Bc) and monotonicity we also know $(\widetilde{h_1'}, \widetilde{h_2'}) \in w_1{\uparrow}.\mathsf{H}(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1})(G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, \widetilde{s_2}))$.
  - Thus by the definition of $\uparrow, \otimes$, we get $(\widetilde{h_1'} \uplus h_1'', \widetilde{h_2'} \uplus h_2'') \in w{\uparrow}.\mathsf{H}(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, \widetilde{s_2})(G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, \widetilde{s_2}))$.
  - From (Bb) and the definition of $\uparrow, \otimes$, we get $(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, \widetilde{s_2}) \sqsupseteq [(s_{\mathrm{ref}}^0, s_1^0, s_2^0), (s_{\mathrm{ref}}, s_1, s_2)]$.
  - Together with (Ba) (Bd) we are done.
- If (C) holds:
  - By *stable*(w_2) there is $\widetilde{s_2} \sqsupseteq_{\mathrm{pub}} s_2$ such that
    $$(h_1'', h_2'') \in w_2.\mathsf{H}(\widetilde{s_{\mathrm{ref}}})(\widetilde{s_2})(G(s_{\mathrm{ref}}, s_1, s_2)) \ .$$
  - By monotonicity of $w_2.\mathsf{H}$, from $G(s_{\mathrm{ref}}, s_1, s_2) \subseteq G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, \widetilde{st_2})$, we have
    $$(h_1'', h_2'') \in w_2.\mathsf{H}(\widetilde{s_{\mathrm{ref}}})(\widetilde{s_2})(G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, \widetilde{st_2})) \ .$$
  - From (Cc) and monotonicity we also know $(\widetilde{h_1'}, \widetilde{h_2'}) \in w_1{\uparrow}.\mathsf{H}(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1})(G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, \widetilde{s_2}))$.
  - Thus by the definition of $\uparrow, \otimes$, we get $(\widetilde{h_1'} \uplus h_1'', \widetilde{h_2'} \uplus h_2'') \in w{\uparrow}.\mathsf{H}(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, \widetilde{s_2})(G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, \widetilde{s_2}))$.
  - From (Cb) and the definition of $\uparrow, \otimes$, we get $(\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, \widetilde{s_2}) \sqsupseteq [(s_{\mathrm{ref}}^0, s_1^0, s_2^0), (s_{\mathrm{ref}}, s_1, s_2)]$.

– Now it remains to show:

$$\forall(\widehat{s_{\mathrm{ref}}}, \widehat{s_1}, \widehat{s_2}) \sqsupseteq_{\mathrm{pub}} (\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, \widetilde{s_2}).\ \forall G' \geq G.\ (K_1, K_2) \in \mathbf{K}'_{w\uparrow}(G')((s^0_{\mathrm{ref}}, s^0_1, s^0_2), (\widehat{s_{\mathrm{ref}}}, \widehat{s_1}, \widehat{s_2}))(\widetilde{\tau}, \tau)$$

– So suppose $(\widehat{s_{\mathrm{ref}}}, \widehat{s_1}, \widehat{s_2}) \sqsupseteq_{\mathrm{pub}} (\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1}, \widetilde{s_2})$ and $G' \geq G$.
– Note that $(\widehat{s_{\mathrm{ref}}}, \widehat{s_1}) \sqsupseteq_{\mathrm{pub}} (\widetilde{s_{\mathrm{ref}}}, \widetilde{s_1})$ and, by monotonicity, $G'(-,-,\widehat{s_2}) \geq G(-,-,s_2)$.
– From (Ce) we therefore get $(K_1, K_2) \in \mathbf{K}_{w_1\uparrow}(G'(-,-,\widehat{s_2}))((s^0_{\mathrm{ref}}, s^0_1), (\widehat{s_{\mathrm{ref}}}, \widehat{s_1}))(\widetilde{\tau}, \tau)$.
– By definition of $\mathbf{K}'_{w\uparrow}$ this implies

$$(K_1, K_2) \in \mathbf{K}'_{w\uparrow}(G')((s^0_{\mathrm{ref}}, s^0_1, s^0_2), (\widehat{s_{\mathrm{ref}}}, \widehat{s_1}, \widehat{s_2}))(\widetilde{\tau}, \tau)$$

For (2):

- Suppose $(K_1, K_2) \in \mathbf{K}'_{w\uparrow}(G)((s^0_{\mathrm{ref}}, s^0_1, s^0_2), (s_{\mathrm{ref}}, s_1, s_2))(\tau', \tau)$ and $(v_1, v_2) \in \overline{G(s_{\mathrm{ref}}, s_1, s_2)}(\tau')$.
- By definition of $\mathbf{K}'_{w\uparrow}$ we know $s_2 \sqsupseteq_{\mathrm{pub}} s^0_2$ and $(K_1, K_2) \in \mathbf{K}_{w_1\uparrow}(G(-,-,s_2))((s^0_{\mathrm{ref}}, s^0_1), (s_{\mathrm{ref}}, s_1))(\tau', \tau)$.
- We must show $(K_1[v_1], K_2[v_2]) \in \mathbf{E}'_{w\uparrow}(G)((s^0_{\mathrm{ref}}, s^0_1, s^0_2), (s_{\mathrm{ref}}, s_1, s_2))(\tau)$.
- By definition of $\mathbf{E}'_{w\uparrow}$ it suffices to show

$$(K_1[v_1], K_2[v_2]) \in \mathbf{E}_{w_1\uparrow}(G(-,-,s_2))((s^0_{\mathrm{ref}}, s^0_1), (s_{\mathrm{ref}}, s_1))(\tau).$$

- Since $(v_1, v_2) \in \overline{G(s_{\mathrm{ref}}, s_1, s_2)}(\tau')$, we are done.

□

Lemma 11. If $w = w_1 \otimes w_2$ with $w_1, w_2 \in$ LWorld and *stable*(w_1), then for all $G \in \mathrm{GK}(w\uparrow)$ and for all $s^0_{\mathrm{ref}}, s_{\mathrm{ref}} \in W_{\mathrm{ref}}.\mathsf{S}$, $s^0_1, s_1 \in w_1.\mathsf{S}$, $s^0_2, s_2 \in w_2.\mathsf{S}$ with $s_1 \sqsupseteq_{\mathrm{pub}} s^0_1$:

1. $\mathbf{E}_{w_2\uparrow}(G(-,s_1,-))((s^0_{\mathrm{ref}}, s^0_2), (s_{\mathrm{ref}}, s_2)) \leq \mathbf{E}_{w\uparrow}(G)((s^0_{\mathrm{ref}}, s^0_1, s^0_2), (s_{\mathrm{ref}}, s_1, s_2))$
2. $\mathbf{K}_{w_2\uparrow}(G(-,s_1,-))((s^0_{\mathrm{ref}}, s^0_2), (s_{\mathrm{ref}}, s_2) \leq \mathbf{K}_{w\uparrow}(G)((s^0_{\mathrm{ref}}, s^0_1, s^0_2), (s_{\mathrm{ref}}, s_1, s_2))$

Proof. Similar to Lemma 10. □

Lemma 12. If $w = w_1 \otimes w_2$ with $w_1, w_2 \in$ LWorld and *stable*(w_1), *stable*(w_2), then:

1. *stable*(w)
2. If *inhabited*$(w_1\uparrow)$ and *inhabited*$(w_2\uparrow)$, then *inhabited*$(w\uparrow)$.
3. If *consistent*$(w_1\uparrow)$ and *consistent*$(w_2\uparrow)$, then *consistent*$(w\uparrow)$.

Proof.

1. - Suppose $G \in \mathrm{GK}((w_1 \otimes w_2)\uparrow)$, $(h_1, h_2) \in (w_1 \otimes w_2).\mathsf{H}(s_{\mathrm{ref}})(s_1, s_2)(G(s_{\mathrm{ref}}, s_1, s_2))$ and $s'_{\mathrm{ref}} \sqsupseteq s_{\mathrm{ref}}$.
   - Further suppose $(h'_1, h'_2) \in W_{\mathrm{ref}}.\mathsf{H}(s'_{\mathrm{ref}})(G(s'_{\mathrm{ref}}, s))$ and defined$(h'_1 \uplus h_1)$ and defined$(h'_2 \uplus h_2)$.
   - We must show that there is $(s'_1, s'_2) \sqsupseteq_{\mathrm{pub}} (s_1, s_2)$ such that

   $$(h_1, h_2) \in (w_1 \otimes w_2).\mathsf{H}(s'_{\mathrm{ref}})(s'_1, s'_2)(G(s'_{\mathrm{ref}}, s'_1, s'_2)).$$

   - Decomposing $(w_1 \otimes w_2).\mathsf{H}$ gives us $h^1_1, h^1_2, h^2_1, h^2_2$ such that:
     – $h_1 = h^1_1 \uplus h^2_1$ and $h_2 = h^1_2 \uplus h^2_2$
     – $(h^1_1, h^1_2) \in w_1.\mathsf{H}(s_{\mathrm{ref}})(s_1)(G(s_{\mathrm{ref}}, s_1, s_2))$

  - defined$(h'_1 \uplus h^1_1)$ and defined$(h'_2 \uplus h^1_2)$
  - $(h^2_1, h^2_2) \in w_2.\mathsf{H}(s_{\text{ref}})(s_2)(G(s_{\text{ref}}, s_1, s_2))$
  - defined$(h'_1 \uplus h^2_1)$ and defined$(h'_2 \uplus h^2_2)$
- From this, Lemmas 8–11, and the assumptions, we get $s'_1 \sqsupseteq_{\text{pub}} s_1$ and $s'_2 \sqsupseteq_{\text{pub}} s_2$ such that:
  (a) $(h^1_1, h^1_2) \in w_1.\mathsf{H}(s'_{\text{ref}})(s'_1)(G(s'_{\text{ref}}, s'_1, s_2))$
  (b) $(h^2_1, h^2_2) \in w_2.\mathsf{H}(s'_{\text{ref}})(s'_2)(G(s'_{\text{ref}}, s_1, s'_2))$
- Using monotonicity and then composing this gives us

$$(h_1, h_2) \in (w_1 \otimes w_2).\mathsf{H}(s'_{\text{ref}})(s'_1, s'_2)(G(s'_{\text{ref}}, s'_1, s'_2)).$$

2. - Suppose $G \in \text{GK}(w\!\uparrow)$.
   - From the assumptions, Lemma 2, and definition of $\uparrow$ and W_{ref} we get s_1, s_2 such that
     $(\emptyset, \emptyset) \in w_1.\mathsf{H}(\emptyset)(s_1)([w_1\!\uparrow](\emptyset, s_1))$ and
     $(\emptyset, \emptyset) \in w_2.\mathsf{H}(\emptyset)(s_2)([w_2\!\uparrow](\emptyset, s_2))$.
   - From Lemmas 2, 3, 8, 9, we know $[w_1\!\uparrow] \leq [w\!\uparrow](-, (-, s_2))$ and $[w_2\!\uparrow] \leq [w\!\uparrow](-, (s_1, -))$.
   - Hence $(\emptyset, \emptyset) \in w\!\uparrow.\mathsf{H}(\emptyset, (s_1, s_2))([w\!\uparrow](\emptyset, (s_1, s_2)))$ by monotonicity and definition of $\otimes, \uparrow$.

3. - We suppose
     (a) $s = (s_{\text{ref}}, s_1, s_2) \in w\!\uparrow.\mathsf{S}$
     (b) $G \in \text{GK}(w\!\uparrow)$
     (c) $(\tau, e_1, e_2) \in \mathbf{S}(w\!\uparrow.\mathsf{L}(s)(G(s)), G(s))$
     and must show $(\tau, \mathit{beta}(e_1), \mathit{beta}(e_2)) \in \mathbf{E}_{w\uparrow}(G)(s, s)$.
   - From (c) and the definitions of $\uparrow$, $\otimes$ and $\mathbf{S}$ we know:

$$\begin{aligned}(\tau, e_1, e_2) &\in \mathbf{S}(W_{\text{ref}}.\mathsf{L}(s_{\text{ref}})(G(s)), G(s)) \lor \\ (\tau, e_1, e_2) &\in \mathbf{S}(w_1.\mathsf{L}(s_{\text{ref}})(s_1)(G(s)), G(s)) \lor \\ (\tau, e_1, e_2) &\in \mathbf{S}(w_2.\mathsf{L}(s_{\text{ref}})(s_2)(G(s)), G(s))\end{aligned}$$

   - This implies:

$$\begin{aligned}(\tau, e_1, e_2) &\in \mathbf{S}(w_1\!\uparrow.\mathsf{L}(s_{\text{ref}}, s_1)(G(s)), G(s)) \lor \\ (\tau, e_1, e_2) &\in \mathbf{S}(w_2\!\uparrow.\mathsf{L}(s_{\text{ref}}, s_2)(G(s)), G(s))\end{aligned}$$

   - If the former is true, the goal follows from $\mathit{consistent}(w_1\!\uparrow)$ with the help of Lemmas 8 and 10.
   - If the latter is true, the goal follows from $\mathit{consistent}(w_2\!\uparrow)$ with the help of Lemmas 9 and 11.

□

Lemma 13. For $G \in \text{GK}(W)$, $s_0, s'_0, s \in W.\mathsf{S}$, $\tau, \tau' \in \text{CType}$, $K_1, K_2 \in \text{Cont}$, if

$$\forall s' \sqsupseteq [s'_0, s].\forall G' \geq G.\ (\tau', \tau, K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')\,,$$

then:

1. $(\tau', e_1, e_2) \in \mathbf{E}_W(G)(s'_0, s)$ implies $(\tau, K_1[e_1], K_2[e_2]) \in \mathbf{E}_W(G)(s_0, s)$.
2. $(\tau'', \tau', K'_1, K'_2) \in \mathbf{K}_W(G)(s'_0, s)$ implies $(\tau'', \tau, K_1[K'_1], K_2[K'_2]) \in \mathbf{K}_W(G)(s_0, s)$.

Proof. We define $\mathbf{E}'_W$ and $\mathbf{K}'_W$ as follows:

$$\begin{aligned}\mathbf{E}'_W(G)(s_0, s) = \{\, (\tau, K_1[e_1], K_2[e_2]) \mid \exists \tau', s'_0.\ &(\tau', e_1, e_2) \in \mathbf{E}_W(G)(s'_0, s) \land \\ &\forall s' \sqsupseteq [s'_0, s].\forall G' \geq G.\ (\tau', \tau, K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')\,\}\end{aligned}$$

$$\begin{aligned}\mathbf{K}'_W(G)(s_0, s) = \{\, (\tau'', \tau, K_1[K'_1], K_2[K'_2]) \mid \exists \tau', s'_0.\ &(\tau'', \tau', K'_1, K'_2) \in \mathbf{K}_W(G)(s'_0, s) \land \\ &\forall s' \sqsupseteq [s'_0, s].\forall G' \geq G.\ (\tau', \tau, K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')\,\}\end{aligned}$$

It suffices to show $\mathbf{E}'_W \leq \mathbf{E}_W$ and $\mathbf{K}'_W \leq \mathbf{K}_W$, which we do by coinduction. Concretely, we have to show:

1. $\forall K_1, K_2, e_1, e_2, G, s_0, s, \tau.$
   $(K_1[e_1], K_2[e_2]) \in \mathbf{E}'_W(G)(s_0, s)(\tau) \implies$
   $\forall (h_1, h_2) \in W.\mathsf{H}(s)(G(s)). \forall h_1^{\mathrm{F}}, h_2^{\mathrm{F}}.$
   $((h_1, h_1^{\mathrm{F}}, K_1[e_1]), (h_2, h_2^{\mathrm{F}}, K_2[e_2])) \in \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0, s)(\tau)$

2. $\forall K_1, K_2, K'_1, K'_2, G, s_0, s, \tau'', \tau.$
   $(K_1[K'_1], K_2[K'_2]) \in \mathbf{K}'_W(G)(s_0, s)(\tau'', \tau) \implies$
   $\forall (v_1, v_2) \in \overline{G(s)}(\tau'').\ (K_1[K'_1][v_1], K_2[K'_2][v_2]) \in \mathbf{E}'_W(G)(s_0, s)(\tau)$

For (1):

- Suppose $(K_1[e_1], K_2[e_2]) \in \mathbf{E}'_W(G)(s_0, s)(\tau)$ and $(h_1, h_2) \in W.\mathsf{H}(s)(G(s))$.
- By definition of $\mathbf{E}'_W$ we know $(e_1, e_2) \in \mathbf{E}_W(G)(s'_0, s)(\tau')$ and

  $$\forall s' \sqsupseteq [s'_0, s]. \forall G' \geq G.\ (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau)$$

  for some s'_0 and τ'.
- We must show $((h_1, h_1^{\mathrm{F}}, K_1[e_1]), (h_2, h_2^{\mathrm{F}}, K_2[e_2])) \in \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0, s)(\tau)$.
- So suppose defined$(h_1 \uplus h_1^{\mathrm{F}})$ and defined$(h_2 \uplus h_2^{\mathrm{F}})$.
- We know $((h_1, h_1^{\mathrm{F}}, e_1), (h_2, h_2^{\mathrm{F}}, e_2)) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s'_0, s)(\tau')$.
- Hence at least one of the following three properties holds:
  A) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \uparrow$ and $h_2 \uplus h_2^{\mathrm{F}}, e_2 \uparrow$
  B) (a) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h'_1 \uplus h_1^{\mathrm{F}}, v_1$ and $h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h'_2 \uplus h_2^{\mathrm{F}}, v_2$
     (b) $s' \sqsupseteq [s'_0, s]$
     (c) $(h'_1, h'_2) \in W.\mathsf{H}(s')(G(s'))$
     (d) $(v_1, v_2) \in \overline{G(s')}(\tau')$
  C) (a) $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h'_1 \uplus h_1^{\mathrm{F}}, K'_1[e'_1]$ and $h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h'_2 \uplus h_2^{\mathrm{F}}, K'_2[e'_2]$
     (b) $s' \sqsupseteq s$
     (c) $(h'_1, h'_2) \in W.\mathsf{H}(s')(G(s'))$
     (d) $(e'_1, e'_2) \in \mathbf{S}(G(s'), G(s'))(\widetilde{\tau})$
     (e) $\forall s'' \sqsupseteq_{\mathrm{pub}} s'.\ \forall G' \geq G.\ (K'_1, K'_2) \in \mathbf{K}_W(G')(s'_0, s'')(\widetilde{\tau}, \tau')$
- If (A) holds:
  - Then $h_1 \uplus h_1^{\mathrm{F}}, K_1[e_1] \uparrow$ and $h_2 \uplus h_2^{\mathrm{F}}, K_2[e_2] \uparrow$, so we are done.
- If (B) holds:
  - Then $h_1 \uplus h_1^{\mathrm{F}}, K_1[e_1] \hookrightarrow^* h'_1 \uplus h_1^{\mathrm{F}}, K_1[v_1]$ and $h_2 \uplus h_2^{\mathrm{F}}, K_2[e_2] \hookrightarrow^* h'_2 \uplus h_2^{\mathrm{F}}, K_2[v_2]$ from (Ba).
  - Since $(K_1, K_2) \in \mathbf{K}_W(G)(s_0, s')(\tau', \tau)$ from (Bb), we get $(K_1[v_1], K_2[v_2]) \in \mathbf{E}_W(G)(s_0, s')(\tau)$ from (Bd).
  - Using (Bc), this implies $((h'_1, h_1^{\mathrm{F}}, K_1[v_1]), (h'_2, h_2^{\mathrm{F}}, K_2[v_2])) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s_0, s')(\tau)$.
  - We show $\mathbf{O}_W(\mathbf{K}_W)(G)(s_0, s')(\tau) \subseteq \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0, s')(\tau)$:
    * It suffices to show $\mathbf{K}_W \leq \mathbf{K}'_W$.
    * By definition of the latter, this follows from Lemmas 7 and 6.
  - Consequently, $((h'_1, h_1^{\mathrm{F}}, K_1[v_1]), (h'_2, h_2^{\mathrm{F}}, K_2[v_2])) \in \mathbf{O}_W(\mathbf{K}'_W)(G)(s_0, s')(\tau)$.
  - We are done by (Bb) and Lemma 4.

- If (C) holds:
  - Then $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, K_1[K_1'][e_1']$ and $h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, K_2[K_2'][e_2']$ from (Ca).
  - Due to (Cb–d) it remains to show:

$$\forall s'' \sqsupseteq_{\mathrm{pub}} s'.\ \forall G' \geq G.\ (K_1[K_1'], K_2[K_2']) \in \mathbf{K}_W'(G')(s_0, s'')(\widetilde{\tau}, \tau)$$

  - So suppose $s'' \sqsupseteq_{\mathrm{pub}} s'$ and $G' \geq G$.
  - By definition of $\mathbf{K}_W'$ it suffices to show $(K_1', K_2') \in \mathbf{K}_W(G')(s_0', s'')(\widetilde{\tau}, \tau')$ and

$$\forall s''' \sqsupseteq [s_0', s''].\forall G'' \geq G'.\ (K_1, K_2) \in \mathbf{K}_W(G'')(s_0, s''')(\tau', \tau).$$

  - The former follows from (Ce).
  - For the latter, recall that

$$\forall s' \sqsupseteq [s_0', s].\forall G' \geq G.\ (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau).$$

  - Since $s'' \sqsupseteq_{\mathrm{pub}} s' \sqsupseteq s$ and $G'' \geq G' \geq G$, we are done.

For (2):

- Suppose $(K_1[K_1'], K_2[K_2']) \in \mathbf{K}_W'(G)(s_0, s)(\tau'', \tau)$ and $(v_1, v_2) \in \overline{G(s)}(\tau'')$.
- By definition of $\mathbf{K}_W'$ we know $(K_1', K_2') \in \mathbf{K}_W(G)(s_0', s)(\tau'', \tau')$ and

$$\forall s' \sqsupseteq [s_0', s].\forall G' \geq G.\ (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau)$$

  for some s_0' and τ'.
- We must show $(K_1[K_1'][v_1], K_2[K_2'][v_2]) \in \mathbf{E}_W'(G)(s_0, s)(\tau)$.
- By definition of $\mathbf{E}_W'$ it suffices to show $(K_1'[v_1], K_2'[v_2]) \in \mathbf{E}_W(G)(s_0', s)(\tau')$ and

$$\forall s' \sqsupseteq [s_0', s].\forall G' \geq G.\ (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau).$$

- The latter is given and the former follows from $(K_1', K_2') \in \mathbf{K}_W(G)(s_0', s)(\tau'', \tau')$ and $(v_1, v_2) \in \overline{G(s)}(\tau'')$.

∎

Lemma 14. If *inhabited*$(w_2\uparrow)$, *consistent*$(w_2\uparrow)$, *stable*(w_2), and defined$(w_1 \otimes w_2)$, then:

$$\Delta; \Gamma \vdash e_1 \sim_{w_1} e_2 : \sigma \quad \Longrightarrow \quad \Delta; \Gamma \vdash e_1 \sim_{w_1 \otimes w_2} e_2 : \sigma$$

Proof.

- Using the assumptions and Lemma 12, we get *inhabited*$((w_1 \otimes w_2)\uparrow)$ and *consistent*$((w_1 \otimes w_2)\uparrow)$ as well as *stable*$(w_1 \otimes w_2)$.
- Now suppose $G \in \mathrm{GK}((w_1 \otimes w_2)\uparrow)$ and $\delta \in \mathrm{TyEnv}(\Delta), (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{ref}}, s, s'))$.
- We must show $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{(w_1 \otimes w_2)\uparrow}(G)((s_{\mathrm{ref}}, s, s'), (s_{\mathrm{ref}}, s, s'))(\delta\sigma)$.
- From $\Delta; \Gamma \vdash e_1 \sim_{w_1} e_2 : \sigma$ and Lemma 8 we know:

$$(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{w_1\uparrow}(G(-, -, s'))((s_{\mathrm{ref}}, s), (s_{\mathrm{ref}}, s))(\delta\sigma)$$

- We are done by Lemma 10.

□

Lemma 15. If $\forall w.\ \big(\forall i \in \{1 \dots n\}.\ \Delta_i; \Gamma_i \vdash e_i \sim_w e'_i : \sigma_i\big) \implies \Delta; \Gamma \vdash e \sim_{w\uparrow} e' : \sigma$, then

$$\big(\forall i \in \{1 \dots n\}.\ \Delta_i; \Gamma_i \vdash e_i \sim e'_i : \sigma_i\big) \implies \Delta; \Gamma \vdash e \sim e' : \sigma\ .$$

Proof.

- Suppose $\forall w.\ \big(\forall i \in \{1 \dots n\}.\ \Delta_i; \Gamma_i \vdash e_i \sim_w e'_i : \sigma_i\big) \implies \Delta; \Gamma \vdash e \sim_{w\uparrow} e' : \sigma$ and $\forall i \in \{1 \dots n\}.\ \Delta_i; \Gamma_i \vdash e_i \sim e'_i : \sigma_i$.
- Given $\mathcal{N} \in$ Names, since $\mathcal{N}$ is countably infinite, we can split it into $\mathcal{N}_i$'s such that $\mathcal{N} = \mathcal{N}_1 \uplus \dots \uplus \mathcal{N}_n$.
- Thus by the premise we have w_i's such that for all i, $w_i.\mathsf{N} \subseteq \mathcal{N}_i$ and $\Delta_i; \Gamma_i \vdash e_i \sim_{w_i} e'_i : \sigma_i$.
- Since $w_i.\mathsf{N}$'s are disjoint, by applying Lemma 14 repeatedly, we have $\Delta_i; \Gamma_i \vdash e_i \sim_{w_1 \otimes \dots \otimes w_n} e'_i : \sigma_i$ for all i.
- By the assumption we thus have $\Delta; \Gamma \vdash e \sim_{(w_1 \otimes \dots \otimes w_n)\uparrow} e' : \sigma$.
- Using Lemma 12 we get $\mathit{stable}(w_1 \otimes \dots \otimes w_n)$ and thus $\Delta; \Gamma \vdash e \sim_{w_1 \otimes \dots \otimes w_n} e' : \sigma$
- By definition of $\otimes$, we have $(w_1 \otimes \dots \otimes w_n).\mathsf{N} \subseteq \mathcal{N}_1 \uplus \dots \uplus \mathcal{N}_n = \mathcal{N}$, and thus $\Delta; \Gamma \vdash e \sim e' : \sigma$.

□

Lemma 16. If $\forall W.\ \big(\forall i \in \{1 \dots n\}.\ \Delta_i; \Gamma_i \vdash e_i \sim_W e'_i : \sigma_i\big) \implies \Delta; \Gamma \vdash e \sim_W e' : \sigma$, then:

$$\big(\forall i \in \{1 \dots n\}.\ \Delta_i; \Gamma_i \vdash e_i \sim e'_i : \sigma_i\big) \implies \Delta; \Gamma \vdash e \sim e' : \sigma$$

Proof. Immediate consequence of Lemma 15. □

Lemma 17. If $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s)).\ (\gamma_1 K_1, \gamma_2 K_2) \in \mathbf{K}_W(G)(s, s)(\delta\sigma', \delta\sigma)$ then

$$\Delta; \Gamma \vdash e_1 \sim_W e_2 : \sigma' \quad \implies \quad \Delta; \Gamma \vdash K_1[e_1] \sim_W K_2[e_2] : \sigma$$

Proof.

- Suppose $G \in \mathrm{GK}(W)$, $\delta \in \mathrm{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$.
- We must show $((\gamma_1 K_1)[\gamma_1 e_1], (\gamma_2 K_2)[\gamma_2 e_2]) \in \mathbf{E}_W(G)(s, s)(\delta\sigma)$.
- From the premise we get $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_W(G)(s, s)(\delta\sigma')$.
- By Lemma 13 it suffices to show

  $$(\gamma_1 K_1, \gamma_2 K_2) \in \mathbf{K}_W(G')(s, s^\circ)(\delta\sigma', \delta\sigma)$$

  for $s^\circ \sqsupseteq_{\mathrm{pub}} s$ and $G' \geq G$.
- By Lemma 7 it then suffices to show

  $$(\gamma_1 K_1, \gamma_2 K_2) \in \mathbf{K}_W(G')(s^\circ, s^\circ)(\delta\sigma', \delta\sigma),$$

  which follows from Lemma 1 and the assumption.

□

Lemma 18 (External call)**.** For any $G \in \mathrm{GK}(W)$ and $\boldsymbol{\mathcal{R}} \in W.\mathsf{S} \to \mathrm{VRelF}$, if

$$consistent(W) \ \wedge \ \forall s.\ G(s) = W.\mathsf{L}(s)(G(s)) \cup \boldsymbol{\mathcal{R}}(s) \ ,$$

then we have

$$\begin{array}{l}
\forall (\tau, e_1, e_2) \in \mathbf{E}_W(G)(s_0, s).\ \forall (h_1, h_2) \in W.\mathsf{H}(s)(G(s)).\\
\forall h_1^{\mathrm{F}}, h_2^{\mathrm{F}}.\ h_1 \uplus h_1^{\mathrm{F}} \text{ defined} \wedge h_2 \uplus h_2^{\mathrm{F}} \text{ defined} \implies \\
\quad (h_1 \uplus h_1^{\mathrm{F}}, e_1 \uparrow \wedge\, h_2 \uplus h_2^{\mathrm{F}}, e_2 \uparrow) \\
\quad \vee\ (\exists h_1', h_2', v_1, v_2.\ h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, v_1 \wedge h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, v_2 \wedge \\
\quad\quad \exists s' \sqsupseteq [s_0, s].\ (h_1', h_2') \in W.\mathsf{H}(s')(G(s')) \wedge (v_1, v_2) \in \overline{G(s')}(\tau)) \\
\quad \vee\ (\exists h_1', h_2', \tau', K_1, K_2, e_1', e_2'. \\
\quad\quad h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, K_1[e_1'] \wedge h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, K_2[e_2'] \wedge \\
\quad\quad \exists s' \sqsupseteq s.\ (h_1', h_2') \in W.\mathsf{H}(s')(G(s')) \wedge (\tau', e_1', e_2') \in \mathbf{S}(\boldsymbol{\mathcal{R}}(s'), G(s')) \wedge \\
\quad\quad \forall s'' \sqsupseteq_{\mathrm{pub}} s'.\ \forall G' \geq G.\ (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s'')(\tau', \tau))
\end{array}$$

Proof.

- We prove the following proposition by induction on n.

$$\begin{array}{l}
\forall (\tau, e_1, e_2) \in \mathbf{E}_W(G)(s_0, s).\ \forall (h_1, h_2) \in W.\mathsf{H}(s)(G(s)).\\
\forall h_1^{\mathrm{F}}, h_2^{\mathrm{F}}.\ h_1 \uplus h_1^{\mathrm{F}} \text{ defined} \wedge h_2 \uplus h_2^{\mathrm{F}} \text{ defined} \implies \\
\quad (h_1 \uplus h_1^{\mathrm{F}}, e_1 \uparrow^n \wedge\, h_2 \uplus h_2^{\mathrm{F}}, e_2 \uparrow^n) \\
\quad \vee\ (\exists h_1', h_2', v_1, v_2.\ h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, v_1 \wedge h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, v_2 \wedge \\
\quad\quad \exists s' \sqsupseteq [s_0, s].\ (h_1', h_2') \in W.\mathsf{H}(s')(G(s')) \wedge (v_1, v_2) \in \overline{G(s')}(\tau)) \\
\quad \vee\ (\exists h_1', h_2', \tau', K_1, K_2, e_1', e_2'. \\
\quad\quad h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, K_1[e_1'] \wedge h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, K_2[e_2'] \wedge \\
\quad\quad \exists s' \sqsupseteq s.\ (h_1', h_2') \in W.\mathsf{H}(s')(G(s')) \wedge (\tau', e_1', e_2') \in \mathbf{S}(\boldsymbol{\mathcal{R}}(s'), G(s')) \wedge \\
\quad\quad \forall s'' \sqsupseteq_{\mathrm{pub}} s'.\ \forall G' \geq G.\ (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s'')(\tau', \tau))
\end{array} \tag{1}$$

- When $n = 0$, the first case holds vacuously.
- When $n > 0$, we assume that the goal (1) holds for $n-1$. Then we need to show that the goal (1) holds for n.
- By definition of $\mathbf{E}_W(G)(s_0, s)$, we have three cases.
- In the first two cases, the goal (1) is trivially satisfied.
- In the third case, we have

$$\begin{array}{l}
\exists h_1', h_2', \tau', K_1, K_2, e_1', e_2'. \\
\quad h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, K_1[e_1'] \wedge h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, K_2[e_2'] \wedge \\
\quad \exists s' \sqsupseteq s.\ (h_1', h_2') \in W.\mathsf{H}(s')(G(s')) \wedge (\tau', e_1', e_2') \in \mathbf{S}(G(s'), G(s')) \wedge \\
\quad \forall s'' \sqsupseteq_{\mathrm{pub}} s'.\ \forall G' \geq G.\ (K_1, K_2) \in \mathbf{K}_W(G')(s_0, s'')(\tau', \tau)
\end{array}$$

- As $G(s') = W.\mathsf{L}(s')(G(s')) \cup \boldsymbol{\mathcal{R}}(s')$, by definition of $\mathbf{S}$, we have

$$(\tau', e_1', e_2') \in \mathbf{S}(G(s'), G(s')) = \mathbf{S}(W.\mathsf{L}(s')(G(s')), G(s')) \cup \mathbf{S}(\boldsymbol{\mathcal{R}}(s'), G(s')) \ .$$

- If $(\tau', e_1', e_2') \in \mathbf{S}(\boldsymbol{\mathcal{R}}(s'), G(s'))$, then the goal (1) is satisfied.
- If $(\tau', e_1', e_2') \in \mathbf{S}(W.\mathsf{L}(s')(G(s')), G(s'))$, then by $consistent(W)$, we have that $h_1' \uplus h_1^{\mathrm{F}}, K_1[e_1'] \hookrightarrow^1 h_1' \uplus h_1^{\mathrm{F}}, K_1[beta(e_1')]$ and $h_2' \uplus h_2^{\mathrm{F}}, K_2[e_2'] \hookrightarrow^1 h_2' \uplus h_2^{\mathrm{F}}, K_2[beta(e_2')]$ and $(\tau', beta(e_1'), beta(e_2')) \in \mathbf{E}_W(G)(s', s')$.

- By Lemma 13, we have $(\tau, K_1[beta(e_1')], K_2[beta(e_2')]) \in \mathbf{E}_W(G)(s_0, s')$.
- As $(h_1', h_2') \in W.\mathsf{H}(s')(G(s'))$, by induction hypothesis we have that $h_1' \uplus h_1^{\mathrm{F}}, K_1[beta(e_1')]$ and $h_2' \uplus h_2^{\mathrm{F}}, K_2[beta(e_2')]$ satisfy the goal (1) for $n-1$ w.r.t. (s_0, s').
- As $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^+ h_1' \uplus h_2^{\mathrm{F}}, K_1[beta(e_1')] \wedge h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^+ h_2' \uplus h_2^{\mathrm{F}}, K_2[beta(e_2')]$ and $s' \sqsupseteq s$, we have that $h_1 \uplus h_1^{\mathrm{F}}, e_1$ and $h_2 \uplus h_2^{\mathrm{F}}, e_2$ satisfy the goal (1) for n w.r.t. (s_0, s), so we are done.
- The original goal is obtained from the sub-goal (1) by pushing the quantification over n inside the first case and then observing that $\forall n.h, e\uparrow^n$ is equivalent to $h, e\uparrow$.

□

Corollary 19. If

- $consistent(W)$
- $\forall s.\ G(s) = W.\mathsf{L}(s)(G(s))$
- $(\tau, e_1, e_2) \in \mathbf{E}_W(G)(s_0, s)$
- $(h_1, h_2) \in W.\mathsf{H}(s)(G(s))$ and $h_1 \uplus h_1^{\mathrm{F}}$, $h_2 \uplus h_2^{\mathrm{F}}$ defined

then one of the following holds:

1. $h_1 \uplus h_1^{\mathrm{F}}, e_1\uparrow \wedge h_2 \uplus h_2^{\mathrm{F}}, e_2\uparrow$
2. $\exists h_1', h_2', v_1, v_2, s'.$
   $h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}}, v_1 \wedge h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}}, v_2 \wedge$
   $s' \sqsupseteq_{\mathrm{pub}} [s_0, s] \wedge (h_1', h_2') \in W.\mathsf{H}(s')(G(s')) \wedge (\tau, v_1, v_2) \in \overline{G(s')}$

Proof. Follows from Lemma 18 for $\mathcal{R} = \lambda s.\emptyset$. □

2.3 Compatibility

Lemma 20 (Compatibility: Var)**.**

$$\frac{\Delta \vdash \Gamma \quad x{:}\sigma \in \Gamma}{\Delta; \Gamma \vdash x \sim x : \sigma}$$

Proof.

- Let $w_{\text{id}} = w_{\text{single}}(\lambda R.\emptyset, \lambda R.\{(\emptyset, \emptyset)\})$ (so $w_{\text{id}}.\mathsf{N} \subseteq \mathcal{N}$ for any $\mathcal{N}$).
- We are done if we can show $\Delta; \Gamma \vdash x \sim_{w_{\text{id}}} x : \sigma$.
- It is obvious that *stable*(w_{id}) (the dependency is vacuous) and that *consistent*($w_{\text{id}}\uparrow$) (neither W_{ref} nor w_{id} relates any functions).
- *inhabited*($w_{\text{id}}\uparrow$) is witnessed by state $(\emptyset, *)$.
- Now suppose $G \in \text{GK}(w_{\text{id}}\uparrow)$ and $\delta \in \text{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s))$.
- We must show $(\gamma_1(x), \gamma_2(x)) \in \mathbf{E}_{w_{\text{id}}\uparrow}(G)(s, s)(\delta\sigma)$.
- From $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s))$ we know $(\gamma_1(x), \gamma_2(x)) \in \overline{G(s)}(\delta\sigma)$.
- We are done by Lemma 5.

□

Lemma 21.

1. If $(\tau, v_1, v_2) \in \overline{G(s)}$, then $(\tau', \tau \times \tau', \langle v_1, \bullet\rangle, \langle v_2, \bullet\rangle) \in \mathbf{K}_W(G)(s, s)$.
2. If $(\tau', e_1', e_2') \in \mathbf{E}_W(G)(s_0, s)$, then $(\tau, \tau \times \tau', \langle \bullet, e_1'\rangle, \langle \bullet, e_2'\rangle) \in \mathbf{K}_W(G)(s_0, s)$.

Proof.

1.
   - Suppose $(v_1', v_2') \in \overline{G(s)}(\tau')$.
   - We need to show $(\langle v_1, v_1'\rangle, \langle v_2, v_2'\rangle) \in \mathbf{E}_W(G)(s, s)(\tau \times \tau')$.
   - By Lemma 5 it suffices to show $(\langle v_1, v_1'\rangle, \langle v_2, v_2'\rangle) \in \overline{G(s)}(\tau \times \tau')$.
   - Hence it suffices to show $(v_1, v_2) \in \overline{G(s)}(\tau)$ and $(v_1', v_2') \in \overline{G(s)}(\tau')$, which we both already have.
2.
   - Suppose $(v_1, v_2) \in \overline{G(s)}(\tau)$.
   - We need to show $(\langle v_1, e_1'\rangle, \langle v_2, e_2'\rangle) \in \mathbf{E}_W(G)(s_0, s)(\tau \times \tau')$.
   - By Lemma 13 it suffices to show

     $$(\langle v_1, \bullet\rangle, \langle v_2, \bullet\rangle) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau \times \tau')$$

     for $s' \sqsupseteq [s_0, s]$ and $G' \geq G$.
   - By Lemma 7 it suffices to show $(\langle v_1, \bullet\rangle, \langle v_2, \bullet\rangle) \in \mathbf{K}_W(G')(s', s')(\tau', \tau \times \tau')$.
   - By part (1) it then suffices to show $(v_1, v_2) \in \overline{G'(s')}(\tau)$, which follows from $(v_1, v_2) \in \overline{G(s)}(\tau)$ by Lemma 1.

□

Lemma 22 (Compatibility: Pair)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma \qquad \Delta; \Gamma \vdash e_1' \sim e_2' : \sigma'}{\Delta; \Gamma \vdash \langle e_1, e_1'\rangle \sim \langle e_2, e_2'\rangle : \sigma \times \sigma'}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,

$$(\langle \bullet, \gamma_1 e_1' \rangle, \langle \bullet, \gamma_2 e_2' \rangle) \in \mathbf{K}_W(G)(s,s)(\delta\sigma, \delta\sigma \times \delta\sigma')$$

  assuming $\Delta; \Gamma \vdash e_1' \sim_W e_2' : \sigma'$.

- By Lemma 21 it suffices to show $(\gamma_1 e_1', \gamma_2 e_2') \in \mathbf{E}_W(G)(s,s)(\delta\sigma')$, which follows from the assumption.

□

Lemma 23 (Compatibility: Fst (Snd analogously))**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma \times \sigma'}{\Delta; \Gamma \vdash e_1.1 \sim e_2.1 : \sigma}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,

$$(\bullet.1, \bullet.1) \in \mathbf{K}_W(G)(s,s)(\delta\sigma \times \delta\sigma', \delta\sigma)\ .$$

- Suppose $(v_1^\circ, v_2^\circ) \in \overline{G(s)}(\delta\sigma \times \delta\sigma')$.
- We need to show $(v_1^\circ.1, v_2^\circ.1) \in \mathbf{E}_W(G)(s,s)(\delta\sigma)$.
- Suppose $(h_1, h_2) \in W.\mathsf{H}(s)(G(s))$ as well as defined$(h_1 \uplus h_1^{\mathrm{F}})$ and defined$(h_2 \uplus h_2^{\mathrm{F}})$.
- We know $v_1^\circ = \langle v_1, v_1' \rangle$ and $v_2^\circ = \langle v_2, v_2' \rangle$ with $(v_1, v_2) \in \overline{G(s)}(\delta\sigma)$.
- Hence $h_1 \uplus h_1^{\mathrm{F}}, v_1^\circ.1 \hookrightarrow h_1 \uplus h_1^{\mathrm{F}}, v_1$ and $h_2 \uplus h_2^{\mathrm{F}}, v_2^\circ.1 \hookrightarrow h_2 \uplus h_2^{\mathrm{F}}, v_2$.
- Since $s \sqsupseteq [s, s]$, we are done.

□

Lemma 24 (Compatibility: Inl (Inr analogously))**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma}{\Delta; \Gamma \vdash \mathsf{inj}^1\, e_1 \sim \mathsf{inj}^1\, e_2 : \sigma + \sigma'}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,

$$(\mathsf{inj}^1\, \bullet, \mathsf{inj}^1\, \bullet) \in \mathbf{K}_W(G)(s,s)(\delta\sigma, \delta\sigma + \delta\sigma')\ .$$

- Suppose $(v_1, v_2) \in \overline{G(s)}(\delta\sigma)$.
- We need to show $(\mathsf{inj}^1\, v_1, \mathsf{inj}^1\, v_2) \in \mathbf{E}_W(G)(s,s)(\delta\sigma + \delta\sigma')$.
- By Lemma 5 it suffices to show $(\mathsf{inj}^1\, v_1, \mathsf{inj}^1\, v_2) \in \overline{G(s)}(\delta\sigma + \delta\sigma')$.
- This follows from $(v_1, v_2) \in \overline{G(s)}(\delta\sigma)$.

□

Lemma 25 (Compatibility: Case)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma' + \sigma'' \qquad \Delta; \Gamma, x{:}\sigma' \vdash e_1' \sim e_2' : \sigma \qquad \Delta; \Gamma, x{:}\sigma'' \vdash e_1'' \sim e_2'' : \sigma}{\Delta; \Gamma \vdash \mathsf{case}\, e_1\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow e_1' \,|\, \mathsf{inj}^2\, x \Rightarrow e_1'' \sim \mathsf{case}\, e_2\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow e_2' \,|\, \mathsf{inj}^2\, x \Rightarrow e_2'' : \sigma}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,

  $$(\mathsf{case} \bullet \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_1 e_1' \,|\, \mathsf{inj}^2\, x \Rightarrow \gamma_1 e_1'', \mathsf{case} \bullet \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_2 e_2' \,|\, \mathsf{inj}^2\, x \Rightarrow \gamma_2 e_2'') \in \mathbf{K}_W(G)(s,s)(\delta\sigma' {+} \delta\sigma'', \delta\sigma)\ .$$

  assuming $\Delta; \Gamma, x{:}\sigma' \vdash e_1' \sim_W e_2' : \sigma$ and $\Delta; \Gamma, x{:}\sigma'' \vdash e_1'' \sim_W e_2'' : \sigma$.
- Thus it suffices to show that $\forall (v_1, v_2) \in \overline{G(s)}(\delta\sigma' + \delta\sigma'')$,

  $$(\mathsf{case}\, v_1\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_1 e_1' \,|\, \mathsf{inj}^2\, x \Rightarrow \gamma_1 e_1'', \mathsf{case}\, v_2\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_2 e_2' \,|\, \mathsf{inj}^2\, x \Rightarrow \gamma_2 e_2'') \in \mathbf{E}_W(G)(s,s)(\delta\sigma)$$

- By definition of $\overline{G(s)}(\delta\sigma' + \delta\sigma'')$, we have v_1', v_2' such that either
  1. $v_1 = \mathsf{inj}^1\, v_1' \wedge v_2 = \mathsf{inj}^1\, v_2' \wedge (v_1', v_2') \in \overline{G(s)}(\delta\sigma')$; or
  2. $v_1 = \mathsf{inj}^2\, v_1' \wedge v_2 = \mathsf{inj}^2\, v_2' \wedge (v_1', v_2') \in \overline{G(s)}(\delta\sigma'')$.
- We show the former case (the latter case can be done analogousely).
- Let $\gamma_1' := \gamma_1, x {\mapsto} v_1'$ and $\gamma_2' := \gamma_2, x {\mapsto} v_2'$.
- Now suppose $(h_1, h_2) \in W.\mathsf{H}(s)(G(s))$ and $h_1^{\mathrm{F}}, h_2^{\mathrm{F}} \in \mathrm{Heap}$ with $h_1 \uplus h_1^{\mathrm{F}}, h_2 \uplus h_2^{\mathrm{F}}$ defined.
- We have

  $$h_1 \uplus h_1^{\mathrm{F}}, \mathsf{case}\, v_1\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_1 e_1' \,|\, \mathsf{inj}^2\, x \Rightarrow \gamma_1 e_1'' \hookrightarrow h_1 \uplus h_1^{\mathrm{F}}, \gamma_1' e_1'$$

  and

  $$h_2 \uplus h_2^{\mathrm{F}}, \mathsf{case}\, v_2\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_2 e_2' \,|\, \mathsf{inj}^2\, x \Rightarrow \gamma_2 e_2'' \hookrightarrow h_2 \uplus h_2^{\mathrm{F}}, \gamma_2' e_2'$$

- Thus by Lemma 4, it suffices to show

  $$(\delta\sigma', (h_1, h_1^{\mathrm{F}}, \gamma_1' e_1'), (h_2, h_2^{\mathrm{F}}, \gamma_2' e_2')) \in \mathbf{O}_W(\mathbf{E}_W)(G)(s,s)\ .$$

- This follows from the assumption and $(\gamma_1', \gamma_2') \in \mathrm{Env}(\delta(\Gamma, x : \sigma'), G(s))$.

□

Lemma 26 (Compatibility: Fix)**.**

$$\frac{\Delta; \Gamma, f{:}\sigma' \to \sigma, x{:}\sigma' \vdash e_1 \sim e_2 : \sigma}{\Delta; \Gamma \vdash \mathsf{fix}\, f(x).\, e_1 \sim \mathsf{fix}\, f(x).\, e_2 : \sigma' \to \sigma}$$

Proof.

- For any $\mathcal{N}$, from the premise we have w such that $w.\mathsf{N} \subseteq \mathcal{N}$ and $\Delta; \Gamma, f{:}\sigma' \to \sigma, x{:}\sigma' \vdash e_1 \sim_w e_2 : \sigma$.
- Let $w' = w_{\mathrm{single}}(\lambda R.\ \{(\delta\sigma' \to \delta\sigma, \gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \mid \delta \in \mathrm{TyEnv}(\Delta), (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, R)\}, \lambda R.\ \{(\emptyset, \emptyset)\})$.
- Since $(w \otimes w').\mathsf{N} = w.\mathsf{N} \subseteq \mathcal{N}$, it suffices to show $\Delta; \Gamma \vdash \mathsf{fix}\, f(x).\, e_1 \sim_{w \otimes w'} \mathsf{fix}\, f(x).\, e_2 : \sigma' \to \sigma$.
- To do so, we first prove *inhabited*$((w \otimes w')\!\uparrow)$ and *consistent*$((w \otimes w')\!\uparrow)$:

- $\mathit{inhabited}(w'\uparrow)$ is witnessed by state $(\emptyset, *)$, so $\mathit{inhabited}((w \otimes w')\uparrow)$ holds by Lemma 12.
- The part of $\mathit{consistent}((w \otimes w')\uparrow)$ concerning universal types follows from $\mathit{consistent}(w\uparrow)$ by Lemma 12, because $w'.\mathsf{L}$ doesn't relate anything at universal types.
- Regarding the part concerning arrow types, we suppose
  1. $G \in \mathrm{GK}((w \otimes w')\uparrow)$
  2. $(v_1, v_2) \in (w \otimes w')\uparrow.\mathsf{L}(s_{\mathrm{ref}}, s, s')(G(s_{\mathrm{ref}}, s, s'))(\widetilde{\sigma'} \to \widetilde{\sigma})$
  3. $(v_1', v_2') \in \overline{G(s_{\mathrm{ref}}, s, s')}(\widetilde{\sigma'})$

  and must show:

$$(\mathit{beta}(v_1\ v_1'), \mathit{beta}(v_2\ v_2')) \in \mathbf{E}_{(w \otimes w')\uparrow}(G)((s_{\mathrm{ref}}, s, s'), (s_{\mathrm{ref}}, s, s'))(\widetilde{\sigma})$$

- From (2) and the definition of $\uparrow$ and $\otimes$ we know:

$$\begin{aligned}&(v_1, v_2) \in w\uparrow.\mathsf{L}(s_{\mathrm{ref}}, s)(G(s_{\mathrm{ref}}, s, s'))(\widetilde{\sigma'} \to \widetilde{\sigma}) \vee \\ &(v_1, v_2) \in w'.\mathsf{L}(s_{\mathrm{ref}})(s')(G(s_{\mathrm{ref}}, s, s'))(\widetilde{\sigma'} \to \widetilde{\sigma})\end{aligned}$$

- If the former is true, the claim follows from $\mathit{consistent}(w\uparrow)$ with the help of Lemmas 8 and 10.
- So suppose the latter.
- Then $\widetilde{\sigma'} \to \widetilde{\sigma} = \delta\sigma' \to \delta\sigma$ and $v_1 = \gamma_1 \mathsf{fix}\, f(x).\, e_1$ and $v_2 = \gamma_2 \mathsf{fix}\, f(x).\, e_2$ for $\delta \in \mathrm{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{ref}}, s, s'))$.
- Let $\gamma_1' = \gamma_1, f{\mapsto}\gamma_1 \mathsf{fix}\, f(x).\, e_1, x{\mapsto}v_1'$ and $\gamma_2' = \gamma_2, f{\mapsto}\gamma_2 \mathsf{fix}\, f(x).\, e_2, x{\mapsto}v_2'$
- It remains to show $(\gamma_1' e_1, \gamma_2' e_2) \in \mathbf{E}_{(w \otimes w')\uparrow}(G)((s_{\mathrm{ref}}, s, s'), (s_{\mathrm{ref}}, s, s'))(\delta\sigma)$.
- By Lemmas 8 and 10 it suffices to show $(\gamma_1' e_1, \gamma_2' e_2) \in \mathbf{E}_{w\uparrow}(G(-, -, s'))((s_{\mathrm{ref}}, s), (s_{\mathrm{ref}}, s))(\delta\sigma)$.
- This follows from the premise if we can show $(\gamma_1', \gamma_2') \in \mathrm{Env}((\delta\Gamma, f{:}\delta\sigma' \to \delta\sigma, x{:}\delta\sigma'), G(s_{\mathrm{ref}}, s, s'))$.
- This reduces to showing $(v_1', v_2') \in \overline{G(s_{\mathrm{ref}}, s, s')}(\delta\sigma')$ and

$$(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in \overline{G(s_{\mathrm{ref}}, s, s')}(\delta\sigma' \to \delta\sigma).$$

- The former is given as (3).
- For the latter, note that by definition of GK it suffices to show

$$(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in (w \otimes w')\uparrow.\mathsf{L}(s_{\mathrm{ref}}, s, s')(G(s_{\mathrm{ref}}, s, s'))(\delta\sigma' \to \delta\sigma).$$

- By definition of $\uparrow$ and $\otimes$ it then suffices to show

$$(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in w'.\mathsf{L}(s_{\mathrm{ref}})(s')(G(s_{\mathrm{ref}}, s, s'))(\delta\sigma' \to \delta\sigma).$$

- Since $\delta \in \mathrm{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{ref}}, s, s'))$, this holds by construction.

- Now suppose $G \in \mathrm{GK}((w \otimes w')\uparrow)$ and $\delta \in \mathrm{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{ref}}, s, s'))$.
- We must show $(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in \mathbf{E}_{(w \otimes w')\uparrow}(G)((s_{\mathrm{ref}}, s, s'), (s_{\mathrm{ref}}, s, s'))(\delta\sigma' \to \delta\sigma)$.
- By Lemma 5 it suffices to show $(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in G(s_{\mathrm{ref}}, s, s')(\delta\sigma' \to \delta\sigma)$.
- By definition of GK it suffices to show:

$$(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in (w \otimes w')\uparrow.\mathsf{L}(s_{\mathrm{ref}}, s, s')(G(s_{\mathrm{ref}}, s, s'))(\delta\sigma' \to \delta\sigma)$$

- By definition of $\uparrow$ and $\otimes$ it suffices to show $(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in w'.\mathsf{L}(s_{\mathrm{ref}})(s')(G(s_{\mathrm{ref}}, s, s'))(\delta\sigma' \to \delta\sigma)$.

- Since $\delta \in \mathrm{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{ref}}, s, s'))$, this holds by construction of w'.

$\square$

Lemma 27.

1. If $(\tau' \to \tau, v_1, v_2) \in \overline{G(s)}$, then $(\tau', \tau, v_1\ \bullet, v_2\ \bullet) \in \mathbf{K}_W(G)(s, s)$.
2. If $(\tau', e_1', e_2') \in \mathbf{E}_W(G)(s_0, s)$, then $(\tau' \to \tau, \tau, \bullet\ e_1', \bullet\ e_2') \in \mathbf{K}_W(G)(s_0, s)$.

Proof.

1.
   - Suppose $(v_1', v_2') \in \overline{G(s)}(\tau')$.
   - We need to show $(v_1\ v_1', v_2\ v_2') \in \mathbf{E}_W(G)(s, s)(\tau)$.
   - By definition of $\mathbf{E}_W$ it suffices to show the following:
     (a) $(v_1, v_2) \in \overline{G(s)}(\tau' \to \tau)$
     (b) $(v_1', v_2') \in \overline{G(s)}(\tau')$
     (c) $\forall s' \sqsupseteq_{\mathrm{pub}} s. \forall G' \geq G.\ (\bullet, \bullet) \in \mathbf{K}_W(G')(s, s')(\tau, \tau)$
   - (a) and (b) are already given.
   - (c) follows by Lemmas 6 and 7.
2.
   - Suppose $(v_1, v_2) \in \overline{G(s)}(\tau' \to \tau)$.
   - We need to show $(v_1\ e_1', v_2\ e_2') \in \mathbf{E}_W(G)(s_0, s)(\tau)$.
   - By Lemma 13 it suffices to show
     $$(v_1\ \bullet, v_2\ \bullet) \in \mathbf{K}_W(G')(s_0, s')(\tau', \tau)$$
     for $s' \sqsupseteq [s_0, s]$ and $G' \geq G$.
   - By Lemma 7 it suffices to show $(v_1\ \bullet, v_2\ \bullet) \in \mathbf{K}_W(G')(s', s')(\tau', \tau)$.
   - By part (1) it then suffices to show $(v_1, v_2) \in \overline{G'(s')}(\tau' \to \tau)$.
   - This follows from $(v_1, v_2) \in \overline{G(s)}(\tau' \to \tau)$ by Lemma 1.

$\square$

Lemma 28 (Compatibility: App)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma' \to \sigma \qquad \Delta; \Gamma \vdash e_1' \sim e_2' : \sigma'}{\Delta; \Gamma \vdash e_1\ e_1' \sim e_2\ e_2' : \sigma}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,
  $$(\bullet\ \gamma_1 e_1', \bullet\ \gamma_2 e_2') \in \mathbf{K}_W(G)(s, s)(\delta\sigma' \to \delta\sigma, \delta\sigma)$$
  assuming $\Delta; \Gamma \vdash e_1' \sim_W e_2' : \sigma'$.
- By Lemma 27 it suffices to show $(\gamma_1 e_1', \gamma_2 e_2') \in \mathbf{E}_W(G)(s, s)(\delta\sigma')$, which follows from the assumption.

$\square$

Lemma 29 (Compatibility: Roll)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma[\mu\alpha.\, \sigma/\alpha]}{\Delta; \Gamma \vdash \mathsf{roll}\ e_1 \sim \mathsf{roll}\ e_2 : \mu\alpha.\, \sigma}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s.\ \forall \delta \in \text{TyEnv}(\Delta).\ \forall(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s))$,

$$(\mathsf{roll}\ \bullet, \mathsf{roll}\ \bullet) \in \mathbf{K}_W(G)(s, s)(\delta\sigma[\mu\alpha.\, \delta\sigma/\alpha], \mu\alpha.\, \delta\sigma)\ .$$

- Suppose $(v_1, v_2) \in \overline{G(s)}(\delta\sigma[\mu\alpha.\, \delta\sigma/\alpha])$.
- We need to show $(\mathsf{roll}\ v_1, \mathsf{roll}\ v_2) \in \mathbf{E}_W(G)(s, s)(\mu\alpha.\, \delta\sigma)$.
- By Lemma 5 it suffices to show $(\mathsf{roll}\ v_1, \mathsf{roll}\ v_2) \in \overline{G(s)}(\mu\alpha.\, \delta\sigma)$.
- This follows from $(v_1, v_2) \in \overline{G(s)}(\delta\sigma[\mu\alpha.\, \delta\sigma/\alpha])$.

□

Lemma 30 (Compatibility: Unroll)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \mu\alpha.\, \sigma}{\Delta; \Gamma \vdash \mathsf{unroll}\ e_1 \sim \mathsf{unroll}\ e_2 : \sigma[\mu\alpha.\, \sigma/\alpha]}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s.\ \forall \delta \in \text{TyEnv}(\Delta).\ \forall(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s))$,

$$(\mathsf{unroll}\ \bullet, \mathsf{unroll}\ \bullet) \in \mathbf{K}_W(G)(s, s)(\mu\alpha.\, \delta\sigma, \delta\sigma[\mu\alpha.\, \delta\sigma/\alpha])\ .$$

- Suppose $(v_1^\circ, v_2^\circ) \in \overline{G(s)}(\mu\alpha.\, \delta\sigma)$.
- We need to show $(\mathsf{unroll}\ v_1^\circ, \mathsf{unroll}\ v_2^\circ) \in \mathbf{E}_W(G)(s, s)(\delta\sigma[\mu\alpha.\, \delta\sigma/\alpha])$.
- Suppose $(h_1, h_2) \in W.\mathsf{H}(s)(G(s))$ as well as defined$(h_1 \uplus h_1^{\text{F}})$ and defined$(h_2 \uplus h_2^{\text{F}})$.
- We know $v_1^\circ = \mathsf{roll}\ v_1$ and $v_2^\circ = \mathsf{roll}\ v_2$ with $(v_1, v_2) \in \overline{G(s)}(\delta\sigma[\mu\alpha.\, \delta\sigma/\alpha])$.
- Hence $h_1 \uplus h_1^{\text{F}}, \mathsf{unroll}\ v_1^\circ \hookrightarrow h_1 \uplus h_1^{\text{F}}, v_1$ and $h_2 \uplus h_2^{\text{F}}, \mathsf{unroll}\ v_2^\circ \hookrightarrow h_2 \uplus h_2^{\text{F}}, v_2$.
- Since $s \sqsupseteq [s, s]$, we are done.

□

Lemma 31 (Compatibility: Ref)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma}{\Delta; \Gamma \vdash \mathsf{ref}\ e_1 \sim \mathsf{ref}\ e_2 : \mathsf{ref}\ \sigma}$$

Proof.

- By Lemmas 15 and 17, it suffices to show $\forall G, s_{\text{ref}}, s.\ \forall \delta \in \text{TyEnv}(\Delta).\ \forall(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s))$,

$$(\mathsf{ref}\ \bullet, \mathsf{ref}\ \bullet) \in \mathbf{K}_{w\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))(\delta\sigma, \mathsf{ref}\ \delta\sigma)\ .$$

- Suppose $(v_1, v_2) \in \overline{G(s_{\text{ref}}, s)}(\delta\sigma)$.
- We need to show $(\mathsf{ref}\ v_1, \mathsf{ref}\ v_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))(\mathsf{ref}\ \delta\sigma)$.
- Suppose $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\text{ref}}, s)(G(s_{\text{ref}}, s))$ as well as defined$(h_1 \uplus h_1^{\text{F}})$ and defined$(h_2 \uplus h_2^{\text{F}})$.
- We know $h_1 \uplus h_1^{\text{F}}, \mathsf{ref}\ v_1 \hookrightarrow h_1 \uplus [\ell_1 \mapsto v_1] \uplus h_1^{\text{F}}, \ell_1$ for $\ell_1 \notin \text{dom}(h_1 \uplus h_1^{\text{F}})$.
- Similarly, $h_2 \uplus h_2^{\text{F}}, \mathsf{ref}\ v_2 \hookrightarrow h_2 \uplus [\ell_2 \mapsto v_2] \uplus h_2^{\text{F}}, \ell_2$ for $\ell_2 \notin \text{dom}(h_2 \uplus h_2^{\text{F}})$.

- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $(\widetilde{s_{\text{ref}}}, \widetilde{s}) \sqsupseteq [(s_{\text{ref}}, s), (s_{\text{ref}}, s)]$ such that:
  1. $(h_1 \uplus [\ell_1 \mapsto v_1], h_2 \uplus [\ell_2 \mapsto v_2]) \in w\uparrow.\mathsf{H}(\widetilde{s_{\text{ref}}}, \widetilde{s})(G(\widetilde{s_{\text{ref}}}, \widetilde{s}))$
  2. $(\ell_1, \ell_2) \in \overline{G(\widetilde{s_{\text{ref}}}, \widetilde{s})}(\mathsf{ref}\ \delta\sigma)$
- From $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\text{ref}}, s)(G(s_{\text{ref}}, s))$ we know $h_i = h_i' \uplus h_i''$ for some h_1', h_1'', h_2', h_2'' with $(h_1', h_2') \in W_{\text{ref}}.\mathsf{H}(s_{\text{ref}})(G(s_{\text{ref}}, s))$ and $(h_1'', h_2'') \in w.\mathsf{H}(s_{\text{ref}})(s)(G(s_{\text{ref}}, s))$.
- Since $\ell_1 \notin \text{dom}(h_1')$ and $\ell_2 \notin \text{dom}(h_2')$, we therefore know that $s_{\text{ref}} \uplus \{(\delta\sigma, \ell_1, \ell_2)\}$ is well-defined and that $s_{\text{ref}} \uplus \{(\delta\sigma, \ell_1, \ell_2)\} \in W_{\text{ref}}.\mathsf{S}$.
- We choose $\widetilde{s_{\text{ref}}} = s_{\text{ref}} \uplus \{(\delta\sigma, \ell_1, \ell_2)\}$.
- Note that $\widetilde{s_{\text{ref}}} \sqsupseteq_{\text{pub}} s_{\text{ref}}$ and that $(h_1' \uplus [\ell_1 \mapsto v_1], h_2' \uplus [\ell_2 \mapsto v_2]) \in W_{\text{ref}}.\mathsf{H}(\widetilde{s_{\text{ref}}})(G(s_{\text{ref}}, s))$.
- By dependent monotonicity we also get $\widetilde{s} \sqsupseteq_{\text{pub}} s$ such that $(h_1'', h_2'') \in w.\mathsf{H}(\widetilde{s_{\text{ref}}})(\widetilde{s})(G(s_{\text{ref}}, s))$.
- Together this yields $(h_1 \uplus [\ell_1 \mapsto v_1], h_2 \uplus [\ell_2 \mapsto v_2]) \in w\uparrow.\mathsf{H}(\widetilde{s_{\text{ref}}}, \widetilde{s})(G(s_{\text{ref}}, s))$ and then (1) by monotonicity.
- To show (2) it suffices, by definition of GK, to show $(\ell_1, \ell_2) \in w\uparrow.\mathsf{L}(\widetilde{s_{\text{ref}}}, \widetilde{s})(G(\widetilde{s_{\text{ref}}}, \widetilde{s}))(\mathsf{ref}\ \delta\sigma)$.
- By definition of $\uparrow$ and W_{ref}, this in turn reduces to showing $(\delta\sigma, \ell_1, \ell_2) \in \widetilde{s_{\text{ref}}}$, which holds by construction.

$\square$

Lemma 32 (Compatibility: Deref)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \mathsf{ref}\ \sigma}{\Delta; \Gamma \vdash !e_1 \sim !e_2 : \sigma}$$

Proof.

- By Lemmas 15 and 17, it suffices to show $\forall G, s_{\text{ref}}, s.\ \forall \delta \in \text{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s))$,

$$(!\bullet, !\bullet) \in \mathbf{K}_{w\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))(\mathsf{ref}\ \delta\sigma, \delta\sigma)\ .$$

- Suppose $(v_1, v_2) \in \overline{G(s_{\text{ref}}, s)}(\mathsf{ref}\ \delta\sigma)$.
- We need to show $(!v_1, !v_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))(\delta\sigma)$.
- Suppose $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\text{ref}}, s)(G(s_{\text{ref}}, s))$ as well as defined$(h_1 \uplus h_1^{\text{F}})$ and defined$(h_2 \uplus h_2^{\text{F}})$.
- From $(v_1, v_2) \in \overline{G(s_{\text{ref}}, s)}(\mathsf{ref}\ \delta\sigma)$ we know by definition of GK and W_{ref} that $(\delta\sigma, v_1, v_2) \in s_{\text{ref}}$.
- From $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\text{ref}}, s)(G(s_{\text{ref}}, s))$ we know $(h_1', h_2') \in W_{\text{ref}}.\mathsf{H}(s_{\text{ref}})(G(s_{\text{ref}}, s))$ for some $h_1' \subseteq h_1$ and $h_2' \subseteq h_2$.
- From the definition of W_{ref} we thus get $(h_1'(v_1), h_2'(v_2)) \in \overline{G(s_{\text{ref}}, s)}(\delta\sigma)$.
- Hence we know $h_1 \uplus h_1^{\text{F}}, !v_1 \hookrightarrow h_1 \uplus h_1^{\text{F}}, h_1'(v_1)$ and $h_2 \uplus h_2^{\text{F}}, !v_2 \hookrightarrow h_2 \uplus h_2^{\text{F}}, h_2'(v_2)$.
- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $(\widetilde{s_{\text{ref}}}, \widetilde{s}) \sqsupseteq_{\text{pub}} (s_{\text{ref}}, s)$ such that:
  1. $(h_1, h_2) \in w\uparrow.\mathsf{H}(\widetilde{s_{\text{ref}}}, \widetilde{s})(G(\widetilde{s_{\text{ref}}}, \widetilde{s}))$
  2. $(h_1'(v_1), h_2'(v_2)) \in \overline{G(\widetilde{s_{\text{ref}}}, \widetilde{s})}(\delta\sigma)$
- We choose $(\widetilde{s_{\text{ref}}}, \widetilde{s}) = (s_{\text{ref}}, s)$ and are done.

$\square$

Lemma 33.

1. If $(\mathsf{ref}\,\tau, v_1, v_2) \in \overline{G(s_{\mathrm{ref}}, s)}$,
   then $(\tau, \mathsf{unit}, v_1 := \bullet, v_2 := \bullet) \in \mathbf{K}_{w\uparrow}(G)((s_{\mathrm{ref}}, s), (s_{\mathrm{ref}}, s))$.
2. If $(\tau, e_1', e_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{ref}}, s), (s_{\mathrm{ref}}, s))$,
   then $(\mathsf{ref}\,\tau, \mathsf{unit}, \bullet := e_1', \bullet := e_2') \in \mathbf{K}_{w\uparrow}(G)((s_{\mathrm{ref}}, s), (s_{\mathrm{ref}}, s))$.

Proof.

1.
   - Suppose $(v_1', v_2') \in \overline{G(s_{\mathrm{ref}}, s)}(\tau)$.
   - We need to show $(v_1 := v_1', v_2 := v_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{ref}}, s), (s_{\mathrm{ref}}, s))(\mathsf{unit})$.
   - Suppose $(h_1, h_2) \in w\!\uparrow\!.\mathsf{H}(s_{\mathrm{ref}}, s)(G(s_{\mathrm{ref}}, s))$ as well as defined$(h_1 \uplus h_1^{\mathrm{F}})$ and defined$(h_2 \uplus h_2^{\mathrm{F}})$.
   - From $(v_1, v_2) \in \overline{G(s_{\mathrm{ref}}, s)}(\mathsf{ref}\,\tau)$ we know by definition of GK and W_{ref} that $(\tau, v_1, v_2) \in s_{\mathrm{ref}}$.
   - From $(h_1, h_2) \in w\!\uparrow\!.\mathsf{H}(s_{\mathrm{ref}}, s)(G(s_{\mathrm{ref}}, s))$ we know $h_i = h_i' \uplus h_i''$ for some h_1', h_1'', h_2', h_2'' with $(h_1', h_2') \in W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{ref}})(G(s_{\mathrm{ref}}, s))$ and $(h_1'', h_2'') \in w.\mathsf{H}(s_{\mathrm{ref}})(s)(G(s_{\mathrm{ref}}, s))$.
   - From the definition of W_{ref} we thus get $v_1 \in \mathrm{dom}(h_1')$ and $v_2 \in \mathrm{dom}(h_2')$.
   - Hence $h_1 \uplus h_1^{\mathrm{F}}, v_1 := v_1' \hookrightarrow h_1[v_1 \mapsto v_1'] \uplus h_1^{\mathrm{F}}, \langle\rangle$ and $h_2 \uplus h_2^{\mathrm{F}}, v_2 := v_2' \hookrightarrow h_2[v_2 \mapsto v_2'] \uplus h_2^{\mathrm{F}}, \langle\rangle$.
   - By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $(\widetilde{s_{\mathrm{ref}}}, \widetilde{s}) \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{ref}}, s)$ such that:
     (a) $(h_1[v_1 \mapsto v_1'], h_2[v_2 \mapsto v_2']) \in w\!\uparrow\!.\mathsf{H}(\widetilde{s_{\mathrm{ref}}}, \widetilde{s})(G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s}))$
     (b) $(\langle\rangle, \langle\rangle) \in \overline{G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s})}(\mathsf{unit})$
   - We choose $(\widetilde{s_{\mathrm{ref}}}, \widetilde{s}) = (s_{\mathrm{ref}}, s)$.
   - Note that (b) is immediate.
   - Showing (a) reduces to showing $(v_1', v_2') \in \overline{G(\widetilde{s_{\mathrm{ref}}}, \widetilde{s})}(\tau)$, which is given.
2.
   - Suppose $(v_1, v_2) \in \overline{G(s_{\mathrm{ref}}, s)}(\mathsf{ref}\,\tau)$.
   - We need to show $(v_1 := e_1', v_2 := e_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{ref}}, s), (s_{\mathrm{ref}}, s))(\mathsf{unit})$.
   - By Lemma 13 it suffices to show
     $$(v_1 := \bullet, v_2 := \bullet) \in \mathbf{K}_{w\uparrow}(G')((s_{\mathrm{ref}}, s), (\widetilde{s_{\mathrm{ref}}}, \widetilde{s}))(\tau, \mathsf{unit})$$
     for $(\widetilde{s_{\mathrm{ref}}}, \widetilde{s}) \sqsupseteq_{\mathrm{pub}} (s_{\mathrm{ref}}, s)$ and $G' \geq G$.
   - By Lemma 7 it suffices to show $(v_1 := \bullet, v_2 := \bullet) \in \mathbf{K}_{w\uparrow}(G')((\widetilde{s_{\mathrm{ref}}}, \widetilde{s}), (\widetilde{s_{\mathrm{ref}}}, \widetilde{s}))(\tau, \mathsf{unit})$.
   - By part (1) it then suffices to show $(v_1, v_2) \in \overline{G'(\widetilde{s_{\mathrm{ref}}}, \widetilde{s})}(\mathsf{ref}\,\tau)$.
   - This follows from $(v_1, v_2) \in \overline{G(s_{\mathrm{ref}}, s)}(\mathsf{ref}\,\tau)$ by Lemma 1.

□

Lemma 34 (Compatibility: Assign)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \mathsf{ref}\,\sigma \qquad \Delta; \Gamma \vdash e_1' \sim e_2' : \sigma}{\Delta; \Gamma \vdash e_1 := e_1' \sim e_2 := e_2' : \mathsf{unit}}$$

Proof.

- By Lemmas 15 and 17, it suffices to show $\forall G, s_{\mathrm{ref}}, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,
  $$(\mathsf{ref}\,\delta\sigma, \mathsf{unit}, \bullet := \gamma_1 e_1', \bullet := \gamma_2 e_2') \in \mathbf{K}_{w\uparrow}(G)((s_{\mathrm{ref}}, s), (s_{\mathrm{ref}}, s))$$
  assuming $\Delta; \Gamma \vdash e_1' \sim_{w\uparrow} e_2' : \sigma$.

- By Lemma 33 it suffices to show $(\gamma_1 e_1', \gamma_2 e_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))(\delta\sigma)$, which follows from the assumption.

□

Lemma 35.

1. If $(\mathsf{ref}\,\tau, v_1, v_2) \in \overline{G(s_{\text{ref}}, s)}$,
   then $(\mathsf{ref}\,\tau, \mathsf{bool}, v_1 == \bullet, v_2 == \bullet) \in \mathbf{K}_{w\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))$.
2. If $(\mathsf{ref}\,\tau, e_1', e_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))$,
   then $(\mathsf{ref}\,\tau, \mathsf{bool}, \bullet == e_1', \bullet == e_2') \in \mathbf{K}_{w\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))$.

Proof.

1. - Suppose $(v_1', v_2') \in \overline{G(s_{\text{ref}}, s)}(\mathsf{ref}\,\tau)$.
   - We need to show $(v_1 == v_1', v_2 == v_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))(\mathsf{bool})$.
   - Suppose $(h_1, h_2) \in w\uparrow.\mathsf{H}(s_{\text{ref}}, s)(G(s_{\text{ref}}, s))$ as well as defined$(h_1 \uplus h_1^{\text{F}})$ and defined$(h_2 \uplus h_2^{\text{F}})$.
   - From $(v_1', v_2') \in \overline{G(s_{\text{ref}}, s)}(\mathsf{ref}\,\tau)$ we know by definition of GK and W_{ref} that $(\mathsf{ref}\,\tau, v_1', v_2') \in s_{\text{ref}}$.
   - From $(v_1, v_2) \in \overline{G(s_{\text{ref}}, s)}(\mathsf{ref}\,\tau)$ we know by definition of GK and W_{ref} that $(\mathsf{ref}\,\tau, v_1, v_2) \in s_{\text{ref}}$.
   - By definition of $W_{\text{ref}}.\mathsf{S}$ this yields $v_1 = v_1' \iff v_2 = v_2'$.
   - Hence either $h_1 \uplus h_1^{\text{F}}, v_1 == v_1' \hookrightarrow h_1 \uplus h_1^{\text{F}}, \mathsf{tt}$ and $h_2 \uplus h_2^{\text{F}}, v_2 == v_2' \hookrightarrow h_2 \uplus h_2^{\text{F}}, \mathsf{tt}$ or $h_1 \uplus h_1^{\text{F}}, v_1 == v_1' \hookrightarrow h_1 \uplus h_1^{\text{F}}, \mathsf{ff}$ and $h_2 \uplus h_2^{\text{F}}, v_2 == v_2' \hookrightarrow h_2 \uplus h_2^{\text{F}}, \mathsf{ff}$.
   - By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $(\widetilde{s_{\text{ref}}}, \widetilde{s}) \sqsupseteq_{\text{pub}} (s_{\text{ref}}, s)$ such that:
     (a) $(h_1, h_2) \in w\uparrow.\mathsf{H}(\widetilde{s_{\text{ref}}}, \widetilde{s})(G(\widetilde{s_{\text{ref}}}, \widetilde{s}))$
     (b) $(\mathsf{tt}, \mathsf{tt}) \in \overline{G(\widetilde{s_{\text{ref}}}, \widetilde{s})}(\mathsf{bool})$
     (c) $(\mathsf{ff}, \mathsf{ff}) \in \overline{G(\widetilde{s_{\text{ref}}}, \widetilde{s})}(\mathsf{bool})$
   - We choose $(\widetilde{s_{\text{ref}}}, \widetilde{s}) = (s_{\text{ref}}, s)$, and are done.
2. - Suppose $(v_1, v_2) \in \overline{G(s_{\text{ref}}, s)}(\mathsf{ref}\,\tau)$.
   - We need to show $(v_1 == e_1', v_2 == e_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))(\mathsf{bool})$.
   - By Lemma 13 it suffices to show

     $$(v_1 == \bullet, v_2 == \bullet) \in \mathbf{K}_{w\uparrow}(G')((s_{\text{ref}}, s), (\widetilde{s_{\text{ref}}}, \widetilde{s}))(\mathsf{ref}\,\tau, \mathsf{bool})$$

     for $(\widetilde{s_{\text{ref}}}, \widetilde{s}) \sqsupseteq_{\text{pub}} (s_{\text{ref}}, s)$ and $G' \geq G$.
   - By Lemma 7 it suffices to show $(v_1 == \bullet, v_2 == \bullet) \in \mathbf{K}_{w\uparrow}(G')((\widetilde{s_{\text{ref}}}, \widetilde{s}), (\widetilde{s_{\text{ref}}}, \widetilde{s}))(\mathsf{ref}\,\tau, \mathsf{bool})$.
   - By part (1) it then suffices to show $(v_1, v_2) \in \overline{G'(\widetilde{s_{\text{ref}}}, \widetilde{s})}(\mathsf{ref}\,\tau)$.
   - This follows from $(v_1, v_2) \in \overline{G(s_{\text{ref}}, s)}(\mathsf{ref}\,\tau)$ by Lemma 1.

□

Lemma 36 (Compatibility: Refeq)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \mathsf{ref}\,\sigma \qquad \Delta; \Gamma \vdash e_1' \sim e_2' : \mathsf{ref}\,\sigma}{\Delta; \Gamma \vdash e_1 == e_1' \sim e_2 == e_2' : \mathsf{bool}}$$

Proof.

- By Lemmas 15 and 17, it suffices to show $\forall G, s_{\text{ref}}, s.\ \forall \delta \in \text{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s))$,

$$(\mathsf{ref}\ \delta\sigma, \mathsf{bool}, \bullet == \gamma_1 e_1', \bullet == \gamma_2 e_2') \in \mathbf{K}_{w\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))$$

assuming $\Delta; \Gamma \vdash e_1' \sim_{w\uparrow} e_2' : \mathsf{ref}\ \sigma$.

- By Lemma 35 it suffices to show $(\gamma_1 e_1', \gamma_2 e_2') \in \mathbf{E}_{w\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))(\mathsf{ref}\ \delta\sigma)$, which follows from the assumption.

□

Lemma 37 (Compatibility: Gen)**.**

$$\frac{\Delta, \alpha; \Gamma \vdash e_1 \sim e_2 : \sigma}{\Delta; \Gamma \vdash \Lambda.\, e_1 \sim \Lambda.\, e_2 : \forall \alpha.\, \sigma}$$

Proof.

- For any $\mathcal{N}$, from the premise we have w such that $w.\mathsf{N} \subseteq \mathcal{N}$ and $\Delta, \alpha; \Gamma \vdash e_1 \sim_w e_2 : \sigma$.
- Let $w' = w_{\text{single}}(\lambda R.\ \{\ (\forall \alpha.\, \delta\sigma, \Lambda.\, \gamma_1 e_1, \Lambda.\, \gamma_2 e_2) \mid \delta \in \text{TyEnv}(\Delta), (\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, R)\}, \lambda R.\ \{(\emptyset, \emptyset)\ \})$.
- Since $(w \otimes w').\mathsf{N} = w.\mathsf{N} \subseteq \mathcal{N}$, it suffices to show $\Delta; \Gamma \vdash \Lambda.\, e_1 \sim_{w \otimes w'} \Lambda.\, e_2 : \forall \alpha.\, \sigma$.
- To do so, we first prove *inhabited*$((w \otimes w')\uparrow)$ and *consistent*$((w \otimes w')\uparrow)$:
  - *inhabited*$(w'\uparrow)$ is witnessed by state $(\emptyset, *)$, so *inhabited*$((w \otimes w')\uparrow)$ holds by Lemma 12.
  - The part of *consistent*$((w \otimes w')\uparrow)$ concerning arrow types follows from *consistent*$(w\uparrow)$ by Lemma 12, because $w'.\mathsf{L}$ doesn't relate anything at arrow types.
  - Regarding the part concerning universal types, we suppose
    1. $G \in \text{GK}((w \otimes w')\uparrow)$
    2. $(v_1, v_2) \in (w \otimes w')\uparrow.\mathsf{L}(s_{\text{ref}}, s, s')(G(s_{\text{ref}}, s, s'))(\forall \alpha.\, \widetilde{\sigma})$

    and must show:

$$\forall \tau \in \text{CType}.\ (\mathit{beta}(v_1[]), \mathit{beta}(v_2[])) \in \mathbf{E}_{(w \otimes w')\uparrow}(G)((s_{\text{ref}}, s, s'), (s_{\text{ref}}, s, s'))(\widetilde{\sigma}[\tau/\alpha])$$

  - From (2) and the definition of $\uparrow$ and $\otimes$ we know:

$$\begin{array}{l}(v_1, v_2) \in w\uparrow.\mathsf{L}(s_{\text{ref}}, s)(G(s_{\text{ref}}, s, s'))(\forall \alpha.\, \widetilde{\sigma}) \vee \\ (v_1, v_2) \in w'.\mathsf{L}(s_{\text{ref}})(s')(G(s_{\text{ref}}, s, s'))(\forall \alpha.\, \widetilde{\sigma})\end{array}$$

  - If the former is true, the claims follow from *consistent*$(w\uparrow)$ with the help of Lemmas 8 and 10.
  - So suppose the latter.
  - Then $\forall \alpha.\, \widetilde{\sigma} = \forall \alpha.\, \delta\sigma$ and $v_1 = \Lambda.\, \gamma_1 e_1$ and $v_2 = \Lambda.\, \gamma_2 e_2$ for $\delta \in \text{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_{\text{ref}}, s, s'))$.
  - Let $\delta' := \delta, \alpha \mapsto \tau$.
  - It remains to show $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{(w \otimes w')\uparrow}(G)((s_{\text{ref}}, s, s'), (s_{\text{ref}}, s, s'))(\delta'\sigma)$ since $\widetilde{\sigma}[\tau/\alpha] = \delta\sigma[\tau/\alpha] = \delta'\sigma$.
  - By Lemmas 8 and 10 it suffices to show $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}_{w\uparrow}(G(-, -, s'))((s_{\text{ref}}, s), (s_{\text{ref}}, s))(\delta'\sigma)$.
  - This follows from the premise since $\delta' \in \text{TyEnv}(\Delta, \alpha)$ and $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_{\text{ref}}, s, s')) = \text{Env}(\delta'\Gamma, G(s_{\text{ref}}, s, s'))$.
- Now suppose $G \in \text{GK}((w \otimes w')\uparrow)$ and $\delta \in \text{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s_{\text{ref}}, s, s'))$.

- We must show $(\Lambda.\, \gamma_1 e_1, \Lambda.\, \gamma_2 e_2) \in \mathbf{E}_{(w \otimes w')\uparrow}(G)((s_{\mathrm{ref}}, s, s'), (s_{\mathrm{ref}}, s, s'))(\forall \alpha.\, \delta\sigma)$.
- By Lemma 5 it suffices to show $(\Lambda.\, \gamma_1 e_1, \Lambda.\, \gamma_2 e_2) \in G(s_{\mathrm{ref}}, s, s')(\forall \alpha.\, \delta\sigma)$.
- By definition of GK it suffices to show:

$$(\Lambda.\, \gamma_1 e_1, \Lambda.\, \gamma_2 e_2) \in (w \otimes w')\uparrow.\mathsf{L}(s_{\mathrm{ref}}, s, s')(G(s_{\mathrm{ref}}, s, s'))(\forall \alpha.\, \delta\sigma)$$

- By definition of $\uparrow$ and $\otimes$ it suffices to show $(\Lambda.\, \gamma_1 e_1, \Lambda.\, \gamma_2 e_2) \in w'.\mathsf{L}(s')(G(s_{\mathrm{ref}}, s, s'))(\forall \alpha.\, \delta\sigma)$.
- Since $\delta \in \mathrm{TyEnv}(\Delta)$, $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{ref}}, s, s'))$, this holds by construction of w'.

□

Lemma 38 (Compatibility: Inst)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \forall \alpha.\, \sigma \quad \Delta \vdash \sigma'}{\Delta; \Gamma \vdash e_1[] \sim e_2[] : \sigma[\sigma'/\alpha]}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,

$$(\bullet[], \bullet[]) \in \mathbf{K}_W(G)(s, s)(\forall \alpha.\, \delta\sigma, \delta\sigma[\delta\sigma'/\alpha])\ .$$

- Suppose $(v_1^\circ, v_2^\circ) \in \overline{G(s)}(\forall \alpha.\, \delta\sigma)$.
- We need to show $(v_1^\circ[], v_2^\circ[]) \in \mathbf{E}_W(G)(s, s)(\delta\sigma[\delta\sigma'/\alpha])$.
- Since $(v_1^\circ, v_2^\circ) \in \overline{G(s)}(\forall \alpha.\, \delta\sigma)$, by definition of $\mathbf{E}_W$, it suffices to show

$$\forall s' \sqsupseteq_{\mathrm{pub}} s.\ \forall G' \geq G.\ (\bullet, \bullet) \in \mathbf{K}_W(G')(s, s')(\delta\sigma[\delta\sigma'/\alpha], \delta\sigma[\delta\sigma'/\alpha])$$

  which holds by Lemma 6.

□

Lemma 39 (Compatibility: Pack)**.**

$$\frac{\Delta \vdash \sigma' \quad \Delta; \Gamma \vdash e_1 \sim e_2 : \sigma[\sigma'/\alpha]}{\Delta; \Gamma \vdash \mathsf{pack}\ e_1 \sim \mathsf{pack}\ e_2 : \exists \alpha.\, \sigma}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,

$$(\mathsf{pack}\ \bullet, \mathsf{pack}\ \bullet) \in \mathbf{K}_W(G)(s, s)(\delta\sigma[\delta\sigma'/\alpha], \exists \alpha.\, \delta\sigma)\ .$$

- Suppose $(v_1, v_2) \in \overline{G(s)}(\delta\sigma[\delta\sigma'/\alpha])$.
- We need to show $(\mathsf{pack}\ v_1, \mathsf{pack}\ v_2) \in \mathbf{E}_W(G)(s, s)(\exists \alpha.\, \delta\sigma)$.
- By Lemma 5 it suffices to show $(\mathsf{pack}\ v_1, \mathsf{pack}\ v_2) \in \overline{G(s)}(\exists \alpha.\, \delta\sigma)$.
- This follows from $(v_1, v_2) \in \overline{G(s)}(\delta\sigma[\delta\sigma'/\alpha])$.

□

Lemma 40 (Compatibility: Unpack)**.**

$$\frac{\Delta; \Gamma \vdash e_1 \sim e_2 : \exists \alpha.\, \sigma \qquad \Delta, \alpha; \Gamma, x : \sigma \vdash e_1' \sim e_2' : \sigma' \qquad \Delta \vdash \sigma'}{\Delta; \Gamma \vdash \mathsf{unpack}\ e_1\ \mathsf{as}\ x\ \mathsf{in}\ e_1' \sim \mathsf{unpack}\ e_2\ \mathsf{as}\ x\ \mathsf{in}\ e_2' : \sigma'}$$

Proof.

- By Lemmas 16 and 17, it suffices to show $\forall G, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s))$,

  $$(\exists \alpha.\, \delta\sigma, \delta\sigma', \mathsf{unpack}\ \bullet\ \mathsf{as}\ x\ \mathsf{in}\ \gamma_1 e_1', \mathsf{unpack}\ \bullet\ \mathsf{as}\ x\ \mathsf{in}\ \gamma_2 e_2') \in \mathbf{K}_W(G)(s, s)$$

  assuming $\Delta, \alpha; \Gamma, x : \sigma \vdash e_1' \sim_W e_2' : \sigma'$.

- Thus it suffices to show that $\forall (v_1, v_2) \in \overline{G(s)}(\exists \alpha.\, \delta\sigma)$,

  $$(\delta\sigma', \mathsf{unpack}\ v_1\ \mathsf{as}\ x\ \mathsf{in}\ \gamma_1 e_1', \mathsf{unpack}\ v_2\ \mathsf{as}\ x\ \mathsf{in}\ \gamma_2 e_2') \in \mathbf{E}_W(G)(s, s)$$

- By definition of $\overline{G(s)}(\exists \alpha.\, \delta\sigma)$, we have v_1', v_2' and $\tau \in \mathrm{CType}$ such that

  $$v_1 = \mathsf{pack}\ v_1' \wedge v_2 = \mathsf{pack}\ v_2' \wedge (v_1', v_2') \in \overline{G(s)}(\delta\sigma[\tau/\alpha])$$

- Let $\delta' := \delta, \alpha \mapsto \tau$ and $\gamma_1' := \gamma_1, x \mapsto v_1'$ and $\gamma_2' := \gamma_2, x \mapsto v_2'$.
- Now suppose $(h_1, h_2) \in W.\mathsf{H}(s)(G(s))$ and $h_1^{\mathrm{F}}, h_2^{\mathrm{F}} \in \mathrm{Heap}$ with $h_1 \uplus h_1^{\mathrm{F}}, h_2 \uplus h_2^{\mathrm{F}}$ defined.
- We have $h_1 \uplus h_1^{\mathrm{F}}, \mathsf{unpack}\ v_1\ \mathsf{as}\ x\ \mathsf{in}\ \gamma_1 e_1' \hookrightarrow h_1 \uplus h_1^{\mathrm{F}}, \gamma_1' e_1'$ and $h_2 \uplus h_2^{\mathrm{F}}, \mathsf{unpack}\ v_2\ \mathsf{as}\ x\ \mathsf{in}\ \gamma_2 e_2' \hookrightarrow h_2 \uplus h_2^{\mathrm{F}}, \gamma_2' e_2'$ and thus by Lemma 4, it suffices to show

  $$(\delta\sigma', (h_1, h_1^{\mathrm{F}}, \gamma_1' e_1'), (h_2, h_2^{\mathrm{F}}, \gamma_2' e_2')) \in \mathbf{O}_W(\mathbf{E}_W)(G)(s, s)\ .$$

- This follows from the assumption and $\delta\sigma' = \delta'\sigma'$, $\delta' \in \mathrm{TyEnv}(\Delta, \alpha)$, $(\gamma_1', \gamma_2') \in \mathrm{Env}(\delta'(\Gamma, x : \tau), G(s))$.

□

2.4 Soundness

Theorem 41 (Fundamental Property)**.** If $\Delta; \Gamma \vdash p : \sigma$, then $\Delta; \Gamma \vdash |p| \sim |p| : \sigma$.

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

Lemma 42 (Weakening)**.** If $\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma$ and $\Delta \subseteq \Delta' \wedge \Gamma \subseteq \Gamma'$, then $\Delta'; \Gamma' \vdash e_1 \sim e_2 : \sigma$.

Proof. One can easily see that the goal is a direct consequence of the definition from the following observation:

$$\begin{array}{l} \forall R.\ \forall \delta \in \mathrm{TyEnv}(\Delta').\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma', R). \\ \lfloor \delta \rfloor_\Delta \in \mathrm{TyEnv}(\Delta) \wedge \lfloor \gamma \rfloor_{\mathrm{dom}(\Gamma)} \in \mathrm{Env}(\lfloor \delta \rfloor_\Delta \Gamma, R) \wedge \\ \gamma_1 e_1 = \lfloor \gamma \rfloor_{\mathrm{dom}(\Gamma)_{(1)}} e_1 \wedge \gamma_2 e_2 = \lfloor \gamma \rfloor_{\mathrm{dom}(\Gamma)_{(2)}} e_2 \end{array}$$

where $\lfloor f \rfloor_d$ denotes the restriction of the function f on domain d. □

Lemma 43 (Congruence)**.** If $\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma$ and $\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\Delta'; \Gamma'; \sigma')$, then

$$\Delta'; \Gamma' \vdash |C|[e_1] \sim |C|[e_2] : \sigma' \ .$$

Proof. By induction on the derivation of the context typing: in each case using the corresponding compatibility lemma. For a context containing subterms we also need Theorem 41. The rule for an empty context requires Lemma 42. □

Lemma 44 (Adequacy)**.** If $\cdot; \cdot \vdash e_1 \sim e_2 : \tau$, then

1. $\forall h_1, h_2$. neither h_1, e_1 nor h_2, e_2 gets stuck.
2. $\forall h_1, h_2$. $h_1, e_1 \uparrow \iff h_2, e_2 \uparrow$.

Proof.

- We know $\cdot; \cdot \vdash e_1 \sim_w e_2 : \tau$ for some w with $w.\mathsf{N} \subseteq \mathrm{TypeName}$.
- Hence we have *consistent*$(w\Uparrow)$ and *inhabited*$(w\Uparrow)$.
- Thus, using Lemma 2, there is s_0 such that $(\emptyset, \emptyset) \in w\Uparrow.\mathsf{H}(s_0)([w\Uparrow](s_0))$.
- We also have $(e_1, e_2) \in \mathbf{E}_{w\Uparrow}([w\Uparrow])(s_0, s_0)(\tau)$.
- Since *consistent*$(w\Uparrow)$, $(\emptyset, \emptyset) \in w\Uparrow.\mathsf{H}(s_0)([w\Uparrow](s_0))$ and $\forall s.\ [w\Uparrow](s) = w\Uparrow.\mathsf{L}(s)([w\Uparrow](s))$, by Corollary 19 for any heaps h_1, h_2 both h_1, e_1 and h_2, e_2 diverge or both terminate without getting stuck.

□

Theorem 45 (Soundness)**.** If $\Delta; \Gamma \vdash p_1 : \sigma$ and $\Delta; \Gamma \vdash p_2 : \sigma$, then:

$$\Delta; \Gamma \vdash |p_1| \sim |p_2| : \sigma \implies \Delta; \Gamma \vdash p_1 \sim_{\mathrm{ctx}} p_2 : \sigma$$

Proof.

- Suppose $\Delta; \Gamma \vdash |p_1| \sim |p_2| : \sigma$ as well as $\vdash C : (\Delta; \Gamma; \sigma) \rightsquigarrow (\cdot; \cdot; \tau)$.
- By congruence (Lemma 43), we have $\cdot; \cdot \vdash |C[p_1]| \sim |C[p_2]| : \tau$.
- By adequacy (Lemma 44), we have $h, |C[p_1]| \uparrow \iff h, |C[p_2]| \uparrow$ for any h, so we are done.

□

2.5 Symmetry

Definition 2. Given $R \in \text{VRel}$ (or VRelF), we define $R^{-1} \in \text{VRel}$ (or VRelF) as follows:

$$R^{-1} := \lambda\tau.\ R(\tau)^{-1}$$

Lemma 46. $(\overline{R})^{-1} = \overline{R^{-1}}$

Proof. Easy to check by induction. □

Lemma 47. $\mathbf{S}(R_f^{-1}, R_v^{-1}) = \big(\mathbf{S}(R_f, R_v)\big)^{-1}$

Proof. Easy to check. □

Definition 3. Given $w \in \text{LWorld}$, we define $w^{-1} \in \text{LWorld}$ as follows:

$$\begin{array}{lcl}
w^{-1}.\mathsf{N} & := & w.\mathsf{N} \\
w^{-1}.\mathsf{S} & := & w.\mathsf{S} \\
w^{-1}.\sqsupseteq & := & w.\sqsupseteq \\
w^{-1}.\sqsupseteq_{\text{pub}} & := & w.\sqsupseteq_{\text{pub}} \\
w^{-1}.\mathsf{L}(s_{\text{ref}})(s)(R) & := & \big(w.\mathsf{L}(s_{\text{ref}}^{-1})(s)(R^{-1})\big)^{-1} \\
w^{-1}.\mathsf{H}(s_{\text{ref}})(s)(R) & := & \big(w.\mathsf{H}(s_{\text{ref}}^{-1})(s)(R^{-1})\big)^{-1}
\end{array}$$

where $s_{\text{ref}}^{-1} \ := \ \lambda\tau.\ s_{\text{ref}}(\tau)^{-1}$.

Lemma 48. $w^{-1}{\uparrow}.\mathsf{H}(s_{\text{ref}}, s)(R) = \big(w{\uparrow}.\mathsf{H}(s_{\text{ref}}^{-1}, s)(R^{-1})\big)^{-1}$

Proof.

$$\begin{array}{cl}
 & w^{-1}{\uparrow}.\mathsf{H}(s_{\text{ref}}, s)(R) \\
= & W_{\text{ref}}.\mathsf{H}(s_{\text{ref}})(R) \otimes w^{-1}.\mathsf{H}(s_{\text{ref}})(s)(R) \\
= & \Big(\big(W_{\text{ref}}.\mathsf{H}(s_{\text{ref}})(R)\big)^{-1} \otimes \big(w^{-1}.\mathsf{H}(s_{\text{ref}})(s)(R)\big)^{-1}\Big)^{-1} \\
= & \big(W_{\text{ref}}.\mathsf{H}(s_{\text{ref}}^{-1})(R^{-1}) \otimes w.\mathsf{H}(s_{\text{ref}}^{-1})(s)(R^{-1})\big)^{-1} \\
= & \big(w{\uparrow}.\mathsf{H}(s_{\text{ref}}^{-1}, s)(R^{-1})\big)^{-1}
\end{array}$$

□

Lemma 49. $w^{-1}{\uparrow}.\mathsf{L}(s_{\text{ref}}, s)(R) = \big(w{\uparrow}.\mathsf{L}(s_{\text{ref}}^{-1}, s)(R^{-1})\big)^{-1}$

Proof. Analogous to Lemma 48. □

Definition 4. If $G \in \text{GK}(w^{-1}{\uparrow})$, we define $G^{-1} := \lambda s_{\text{ref}}, s.\ G(s_{\text{ref}}^{-1}, s)^{-1}$.

Lemma 50. If $G \in \text{GK}(w^{-1}{\uparrow})$, then $G^{-1} \in \text{GK}(w{\uparrow})$.

Proof.

1. Monotonicity of G^{-1} follows immediately from monotonicity of G.

2. It remains to show $\forall s_{\text{ref}}, s.\ G^{-1}(s_{\text{ref}}, s) \geq_{\text{ref}}^{w\uparrow.\mathsf{N}} w{\uparrow}.\mathsf{L}(s_{\text{ref}}, s)(G^{-1}(s_{\text{ref}}, s))$:

$$\begin{array}{cl}
 & G^{-1}(s_{\text{ref}}, s) \\
= & G(s_{\text{ref}}^{-1}, s)^{-1} \\
\geq_{\text{ref}}^{w\uparrow.\mathsf{N}} & \big(w^{-1}{\uparrow}.\mathsf{L}(s_{\text{ref}}^{-1}, s)(G(s_{\text{ref}}^{-1}, s))\big)^{-1} \\
= & w{\uparrow}.\mathsf{L}(s_{\text{ref}}, s)(G(s_{\text{ref}}^{-1}, s)^{-1}) \\
= & w{\uparrow}.\mathsf{L}(s_{\text{ref}}, s)(G^{-1}(s_{\text{ref}}, s))
\end{array}$$

□

Lemma 51. If $stable(w)$, then $stable(w^{-1})$.

Proof.

- We suppose
  1. $G \in \mathrm{GK}(w^{-1}\!\uparrow)$
  2. $(h_1, h_2) \in w^{-1}.\mathsf{H}(s_{\mathrm{ref}})(s)(G(s_{\mathrm{ref}}, s))$
  3. $s'_{\mathrm{ref}} \sqsupseteq s_{\mathrm{ref}}$
  4. $(h^1_{\mathrm{ref}}, h^2_{\mathrm{ref}}) \in W_{\mathrm{ref}}.\mathsf{H}(s'_{\mathrm{ref}})(G(s'_{\mathrm{ref}}, s))$
  5. $h^1_{\mathrm{ref}} \uplus h_1$ defined $\wedge\, h^2_{\mathrm{ref}} \uplus h_2$ defined

  and must show: $\exists s' \sqsupseteq_{\mathrm{pub}} s.\ (h_1, h_2) \in w^{-1}.\mathsf{H}(s'_{\mathrm{ref}})(s')(G(s'_{\mathrm{ref}}, s'))$
- From (2) we know $(h_2, h_1) \in w.\mathsf{H}(s^{-1}_{\mathrm{ref}})(s)(G(s_{\mathrm{ref}}, s)^{-1}) = w.\mathsf{H}(s^{-1}_{\mathrm{ref}})(s)(G^{-1}(s^{-1}_{\mathrm{ref}}, s))$.
- From (3) we know $s'^{-1}_{\mathrm{ref}} \sqsupseteq s^{-1}_{\mathrm{ref}}$.
- From (4) and Lemma 46 we know $(h^2_{\mathrm{ref}}, h^1_{\mathrm{ref}}) \in W_{\mathrm{ref}}.\mathsf{H}(s'^{-1}_{\mathrm{ref}})(G(s'_{\mathrm{ref}}, s)^{-1}) = W_{\mathrm{ref}}.\mathsf{H}(s'^{-1}_{\mathrm{ref}})(G^{-1}(s'^{-1}_{\mathrm{ref}}, s))$.
- Hence, using Lemma 50, the assumption yields $s' \sqsupseteq_{\mathrm{pub}} s$ such that

$$(h_2, h_1) \in w.\mathsf{H}(s'^{-1}_{\mathrm{ref}})(s')(G^{-1}(s'^{-1}_{\mathrm{ref}}, s')).$$

- This implies $(h_1, h_2) \in w^{-1}.\mathsf{H}(s'_{\mathrm{ref}})(s')(G(s'_{\mathrm{ref}}, s'))$.

□

Lemma 52. If $inhabited(w\!\uparrow)$, then $inhabited(w^{-1}\!\uparrow)$.

Proof.

- We suppose $G \in \mathrm{GK}(w^{-1}\!\uparrow)$ and must show $\exists s_0.\ (\emptyset, \emptyset) \in w^{-1}\!\uparrow.\mathsf{H}(s_0)(G(s_0))$.
- Using the assumption and Lemma 50, we get (s_{ref}, s) such that $(\emptyset, \emptyset) \in w\!\uparrow.\mathsf{H}(s_{\mathrm{ref}}, s)(G^{-1}(s_{\mathrm{ref}}, s))$.
- Lemma 48 implies $(\emptyset, \emptyset) \in w^{-1}\!\uparrow.\mathsf{H}(s^{-1}_{\mathrm{ref}}, s)(G(s^{-1}_{\mathrm{ref}}, s))$.

□

Lemma 53. If $G \in \mathrm{GK}(w^{-1}\!\uparrow)$, then:

$$\left(\mathbf{E}_{w\uparrow}(G^{-1})((s^{-1}_{\mathrm{ref}\,0}, s_0), (s^{-1}_{\mathrm{ref}}, s))\right)^{-1} \subseteq \mathbf{E}_{w^{-1}\uparrow}(G)((s_{\mathrm{ref}\,0}, s_0), (s_{\mathrm{ref}}, s))$$

Proof. Let

$$\begin{aligned}
\mathbf{E}'_{w^{-1}\uparrow}(G)((s_{\mathrm{ref}\,0}, s_0), (s_{\mathrm{ref}}, s))(\tau) \quad &:= \quad \left(\mathbf{E}_{w\uparrow}(G^{-1})((s^{-1}_{\mathrm{ref}\,0}, s_0), (s^{-1}_{\mathrm{ref}}, s))(\tau)\right)^{-1}, \\
\mathbf{K}'_{w^{-1}\uparrow}(G)((s_{\mathrm{ref}\,0}, s_0), (s_{\mathrm{ref}}, s))(\tau', \tau) \quad &:= \quad \left(\mathbf{K}_{w\uparrow}(G^{-1})((s^{-1}_{\mathrm{ref}\,0}, s_0), (s^{-1}_{\mathrm{ref}}, s))(\tau', \tau)\right)^{-1}.
\end{aligned}$$

By coinduction, it suffices to show:

1. $\forall e_2, e_1, G, s_{\mathrm{ref}\,0}, s_0, s_{\mathrm{ref}}, s, \tau.$
   $(e_2, e_1) \in \mathbf{E}'_{w^{-1}\uparrow}(G)((s_{\mathrm{ref}\,0}, s_0), (s_{\mathrm{ref}}, s))(\tau) \implies$
   $\forall (h_2, h_1) \in w^{-1}\!\uparrow.\mathsf{H}(s_{\mathrm{ref}}, s)(G(s_{\mathrm{ref}}, s)).\ \forall h^{\mathrm{F}}_2, h^{\mathrm{F}}_1.$
   $((h_2, h^{\mathrm{F}}_2, e_2), (h_1, h^{\mathrm{F}}_1, e_1)) \in \mathbf{O}_{w^{-1}\uparrow}(\mathbf{K}'_{w^{-1}\uparrow})(G)((s_{\mathrm{ref}\,0}, s_0), (s_{\mathrm{ref}}, s))(\tau)$

2. $\forall K_2, K_1, G, s_{\mathrm{ref}0}, s_0, s_{\mathrm{ref}}, s, \tau', \tau.$
$(K_2, K_1) \in \mathbf{K}'_{w^{-1}\uparrow}(G)((s_{\mathrm{ref}0}, s_0), (s_{\mathrm{ref}}, s))(\tau', \tau) \implies$
$\forall (v_2, v_1) \in \overline{G(s_{\mathrm{ref}}, s)}(\tau').$
$(K_2[v_2], K_1[v_1]) \in \mathbf{E}'_{w^{-1}\uparrow}(G)((s_{\mathrm{ref}0}, s_0), (s_{\mathrm{ref}}, s))(\tau)$

For (1):

- By definition of $\mathbf{E}'_{w^{-1}\uparrow}$ and Lemma 48, suppose $(e_1, e_2) \in \mathbf{E}_{w\uparrow}(G^{-1})((s^{-1}_{\mathrm{ref}0}, s_0), (s^{-1}_{\mathrm{ref}}, s))(\tau)$ and $(h_1, h_2) \in w\uparrow.\mathsf{H}(s^{-1}_{\mathrm{ref}}, s)(G^{-1}(s^{-1}_{\mathrm{ref}}, s))$.
- By definition of $\mathbf{E}_{w\uparrow}$ we have $((h_1, h^{\mathrm{F}}_1, e_1), (h_2, h^{\mathrm{F}}_2, e_2)) \in \mathbf{O}_{w\uparrow}(\mathbf{K}_{w\uparrow})(G^{-1})((s^{-1}_{\mathrm{ref}0}, s_0), (s^{-1}_{\mathrm{ref}}, s))(\tau)$.
- Using all the lemmas above, it is easy to check that this implies

$$((h_2, h^{\mathrm{F}}_2, e_2), (h_1, h^{\mathrm{F}}_1, e_1)) \in \mathbf{O}_{w^{-1}\uparrow}(\mathbf{K}'_{w^{-1}\uparrow})(G)((s_{\mathrm{ref}0}, s_0), (s_{\mathrm{ref}}, s))(\tau) \ .$$

For (2):

- By definition of $\mathbf{K}'_{w^{-1}\uparrow}$ and Lemma 46, suppose $(K_1, K_2) \in \mathbf{K}_{w\uparrow}(G^{-1})((s^{-1}_{\mathrm{ref}0}, s_0), (s^{-1}_{\mathrm{ref}}, s))(\tau', \tau)$ and $(v_1, v_2) \in \overline{G^{-1}(s^{-1}_{\mathrm{ref}}, s)}(\tau')$.
- By definition of $\mathbf{K}_{w\uparrow}$ we have $(K_1[v_1], K_2[v_2]) \in \mathbf{E}_{w\uparrow}(G^{-1})((s^{-1}_{\mathrm{ref}0}, s_0), (s^{-1}_{\mathrm{ref}}, s))(\tau)$.
- By definition of $\mathbf{E}'_{w^{-1}\uparrow}$, it implies that $(K_2[v_2], K_1[v_1]) \in \mathbf{E}'_{w^{-1}\uparrow}(G)((s_{\mathrm{ref}0}, s_0), (s_{\mathrm{ref}}, s))(\tau)$.

□

Lemma 54. If *consistent*$(w\uparrow)$, then *consistent*$(w^{-1}\uparrow)$.

Proof.

- We suppose $G \in \mathrm{GK}(w^{-1}\uparrow)$ and $(e_1, e_2) \in \mathbf{S}(w^{-1}\uparrow.\mathsf{L}(s_{\mathrm{ref}}, s)(G(s_{\mathrm{ref}}, s)), G(s_{\mathrm{ref}}, s))(\tau)$, and must show $(\mathit{beta}(e_1), \mathit{beta}(e_2)) \in \mathbf{E}_{w^{-1}\uparrow}(G)((s_{\mathrm{ref}}, s), (s_{\mathrm{ref}}, s))(\tau)$.
- By Lemma 47 we know $(e_2, e_1) \in \mathbf{S}(w\uparrow.\mathsf{L}(s^{-1}_{\mathrm{ref}}, s)(G^{-1}(s^{-1}_{\mathrm{ref}}, s)), G^{-1}(s^{-1}_{\mathrm{ref}}, s))(\tau)$.
- Using the assumption and Lemma 50, we get $(\mathit{beta}(e_2), \mathit{beta}(e_1)) \in \mathbf{E}_{w\uparrow}(G^{-1})((s^{-1}_{\mathrm{ref}}, s), (s^{-1}_{\mathrm{ref}}, s))(\tau)$.
- We are done by Lemma 53.

□

Theorem 55. If $\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma$, then $\Delta; \Gamma \vdash e_2 \sim e_1 : \sigma$.

Proof. Suppose $\Delta; \Gamma \vdash e_1 \sim_w e_2 : \sigma$ with *stable*(w). By Lemma 51 it suffices to show $\Delta; \Gamma \vdash e_2 \sim_{w^{-1}} e_1 : \sigma$. Using Lemmas 52 and 54, this in turn reduces to showing:

$$\begin{array}{l}\forall G \in \mathrm{GK}(w^{-1}\uparrow).\ \forall s_{\mathrm{ref}}, s.\ \forall \delta \in \mathrm{TyEnv}(\Delta).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{ref}}, s)).\\ \quad (\gamma_1 e_2, \gamma_2 e_1) \in \mathbf{E}_{w^{-1}\uparrow}(G)((s_{\mathrm{ref}}, s), (s_{\mathrm{ref}}, s))(\delta\sigma)\end{array}$$

From $(\gamma_1, \gamma_2) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{ref}}, s))$ we have $(\gamma_2, \gamma_1) \in \mathrm{Env}(\delta\Gamma, G(s_{\mathrm{ref}}, s)^{-1}) = \mathrm{Env}(\delta\Gamma, G^{-1}(s^{-1}_{\mathrm{ref}}, s))$. Lemma 50 and the assumption thus yield $(\gamma_2 e_1, \gamma_1 e_2) \in \mathbf{E}_{w\uparrow}(G^{-1})((s^{-1}_{\mathrm{ref}}, s), (s^{-1}_{\mathrm{ref}}, s))(\delta\sigma)$. We are done by Lemma 53. □

3 Examples

3.1 World Generator

$$\text{NLWorld} := \{\, \mathcal{W} \in \text{Names} \to \text{LWorld} \mid \forall \mathcal{N}.\ \mathcal{W}(\mathcal{N}).\mathsf{N} \subseteq \mathcal{N} \,\}$$

Definition 5. We define $\mathbf{G} : \text{NLWorld} \to \text{NLWorld}$ as follows.

$$\begin{array}{ll} \mathbf{G}(\mathcal{W})(\mathcal{N}).\mathsf{N} & := \mathcal{N} \\ \mathbf{G}(\mathcal{W})(\mathcal{N}).\mathsf{S} & := \{\, (s_1, \ldots, s_n) \mid n \in \mathbb{N} \wedge \forall i \in \{1 \ldots n\}.\ s_i \in \mathcal{W}(\mathcal{N}_i).\mathsf{S} \,\} \\ \mathbf{G}(\mathcal{W})(\mathcal{N}).\mathsf{L}(s_{\text{ref}})(s_1, \ldots, s_n)(R) & := \bigcup_{i \in \{1 \ldots n\}} \mathcal{W}(\mathcal{N}_i).\mathsf{L}(s_{\text{ref}})(s_i)(R) \\ \mathbf{G}(\mathcal{W})(\mathcal{N}).\mathsf{H}(s_{\text{ref}})(s_1, \ldots, s_n)(R) & := \otimes_{i \in \{1 \ldots n\}} \mathcal{W}(\mathcal{N}_i).\mathsf{H}(s_{\text{ref}})(s_i)(R) \end{array}$$

where $\{\, \mathcal{N}_i \,\}$ is a countably infinite splitting of $\mathcal{N}$ *i.e.*, $\mathcal{N} = \mathcal{N}_1 \uplus \mathcal{N}_2 \uplus \mathcal{N}_3 \uplus \ldots$.
The transition on $\mathbf{G}(\mathcal{W})(\mathcal{N})$ is generated by the following rule.

$$\begin{array}{rll} (s_1, \ldots, s_k, s_{k+1}) \sqsupseteq_{\text{pub}} (s_1, \ldots, s_k) & & \\ (s'_1, \ldots, s'_k) \sqsupseteq_{\text{pub}} (s_1, \ldots, s_k) & \text{if} & s'_1 \sqsupseteq_{\text{pub}} s_1 \wedge \ldots \wedge s'_k \sqsupseteq_{\text{pub}} s_k \\ (s'_1, \ldots, s'_k) \sqsupseteq (s_1, \ldots, s_k) & \text{if} & s'_1 \sqsupseteq s_1 \wedge \ldots \wedge s'_k \sqsupseteq s_k \\ (s'_1, \ldots, s'_j) \sqsupseteq (s_1, \ldots, s_k) & \text{if} & (s'_1, \ldots, s'_j) \sqsupseteq_{\text{pub}} (s_1, \ldots, s_k) \end{array}$$

We define the following notation.

$$\begin{array}{rcl} \{n \backslash i\} & := & \{\, 1, \ldots, i-1, i+1, \ldots, n \,\} \\ G(\{s_k\}_{k \in \{n \backslash i\}}) & := & G(-, s_1, \ldots, s_{i-1}, -, s_{i+1}, \ldots, s_n) \end{array}$$

Lemma 56.

$$\forall G \in \text{GK}(\mathbf{G}(\mathcal{W})(\mathcal{N})\!\uparrow).\ \forall s_1 \ldots s_{i-1}, s_{i+1} \ldots s_n.\ G(\{s_k\}_{k \in \{n \backslash i\}}) \in \text{GK}(\mathcal{W}(\mathcal{N}_i)\!\uparrow)$$

Proof.

- We need to show $G(\{s_k\}_{k \in \{n \backslash i\}})$ is monotone w.r.t. $\sqsubseteq$, which follows directly from the definition of $\sqsubseteq$ and monotonicity of G.
- We have

$$\begin{array}{ll} & G(\{s_k\}_{k \in \{n \backslash i\}})(s_{\text{ref}}, s_i) \\ = & G(s_{\text{ref}}, s_1 \ldots s_n) \\ \geq^{\mathcal{N}}_{\text{ref}} & \mathbf{G}(\mathcal{W})(\mathcal{N})\!\uparrow.\mathsf{L}(s_{\text{ref}}, s_1 \ldots s_n)(G(s_{\text{ref}}, s_1 \ldots s_n)) \\ \geq & \mathcal{W}(\mathcal{N}_i)\!\uparrow.\mathsf{L}(s_{\text{ref}}, s_i)(G(s_{\text{ref}}, s_1, \ldots, s_n)) \\ = & \mathcal{W}(\mathcal{N}_i)\!\uparrow.\mathsf{L}(s_{\text{ref}}, s_i)(G(\{s_k\}_{k \in \{n \backslash i\}})(s_{\text{ref}}, s_i))\ . \end{array}$$

- Now it suffices to show that the latter inequality is contained in $\geq^{\mathcal{N}_i}_{\text{ref}}$, which follows from $\forall i.\ \mathcal{W}(\mathcal{N}_i) \in$ LWorld and the fact that $\mathcal{N}_1, \ldots, \mathcal{N}_n$ are disjoint.

□

Lemma 57. If $W = \mathbf{G}(\mathcal{W})(\mathcal{N})\!\uparrow$ and $\forall \mathcal{N}'.\ \textit{stable}(\mathcal{W}(\mathcal{N}'))$ and $G \in \text{GK}(W)$, then:

1. $\mathbf{E}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \backslash i\}}))((s^0_{\text{ref}}, s^0_i), (s_{\text{ref}}, s_i)) \leq \mathbf{E}_W(G)((s^0_{\text{ref}}, s_1 \ldots s_{i-1}, s^0_i, s_{i+1} \ldots s_n), (s_{\text{ref}}, s_1 \ldots s_n))$
2. $\mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \backslash i\}}))((s^0_{\text{ref}}, s^0_i), (s_{\text{ref}}, s_i)) \leq \mathbf{K}_W(G)((s^0_{\text{ref}}, s_1 \ldots s_{i-1}, s^0_i, s_{i+1} \ldots s_n), (s_{\text{ref}}, s_1 \ldots s_n))$

Proof. We define $\mathbf{E}'_W$ and $\mathbf{K}'_W$ as follows:

$$\begin{array}{l} \mathbf{E}'_W(G)((s^0_{\text{ref}}, s^0_1 \ldots s^0_{n_0}), (s_{\text{ref}}, s_1 \ldots s_n)) = \{\, (\tau, e_1, e_2) \mid \\ \qquad (\forall k \in \{n_0 \backslash i\}.\ s_k \sqsupseteq_{\text{pub}} s^0_k) \wedge (\tau, e_1, e_2) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \backslash i\}}))((s^0_{\text{ref}}, s^0_i), (s_{\text{ref}}, s_i)) \,\} \\ \mathbf{K}'_W(G)((s^0_{\text{ref}}, s^0_1 \ldots s^0_{n_0}), (s_{\text{ref}}, s_1 \ldots s_n)) = \{\, (\tau', \tau, K_1, K_2) \mid \\ \qquad (\forall k \in \{n_0 \backslash i\}.\ s_k \sqsupseteq_{\text{pub}} s^0_k) \wedge (\tau', \tau, K_1, K_2) \in \mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \backslash i\}}))((s^0_{\text{ref}}, s^0_i), (s_{\text{ref}}, s_i)) \,\} \end{array}$$

Then it suffices to show $\mathbf{E}'_W \leq \mathbf{E}_W$ and $\mathbf{K}'_W \leq \mathbf{K}_W$ by coinduction. Concretely, we have to show:

1. $\forall e_1, e_2, G, s^0_{\text{ref}}, s^0_1 \ldots s^0_{n_0}, s_{\text{ref}}, s_1 \ldots s_n, \tau.$
   $(e_1, e_2) \in \mathbf{E}'_W(G)((s^0_{\text{ref}}, s^0_1 \ldots s^0_{n_0}), (s_{\text{ref}}, s_1 \ldots s_n))(\tau) \implies$
   $\forall (h_1, h_2) \in W.\mathsf{H}(s_{\text{ref}}, s_1 \ldots s_n)(G(s_{\text{ref}}, s_1 \ldots s_n)). \forall h^{\text{F}}_1, h^{\text{F}}_2.$
   $((h_1, h^{\text{F}}_1, e_1), (h_2, h^{\text{F}}_2, e_2)) \in \mathbf{O}_W(\mathbf{K}'_W)(G)((s^0_{\text{ref}}, s^0_1 \ldots s^0_{n_0}), (s_{\text{ref}}, s_1 \ldots s_n))(\tau)$

2. $\forall K_1, K_2, G, s^0_{\text{ref}}, s^0_1 \ldots s^0_{n_0}, s_{\text{ref}}, s_1 \ldots s_n, \tau', \tau.$
   $(K_1, K_2) \in \mathbf{K}'_W(G)((s^0_{\text{ref}}, s^0_1 \ldots s^0_{n_0}), (s_{\text{ref}}, s_1 \ldots s_n))(\tau', \tau) \implies$
   $\forall (v_1, v_2) \in \overline{G(s_{\text{ref}}, s_1 \ldots s_n)}(\tau').\ (K_1[v_1], K_2[v_2]) \in \mathbf{E}'_W(G)((s^0_{\text{ref}}, s^0_1 \ldots s^0_{n_0}), (s_{\text{ref}}, s_1 \ldots s_n))(\tau)$

For (1):

- Suppose $(e_1, e_2) \in \mathbf{E}'_W(G)((s^0_{\text{ref}}, s^0_1 \ldots s^0_{n_0}), (s_{\text{ref}}, s_1 \ldots s_n))(\tau)$ and $(h_1, h_2) \in W.\mathsf{H}(s_{\text{ref}}, s_1 \ldots s_n)(G(s_{\text{ref}}, s_1 \ldots s_n))$.
- By definition of $\mathbf{E}'_W$ we have $(\forall k \in \{n_0 \backslash i\}.\ s_k \sqsupseteq_{\text{pub}} s^0_k)$ and

$$(\tau, e_1, e_2) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k \in \{n \backslash i\}}))((s^0_{\text{ref}}, s^0_i), (s_{\text{ref}}, s_i))\ .$$

- We must show $((h_1, h^{\text{F}}_1, e_1), (h_2, h^{\text{F}}_2, e_2)) \in \mathbf{O}_W(\mathbf{K}'_W)(G)((s^0_{\text{ref}}, s^0_1 \ldots s^0_{n_0}), (s_{\text{ref}}, s_1 \ldots s_n))(\tau)$.
- So suppose defined$(h_1 \uplus h^{\text{F}}_1)$ and defined$(h_2 \uplus h^{\text{F}}_2)$.
- From $(h_1, h_2) \in W.\mathsf{H}(s_{\text{ref}}, s_1 \ldots s_n)(G(s_{\text{ref}}, s_1 \ldots s_n))$, we have $h_1 = h'_1 \uplus h''_1$ and $h_2 = h'_2 \uplus h''_2$ with $(h'_1, h'_2) \in \mathcal{W}(\mathcal{N}_i)\uparrow.\mathsf{H}(s_{\text{ref}}, s_i)(G(s_{\text{ref}}, s_1 \ldots s_n))$ and $(h''_1, h''_2) \in \otimes_{k \in \{n \backslash i\}} \mathcal{W}(\mathcal{N}_k).\mathsf{H}(s_{\text{ref}})(s_k)(G(s_{\text{ref}}, s_1 \ldots s_n))$.
- Hence $((h'_1, h''_1 \uplus h^{\text{F}}_1, e_1), (h'_2, h''_2 \uplus h^{\text{F}}_2, e_2)) \in \mathbf{O}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(\mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow})(G(\{s_k\}_{k \in \{n \backslash i\}}))((s^0_{\text{ref}}, s^0_i), (s_{\text{ref}}, s_i))(\tau)$.
- Consequently at least one of the following three properties holds:

  A) $h_1 \uplus h^{\text{F}}_1, e_1 \uparrow$ and $h_2 \uplus h^{\text{F}}_2, e_2 \uparrow$

  B) (a) $h_1 \uplus h^{\text{F}}_1, e_1 \hookrightarrow^* \widetilde{h'_1} \uplus h''_1 \uplus h^{\text{F}}_1, v_1$ and $h_2 \uplus h^{\text{F}}_2, e_2 \hookrightarrow^* \widetilde{h'_2} \uplus h''_2 \uplus h^{\text{F}}_2, v_2$
     (b) $(\widetilde{s_{\text{ref}}}, \widetilde{s_i}) \sqsupseteq [(s^0_{\text{ref}}, s^0_i), (s_{\text{ref}}, s_i)]$
     (c) $(\widetilde{h'_1}, \widetilde{h'_2}) \in \mathcal{W}(\mathcal{N}_i)\uparrow.\mathsf{H}(\widetilde{s_{\text{ref}}}, \widetilde{s_i})(G(\widetilde{s_{\text{ref}}}, s_1 \ldots s_{i-1}, \widetilde{s_i}, s_{i+1} \ldots s_n))$
     (d) $(v_1, v_2) \in \overline{G(\widetilde{s_{\text{ref}}}, s_1 \ldots s_{i-1}, \widetilde{s_i}, s_{i+1} \ldots s_n)}(\tau)$

  C) (a) $h_1 \uplus h^{\text{F}}_1, e_1 \hookrightarrow^* \widetilde{h'_1} \uplus h''_1 \uplus h^{\text{F}}_1, v_1$ and $h_2 \uplus h^{\text{F}}_2, e_2 \hookrightarrow^* \widetilde{h'_2} \uplus h''_2 \uplus h^{\text{F}}_2, v_2$
     (b) $(\widetilde{s_{\text{ref}}}, \widetilde{s_i}) \sqsupseteq (s_{\text{ref}}, s_i)$
     (c) $(\widetilde{h'_1}, \widetilde{h'_2}) \in \mathcal{W}(\mathcal{N}_i)\uparrow.\mathsf{H}(\widetilde{s_{\text{ref}}}, \widetilde{s_i})(G(\widetilde{s_{\text{ref}}}, s_1 \ldots s_{i-1}, \widetilde{s_i}, s_{i+1} \ldots s_n))$
     (d) $(e'_1, e'_2) \in \mathbf{S}(G(\widetilde{s_{\text{ref}}}, s_1 \ldots s_{i-1}, \widetilde{s_i}, s_{i+1} \ldots s_n), G(\widetilde{s_{\text{ref}}}, s_1 \ldots s_{i-1}, \widetilde{s_i}, s_{i+1} \ldots s_n))(\widetilde{\tau})$
     (e) $\forall (\widehat{s_{\text{ref}}}, \widehat{s_i}) \sqsupseteq_{\text{pub}} (\widetilde{s_{\text{ref}}}, \widetilde{s_i}).\ \forall G' \geq G(\{s_k\}_{k \in \{n \backslash i\}}).\ (K_1, K_2) \in \mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G')((s^0_{\text{ref}}, s^0_i), (\widehat{s_{\text{ref}}}, \widehat{s_i}))(\widetilde{\tau}, \tau)$

- If (A) holds, then we are done.
- If (B) holds:
  - For all $k \in \{n \setminus i\}$, iteratively applying *stable*$(\mathcal{W}(\mathcal{N}_k))$ and using monotonicity gets us $\widetilde{s_k} \sqsupseteq_{\text{pub}} s_k$ such that:

$$(h''_1, h''_2) \in \otimes_{k \in \{n \backslash i\}} \mathcal{W}(\mathcal{N}_k).\mathsf{H}(\widetilde{s_{\text{ref}}})(\widetilde{s_k})(G(\widetilde{s_{\text{ref}}}, \widetilde{s_1} \ldots \widetilde{s_n}))$$

  - Thus from (Bc), monotonicity, and the definition of W we get

$$(\widetilde{h'_1} \uplus h''_1, \widetilde{h'_2} \uplus h''_2) \in W.\mathsf{H}(\widetilde{s_{\text{ref}}}, \widetilde{s_1} \ldots \widetilde{s_n})(G(\widetilde{s_{\text{ref}}}, \widetilde{s_1} \ldots \widetilde{s_n}))$$

  - From (Bb) we get $(\widetilde{s_{\text{ref}}}, \widetilde{s_1} \ldots \widetilde{s_n}) \sqsupseteq [(s^0_{\text{ref}}, s^0_1 \ldots s^0_{n_0}), (s_{\text{ref}}, s_1 \ldots s_n)]$.
  - Together with (Ba), (Bd), and monotonicity we are done.

- If (C) holds:
  - For all $k \in \{n \setminus i\}$, iteratively applying $\mathit{stable}(\mathcal{W}(\mathcal{N}_k))$ and using monotonicity gets us $\widetilde{s_k} \sqsupseteq_{\text{pub}} s_k$ such that:
$$(h_1'', h_2'') \in \otimes_{k\in\{n\setminus i\}} \mathcal{W}(\mathcal{N}_k).\mathsf{H}(\widetilde{s_{\text{ref}}})(\widetilde{s_k})(G(\widetilde{s_{\text{ref}}}, \widetilde{s_1} \dots \widetilde{s_n}))$$
  - Thus from (Cc), monotonicity, and the definition of W we get
$$(\widetilde{h_1'} \uplus h_1'', \widetilde{h_2'} \uplus h_2'') \in W.\mathsf{H}(\widetilde{s_{\text{ref}}}, \widetilde{s_1} \dots \widetilde{s_n})(G(\widetilde{s_{\text{ref}}}, \widetilde{s_1} \dots \widetilde{s_n}))$$
  - From (Cb) we get $(\widetilde{s_{\text{ref}}}, \widetilde{s_1} \dots \widetilde{s_n}) \sqsupseteq [(s^0_{\text{ref}}, s^0_1 \dots s^0_{n_0}), (s_{\text{ref}}, s_1 \dots s_n)]$.
  - After applying monotonicity to (Cd), it remains to show:
$$\begin{array}{l}\forall(\widehat{s_{\text{ref}}}, \widehat{s_1} \dots \widehat{s_m}) \sqsupseteq_{\text{pub}} (\widetilde{s_{\text{ref}}}, \widetilde{s_1} \dots \widetilde{s_n}).\ \forall G' \geq G.\\ (K_1, K_2) \in \mathbf{K}'_W(G')((s^0_{\text{ref}}, s^0_1 \dots s^0_{n_0}), (\widehat{s_{\text{ref}}}, \widehat{s_1} \dots \widehat{s_m}))(\widetilde{\tau}, \tau)\end{array}$$
  - So suppose $(\widehat{s_{\text{ref}}}, \widehat{s_1} \dots \widehat{s_m}) \sqsupseteq_{\text{pub}} (\widetilde{s_{\text{ref}}}, \widetilde{s_1} \dots \widetilde{s_n})$ and $G' \geq G$.
  - By monotonicity we have $G'(\{\widehat{s_k}\}_{k\in\{m\setminus i\}}) \geq G(\{s_k\}_{k\in\{n\setminus i\}})$.
  - From (Ce) we therefore get $(K_1, K_2) \in \mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G'(\{\widehat{s_k}\}_{k\in\{m\setminus i\}}))((s^0_{\text{ref}}, s^0_i), (\widehat{s_{\text{ref}}}, \widehat{s_i}))(\widetilde{\tau}, \tau)$.
  - By definition of $\mathbf{K}'_W$ this implies $(K_1, K_2) \in \mathbf{K}'_W(G')((s^0_{\text{ref}}, s^0_1 \dots s^0_{n_0}), (\widehat{s_{\text{ref}}}, \widehat{s_1} \dots \widehat{s_m}))(\widetilde{\tau}, \tau)$.

For (2):

- Suppose $(K_1, K_2) \in \mathbf{K}'_W(G)((s^0_{\text{ref}}, s^0_1 \dots s^0_{n_0}), (s_{\text{ref}}, s_1 \dots s_n))(\tau', \tau)$ and $(v_1, v_2) \in \overline{G(s_{\text{ref}}, s_1 \dots s_n)}(\tau')$.
- By definition of $\mathbf{K}'_W$ we have $(\forall k \in \{n_0 \setminus i\}.\ s_k \sqsupseteq_{\text{pub}} s^0_k)$ and
$$(\tau', \tau, K_1, K_2) \in \mathbf{K}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k\in\{n\setminus i\}}))((s^0_{\text{ref}}, s^0_i), (s_{\text{ref}}, s_i))\ .p$$
- We must show $(\tau, K_1[v_1], K_2[v_2]) \in \mathbf{E}'_W(G)((s^0_{\text{ref}}, s^0_1 \dots s^0_{n_0}), (s_{\text{ref}}, s_1 \dots s_n))$.
- By definition of $\mathbf{E}'_W$ it suffices to show
$$(\tau, K_1[v_1], K_2[v_2]) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}_i)\uparrow}(G(\{s_k\}_{k\in\{n\setminus i\}}))((s^0_{\text{ref}}, s^0_i), (s_{\text{ref}}, s_i))\ .$$
- Since $(v_1, v_2) \in \overline{G(s_{\text{ref}}, s_1 \dots s_n)}(\tau')$, we are done.

□

Lemma 58. Suppose $\forall\mathcal{N}.\ \mathit{stable}(\mathcal{W}(\mathcal{N}))$.

1. $\forall\mathcal{N}.\ \mathit{stable}(\mathbf{G}(\mathcal{W})(\mathcal{N}))$
2. If $\forall\mathcal{N}.\ \mathit{consistent}(\mathcal{W}(\mathcal{N})\uparrow)$, then $\forall\mathcal{N}.\ \mathit{consistent}(\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow)$.

Proof.

- We suppose
  (a) $G \in \mathrm{GK}(\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow)$
  (b) $(\tau, e_1, e_2) \in \mathbf{S}(\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow.\mathsf{L}(s_{\text{ref}}, s_1 \dots s_n)(G(s_{\text{ref}}, s_1 \dots s_n)), G(s_{\text{ref}}, s_1 \dots s_n))$

  and must show $(\tau, \mathit{beta}(e_1), \mathit{beta}(e_2)) \in \mathbf{E}_{\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow}(G)((s_{\text{ref}}, s_1 \dots s_n), (s_{\text{ref}}, s_1 \dots s_n))$.
- From (b) and the definition of $\mathbf{S}$ we know: for some i,
$$(\tau, e_1, e_2) \in \mathbf{S}(\mathcal{W}(\mathcal{N}_i)\uparrow.\mathsf{L}(s_{\text{ref}}, s_i)(G(s_{\text{ref}}, s_1 \dots s_n)), G(s_{\text{ref}}, s_1 \dots s_n))$$
- The claim follows from $\mathit{consistent}(\mathcal{W}(\mathcal{N}_i)\uparrow)$ with the help of Lemmas 56 and 57.

□

Lemma 59. $\mathit{inhabited}(\mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow)$

Proof. It is easy to check that $(\emptyset, \emptyset) \in \mathbf{G}(\mathcal{W})(\mathcal{N})\uparrow.\mathsf{H}(\emptyset, ())(R)$ for any R. □

3.2 Substitutivity

Theorem 60.

$$\frac{\Delta; \Gamma, x{:}\sigma' \vdash e_1 \sim e_2 : \sigma \qquad \Delta; \Gamma \vdash v_1 \sim v_2 : \sigma'}{\Delta; \Gamma \vdash e_1[v_1/x] \sim e_2[v_2/x] : \sigma}$$

Proof. By Lemma 16 it suffices to show:

$$\frac{\Delta; \Gamma, x{:}\sigma' \vdash e_1 \sim_W e_2 : \sigma \qquad \Delta; \Gamma \vdash v_1 \sim_W v_2 : \sigma'}{\Delta; \Gamma \vdash e_1[v_1/x] \sim_W e_2[v_2/x] : \sigma}$$

This boils down to showing

$$(\delta\sigma, \gamma_1(e_1[v_1/x]), \gamma_2(e_2[v_2/x])) \in \mathbf{E}_W(G)(s, s)$$

for $\delta \in \text{TyEnv}(\Delta)$ and $(\gamma_1, \gamma_2) \in \text{Env}(\delta\Gamma, G(s))$.

- So suppose $(h_1, h_2) \in W.\mathsf{H}(s)(G(s))$ and $h_1^{\text{F}}, h_2^{\text{F}} \in \text{Heap}$.
- We must show $(\delta\sigma, (h_1, h_1^{\text{F}}, \gamma_1(e_1[v_1/x])), (h_2, h_2^{\text{F}}, \gamma_2(e_2[v_2/x]))) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s, s)$.
- From the second premise we get $(\delta\sigma', \gamma_1 v_1, \gamma_2 v_2) \in \mathbf{E}_W(G)(s, s)$.
- As a consequence of this, there is $s' \sqsupseteq_{\text{pub}} s$ such that:
  1. $(\delta\sigma', \gamma_1 v_1, \gamma_2 v_2) \in \overline{G(s')}$
  2. $(h_1, h_2) \in W.\mathsf{H}(s')(G(s'))$
- Let $\gamma_1' := \gamma_1, x{\mapsto}\gamma_1 v_1$ and $\gamma_2' := \gamma_2, x{\mapsto}\gamma_2 v_2$.
- By monotonicity and (1) we have $\gamma' \in \text{Env}(\delta(\Gamma, x{:}\sigma'), G(s'))$.
- The first premise then yields $(\delta\sigma, \gamma_1' e_1, \gamma_2' e_2) \in \mathbf{E}_W(G)(s', s')$.
- By Lemma 7 we get $(\delta\sigma, \gamma_1' e_1, \gamma_2' e_2) \in \mathbf{E}_W(G)(s, s')$.
- This implies $(\delta\sigma, (h_1, h_1^{\text{F}}, \gamma_1(e_1[v_1/x])), (h_2, h_2^{\text{F}}, \gamma_2(e_2[v_2/x]))) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s, s')$.
- We are done by Lemma 4 and (2).

□

3.3 Expansion

Theorem 61.

$$\frac{\Delta; \Gamma \vdash e_1' \sim e_2' : \sigma \qquad \forall h, \gamma.\ h, \gamma e_1 \hookrightarrow^* h, \gamma e_1' \qquad \forall h, \gamma.\ h, \gamma e_2 \hookrightarrow^* h, \gamma e_2'}{\Delta; \Gamma \vdash e_1 \sim e_2 : \sigma}$$

Proof. By Lemma 16 it suffices to show:

$$\frac{\Delta; \Gamma \vdash e_1' \sim_W e_2' : \sigma \qquad \forall h, \gamma.\ h, \gamma e_1 \hookrightarrow^* h, \gamma e_1' \qquad \forall h, \gamma.\ h, \gamma e_2 \hookrightarrow^* h, \gamma e_2'}{\Delta; \Gamma \vdash e_1 \sim_W e_2 : \sigma}$$

This boils down to showing

$$(\delta\sigma, (h_1, h_1^{\text{F}}, \gamma_1 e_1), (h_2, h_2^{\text{F}}, \gamma_2 e_2)) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s, s)$$

in a context where the premise provides

$$(\delta\sigma, (h_1, h_1^{\text{F}}, \gamma_1 e_1'), (h_2, h_2^{\text{F}}, \gamma_2 e_2')) \in \mathbf{O}_W(\mathbf{K}_W)(G)(s, s).$$

Using the side condition, we are done by Lemma 4. □

3.4 Beta Law

Theorem 62.

$$\frac{\Delta; \Gamma, x{:}\sigma' \vdash e_1 \sim e_2 : \sigma \qquad \Delta; \Gamma \vdash v_1 \sim v_2 : \sigma'}{\Delta; \Gamma \vdash (\lambda x.\, e_1)\ v_1 \sim e_2[v_2/x] : \sigma}$$

Proof. From the premises and Theorem 60 we know $\Delta; \Gamma \vdash e_1[v_1/x] \sim e_2[v_2/x] : \sigma$. Thus the conclusion holds by Theorem 61. □

3.5 Awkward Example

$$\begin{array}{rcl} \tau & := & (\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int} \\ v_1 & := & \lambda f.\, f\ \langle\rangle; 1 \\ e_2 & := & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in} \\ & & \lambda f.\, x := 1; f\ \langle\rangle; !x \end{array}$$

We show $\cdot; \cdot \vdash v_1 \sim e_2 : \tau$. So let $\mathcal{N}$ be given. The proof splits conceptually into three parts:

1. Constructing a local world $\widehat{w}$ with $\widehat{w}.\mathsf{N} \subseteq \mathcal{N}$, *stable*$(\widehat{w})$, and *inhabited*$(\widehat{w}{\uparrow})$.
2. Showing *consistent*$(\widehat{w}{\uparrow})$. This is the meat of the proof.
3. Showing that v_1 and e_2 are related by $\mathbf{E}_{\widehat{w}\uparrow}$.

Constructing the world. First, we define $w \in \mathrm{LWorld}$ as follows:

$$\begin{array}{lcl} w.\mathsf{N} & := & \emptyset \\ w.\mathsf{S} & := & \mathrm{Loc} \times \{0,1\} \\ w.\sqsupseteq & := & w.\sqsupseteq_{\mathrm{pub}} \\ w.\sqsupseteq_{\mathrm{pub}} & := & \{((\ell,1),(\ell,0)) \mid \ell \in \mathrm{Loc}\}^* \\ w.\mathsf{L} & := & \lambda s_{\mathrm{ref}}, (\ell,n), R.\ \{((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}, v_1, (\lambda f.\, \ell := 1; f\ \langle\rangle; !\ell))\} \\ w.\mathsf{H} & := & \lambda s_{\mathrm{ref}}, (\ell,n), R.\ \{(\emptyset, [\ell \mapsto n])\} \end{array}$$

Now let $\widehat{w} = \mathbf{G}(\lambda\mathcal{N}.w)(\mathcal{N})$. By definition of $\mathbf{G}$ we have $\widehat{w}.\mathsf{N} \subseteq \mathcal{N}$. Furthermore, by Lemmas 58 and 59 we know *stable*$(\widehat{w})$ and *inhabited*$(\widehat{w}{\uparrow})$.

Showing consistency. In order to show *consistent*$(\widehat{w}{\uparrow})$, it suffices by Lemma 58 to just show *consistent*$(w{\uparrow})$.

- So suppose $(s_{\mathrm{ref}}, (\ell,n)) \in w{\uparrow}.\mathsf{S}$ and $(v_1', v_2') \in \overline{G(s_{\mathrm{ref}}, (\ell,n))}(\mathsf{unit} \to \mathsf{unit})$.
- We need to show:

$$((v_1'\ \langle\rangle; 1), (\ell := 1; v_2'\ \langle\rangle; !\ell)) \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{ref}}, (\ell,n)), (s_{\mathrm{ref}}, (\ell,n)))(\mathsf{int})$$

- So suppose defined$(h_1 \uplus h_1^{\mathrm{F}})$ and defined$(h_2 \uplus h_2^{\mathrm{F}})$ as well as

$$(h_1, h_2) \in w{\uparrow}.\mathsf{H}(s_{\mathrm{ref}}, (\ell,n))(G(s_{\mathrm{ref}}, (\ell,n))).$$

- Then there are $(h_1^{\mathrm{ref}}, h_2^{\mathrm{ref}}) \in W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{ref}})(G(s_{\mathrm{ref}}, (\ell,n)))$ such that $h_1 = h_1^{\mathrm{ref}}$ and $h_2 = h_2^{\mathrm{ref}} \uplus [\ell \mapsto n]$.
- Therefore we know:

$$h_2 \uplus h_2^{\mathrm{F}}, (\ell := 1; v_2'\ \langle\rangle; !\ell) \hookrightarrow h_2^{\mathrm{ref}} \uplus [\ell \mapsto 1] \uplus h_2^{\mathrm{F}}, (v_2'\ \langle\rangle; !\ell)$$

- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $s' \sqsupseteq (\ell,n)$ such that:

1. $(h_1^{\text{ref}}, h_2^{\text{ref}} \uplus [\ell \mapsto 1]) \in w{\uparrow}.\mathsf{H}(s_{\text{ref}}, s')(G(s_{\text{ref}}, s'))$
2. $(v_1', v_2') \in \overline{G(s_{\text{ref}}, s')}(\mathsf{unit} \to \mathsf{unit})$
3. $(\langle\rangle, \langle\rangle) \in \overline{G(s_{\text{ref}}, s')}(\mathsf{unit})$
4. $\forall (s'_{\text{ref}}, s'') \sqsupseteq_{\text{pub}} (s_{\text{ref}}, s').\forall G' \geq G.\ ((\bullet; 1), (\bullet; !\ell)) \in \mathbf{K}_{w\uparrow}(G')((s_{\text{ref}}, (\ell, n)), (s'_{\text{ref}}, s''))(\mathsf{unit}, \mathsf{int})$

- We pick $s' = (\ell, 1) \sqsupseteq (\ell, n)$.
- (1) follows from monotonicity and $(\emptyset, [\ell \mapsto 1]) \in w.\mathsf{H}(s')(G(s'))$, which holds by construction.
- As (2) holds by monotonicity, and (3) is immediate, it remains to show (4).
- So suppose $(s'_{\text{ref}}, s'') \sqsupseteq_{\text{pub}} (s_{\text{ref}}, s')$ and $G' \geq G$.
- Then necessarily $s'' = s'$.
- We must show $((\langle\rangle; 1), (\langle\rangle; !\ell)) \in \mathbf{E}_{w\uparrow}(G')((s_{\text{ref}}, (\ell, n)), (s'_{\text{ref}}, s''))(\mathsf{int})$.
- So suppose defined$(h_1' \uplus h_1^{\mathrm{F}'})$ and defined$(h_2' \uplus h_2^{\mathrm{F}'})$ as well as $(h_1', h_2') \in w{\uparrow}.\mathsf{H}(s'_{\text{ref}}, s'')(G'(s'_{\text{ref}}, s''))$.
- Then there are $h_1'^{\text{ref}}, h_2'^{\text{ref}}$ such that $h_1' = h_1'^{\text{ref}}$ and $h_2' = h_2'^{\text{ref}} \uplus [\ell \mapsto 1]$.
- Therefore we know:
$$h_2' \uplus h_2^{\mathrm{F}'}, (\langle\rangle; !\ell) \hookrightarrow^* h_2' \uplus h_2^{\mathrm{F}'}, 1$$
- Of course we also know:
$$h_1' \uplus h_1^{\mathrm{F}'}, (\langle\rangle; 1) \hookrightarrow^* h_1' \uplus h_1^{\mathrm{F}'}, 1$$
- Since $(s'_{\text{ref}}, s'') \sqsupseteq_{\text{pub}} (s_{\text{ref}}, (\ell, n))$, it suffices by definition of $\mathbf{E}_{w\uparrow}$ to show $(1, 1) \in \overline{G(s'_{\text{ref}}, s'')}(\mathsf{int})$, which is immediate.

Proving the programs related. It remains to show $(v_1, e_2) \in \mathbf{E}_{\widehat{w}\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))(\tau)$ for any G, s_{ref}, s.

- So suppose $(h_1, h_2) \in \widehat{w}{\uparrow}.\mathsf{H}(s_{\text{ref}}, s)(G(s_{\text{ref}}, s))$ as well as defined$(h_1 \uplus h_1^{\mathrm{F}})$ and defined$(h_2 \uplus h_2^{\mathrm{F}})$.
- Then there are
$$(h_1^{\text{ref}}, h_2^{\text{ref}}) \in W_{\text{ref}}.\mathsf{H}(s_{\text{ref}})(G(s_{\text{ref}}, s)) \text{ and } (\widehat{h_1}, \widehat{h_2}) \in \widehat{w}.\mathsf{H}(s_{\text{ref}})(s)(G(s_{\text{ref}}, s))$$
with $h_1 = h_1^{\text{ref}} \uplus \widehat{h_1}$ and $h_2 = h_2^{\text{ref}} \uplus \widehat{h_2}$.
- Hence we have $h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow h_2^{\text{ref}} \uplus \widehat{h_2} \uplus [\ell \mapsto 0] \uplus h_2^{\mathrm{F}}, v_2$, where $v_2 = \lambda f.\, \ell := 1; f\ \langle\rangle; !\ell$ and ℓ is fresh.
- We are done if we can find $s' \sqsupseteq_{\text{pub}} s$ such that:
  1. $(h_1^{\text{ref}} \uplus \widehat{h_1}, h_2^{\text{ref}} \uplus \widehat{h_2} \uplus [\ell \mapsto 0]) \in \widehat{w}{\uparrow}.\mathsf{H}(s_{\text{ref}}, s')(G(s_{\text{ref}}, s'))$
  2. $(v_1, v_2) \in \overline{G(s_{\text{ref}}, s')}(\tau)$
- We pick $s' = (s, (\ell, 0)) \sqsupseteq_{\text{pub}} s$.
- To show (1), it suffices by monotonicity to show $(\widehat{h_1}, \widehat{h_2} \uplus [\ell \mapsto 0]) \in \widehat{w}.\mathsf{H}(s_{\text{ref}})(s')(G(s_{\text{ref}}, s'))$.
- By monotonicity and construction of $\widehat{w}$ it then suffices to show $(\emptyset, [\ell \mapsto 0]) \in w.\mathsf{H}(s_{\text{ref}})(\ell, 0)(G(s_{\text{ref}}, s'))$, which holds by construction of w.
- To show (2) it suffices by definition of GK to show $(v_1, v_2) \in \widehat{w}{\uparrow}.\mathsf{L}(s_{\text{ref}}, s')(G(s_{\text{ref}}, s'))(\tau)$.
- By construction of $\widehat{w}$ it then suffices to show $(v_1, v_2) \in w.\mathsf{L}(\ell, 0)(G(s_{\text{ref}}, s'))(\tau)$, which also holds by construction of w.

3.6 Well-Bracketed State Change

$$
\begin{array}{rcl}
\tau & := & (\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int} \\
v_1 & := & \lambda f.\, f\ \langle\rangle; f\ \langle\rangle; 1 \\
e_2 & := & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in} \\
 & & \lambda f.\, x := 0; f\ \langle\rangle; x := 1; f\ \langle\rangle; !x
\end{array}
$$

We show $\cdot; \cdot \vdash v_1 \sim e_2 : \tau$. So let $\mathcal{N}$ be given. The proof splits conceptually into three parts:

1. Constructing a local world $\widehat{w}$ with $\widehat{w}.\mathsf{N} \subseteq \mathcal{N}$, $stable(\widehat{w})$, and $inhabited(\widehat{w}\!\uparrow)$.
2. Showing $consistent(\widehat{w}\!\uparrow)$. This is the meat of the proof.
3. Showing that v_1 and e_2 are related by $\mathbf{E}_{\widehat{w}\uparrow}$.

Constructing the world. First, we define $w \in \text{LWorld}$ as follows:

$$
\begin{array}{lcl}
w.\mathsf{N} & := & \emptyset \\
w.\mathsf{S} & := & \text{Loc} \times \{0,1\} \\
w.\sqsupseteq & := & w.\sqsupseteq_{\text{pub}} \cup \{((\ell,0),(\ell,1)) \mid \ell \in \text{Loc}\} \\
w.\sqsupseteq_{\text{pub}} & := & \{((\ell,1),(\ell,0)) \mid \ell \in \text{Loc}\}^* \\
w.\mathsf{L} & := & \lambda s_{\text{ref}}, (\ell,n), R.\ \{((\mathsf{unit} \to \mathsf{unit}) \to \mathsf{int}, v_1, (\lambda f.\, \ell := 0; f\ \langle\rangle; \ell := 1; f\ \langle\rangle; !\ell))\} \\
w.\mathsf{H} & := & \lambda s_{\text{ref}}, (\ell,n), R.\ \{(\emptyset, [\ell \mapsto n])\}
\end{array}
$$

Now let $\widehat{w} = \mathbf{G}(\lambda\mathcal{N}.w)(\mathcal{N})$. By definition of $\mathbf{G}$ we have $\widehat{w}.\mathsf{N} \subseteq \mathcal{N}$. Furthermore, by Lemmas 58 and 59 we know $stable(\widehat{w})$ and $inhabited(\widehat{w}\!\uparrow)$.

Showing consistency. In order to show $consistent(\widehat{w}\!\uparrow)$, it suffices by Lemma 58 to just show $consistent(w\!\uparrow)$.

- So suppose $(s_{\text{ref}}, (\ell,n)) \in w\!\uparrow\!.\mathsf{S}$ and $(v_1', v_2') \in \overline{G(s_{\text{ref}}, (\ell,n))}(\mathsf{unit} \to \mathsf{unit})$.
- We need to show:

$$((v_1'\ \langle\rangle; v_1'\ \langle\rangle; 1), (\ell := 0; v_2'\ \langle\rangle; \ell := 1; v_2'\ \langle\rangle; !\ell)) \in \mathbf{E}_{w\uparrow}(G)((s_{\text{ref}}, (\ell,n)), (s_{\text{ref}}, (\ell,n)))(\mathsf{int})$$

- So suppose defined$(h_1 \uplus h_1^{\text{F}})$ and defined$(h_2 \uplus h_2^{\text{F}})$ as well as

$$(h_1, h_2) \in w\!\uparrow\!.\mathsf{H}(s_{\text{ref}}, (\ell,n))(G(s_{\text{ref}}, (\ell,n))).$$

- Then there are $(h_1^{\text{ref}}, h_2^{\text{ref}}) \in W_{\text{ref}}.\mathsf{H}(s_{\text{ref}})(G(s_{\text{ref}}, (\ell,n)))$ such that $h_1 = h_1^{\text{ref}}$ and $h_2 = h_2^{\text{ref}} \uplus [\ell \mapsto n]$.
- Therefore we know:

$$h_2 \uplus h_2^{\text{F}}, (\ell := 0; v_2'\ \langle\rangle; \ell := 1; v_2'\ \langle\rangle; !\ell) \hookrightarrow h_2^{\text{ref}} \uplus [\ell \mapsto 0] \uplus h_2^{\text{F}}, (v_2'\ \langle\rangle; \ell := 1; v_2'\ \langle\rangle; !\ell)$$

- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $s' \sqsupseteq (\ell,n)$ such that:
  1. $(h_1^{\text{ref}}, h_2^{\text{ref}} \uplus [\ell \mapsto 0]) \in w\!\uparrow\!.\mathsf{H}(s_{\text{ref}}, s')(G(s_{\text{ref}}, s'))$
  2. $(v_1', v_2') \in \overline{G(s_{\text{ref}}, s')}(\mathsf{unit} \to \mathsf{unit})$
  3. $(\langle\rangle, \langle\rangle) \in \overline{G(s_{\text{ref}}, s')}(\mathsf{unit})$
  4. $\forall (s'_{\text{ref}}, \widetilde{s'}) \sqsupseteq_{\text{pub}} (s_{\text{ref}}, s'). \forall G' \geq G.$
     $((\bullet; v_1'\ \langle\rangle; 1), (\bullet; \ell := 1; v_2'\ \langle\rangle; !\ell)) \in \mathbf{K}_{w\uparrow}(G')((s_{\text{ref}}, (\ell,n)), (s'_{\text{ref}}, \widetilde{s'}))(\mathsf{unit}, \mathsf{int})$
- We pick $s' = (\ell, 0) \sqsupseteq (\ell, n)$.

- (1) follows from monotonicity and $(\emptyset, [\ell\mapsto 1]) \in w.\mathsf{H}(s_{\text{ref}})(s')(G(s_{\text{ref}}, s'))$, which holds by construction.
- As (2) holds by monotonicity, and (3) is immediate, it remains to show (4).
- So suppose $(s'_{\text{ref}}, \widetilde{s'}) \sqsupseteq_{\text{pub}} (s_{\text{ref}}, s')$ and $G' \geq G$.
- We need to show:

$$((\langle\rangle; v'_1\ \langle\rangle; 1), (\langle\rangle; \ell := 1; v'_2\ \langle\rangle; !\ell)) \in \mathbf{E}_{w\uparrow}(G')((s_{\text{ref}}, (\ell, n)), (s'_{\text{ref}}, \widetilde{s'}))(\mathsf{int})$$

- So suppose $\text{defined}(h'_1 \uplus h_1^{\text{F}\prime})$ and $\text{defined}(h'_2 \uplus h_2^{\text{F}\prime})$ as well as

$$(h'_1, h'_2) \in w\uparrow.\mathsf{H}(s'_{\text{ref}}, \widetilde{s'})(G'(s'_{\text{ref}}, \widetilde{s'})).$$

- Then there are $(h_1'^{\text{ref}}, h_2'^{\text{ref}}) \in W_{\text{ref}}.\mathsf{H}(s'_{\text{ref}})(G'(s'_{\text{ref}}, \widetilde{s'}))$ such that $h'_1 = h_1'^{\text{ref}}$ and $h'_2 = h_2'^{\text{ref}} \uplus [\ell\mapsto n']$.
- Therefore we know:

$$\begin{array}{rcl} h'_1 \uplus h_1^{\text{F}\prime}, (\langle\rangle; v'_1\ \langle\rangle; 1) & \hookrightarrow & h_1'^{\text{ref}} \uplus h_1^{\text{F}\prime}, (v'_1\ \langle\rangle; 1) \\ h'_2 \uplus h_2^{\text{F}\prime}, (\langle\rangle; \ell := 1; v'_2\ \langle\rangle; !\ell) & \hookrightarrow & h_2'^{\text{ref}} \uplus [\ell\mapsto 1] \uplus h_2^{\text{F}\prime}, (v'_2\ \langle\rangle; !\ell) \end{array}$$

- By definition of $\mathbf{E}_{w\uparrow}$ it suffices to find $s'' \sqsupseteq \widetilde{s'}$ such that:
  1. $(h_1'^{\text{ref}}, h_2'^{\text{ref}} \uplus [\ell\mapsto 1]) \in w\uparrow.\mathsf{H}(s'_{\text{ref}}, s'')(G'(s'_{\text{ref}}, s''))$
  2. $(v'_1, v'_2) \in \overline{G'(s'_{\text{ref}}, s'')}(\mathsf{unit} \to \mathsf{unit})$
  3. $(\langle\rangle, \langle\rangle) \in \overline{G'(s'_{\text{ref}}, s'')}(\mathsf{unit})$
  4. $\forall (s''_{\text{ref}}, \widetilde{s''}) \sqsupseteq_{\text{pub}} (s'_{\text{ref}}, s'').\forall G'' \geq G'.\ ((\bullet; 1), (\bullet; !\ell)) \in \mathbf{K}_{w\uparrow}(G'')((s_{\text{ref}}, (\ell, n)), (s''_{\text{ref}}, \widetilde{s''}))(\mathsf{unit}, \mathsf{int})$
- We pick $s'' = (\ell, 1) \sqsupseteq \widetilde{s'}$.
- (1) follows from monotonicity and $(\emptyset, [\ell\mapsto 1]) \in w.\mathsf{H}(s_{\text{ref}})(s')(G'(s'))$, which holds by construction.
- As (2) holds by monotonicity, and (3) is immediate, it remains to show (4).
- So suppose $(s''_{\text{ref}}, \widetilde{s''}) \sqsupseteq_{\text{pub}} (s'_{\text{ref}}, s'')$ and $G'' \geq G'$.
- Then necessarily $\widetilde{s''} = s''$.
- We must show $((\langle\rangle; 1), (\langle\rangle; !\ell)) \in \mathbf{E}_{w\uparrow}(G'')((s_{\text{ref}}, (\ell, n)), (s''_{\text{ref}}, s''))(\mathsf{int})$.
- So suppose $\text{defined}(h''_1 \uplus h_1^{\text{F}\prime\prime})$ and $\text{defined}(h''_2 \uplus h_2^{\text{F}\prime\prime})$ as well as $(h''_1, h''_2) \in w\uparrow.\mathsf{H}(s''_{\text{ref}}, s'')(G''(s''_{\text{ref}}, s''))$.
- Then there are $h_1''^{\text{ref}}, h_2''^{\text{ref}}$ such that $h''_1 = h_1''^{\text{ref}}$ and $h''_2 = h_2''^{\text{ref}} \uplus [\ell\mapsto 1]$.
- Therefore we know:

$$h''_2 \uplus h_2^{\text{F}\prime\prime}, (\langle\rangle; !\ell) \hookrightarrow^* h''_2 \uplus h_2^{\text{F}\prime\prime}, 1$$

- Of course we also know:

$$h''_1 \uplus h_1^{\text{F}\prime\prime}, (\langle\rangle; 1) \hookrightarrow^* h''_1 \uplus h_1^{\text{F}\prime\prime}, 1$$

- Since $(s''_{\text{ref}}, s'') \sqsupseteq_{\text{pub}} (s_{\text{ref}}, (\ell, n))$, it suffices by definition of $\mathbf{E}_{w\uparrow}$ to show $(1, 1) \in \overline{G(s''_{\text{ref}}, s'')}(\mathsf{int})$, which is immediate.

Proving the programs related. It remains to show $(v_1, e_2) \in \mathbf{E}_{\widehat{w}\uparrow}(G)((s_{\mathrm{ref}}, s), (s_{\mathrm{ref}}, s))(\tau)$ for any G, s_{ref}, s.

- So suppose $(h_1, h_2) \in \widehat{w}\uparrow.\mathsf{H}(s_{\mathrm{ref}}, s)(G(s_{\mathrm{ref}}, s))$ as well as $\mathrm{defined}(h_1 \uplus h_1^{\mathrm{F}})$ and $\mathrm{defined}(h_2 \uplus h_2^{\mathrm{F}})$.
- Then there are
$$(h_1^{\mathrm{ref}}, h_2^{\mathrm{ref}}) \in W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{ref}})(G(s_{\mathrm{ref}}, s)) \text{ and } (\widehat{h_1}, \widehat{h_2}) \in \widehat{w}.\mathsf{H}(s_{\mathrm{ref}})(s)(G(s_{\mathrm{ref}}, s))$$
with $h_1 = h_1^{\mathrm{ref}} \uplus \widehat{h_1}$ and $h_2 = h_2^{\mathrm{ref}} \uplus \widehat{h_2}$.
- Hence we have $h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow h_2^{\mathrm{ref}} \uplus \widehat{h_2} \uplus [\ell \mapsto 0] \uplus h_2^{\mathrm{F}}, v_2$, where $v_2 = \lambda f.\, \ell := 0; f\ \langle\rangle; \ell := 1; f\ \langle\rangle; !\ell$ and ℓ is fresh.
- We are done if we can find $s' \sqsupseteq_{\mathrm{pub}} s$ such that:
  1. $(h_1^{\mathrm{ref}} \uplus \widehat{h_1}, h_2^{\mathrm{ref}} \uplus \widehat{h_2} \uplus [\ell \mapsto 0]) \in \widehat{w}\uparrow.\mathsf{H}(s_{\mathrm{ref}}, s')(G(s_{\mathrm{ref}}, s'))$
  2. $(v_1, v_2) \in \overline{G(s_{\mathrm{ref}}, s')}(\tau)$
- We pick $s' = (s, (\ell, 0)) \sqsupseteq_{\mathrm{pub}} s$.
- To show (1), it suffices by monotonicity to show $(\widehat{h_1}, \widehat{h_2} \uplus [\ell \mapsto 0]) \in \widehat{w}.\mathsf{H}(s_{\mathrm{ref}})(s')(G(s_{\mathrm{ref}}, s'))$.
- By monotonicity and construction of $\widehat{w}$ it then suffices to show $(\emptyset, [\ell \mapsto 0]) \in w.\mathsf{H}(s_{\mathrm{ref}})(\ell, 0)(G(s_{\mathrm{ref}}, s'))$, which holds by construction of w.
- To show (2) it suffices by definition of GK to show $(v_1, v_2) \in \widehat{w}\uparrow.\mathsf{L}(s_{\mathrm{ref}}, s')(G(s_{\mathrm{ref}}, s'))(\tau)$.
- By construction of $\widehat{w}$ it then suffices to show $(v_1, v_2) \in w.\mathsf{L}(s_{\mathrm{ref}})(\ell, 0)(G(s_{\mathrm{ref}}, s'))(\tau)$, which also holds by construction of w.

3.7 Twin Abstraction

$$\begin{array}{rcl}
\tau & := & \exists\alpha.\, \exists\beta.\, (\mathsf{unit} \to \alpha) \times (\mathsf{unit} \to \beta) \times (\alpha \times \beta \to \mathsf{bool}) \\
e_1 & := & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in}\ \mathsf{pack}\ \langle \mathsf{int}, \mathsf{pack}\ \langle \mathsf{int}, \lambda_.\, x := !x + 1; !x, \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad \lambda_.\, x := !x + 1; !x, \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad \lambda p.\, p.1 = p.2 \rangle\rangle \\
e_2 & := & \mathsf{let}\ x = \mathsf{ref}\ 0\ \mathsf{in}\ \mathsf{pack}\ \langle \mathsf{int}, \mathsf{pack}\ \langle \mathsf{int}, \lambda_.\, x := !x + 1; !x, \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad \lambda_.\, x := !x + 1; !x, \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad \lambda p.\, \mathsf{ff} \rangle\rangle
\end{array}$$

We show $\cdot; \cdot \vdash e_1 \sim e_2 : \tau$. So let $\mathcal{N}$ be given. The proof splits conceptually into three parts:

1. Constructing a world w with $w.\mathsf{N} \subseteq \mathcal{N}$, $\mathit{stable}(w)$, and $\mathit{inhabited}(w\uparrow)$.
2. Showing $\mathit{consistent}(w\uparrow)$. This is the meat of the proof.
3. Showing that e_1 and e_2 are related by $\mathbf{E}_{w\uparrow}$.

Constructing the world. First, we define $\mathcal{W} \in \text{NLWorld}$ as follows:

$$
\begin{array}{lcl}
\mathcal{W}(\mathcal{N}').\mathsf{N} & := & \{\mathcal{N}'(1), \mathcal{N}'(2)\} \\
\mathcal{W}(\mathcal{N}').\mathsf{S} & := & \{(\ell_1, \ell_2, S_1, S_2) \in \text{Loc} \times \text{Loc} \times \mathbb{P}(\mathbb{N}_{>0}) \times \mathbb{P}(\mathbb{N}_{>0}) \mid S_1 \cap S_2 = \emptyset\} \\
\mathcal{W}(\mathcal{N}').\sqsupseteq & := & \mathcal{W}(\mathcal{N}').\sqsupseteq_{\text{pub}} \\
\mathcal{W}(\mathcal{N}').\sqsupseteq_{\text{pub}} & := & \{((\ell_1', \ell_2', S_1', S_2'), (\ell_1, \ell_2, S_1, S_2) \mid \ell_1 = \ell_1' \wedge \ell_2 = \ell_2' \wedge S_1 \subseteq S_1' \wedge S_2 \subseteq S_2'\} \\
\mathcal{W}(\mathcal{N}').\mathsf{L} & := & \lambda(\ell_1, \ell_2, S_1, S_2), R.\ \{(\mathcal{N}'(1), n, n) \mid n \in S_1\} \uplus \{(\mathcal{N}'(2), n, n) \mid n \in S_2\} \uplus \\
& & \qquad \{((\mathsf{unit} \to \mathcal{N}'(1)), (\lambda\_.\, \ell_1 := !\ell_1 + 1; !\ell_1), (\lambda\_.\, \ell_1 := !\ell_1 + 1; !\ell_1))\} \uplus \\
& & \qquad \{((\mathsf{unit} \to \mathcal{N}'(2)), (\lambda\_.\, \ell_2 := !\ell_2 + 1; !\ell_2), (\lambda\_.\, \ell_2 := !\ell_2 + 1; !\ell_2))\} \uplus \\
& & \qquad \{((\mathcal{N}'(1) \times \mathcal{N}'(2) \to \mathsf{bool}), (\lambda p.\, p.1 = p.2), (\lambda p.\, \mathsf{ff}))\} \\
\mathcal{W}(\mathcal{N}').\mathsf{H} & := & \lambda(\ell_1, \ell_2, S_1, S_2), R.\ \{([\ell_1 \mapsto n], [\ell_2 \mapsto n]) \mid n = \max(\{0\} \uplus S_1 \uplus S_2)\}
\end{array}
$$

where $\mathcal{N}'(1)$ and $\mathcal{N}'(2)$ denote two distinct elements of $\mathcal{N}'$.

Now let $w = \mathbf{G}(\mathcal{W})(\mathcal{N})$. By definition of $\mathbf{G}$ we have $w.\mathsf{N} \subseteq \mathcal{N}$. Furthermore, by Lemmas 58 and 59 we know *stable*(w) and *inhabited*$(w\!\uparrow)$.

Showing consistency. In order to show *consistent*$(w\!\uparrow)$, it suffices by Lemma 58 to just show *consistent*$(\mathcal{W}(\mathcal{N}')\!\uparrow)$ for any $\mathcal{N}'$. This decomposes into the following subgoals (for any $G, s_{\text{ref}}, s = (\ell_1, \ell_2, S_1, S_2)$):

1. $((\ell_1 := !\ell_1 + 1; !\ell_1), (\ell_1 := !\ell_1 + 1; !\ell_1)) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}')\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))(\mathcal{N}'(1))$
2. $((\ell_2 := !\ell_2 + 1; !\ell_2), (\ell_2 := !\ell_2 + 1; !\ell_2)) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}')\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))(\mathcal{N}'(2))$
3. $\forall (v_1', v_2') \in \overline{G(s_{\text{ref}}, s)}(\mathcal{N}'(1) \times \mathcal{N}'(2)).\ (v_1'.1 = v_1'.2, \mathsf{ff}) \in \mathbf{E}_{\mathcal{W}(\mathcal{N}')\uparrow}(G)((s_{\text{ref}}, s), (s_{\text{ref}}, s))(\mathsf{bool})$

For (1) (part (2) is analogously):

- Suppose $(h_1, h_2) \in \mathcal{W}(\mathcal{N}')\!\uparrow\!.\mathsf{H}(s_{\text{ref}}, s)(G(s_{\text{ref}}, s))$ as well as defined$(h_1 \uplus h_1^{\text{F}})$ and defined$(h_2 \uplus h_2^{\text{F}})$.
- Then there are
$$(h_1^{\text{ref}}, h_2^{\text{ref}}) \in W_{\text{ref}}.\mathsf{H}(s_{\text{ref}})(G(s_{\text{ref}}, s)) \text{ and } (h_1^{\circ}, h_2^{\circ}) \in \mathcal{W}(\mathcal{N}').\mathsf{H}(s_{\text{ref}})(s)(G(s_{\text{ref}}, s))$$
with $h_1 = h_1^{\text{ref}} \uplus h_1^{\circ}$ and $h_2 = h_2^{\text{ref}} \uplus h_2^{\circ}$.
- By construction of $\mathcal{W}(\mathcal{N}')$ we know $h_1^{\circ} = [\ell_1 \mapsto n]$ and $h_2^{\circ} = [\ell_2 \mapsto n]$ where $n = \max(\{0\} \uplus S_1 \uplus S_2\}$.
- Hence $h_1 \uplus h_1^{\text{F}}, (\ell_1 := !\ell_1 + 1; !\ell_1) \hookrightarrow^* h_1^{\text{ref}} \uplus [\ell_1 \mapsto n+1] \uplus h_1^{\text{F}}, n+1$
and $h_2 \uplus h_2^{\text{F}}, (\ell_2 := !\ell_2 + 1; !\ell_2) \hookrightarrow^* h_2^{\text{ref}} \uplus [\ell_2 \mapsto n+1] \uplus h_2^{\text{F}}, n+1$.
- By definition of $\mathbf{E}_{\mathcal{W}(\mathcal{N}')\uparrow}$ it suffices to find $s' \sqsupseteq_{\text{pub}} s$ such that:
  a) $(h_1^{\text{ref}} \uplus [\ell_1 \mapsto n+1], h_1^{\text{ref}} \uplus [\ell_2 \mapsto n+1]) \in \mathcal{W}(\mathcal{N}')\!\uparrow\!.\mathsf{H}(s_{\text{ref}}, s')(G(s_{\text{ref}}, s'))$
  b) $(n+1, n+1) \in \overline{G(s_{\text{ref}}, s')}(\mathcal{N}'(1))$
- We pick $s' = (\ell_1, \ell_2, S_1 \uplus \{n+1\}, S_2)$.
- Note that $n+1 \notin S_1 \cup S_2$ and thus $(S_1 \uplus \{n+1\}) \cap S_2 = \emptyset$, so s' is well-formed.
- Since $n{+}1 = \max\{0\} \uplus S_1 \uplus \{n+1\} \uplus S_2$, (a) follows from $([\ell_1 \mapsto n{+}1], [\ell_2 \mapsto n{+}1]) \in \mathcal{W}(\mathcal{N}').\mathsf{H}(s_{\text{ref}})(s')(G(s_{\text{ref}}, s'))$ by construction of $\mathcal{W}(\mathcal{N}')$.
- To show (b) it suffices, by definition of GK, to show
$$(n+1, n+1) \in \mathcal{W}(\mathcal{N}')\!\uparrow\!.\mathsf{L}(s_{\text{ref}}, s')(G(s_{\text{ref}}, s'))(\mathcal{N}'(1)).$$

- This follows from
$$(n+1, n+1) \in \mathcal{W}(\mathcal{N}').\mathsf{L}(s_{\mathrm{ref}})(s')(G(s_{\mathrm{ref}}, s'))(\mathcal{N}'(1)),$$
which in turns holds by construction of $\mathcal{W}(\mathcal{N}')$.

For (3):

- Suppose $(v_1', v_2') \in \overline{G(s_{\mathrm{ref}}, s)}(\mathcal{N}'(1) \times \mathcal{N}'(2))$.
- Then $v_1' = \langle \widehat{v_1}, \widetilde{v_1} \rangle$ and $v_2' = \langle \widehat{v_2}, \widetilde{v_2} \rangle$ with $(\widehat{v_1}, \widehat{v_2}) \in \overline{G(s_{\mathrm{ref}}, s)}(\mathcal{N}'(1))$ and $(\widetilde{v_1}, \widetilde{v_2}) \in \overline{G(s_{\mathrm{ref}}, s)}(\mathcal{N}'(2))$.
- By definition of GK and construction of $\mathcal{W}(\mathcal{N}')$ we know $\widehat{v_1} = \widehat{v_2} \in S_1$ and $\widetilde{v_1} = \widetilde{v_2} \in S_2$.
- Now suppose $(h_1, h_2) \in \mathcal{W}(\mathcal{N}')\!\uparrow\!.\mathsf{H}(s_{\mathrm{ref}}, s)(G(s_{\mathrm{ref}}, s))$ as well as defined$(h_1 \uplus h_1^{\mathrm{F}})$ and defined$(h_2 \uplus h_2^{\mathrm{F}})$.
- Since $S_1 \cap S_2 = \emptyset$, we get $h_1 \uplus h_1^{\mathrm{F}}, v_1'.1 = v_1'.2 \hookrightarrow^* h_1 \uplus h_1^{\mathrm{F}}, \mathsf{ff}$ and $h_2 \uplus h_2^{\mathrm{F}}, \mathsf{ff} \hookrightarrow^* h_2 \uplus h_2^{\mathrm{F}}, \mathsf{ff}$.
- Since $(\mathsf{ff}, \mathsf{ff}) \in \overline{G(s_{\mathrm{ref}}, s)}(\mathsf{bool})$, we are done.

Proving the programs related. It remains to show $(e_1, e_2) \in \mathbf{E}_{w\uparrow}(G)((s_{\mathrm{ref}}, s), (s_{\mathrm{ref}}, s))(\tau)$ for any G, s_{ref}, s.

- So suppose $(h_1, h_2) \in w\!\uparrow\!.\mathsf{H}(s_{\mathrm{ref}}, s)(G(s_{\mathrm{ref}}, s))$ as well as defined$(h_1 \uplus h_1^{\mathrm{F}})$ and defined$(h_2 \uplus h_2^{\mathrm{F}})$.
- Then there are
$$(h_1^{\mathrm{ref}}, h_2^{\mathrm{ref}}) \in W_{\mathrm{ref}}.\mathsf{H}(s_{\mathrm{ref}})(G(s_{\mathrm{ref}}, s)) \text{ and } (\widehat{h_1}, \widehat{h_2}) \in w.\mathsf{H}(s_{\mathrm{ref}})(s)(G(s_{\mathrm{ref}}, s))$$
with $h_1 = h_1^{\mathrm{ref}} \uplus \widehat{h_1}$ and $h_2 = h_2^{\mathrm{ref}} \uplus \widehat{h_2}$.
- Hence we have
$$h_1 \uplus h_1^{\mathrm{F}}, e_1 \hookrightarrow h_1^{\mathrm{ref}} \uplus \widehat{h_1} \uplus [\ell_1 \mapsto 0] \uplus h_1^{\mathrm{F}}, \mathsf{pack\ pack}\ v_1 \text{ and } h_2 \uplus h_2^{\mathrm{F}}, e_2 \hookrightarrow h_2^{\mathrm{ref}} \uplus \widehat{h_2} \uplus [\ell_2 \mapsto 0] \uplus h_2^{\mathrm{F}}, \mathsf{pack\ pack}\ v_2$$
where ℓ_1 and ℓ_2 are fresh and v_1, v_2 are what you think they are.
- We are done if we can find $s' \sqsupseteq_{\mathrm{pub}} s$ such that:
  1. $(h_1^{\mathrm{ref}} \uplus \widehat{h_1} \uplus [\ell_1 \mapsto 0], h_2^{\mathrm{ref}} \uplus \widehat{h_2} \uplus [\ell_2 \mapsto 0]) \in w\!\uparrow\!.\mathsf{H}(s_{\mathrm{ref}}, s')(G(s_{\mathrm{ref}}, s'))$
  2. $(v_1, v_2) \in \overline{G(s_{\mathrm{ref}}, s')}(\tau)$
- We pick $s' = (s, (\ell_1, \ell_2, \emptyset, \emptyset)) \sqsupseteq_{\mathrm{pub}} s$.
- To show (1), it suffices by monotonicity to show $(\widehat{h_1} \uplus [\ell_1 \mapsto 0], \widehat{h_2} \uplus [\ell_2 \mapsto 0]) \in w.\mathsf{H}(s_{\mathrm{ref}})(s')(G(s_{\mathrm{ref}}, s'))$.
- By monotonicity and construction of w it then suffices to show $([\ell_1 \mapsto 0], [\ell_2 \mapsto 0]) \in \mathcal{W}(\mathcal{N}').\mathsf{H}(s_{\mathrm{ref}})(\ell_1, \ell_2, \emptyset, \emptyset)(G(s_{\mathrm{ref}}, s'))$ (for any $\mathcal{N}'$), which holds by construction of $\mathcal{W}$.
- To show (2), we pick the witness types $\mathcal{N}_n(1)$ and $\mathcal{N}_n(2)$, where $n := |s'|$.
- It thus suffices to show:
$$(v_1, v_2) \in \overline{G(s_{\mathrm{ref}}, s')}((\mathsf{unit} \to \mathcal{N}_n(1)) \times (\mathsf{unit} \to \mathcal{N}_n(2)) \times (\mathcal{N}_n(1) \times \mathcal{N}_n(2) \to \mathsf{bool}))$$
- This in turn reduces to showing the following:
  - $((\mathsf{unit} \to \mathcal{N}_n(1)), (\lambda\_.\, \ell_1 := !\ell_1 + 1; !\ell_1), (\lambda\_.\, \ell_1 := !\ell_1 + 1; !\ell_1)) \in \overline{G(s_{\mathrm{ref}}, s')}$

- $((\mathsf{unit} \to \mathcal{N}_n(2)), (\lambda\_.\, \ell_2 := !\ell_2 + 1; !\ell_2), (\lambda\_.\, \ell_2 := !\ell_2 + 1; !\ell_2)) \in \overline{G(s_{\mathrm{ref}}, s')}$
- $((\mathcal{N}_n(1) \times \mathcal{N}_n(2) \to \mathsf{bool}), (\lambda p.\, p.1 = p.2), (\lambda p.\, \mathsf{ff})) \in \overline{G(s_{\mathrm{ref}}, s')}$

- By definition of GK and construction of w, it suffices to show that these triples are in $\mathcal{W}(\mathcal{N}_n).\mathsf{L}(\ell_1, \ell_2, \emptyset, \emptyset)(G(s_{\mathrm{ref}}, s'))$.
- This is true by construction of $\mathcal{W}$.

Part II
A Relational Model for a Pure Sub-Language

4 Language

We consider the sub-language λ^{μ} of $\mathsf{F}^{\mu!}$ including only the following types.

$$\sigma \in \text{Type} ::= \alpha \mid \mathsf{unit} \mid \mathsf{int} \mid \mathsf{bool} \mid \sigma_1 \times \sigma_2 \mid \sigma_1 + \sigma_2 \mid \mu\alpha.\, \sigma \mid \sigma_1 \to \sigma_2$$

5 Model

5.1 Definitions

$$\begin{array}{lcl}
\text{CType} & := & \{ \tau \in \text{Type} \mid \text{ftv}(\tau) = \emptyset \} \\
\text{CTypeF} & := & \{ (\tau_1 \to \tau_2) \in \text{CType} \} \\
\text{VRelF} & := & \text{CTypeF} \to \mathbb{P}(\text{CVal} \times \text{CVal}) \\
\text{VRel} & := & \text{CType} \to \mathbb{P}(\text{CVal} \times \text{CVal}) \\
\text{ERel} & := & \text{CType} \to \mathbb{P}(\text{CExp} \times \text{CExp}) \\
\text{KRel} & := & \text{CType} \times \text{CType} \to \mathbb{P}(\text{CCont} \times \text{CCont})
\end{array}$$

We define local knowledges as follows.

$$\text{LK} := \{ L \in \text{VRelF} \to \text{VRelF} \mid L \text{ is monotone w.r.t. } \leq \wedge \forall R.\ \forall (f_1, f_2) \in L(R)(\tau_1 \to \tau_2).\ f_1, f_2 \in \text{FunVal} \}$$

Note that in the absence of state, the knowledge does not need to change over time.

We define the closure $\overline{R} \in \text{VRel}$ for $R \in \text{VRelF}$ as the least fixpoint of the following equation.

$$\begin{array}{lcl}
\overline{R}(\tau_{\text{base}}) & := & \text{ID}_{\tau_{\text{base}}} \\
\overline{R}(\tau_1 \times \tau_2) & := & \{ ((v_1, v_1'), (v_2, v_2')) \mid (v_1, v_2) \in \overline{R}(\tau_1) \wedge (v_1', v_2') \in \overline{R}(\tau_2) \} \\
\overline{R}(\tau_1 + \tau_2) & := & \{ (\mathsf{inj}^1\, v_1, \mathsf{inj}^1\, v_2) \mid (v_1, v_2) \in \overline{R}(\tau_1) \} \cup \{ (\mathsf{inj}^2\, v_1, \mathsf{inj}^2\, v_2) \mid (v_1, v_2) \in \overline{R}(\tau_2) \} \\
\overline{R}(\mu\alpha.\, \tau) & := & \{ (\mathsf{roll}\ v_1, \mathsf{roll}\ v_2) \mid (v_1, v_2) \in \overline{R}(\tau[\mu\alpha.\, \tau/\alpha]) \} \\
\overline{R}(\tau_1 \to \tau_2) & := & R(\tau_1 \to \tau_2)
\end{array}$$

We define $\text{GK}(L)$ for a local knowledge L as follows.

$$\text{GK}(L) \quad := \quad \{ G \in \text{VRelF} \mid G \geq L(G) \}$$

For $L \in \text{LK}$, we coinductively define $\mathbf{E} \in \text{VRelF} \to \text{ERel}$ and $\mathbf{K} \in \text{VRelF} \to \text{KRel}$ as follows.

$$\begin{array}{lcl}
\mathbf{E}(G)(\tau) & := & \{ (e_1, e_2) \mid (e_1, e_2) \in \mathbf{O}(\mathbf{K})(G)(\tau) \} \\
\mathbf{K}(G)(\tau_1, \tau_2) & := & \{ (K_1, K_2) \mid \forall (v_1, v_2) \in \overline{G}(\tau_1).\ (K_1[v_1], K_2[v_2]) \in \mathbf{E}(G)(\tau_2) \} \\
\mathbf{O}(R^{\mathbf{K}})(G)(\tau) & := & \{ (e_1, e_2) \mid \\
& & \quad (e_1 \!\uparrow \wedge\, e_2 \!\uparrow) \\
& & \vee\ (\exists v_1, v_2.\ e_1 \hookrightarrow^* v_1 \wedge e_2 \hookrightarrow^* v_2 \wedge (v_1, v_2) \in \overline{G}(\tau)) \\
& & \vee\ (\exists \tau', K_1, K_2, e_1', e_2'.\ e_1 \hookrightarrow^* K_1[e_1'] \wedge e_2 \hookrightarrow^* K_2[e_2'] \wedge (\tau', e_1', e_2') \in \mathbf{S}(G, G) \wedge \\
& & \quad (K_1, K_2) \in R^{\mathbf{K}}(G)(\tau', \tau)) \} \\
\mathbf{S}(R_f, R_v) & := & \{ (\tau, f_1\ v_1, f_2\ v_2) \mid \exists \tau'.\ (f_1, f_2) \in R_f(\tau' \to \tau) \wedge (v_1, v_2) \in \overline{R_v}(\tau') \}
\end{array}$$

We define the following predicate on local knowledges.

$$\begin{array}{lcl}
\mathit{consistent}(L) & \text{iff} & \forall G \in \text{GK}(L).\ \forall (\tau, e_1, e_2) \in \mathbf{S}(L(G), G). \\
& & \quad (\tau, \mathit{beta}(e_1), \mathit{beta}(e_2)) \in \mathbf{E}(G)
\end{array}$$

We define program equivalence $\Gamma \vdash e_1 \sim e_2 : \tau$.

$$\begin{array}{lll} \mathrm{Env}(\Gamma, R) & := & \{\, (\gamma_1, \gamma_2) \mid \gamma_1, \gamma_2 \in \mathrm{dom}(\Gamma) \to \mathrm{CVal} \wedge \forall x.\ (\Gamma(x), \gamma_1(x), \gamma_2(x)) \in \overline{R} \,\} \\ \Gamma \vdash e_1 \sim_L e_2 : \tau & := & \mathit{consistent}(L) \wedge \\ & & \forall G \in \mathrm{GK}(L).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G).\ (\tau, \gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}(G) \\ \Gamma \vdash e_1 \sim e_2 : \tau & := & \exists L.\ \Gamma \vdash e_1 \sim_L e_2 : \tau \end{array}$$

5.2 Basic Properties

Notation. For a monotone function $F \in \mathrm{VRelF} \to \mathrm{VRelF}$ and $R \in \mathrm{VRelF}$, we define $R^{[F]}$ as the least fixpoint of the monotone function $F(-) \cup R$:

$$R^{[F]} := \mu X.\ F(X) \cup R\ .$$

For $L \in \mathrm{LK}$, we define $[L] \in \mathrm{VRelF}$ as follows:

$$[L] := \emptyset^{[L]}\ .$$

Lemma 63. $\forall L \in \mathrm{LK}.\ [L] \in \mathrm{GK}(L)$

Proof. Immediate. ☐

Lemma 64. If

- $e_1 \hookrightarrow^* e_1'$,
- $e_2 \hookrightarrow^* e_2'$,
- $(\tau, e_1', e_2') \in \mathbf{O}(R^{\mathbf{K}})$,

then $(\tau, e_1, e_2) \in \mathbf{O}(R^{\mathbf{K}})$.

Proof. Follows easily from the definition of $\mathbf{O}$. ☐

Lemma 65. $G \leq \overline{G} \leq \mathbf{E}(G)$

Proof. Both inclusions hold immediately by definition. ☐

Lemma 66. $(\tau, \tau, \bullet, \bullet) \in \mathbf{K}(G)$

Proof. We need to show $(\tau, v_1, v_2) \in \mathbf{E}(G)$ for $(\tau, v_1, v_2) \in \overline{G}$, which holds by Lemma 65. ☐

Lemma 67. If $L_1, L_2 \in \mathrm{LK}$ and $G \in \mathrm{GK}(L_1 \cup L_2)$, then $G \in \mathrm{GK}(L_1) \cap \mathrm{GK}(L_2)$.

Proof. We must show $G \geq L_1(G)$ and $G \geq L_2(G)$. Both follow from $G \geq (L_1 \cup L_2)(G)$. ☐

Lemma 68. If $\mathit{consistent}(L_1)$ and $\mathit{consistent}(L_2)$, then $\mathit{consistent}(L_1 \cup L_2)$.

Proof.

- We suppose (1) $G \in \mathrm{GK}(L_1 \cup L_2)$ and (2) $(\tau, e_1, e_2) \in \mathbf{S}((L_1 \cup L_2)(G), G)$.
- We must show $(\tau, \mathit{beta}(e_1), \mathit{beta}(e_2)) \in \mathbf{E}(G)$.
- From (2) we know $(\tau, e_1, e_2) \in \mathbf{S}(L_1(G), G) \vee (\tau, e_1, e_2) \in \mathbf{S}(L_2(G), G)$.
- If the former is true, the goal follows from $\mathit{consistent}(L_1)$ with the help of Lemma 67.
- If the latter is true, the goal follows from $\mathit{consistent}(L_2)$ with the help of Lemma 67.

$\square$

Lemma 69. If $(\tau', \tau, K_1, K_2) \in \mathbf{K}(G)$, then:

1. $(\tau', e_1, e_2) \in \mathbf{E}(G)$ implies $(\tau, K_1[e_1], K_2[e_2]) \in \mathbf{E}(G)$.
2. $(\tau'', \tau', K_1', K_2') \in \mathbf{K}(G)$ implies $(\tau'', \tau, K_1[K_1'], K_2[K_2']) \in \mathbf{K}(G)$.

Proof. We define $\mathbf{E}'_L$ and $\mathbf{K}'_L$ as follows:

$$\mathbf{E}'_L(G) = \{ (\tau, K_1[e_1], K_2[e_2]) \mid \exists \tau'.\ (\tau', e_1, e_2) \in \mathbf{E}(G) \wedge (\tau', \tau, K_1, K_2) \in \mathbf{K}(G) \}$$

$$\mathbf{K}'_L(G) = \{ (\tau'', \tau, K_1[K_1'], K_2[K_2']) \mid \exists \tau'.\ (\tau'', \tau', K_1', K_2') \in \mathbf{K}(G) \wedge (\tau', \tau, K_1, K_2) \in \mathbf{K}(G) \}$$

It suffices to show $\mathbf{E}' \leq \mathbf{E}$ and $\mathbf{K}' \leq \mathbf{K}$, which we do by coinduction. Concretely, we have to show:

1. $\forall K_1, K_2, e_1, e_2, G, \tau.$
   $(K_1[e_1], K_2[e_2]) \in \mathbf{E}'(G)(\tau) \implies (K_1[e_1], K_2[e_2]) \in \mathbf{O}(\mathbf{K}')(G)(\tau)$
2. $\forall K_1, K_2, K_1', K_2', G, \tau'', \tau.$
   $(K_1[K_1'], K_2[K_2']) \in \mathbf{K}'(G)(\tau'', \tau) \implies \forall (v_1, v_2) \in \overline{G}(\tau'').\ (K_1[K_1'][v_1], K_2[K_2'][v_2]) \in \mathbf{E}'(G)(\tau)$

For (1):

- Suppose $(K_1[e_1], K_2[e_2]) \in \mathbf{E}'(G)(\tau)$.
- By definition of $\mathbf{E}'$ we know $(e_1, e_2) \in \mathbf{E}(G)(\tau')$ and

  $$(K_1, K_2) \in \mathbf{K}(G)(\tau', \tau)$$

  for some τ'.
- We must show $(K_1[e_1], K_2[e_2]) \in \mathbf{O}(\mathbf{K}')(G)(\tau)$.
- We know $(e_1, e_2) \in \mathbf{O}(\mathbf{K})(G)(\tau')$.
- Hence at least one of the following three properties holds:
  - A) $e_1\!\uparrow$ and $e_2\!\uparrow$
  - B) (a) $e_1 \hookrightarrow^* v_1$ and $e_2 \hookrightarrow^* v_2$
    (b) $(v_1, v_2) \in \overline{G}(\tau')$
  - C) (a) $e_1 \hookrightarrow^* K_1'[e_1']$ and $e_2 \hookrightarrow^* K_2'[e_2']$
    (b) $(e_1', e_2') \in \mathbf{S}(G, G)(\widetilde{\tau})$
    (c) $(K_1', K_2') \in \mathbf{K}(G)(\widetilde{\tau}, \tau')$
- If (A) holds:
  - Then $K_1[e_1]\!\uparrow$ and $K_2[e_2]\!\uparrow$, so we are done.
- If (B) holds:
  - Then $K_1[e_1] \hookrightarrow^* K_1[v_1]$ and $K_2[e_2] \hookrightarrow^* K_2[v_2]$ from (Ba).
  - Since $(K_1, K_2) \in \mathbf{K}(G)(\tau', \tau)$, we get $(K_1[v_1], K_2[v_2]) \in \mathbf{E}(G)(\tau)$ from (Bb).
  - We show $\mathbf{O}(\mathbf{K})(G)(\tau) \subseteq \mathbf{O}(\mathbf{K}')(G)(\tau)$:
    * It suffices to show $\mathbf{K} \leq \mathbf{K}'$.
    * By definition of the latter, this follows from Lemma 66.

– Consequently, $(K_1[v_1], K_2[v_2]) \in \mathbf{O}(\mathbf{K}')(G)(\tau)$.
– We are done by Lemma 64.

- If (C) holds:
  – Then $e_1 \hookrightarrow^* K_1[K_1'][e_1']$ and $e_2 \hookrightarrow^* K_2[K_2'][e_2']$ from (Ca).
  – Due to (Cb) it remains to show:

$$(K_1[K_1'], K_2[K_2']) \in \mathbf{K}_L'(G)(\widetilde{\tau}, \tau)$$

  – By definition of $\mathbf{K}'$ it suffices to show $(K_1', K_2') \in \mathbf{K}(G)(\widetilde{\tau}, \tau')$ and $(K_1, K_2) \in \mathbf{K}(G)(\tau', \tau)$, which hold by (Cc) and the premise.

For (2):

- Suppose $(K_1[K_1'], K_2[K_2']) \in \mathbf{K}'(G)(\tau'', \tau)$ and $(v_1, v_2) \in \overline{G}(\tau'')$.
- By definition of $\mathbf{K}'$ we know $(K_1', K_2') \in \mathbf{K}(G)(\tau'', \tau')$ and

$$(K_1, K_2) \in \mathbf{K}(G)(\tau', \tau)$$

  for some τ'.
- We must show $(K_1[K_1'][v_1], K_2[K_2'][v_2]) \in \mathbf{E}'(G)(\tau)$.
- By definition of $\mathbf{E}'$ it suffices to show $(K_1'[v_1], K_2'[v_2]) \in \mathbf{E}(G)(\tau')$ and $(K_1, K_2) \in \mathbf{K}(G)(\tau', \tau)$.
- The latter is given and the former follows from $(K_1', K_2') \in \mathbf{K}(G)(\tau'', \tau')$ and $(v_1, v_2) \in \overline{G}(\tau'')$.

□

Lemma 70. If *consistent*(L_2), then:

$$\Gamma \vdash e_1 \sim_{L_1} e_2 : \tau \quad \Longrightarrow \quad \Gamma \vdash e_1 \sim_{L_1 \cup L_2} e_2 : \tau$$

Proof.

- Using the assumptions and Lemma 68, we get *consistent*$(L_1 \cup L_2)$.
- Now suppose $G \in \mathrm{GK}(L_1 \cup L_2)$ and $(\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G)$.
- We must show $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}(G)(\tau)$.
- This follows from $\Gamma \vdash e_1 \sim_{L_1} e_2 : \tau$ and Lemma 67.

□

Lemma 71. If $\forall L \in \mathrm{LK}.\ \big(\forall i \in \{1 \ldots n\}.\ \Gamma_i \vdash e_i \sim_L e_i' : \tau_i\big) \implies \Gamma \vdash e \sim_L e' : \tau$, then:

$$\big(\forall i \in \{1 \ldots n\}.\ \Gamma_i \vdash e_i \sim e_i' : \tau_i\big) \implies \Gamma \vdash e \sim e' : \tau$$

Proof.

- Suppose $\forall L \in \mathrm{LK}.\ \big(\forall i \in \{1 \ldots n\}.\ \Gamma_i \vdash e_i \sim_L e_i' : \tau_i\big) \implies \Gamma \vdash e \sim_L e' : \tau$ and $\forall i \in \{1 \ldots n\}.\ \Gamma_i \vdash e_i \sim e_i' : \tau_i$.
- From the latter we have L_i's such that for all i, $\Gamma_i \vdash e_i \sim_{L_i} e_i' : \tau_i$.
- By applying Lemma 70 repeatedly we get $\Gamma_i \vdash e_i \sim_{L_1 \cup \ldots \cup L_n} e_i' : \tau_i$ for all i.

- By the assumption we thus have $\Gamma \vdash e \sim_{L_1 \cup \ldots \cup L_n} e' : \tau$ and thus $\Gamma \vdash e \sim e' : \tau$.

□

Lemma 72. If $\forall G \in \mathrm{GK}(L).\ \forall(\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G).\ (\gamma_1 K_1, \gamma_2 K_2) \in \mathbf{K}(G)(\tau', \tau)$ then

$$\Gamma \vdash e_1 \sim_L e_2 : \tau' \quad \Longrightarrow \quad \Gamma \vdash K_1[e_1] \sim_L K_2[e_2] : \tau$$

Proof.

- Suppose $G \in \mathrm{GK}(L)$ and $(\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G)$.
- We must show $((\gamma_1 K_1)[\gamma_1 e_1], (\gamma_2 K_2)[\gamma_2 e_2]) \in \mathbf{E}(G)(\tau)$.
- From the premise we get $(\gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}(G)(\tau')$.
- By Lemma 69 it suffices to show $(\gamma_1 K_1, \gamma_2 K_2) \in \mathbf{K}(G)(\tau', \tau)$.
- This follows from the assumption.

□

Lemma 73 (External call)**.** For $G \in \mathrm{GK}(L)$, if $\mathit{consistent}(L) \wedge G = L(G) \cup R$, then we have

$$\begin{aligned}
&\forall(\tau, e_1, e_2) \in \mathbf{E}(G).\\
&\quad (e_1\!\uparrow \wedge\, e_2\!\uparrow)\\
&\vee\ (\exists v_1, v_2.\ e_1 \hookrightarrow^* v_1 \wedge e_2 \hookrightarrow^* v_2 \wedge (v_1, v_2) \in \overline{G}(\tau))\\
&\vee\ (\exists \tau', K_1, K_2, e_1', e_2'.\ e_1 \hookrightarrow^* K_1[e_1'] \wedge e_2 \hookrightarrow^* K_2[e_2'] \wedge (\tau', e_1', e_2') \in \mathbf{S}(R, G) \wedge\\
&\quad (K_1, K_2) \in \mathbf{K}(G)(\tau', \tau))
\end{aligned}$$

Proof.

- We prove the following proposition by induction on n.

$$\begin{aligned}
&\forall(\tau, e_1, e_2) \in \mathbf{E}(G).\\
&\quad (e_1\!\uparrow^n \wedge\, e_2\!\uparrow^n)\\
&\vee\ (\exists v_1, v_2.\ e_1 \hookrightarrow^* v_1 \wedge e_2 \hookrightarrow^* v_2 \wedge (v_1, v_2) \in \overline{G}(\tau))\\
&\vee\ (\exists \tau', K_1, K_2, e_1', e_2'.\ e_1 \hookrightarrow^* K_1[e_1'] \wedge e_2 \hookrightarrow^* K_2[e_2'] \wedge (\tau', e_1', e_2') \in \mathbf{S}(R, G) \wedge\\
&\quad (K_1, K_2) \in \mathbf{K}(G)(\tau', \tau))
\end{aligned} \tag{2}$$

- When $n = 0$, the first case holds vacuously.
- When $n > 0$, we assume that the goal (2) holds for $n - 1$. Then we need to show that the goal (2) holds for n.
- By definition of $\mathbf{E}(G)$, we have three cases.
- In the first two cases, the goal (2) is trivially satisfied.
- In the third case, we have

$$\begin{aligned}
&\exists \tau', K_1, K_2, e_1', e_2'.\ e_1 \hookrightarrow^* K_1[e_1'] \wedge e_2 \hookrightarrow^* K_2[e_2'] \wedge (\tau', e_1', e_2') \in \mathbf{S}(G, G) \wedge\\
&(K_1, K_2) \in \mathbf{K}(G)(\tau', \tau)
\end{aligned}$$

- As $G = L(G) \cup R$, by definition of $\mathbf{S}$, we have

$$(\tau', e_1', e_2') \in \mathbf{S}(G, G) = \mathbf{S}(L(G), G) \cup \mathbf{S}(R, G)\ .$$

- If $(\tau', e'_1, e'_2) \in \mathbf{S}(R, G)$, then the goal (2) is satisfied.
- If $(\tau', e'_1, e'_2) \in \mathbf{S}(L(G), G)$, then by *consistent*$(L)$, we have that $K_1[e'_1] \hookrightarrow^1 K_1[\mathit{beta}(e'_1)]$ and $K_2[e'_2] \hookrightarrow^1 K_2[\mathit{beta}(e'_2)]$ and $(\tau', \mathit{beta}(e'_1), \mathit{beta}(e'_2)) \in \mathbf{E}(G)$.
- By Lemma 69, we have $(\tau, K_1[\mathit{beta}(e'_1)], K_2[\mathit{beta}(e'_2)]) \in \mathbf{E}(G)$.
- By induction hypothesis we have that $K_1[\mathit{beta}(e'_1)]$ and $K_2[\mathit{beta}(e'_2)]$ satisfy the goal (2) for $n-1$.
- As $e_1 \hookrightarrow^+ K_1[\mathit{beta}(e'_1)]$ and $e_2 \hookrightarrow^+ K_2[\mathit{beta}(e'_2)]$, we have that e_1 and e_2 satisfy the goal (2) for n, so we are done.
- The original goal is obtained from the sub-goal (2) by pushing the quantification over n inside the first case and then observing that $\forall n. e\uparrow^n$ is equivalent to $e\uparrow$.

□

Corollary 74. If

- *consistent*(L)
- $G = L(G)$
- $(\tau, e_1, e_2) \in \mathbf{E}(G)$

then one of the following holds:

1. $e_1\uparrow \wedge e_2\uparrow$
2. $\exists v_1, v_2.\ e_1 \hookrightarrow^* v_1 \wedge e_2 \hookrightarrow^* v_2 \wedge (\tau, v_1, v_2) \in \overline{G}$

Proof. Follows from Lemma 73 for $R = \emptyset$. □

5.3 Compatibility

Lemma 75 (Compatibility: Var)**.**

$$\frac{\Gamma \text{ well-formed} \qquad x{:}\tau \in \Gamma}{\Gamma \vdash x \sim x : \tau}$$

Proof.

- Let $L := \lambda R.\emptyset$.
- We are done if we can show $\Gamma \vdash x \sim_L x : \tau$.
- It is obvious that *consistent*(L).
- Now suppose $G \in \mathrm{GK}(L)$ and $(\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G)$.
- We must show $(\gamma_1(x), \gamma_2(x)) \in \mathbf{E}(G)(\tau)$.
- From $(\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G)$ we know $(\gamma_1(x), \gamma_2(x)) \in \overline{G}(\tau)$.
- We are done by Lemma 65.

□

Lemma 76.

1. If $(\tau, v_1, v_2) \in \overline{G}$, then $(\tau', \tau \times \tau', \langle v_1, \bullet\rangle, \langle v_2, \bullet\rangle) \in \mathbf{K}(G)$.

2. If $(\tau', e'_1, e'_2) \in \mathbf{E}(G)$, then $(\tau, \tau \times \tau', \langle \bullet, e'_1 \rangle, \langle \bullet, e'_2 \rangle) \in \mathbf{K}(G)$.

Proof.

1.
   - Suppose $(v'_1, v'_2) \in \overline{G}(\tau')$.
   - We need to show $(\langle v_1, v'_1 \rangle, \langle v_2, v'_2 \rangle) \in \mathbf{E}(G)(\tau \times \tau')$.
   - By Lemma 65 it suffices to show $(\langle v_1, v'_1 \rangle, \langle v_2, v'_2 \rangle) \in \overline{G}(\tau \times \tau')$.
   - Hence it suffices to show $(v_1, v_2) \in \overline{G}(\tau)$ and $(v'_1, v'_2) \in \overline{G}(\tau')$, which we both already have.
2.
   - Suppose $(v_1, v_2) \in \overline{G}(\tau)$.
   - We need to show $(\langle v_1, e'_1 \rangle, \langle v_2, e'_2 \rangle) \in \mathbf{E}(G)(\tau \times \tau')$.
   - By Lemma 69 it suffices to show $(\langle v_1, \bullet \rangle, \langle v_2, \bullet \rangle) \in \mathbf{K}(G)(\tau', \tau \times \tau')$.
   - By part (1) it then suffices to show $(v_1, v_2) \in \overline{G}(\tau)$, which we have.

□

Lemma 77 (Compatibility: Pair)**.**

$$\frac{\Gamma \vdash e_1 \sim e_2 : \tau \qquad \Gamma \vdash e'_1 \sim e'_2 : \tau'}{\Gamma \vdash \langle e_1, e'_1 \rangle \sim \langle e_2, e'_2 \rangle : \tau \times \tau'}$$

Proof.

- By Lemmas 71 and 72 it suffices to show

$$\forall G \in \mathrm{GK}(L).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G).\ (\langle \bullet, \gamma_1 e'_1 \rangle, \langle \bullet, \gamma_2 e'_2 \rangle) \in \mathbf{K}(G)(\tau, \tau \times \tau')$$

  under the assumption $\Gamma \vdash e'_1 \sim_L e'_2 : \tau'$.
- By Lemma 76 it then suffices to show $(\gamma_1 e'_1, \gamma_2 e'_2) \in \mathbf{E}(G)(\tau')$, which follows from the assumption.

□

Lemma 78 (Compatibility: Fst (Snd analogously))**.**

$$\frac{\Gamma \vdash e_1 \sim e_2 : \tau \times \tau'}{\Gamma \vdash e_1.1 \sim e_2.1 : \tau}$$

Proof.

- By Lemmas 71 and 72 it suffices to show

$$\forall L \in \mathrm{LK}.\ \forall G \in \mathrm{GK}(L).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G).\ (\bullet.1, \bullet.1) \in \mathbf{K}(G)(\tau \times \tau', \tau)$$

- Suppose $(v_1^\circ, v_2^\circ) \in \overline{G}(\tau \times \tau')$.
- We need to show $(v_1^\circ.1, v_2^\circ.1) \in \mathbf{E}(G)(\tau)$.
- We know $v_1^\circ = \langle v_1, v'_1 \rangle$ and $v_2^\circ = \langle v_2, v'_2 \rangle$ with $(v_1, v_2) \in \overline{G}(\tau)$.
- Hence $v_1^\circ.1 \hookrightarrow v_1$ and $v_2^\circ.1 \hookrightarrow v_2$, so we are done.

□

Lemma 79 (Compatibility: Inl (Inr analogously))**.**

$$\frac{\Gamma \vdash e_1 \sim e_2 : \tau}{\Gamma \vdash \mathsf{inj}^1\, e_1 \sim \mathsf{inj}^1\, e_2 : \tau + \tau'}$$

Proof.

- By Lemmas 71 and 72 it suffices to show

$$\forall L \in \text{LK}.\ \forall G \in \text{GK}(L).\ \forall(\gamma_1, \gamma_2) \in \text{Env}(\Gamma, G).\ (\mathsf{inj}^1 \bullet, \mathsf{inj}^1 \bullet) \in \mathbf{K}(G)(\tau, \tau + \tau')$$

- Suppose $(v_1, v_2) \in \overline{G}(\tau)$.
- We need to show $(\mathsf{inj}^1\, v_1, \mathsf{inj}^1\, v_2) \in \mathbf{E}(G)(\tau + \tau')$.
- By Lemma 65 it suffices to show $(\mathsf{inj}^1\, v_1, \mathsf{inj}^1\, v_2) \in \overline{G}(\tau + \tau')$.
- This follows from $(v_1, v_2) \in \overline{G}(\tau)$.

□

Lemma 80 (Compatibility: Case)**.**

$$\frac{\Gamma \vdash e_1 \sim e_2 : \tau' + \tau'' \qquad \Gamma, x{:}\tau' \vdash e_1' \sim e_2' : \tau \qquad \Gamma, x{:}\tau'' \vdash e_1'' \sim e_2'' : \tau}{\Gamma \vdash \mathsf{case}\, e_1\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow e_1' \,|\, \mathsf{inj}^2\, x \Rightarrow e_1'' \sim \mathsf{case}\, e_2\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow e_2' \,|\, \mathsf{inj}^2\, x \Rightarrow e_2'' : \tau}$$

Proof.

- By Lemmas 71 and 72 it suffices to show

  $\forall G \in \text{GK}(L).\ \forall(\gamma_1, \gamma_2) \in \text{Env}(\Gamma, G).$
  $(\mathsf{case} \bullet \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_1 e_1' \,|\, \mathsf{inj}^2\, x \Rightarrow \gamma_1 e_1'', \mathsf{case} \bullet \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_2 e_2' \,|\, \mathsf{inj}^2\, x \Rightarrow \gamma_2 e_2'') \in \mathbf{K}(G)(\tau' + \tau'', \tau)$

  assuming $\Gamma, x{:}\tau' \vdash e_1' \sim_L e_2' : \tau$ and $\Gamma, x{:}\tau'' \vdash e_1'' \sim_L e_2'' : \tau$.

- Thus it suffices to show

$$(\mathsf{case}\, v_1\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_1 e_1' \,|\, \mathsf{inj}^2\, x \Rightarrow \gamma_1 e_1'', \mathsf{case}\, v_2\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_2 e_2' \,|\, \mathsf{inj}^2\, x \Rightarrow \gamma_2 e_2'') \in \mathbf{E}(G)(\tau)$$

  for $(v_1, v_2) \in \overline{G}(\tau' + \tau'')$.

- By definition of $\overline{G}(\tau' + \tau'')$, we have v_1', v_2' such that either
  1. $v_1 = \mathsf{inj}^1\, v_1' \wedge v_2 = \mathsf{inj}^1\, v_2' \wedge (v_1', v_2') \in \overline{G}(\tau')$; or
  2. $v_1 = \mathsf{inj}^2\, v_1' \wedge v_2 = \mathsf{inj}^2\, v_2' \wedge (v_1', v_2') \in \overline{G}(\tau'')$.
- We continue for the former case (the latter is analogous).
- Let $\gamma_1' := \gamma_1, x{\mapsto}v_1'$ and $\gamma_2' := \gamma_2, x{\mapsto}v_2'$.
- We have

$$\mathsf{case}\, v_1\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_1 e_1' \,|\, \mathsf{inj}^2\, x \Rightarrow \gamma_1 e_1'' \hookrightarrow \gamma_1' e_1'$$

  and

$$\mathsf{case}\, v_2\, \mathsf{of}\, \mathsf{inj}^1\, x \Rightarrow \gamma_2 e_2' \,|\, \mathsf{inj}^2\, x \Rightarrow \gamma_2 e_2'' \hookrightarrow \gamma_2' e_2'$$

- Thus by Lemma 64 it suffices to show

$$(\tau', \gamma_1' e_1', \gamma_2' e_2') \in \mathbf{O}(\mathbf{E})(G)$$

- This follows from the assumption and $(\gamma_1', \gamma_2') \in \text{Env}((\Gamma, x : \tau'), G)$.

□

Lemma 81 (Compatibility: Fix)**.**

$$\frac{\Gamma, f{:}\tau' \to \tau, x{:}\tau' \vdash e_1 \sim e_2 : \tau}{\Gamma \vdash \mathsf{fix}\, f(x).\, e_1 \sim \mathsf{fix}\, f(x).\, e_2 : \tau' \to \tau}$$

Proof.

- From the premise we have L such that $\Gamma, f{:}\tau' \to \tau, x{:}\tau' \vdash e_1 \sim_L e_2 : \tau$.
- Let $L' := \lambda R.\ \{(\tau' \to \tau, \gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \mid (\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, R)\}$.
- It suffices to show $\Gamma \vdash \mathsf{fix}\, f(x).\, e_1 \sim_{L \cup L'} \mathsf{fix}\, f(x).\, e_2 : \tau' \to \tau$.
- To do so, we first prove $\mathit{consistent}(w \cup w')$:
  - We suppose
    1. $G \in \mathrm{GK}(L \cup L')$
    2. $(v_1, v_2) \in (L \cup L')(G)(\widetilde{\tau'} \to \widetilde{\tau})$
    3. $(v_1', v_2') \in \overline{G}(\widetilde{\tau'})$

    and must show:
    $$(\mathit{beta}(v_1\ v_1'), \mathit{beta}(v_2\ v_2')) \in \mathbf{E}(G)(\widetilde{\tau})$$
  - From (2) we know:
    $$(v_1, v_2) \in L(G)(\widetilde{\tau'} \to \widetilde{\tau}) \lor$$
    $$(v_1, v_2) \in L'(G)(\widetilde{\tau'} \to \widetilde{\tau})$$
  - If the former is true, the claim follows from $\mathit{consistent}(L)$ with the help of Lemma 67.
  - So suppose the latter.
  - Then $\widetilde{\tau'} \to \widetilde{\tau} = \tau' \to \tau$ and $v_1 = \gamma_1 \mathsf{fix}\, f(x).\, e_1$ and $v_2 = \gamma_2 \mathsf{fix}\, f(x).\, e_2$ for $(\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G)$.
  - Let $\gamma_1' = \gamma_1, f{\mapsto}\gamma_1 \mathsf{fix}\, f(x).\, e_1, x{\mapsto}v_1'$ and $\gamma_2' = \gamma_2, f{\mapsto}\gamma_2 \mathsf{fix}\, f(x).\, e_2, x{\mapsto}v_2'$
  - It remains to show $(\gamma_1' e_1, \gamma_2' e_2) \in \mathbf{E}(G)(\tau)$.
  - This follows from the premise if we can show $(\gamma_1', \gamma_2') \in \mathrm{Env}((\Gamma, f{:}\tau' \to \tau, x{:}\tau'), G)$.
  - This reduces to showing $(v_1', v_2') \in \overline{G}(\tau')$ and $(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in \overline{G}(\tau' \to \tau)$.
  - The former is given as (3).
  - For the latter, note that by (1) it suffices to show
    $$(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in (L \cup L')(G)(\tau' \to \tau).$$
  - For this, it suffices to show $(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in L'(G)(\tau' \to \tau)$.
  - Since $(\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G)$, this holds by construction.
- Now suppose $G \in \mathrm{GK}(L \cup L')$ and $(\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G)$.
- We must show $(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in \mathbf{E}(G)(\tau' \to \tau)$.
- By Lemma 65 it suffices to show $(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in G(\tau' \to \tau)$.
- By definition of GK it suffices to show:
  $$(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in (L \cup L')(G)(\tau' \to \tau)$$
- For this, it suffices to show $(\gamma_1 \mathsf{fix}\, f(x).\, e_1, \gamma_2 \mathsf{fix}\, f(x).\, e_2) \in L'(G)(\tau' \to \tau)$.

- Since $(\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G)$, this holds by construction of L'.

$\square$

Lemma 82.

1. If $(\tau' \to \tau, v_1, v_2) \in \overline{G}$, then $(\tau', \tau, v_1 \bullet, v_2 \bullet) \in \mathbf{K}(G)$.
2. If $(\tau', e_1', e_2') \in \mathbf{E}(G)$, then $(\tau' \to \tau, \tau, \bullet\ e_1', \bullet\ e_2') \in \mathbf{K}(G)$.

Proof.

1. - Suppose $(v_1', v_2') \in \overline{G}(\tau')$.
   - We need to show $(v_1\ v_1', v_2\ v_2') \in \mathbf{E}(G)(\tau)$.
   - By definition of $\mathbf{E}$ it suffices to show the following:
     (a) $(v_1, v_2) \in \overline{G}(\tau' \to \tau)$
     (b) $(v_1', v_2') \in \overline{G}(\tau')$
     (c) $(\bullet, \bullet) \in \mathbf{K}(G)(\tau, \tau)$
   - (a) and (b) are already given.
   - (c) holds by Lemma 66.
2. - Suppose $(v_1, v_2) \in \overline{G}(\tau' \to \tau)$.
   - We need to show $(v_1\ e_1', v_2\ e_2') \in \mathbf{E}(G)(\tau)$.
   - By Lemma 69 it suffices to show $(v_1 \bullet, v_2 \bullet) \in \mathbf{K}(G)(\tau', \tau)$.
   - By part (1) it then suffices to show $(v_1, v_2) \in \overline{G}(\tau' \to \tau)$, which we have.

$\square$

Lemma 83 (Compatibility: App)**.**

$$\frac{\Gamma \vdash e_1 \sim e_2 : \tau' \to \tau \qquad \Gamma \vdash e_1' \sim e_2' : \tau'}{\Gamma \vdash e_1\ e_1' \sim e_2\ e_2' : \tau}$$

Proof.

- By Lemmas 71 and 72 it suffices to show

$$\forall G \in \mathrm{GK}(L).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G).\ (\bullet\ \gamma_1 e_1', \bullet\ \gamma_2 e_2') \in \mathbf{K}(G)(\tau' \to \tau, \tau)$$

  assuming $\Gamma \vdash e_1' \sim_L e_2' : \tau'$.
- By Lemma 82 it suffices to show $(\gamma_1 e_1', \gamma_2 e_2') \in \mathbf{E}(G)(\tau')$, which follows from the assumption.

$\square$

Lemma 84 (Compatibility: Roll)**.**

$$\frac{\Gamma \vdash e_1 \sim e_2 : \sigma[\mu\alpha.\,\sigma/\alpha]}{\Gamma \vdash \mathsf{roll}\ e_1 \sim \mathsf{roll}\ e_2 : \mu\alpha.\,\sigma}$$

Proof.

- By Lemmas 71 and 72 it suffices to show

$$\forall L \in \mathrm{LK}.\ \forall G \in \mathrm{GK}(L).\ \forall (\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G).\ (\mathsf{roll}\ \bullet, \mathsf{roll}\ \bullet) \in \mathbf{K}(G)(\sigma[\mu\alpha.\,\sigma/\alpha], \mu\alpha.\,\sigma)$$

- Suppose $(v_1, v_2) \in \overline{G}(\sigma[\mu\alpha.\,\sigma/\alpha])$.
- We need to show $(\mathsf{roll}\ v_1, \mathsf{roll}\ v_2) \in \mathbf{E}(G)(\mu\alpha.\,\sigma)$.
- By Lemma 65 it suffices to show $(\mathsf{roll}\ v_1, \mathsf{roll}\ v_2) \in \overline{G}(\mu\alpha.\,\sigma)$.
- This follows from $(v_1, v_2) \in \overline{G}(\sigma[\mu\alpha.\,\sigma/\alpha])$.

□

Lemma 85 (Compatibility: Unroll)**.**

$$\frac{\Gamma \vdash e_1 \sim e_2 : \mu\alpha.\,\sigma}{\Gamma \vdash \mathsf{unroll}\ e_1 \sim \mathsf{unroll}\ e_2 : \sigma[\mu\alpha.\,\sigma/\alpha]}$$

Proof.

- By Lemmas 71 and 72 it suffices to show

$$\forall L \in \mathrm{LK}.\ \forall G \in \mathrm{GK}(L).\ \forall(\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, G).\ (\mathsf{unroll}\ \bullet, \mathsf{unroll}\ \bullet) \in \mathbf{K}(G)(\mu\alpha.\,\sigma, \sigma[\mu\alpha.\,\sigma/\alpha])$$

- Suppose $(v_1^\circ, v_2^\circ) \in \overline{G}(\mu\alpha.\,\sigma)$.
- We need to show $(\mathsf{unroll}\ v_1^\circ, \mathsf{unroll}\ v_2^\circ) \in \mathbf{E}(G)(\sigma[\mu\alpha.\,\sigma/\alpha])$.
- We know $v_1^\circ = \mathsf{roll}\ v_1$ and $v_2^\circ = \mathsf{roll}\ v_2$ with $(v_1, v_2) \in \overline{G}(\sigma[\mu\alpha.\,\sigma/\alpha])$.
- Hence $\mathsf{unroll}\ v_1^\circ \hookrightarrow v_1$ and $\mathsf{unroll}\ v_2^\circ \hookrightarrow v_2$ and we are done.

□

5.4 Soundness

Theorem 86 (Fundamental Property)**.** If $\Gamma \vdash p : \tau$, then $\Gamma \vdash |p| \sim |p| : \tau$.

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

Lemma 87 (Weakening)**.** If $\Gamma \vdash e_1 \sim e_2 : \tau$ and $\Gamma \subseteq \Gamma'$, then $\Gamma' \vdash e_1 \sim e_2 : \tau$.

Proof. One can easily see that the goal is a direct consequence of the definition from the following observation:

$$\begin{array}{l} \forall R.\ \forall(\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma', R). \\ \lfloor\gamma\rfloor_{\mathrm{dom}(\Gamma)} \in \mathrm{Env}(\Gamma, R) \wedge \\ \gamma_1 e_1 = \lfloor\gamma\rfloor_{\mathrm{dom}(\Gamma)_{(1)}} e_1 \wedge \gamma_2 e_2 = \lfloor\gamma\rfloor_{\mathrm{dom}(\Gamma)_{(2)}} e_2 \end{array}$$

where $\lfloor f \rfloor_d$ denotes the restriction of the function f on domain d. □

Lemma 88 (Congruence)**.** If $\Gamma \vdash e_1 \sim e_2 : \tau$ and $\vdash C : (\Gamma; \tau) \rightsquigarrow (\Gamma'; \tau')$, then

$$\Gamma' \vdash |C|[e_1] \sim |C|[e_2] : \tau'\ .$$

Proof. By induction on the derivation of the context typing: in each case using the corresponding compatibility lemma. For a context containing subterms we also need Theorem 86. The rule for an empty context requires Lemma 87. □

Lemma 89 (Adequacy)**.** If $\cdot \vdash e_1 \sim e_2 : \tau$, then

1. neither e_1 nor e_2 gets stuck.

2. $e_1\!\uparrow \iff e_2\!\uparrow$.

Proof.

- We know $\cdot \vdash e_1 \sim_L e_2 : \tau$ for some L.
- Hence we have *consistent*(L) and, using Lemma 63, $(e_1, e_2) \in \mathbf{E}([L])(\tau)$.
- Since $[L] = L([L])$, by Corollary 74 either e_1 and e_2 diverge or both terminate without getting stuck.

□

Theorem 90 (Soundness)**.** If $\Gamma \vdash p_1 : \tau$ and $\Gamma \vdash p_2 : \tau$, then:

$$\Gamma \vdash |p_1| \sim |p_2| : \tau \implies \Gamma \vdash p_1 \sim_{\text{ctx}} p_2 : \tau$$

Proof.

- Suppose $\Gamma \vdash |p_1| \sim |p_2| : \tau$ as well as $\vdash C : (\Gamma; \tau) \rightsquigarrow (\cdot; \tau)$.
- By congruence (Lemma 88), we have $\cdot \vdash |C[p_1]| \sim |C[p_2]| : \tau$.
- By adequacy (Lemma 89), we have $|C[p_1]| \uparrow \iff |C[p_2]| \uparrow$, so we are done.

□

5.5 Symmetry

Definition 6. Given $R \in$ VRel (or VRelF), we define $R^{-1} \in$ VRel (or VRelF) as follows:

$$R^{-1} := \lambda\tau.\ R(\tau)^{-1}$$

Lemma 91. $(\overline{R})^{-1} = \overline{R^{-1}}$

Proof. Easy to check by induction. □

Lemma 92. $\mathbf{S}(R_f^{-1}, R_v^{-1}) = \big(\mathbf{S}(R_f, R_v)\big)^{-1}$

Proof. Easy to check. □

Definition 7. Given $L \in$ LK, we define $L^{-1} \in$ LK as follows:

$$L^{-1}(R) \ := \ \big(L(R^{-1})\big)^{-1} \ .$$

Lemma 93. If $G \in \text{GK}(L^{-1})$, then $G^{-1} \in \text{GK}(L)$.

Proof. It holds vacuously by definition. □

Lemma 94.

$$\big(\mathbf{E}(G^{-1})\big)^{-1} \subseteq \mathbf{E}(G)$$

Proof. By definition with the help of Lemmas 91 and 92. □

Lemma 95. If *consistent*(L), then *consistent*(L^{-1}).

Proof. By definition with the help of Lemmas 92, 93, and 94. □

Theorem 96. If $\Gamma \vdash e_1 \sim e_2 : \tau$, then $\Gamma \vdash e_2 \sim e_1 : \tau$.

Proof. Suppose $\Gamma \vdash e_1 \sim_L e_2 : \tau$. It suffices to show $\Gamma \vdash e_2 \sim_{L^{-1}} e_1 : \tau$. Using Lemma 95, this in turn reduces to showing:

$$\forall G \in \text{GK}(L^{-1}).\ \forall(\gamma_1, \gamma_2) \in \text{Env}(\Gamma, G).\ (\gamma_1 e_2, \gamma_2 e_1) \in \mathbf{E}(G)(\tau)$$

From $(\gamma_1, \gamma_2) \in \text{Env}(\Gamma, G)$ we have $(\gamma_2, \gamma_1) \in \text{Env}(\Gamma, G^{-1})$. Lemma 93 and the assumption thus yield $(\gamma_2 e_1, \gamma_1 e_2) \in \mathbf{E}(G^{-1})(\tau)$. We are done by Lemma 94. □

6 Transitivity

Definition 8. For $R_1, R_2 \in \text{VRelF}$, we define the composition as follows.

$$(R_1 \circ R_2)(\tau) := \{\, (v_1, v_3) \mid \exists v_2.\ (\tau, v_1, v_2) \in R_1 \wedge (\tau, v_2, v_3) \in R_2 \,\}$$

Since CType and CVal are countable sets, there exists an injective function $\mathbf{I} \in \text{CType} \times \text{CType} \times \text{CVal} \times \text{CVal} \to \mathbb{N}$.

Definition 9. Using the function $\mathbf{I}$, we decompose $R \in \text{VRelF}$ as follows:

$$\begin{array}{lcl} R_{(1)}(\tau_1 \to \tau_2) & := & \{\, (f_1, \mathbf{I}(\tau_1, \tau_2, f_1, f_3)) \mid (f_1, f_3) \in R(\tau_1 \to \tau_2) \,\} \\ R_{(2)}(\tau_1 \to \tau_2) & := & \{\, (\mathbf{I}(\tau_1, \tau_2, f_1, f_3), f_3) \mid (f_1, f_3) \in R(\tau_1 \to \tau_2) \,\} \end{array}$$

Definition 10. For a monotone function $F \in \text{VRelF} \to \text{VRelF}$ and $R \in \text{VRelF}$, we define $R^{[F]}$ as the least fixpoint of the monotone function $F(-) \cup R$.

Definition 11. For any local knowledges L_1, L_2, we define $L_1 \circ L_2$ as follows.

$$(L_1 \circ L_2)(R) \ := \ L_1({R_{(1)}}^{[L_1]}) \circ L_2({R_{(2)}}^{[L_2]})$$

Note that

$${R_{(1)}}^{[L_1]} \in \text{GK}(L_1) \quad \wedge \quad {R_{(2)}}^{[L_2]} \in \text{GK}(L_2)$$

because ${R_{(1)}}^{[L_1]} = L_1({R_{(1)}}^{[L_1]}) \cup R_{(1)}$; and ${R_{(2)}}^{[L_2]} = L_2({R_{(2)}}^{[L_2]}) \cup R_{(2)}$.

Lemma 97. For any $R, R' \in \text{VRelF}$, we have

$$(L(R) \circ R'_{(2)})(\tau_1 \to \tau_2) = (R'_{(1)} \circ L(R))(\tau_1 \to \tau_2) = \emptyset$$

Proof. The claim holds vacuously since we have $f_1, f_2 \in \text{FunVal}$ for any $(f_1, f_2) \in L(R)(\tau_1 \to \tau_2)$ and $\mathbf{I}(\tau_1, \tau_2, v_1, v_2) \notin \text{FunVal}$ for any τ_1, τ_2, v_1, v_2. □

Lemma 98. $\forall R_1, R_2 \in \text{VRelF}.\ \overline{R_1} \circ \overline{R_2} = \overline{R_1 \circ R_2}$

Proof. Recall that $\overline{R}$ is the least fixpoint of the monotone function F_R given as follows:

$$\begin{array}{lcl} F_R(X)(\tau_{\text{base}}) & := & \text{ID}_{\tau_{\text{base}}} \\ F_R(X)(\tau_1 \times \tau_2) & := & \{\, ((v_1, v_1'), (v_2, v_2')) \mid (v_1, v_2) \in X(\tau_1) \wedge (v_1', v_2') \in X(\tau_2) \,\} \\ F_R(X)(\tau_1 + \tau_2) & := & \{\, (\mathsf{inj}^1\, v_1, \mathsf{inj}^1\, v_2) \mid (v_1, v_2) \in X(\tau_1) \,\} \cup \{\, (\mathsf{inj}^2\, v_1, \mathsf{inj}^2\, v_2) \mid (v_1, v_2) \in X(\tau_2) \,\} \\ F_R(X)(\mu\alpha.\, \tau) & := & \{\, (\mathsf{roll}\ v_1, \mathsf{roll}\ v_2) \mid (v_1, v_2) \in X(\tau[\mu\alpha.\, \tau/\alpha]) \,\} \\ F_R(X)(\tau_1 \to \tau_2) & := & R(\tau_1 \to \tau_2) \end{array}$$

By case analysis on types, one can easily check that the following equality holds.

$$\forall X, Y.\ F_{R_1}(X) \circ F_{R_2}(Y) = F_{R_1 \circ R_2}(X \circ Y)$$

(Part 1: $\overline{R_1} \circ \overline{R_2} \subseteq \overline{R_1 \circ R_2}$)

- We define the set S_1 as $\{\, (\tau, v_1, v_2) \mid \forall v_3.\ (\tau, v_2, v_3) \in \overline{R_2} \implies (\tau, v_1, v_3) \in \overline{R_1 \circ R_2} \,\}$.
- Then we have the property that $\forall X.\ X \subseteq S_1 \iff X \circ \overline{R_2} \subseteq \overline{R_1 \circ R_2}$.
- Thus it suffices to show that $\overline{R_1} \subseteq S_1$, which is equivalent to show that $F_{R_1}(S_1) \subseteq S_1$ (since $\overline{R_1}$ is the least fixpoint of F_{R_1}), which is again equivalent to show that $F_{R_1}(S_1) \circ \overline{R_2} \subseteq \overline{R_1 \circ R_2}$:

$$F_{R_1}(S_1) \circ \overline{R_2} = F_{R_1}(S_1) \circ F_{R_2}(\overline{R_2}) = F_{R_1 \circ R_2}(S_1 \circ \overline{R_2}) \subseteq F_{R_1 \circ R_2}(\overline{R_1 \circ R_2}) = \overline{R_1 \circ R_2}\ .$$

(Part 2: $\overline{R_1 \circ R_2} \subseteq \overline{R_1} \circ \overline{R_2}$)

- Since $\overline{R_1 \circ R_2}$ is the least fixpoint of $F_{R_1 \circ R_2}$, it suffices to show that $F_{R_1 \circ R_2}(\overline{R_1} \circ \overline{R_2}) \subseteq \overline{R_1} \circ \overline{R_2}$:

$$F_{R_1 \circ R_2}(\overline{R_1} \circ \overline{R_2}) = F_{R_1}(\overline{R_1}) \circ F_{R_2}(\overline{R_2}) = \overline{R_1} \circ \overline{R_2} \ .$$

□

Lemma 99. For any $G \in \mathrm{GK}(L_1 \circ L_2)$, we have

$$\overline{G_{(1)}}^{[L_1]} \circ \overline{G_{(2)}}^{[L_2]} = G \ .$$

Proof. Let $L := L_1 \circ L_2$ and $\tau := \tau_1 \to \tau_2$. Then the goal follows from

$$\begin{array}{ll} & \overline{G_{(1)}}^{[L_1]}(\tau) \circ \overline{G_{(2)}}^{[L_2]}(\tau) \\ = & (L_1(\overline{G_{(1)}}^{[L_1]})(\tau) \cup G_{(1)}(\tau)) \circ (L_2(\overline{G_{(2)}}^{[L_2]})(\tau) \cup G_{(2)}(\tau)) \\ = & \big(L_1(\overline{G_{(1)}}^{[L_1]})(\tau) \circ L_2(\overline{G_{(2)}}^{[L_2]})(\tau)\big) \cup \big(G_{(1)}(\tau) \circ G_{(2)}(\tau)\big) \quad \text{(by Lemma 97)} \\ = & L(G)(\tau) \cup G(\tau) \\ = & G(\tau) \ . \qquad \text{(by } G \geq L(G)\text{)} \end{array}$$

□

Lemma 100. For any L_1, L_2 with *consistent*(L_1), *consistent*(L_2), let $L := L_1 \circ L_2$. Then for any $G \in \mathrm{GK}(L)$, we have

1. $(\exists e_2.\ (\tau, e_1, e_2) \in \mathbf{E}(\overline{G_{(1)}}^{[L_1]}) \wedge (\tau, e_2, e_3) \in \mathbf{E}(\overline{G_{(2)}}^{[L_2]}))$
   $\Longrightarrow (\tau, e_1, e_3) \in \mathbf{E}(G)$
2. $(\exists K_2.\ (\tau_1, \tau_2, K_1, K_2) \in \mathbf{K}(\overline{G_{(1)}}^{[L_1]}) \wedge (\tau_1, \tau_2, K_2, K_3) \in \mathbf{K}(\overline{G_{(2)}}^{[L_2]}))$
   $\Longrightarrow (\tau_1, \tau_2, K_1, K_3) \in \mathbf{K}(G)$

Proof.

- Let

$$\begin{aligned} \mathbf{E}'(G) &= \{\, (\tau, e_1, e_3) \mid \exists e_2.\ (\tau, e_1, e_2) \in \mathbf{E}(\overline{G_{(1)}}^{[L_1]}) \wedge (\tau, e_2, e_3) \in \mathbf{E}(\overline{G_{(2)}}^{[L_2]}) \,\} \\ \mathbf{K}'(G) &= \{\, (\tau_1, \tau_2, K_1, K_3) \mid \exists K_2.\ (\tau_1, \tau_2, K_1, K_2) \in \mathbf{K}(\overline{G_{(1)}}^{[L_1]}) \wedge \\ &\qquad (\tau_1, \tau_2, K_2, K_3) \in \mathbf{K}(\overline{G_{(2)}}^{[L_2]}) \,\} \end{aligned}$$

- Now it suffices to show that $\mathbf{E}', \mathbf{K}'$ forms a post-fixpoint.
- From $(\tau, e_1, e_2) \in \mathbf{E}(\overline{G_{(1)}}^{[L_1]})$ and $\overline{G_{(1)}}^{[L_1]} = L_1(\overline{G_{(1)}}^{[L_1]}) \cup G_{(1)}$, by Lemma 73, we have three cases.
- When $e_1 \uparrow$ and $e_2 \uparrow$:
  From $(\tau, e_2, e_3) \in \mathbf{E}(\overline{G_{(2)}}^{[L_2]})$ and $\overline{G_{(2)}}^{[L_2]} = L_2(\overline{G_{(2)}}^{[L_2]}) \cup G_{(2)}$, by Lemma 73, we have three cases.
  - When $e_2 \uparrow$ and $e_3 \uparrow$:
    We are done because $e_1 \uparrow$ and $e_3 \uparrow$.
  - When $e_2 \hookrightarrow^* v_2 \wedge e_3 \hookrightarrow^* v_3$ with $(\tau, v_2, v_3) \in \overline{G_{(2)}}^{[L_2]}$:
    It is a contradiction.
  - When $e_2 \hookrightarrow^* K_2[e_2'] \wedge e_3 \hookrightarrow^* K_3[e_3']$ with
    – $(\tau', e_2', e_3') \in \mathbf{S}(G_{(2)}, \overline{G_{(2)}}^{[L_2]})$ and
    – $(\tau', \tau, K_2, K_3) \in \mathbf{K}(\overline{G_{(2)}}^{[L_2]})$:
    Since $e_2' = \mathbf{I}(\widetilde{\tau}, \tau', f_1, f_3)\ v_2$ for some $\widetilde{\tau}, f_1, f_3, v_2$, we know e_2' and thus e_2 gets stuck. Contradiction.

- When $e_1 \hookrightarrow^* v_1 \wedge e_2 \hookrightarrow^* v_2$ with $(\tau, v_1, v_2) \in \overline{G_{(1)}{}^{[L_1]}}$:
  From $(\tau, e_2, e_3) \in \mathbf{E}(G_{(2)}{}^{[L_2]})$ and $G_{(2)}{}^{[L_2]} = L_2(G_{(2)}{}^{[L_2]}) \cup G_{(2)}$, by Lemma 73, we have three cases.

  - When $e_2 \uparrow$ and $e_3 \uparrow$:
    It is a contradiction.
  - When $e_2 \hookrightarrow^* v_2' \wedge e_3 \hookrightarrow^* v_3$ with $(\tau, v_2', v_3) \in \overline{G_{(2)}{}^{[L_2]}}$:
    We are done because we have $v_2 = v_2'$ and thus $(\tau, v_1, v_3) \in \overline{G}$ by Lemmas 98 and 99 since $(\tau, v_1, v_2) \in \overline{G_{(1)}{}^{[L_1]}}$ and $(\tau, v_2, v_3) \in \overline{G_{(2)}{}^{[L_2]}}$.
  - When $e_2 \hookrightarrow^* K_2[e_2'] \wedge e_3 \hookrightarrow^* K_3[e_3']$ with
    – $(\tau', e_2', e_3') \in \mathbf{S}(G_{(2)}, G_{(2)}{}^{[L_2]})$ and
    – $(\tau', \tau, K_2, K_3) \in \mathbf{K}(G_{(2)}{}^{[L_2]})$:
    Since $e_2' = \mathbf{I}(\widetilde{\tau}, \tau', f_1, f_3)\ v_2$ for some $\widetilde{\tau}, f_1, f_3, v_2$, we know e_2' and thus e_2 gets stuck. Contradiction.

- When $e_1 \hookrightarrow^* K_1[e_1'] \wedge e_2 \hookrightarrow^n K_2[e_2']$ with
  – $(\tau', e_1', e_2') \in \mathbf{S}(G_{(1)}, G_{(1)}{}^{[L_1]})$ and
  – $(\tau', \tau, K_1, K_2) \in \mathbf{K}(G_{(1)}{}^{[L_1]})$:
  From $(\tau, e_2, e_3) \in \mathbf{E}(G_{(2)}{}^{[L_2]})$ and $G_{(2)}{}^{[L_2]} = L_2(G_{(2)}{}^{[L_2]}) \cup G_{(2)}$, by Lemma 73, we have three cases.

  - When $e_2 \uparrow$ and $e_3 \uparrow$:
    Since $e_2' = \mathbf{I}(\widetilde{\tau}, \tau', f_1, f_3)\ v_2$ for some $\widetilde{\tau}, f_1, f_3, v_2$, we know e_2' and thus e_2 gets stuck. Contradiction.
  - When $e_2 \hookrightarrow^* v_2 \wedge e_3 \hookrightarrow^* v_3$ with $(\tau, v_2, v_3) \in \overline{G_{(2)}{}^{[L_2]}}$:
    Since $e_2' = \mathbf{I}(\widetilde{\tau}, \tau', f_1, f_3)\ v_2$ for some $\widetilde{\tau}, f_1, f_3, v_2$, we know e_2' and thus e_2 gets stuck. Contradiction.
  - When $e_2 \hookrightarrow^m K_2'[e_2''] \wedge e_3 \hookrightarrow^* K_3[e_3']$ with
    – $(\tau'', e_2'', e_3') \in \mathbf{S}(G_{(2)}, G_{(2)}{}^{[L_2]})$ and
    – $(\tau'', \tau, K_2, K_3) \in \mathbf{K}(G_{(2)}{}^{[L_2]})$:
    By definition of $\mathbf{S}$ and $G_{(1)}$, we have for some $\widetilde{\tau}, f_1, f_3, v_1, v_2$,
    – $e_1' = f_1\ v_1$;
    – $e_2' = \mathbf{I}(\widetilde{\tau}, \tau', f_1, f_3)\ v_2$;
    – $(\widetilde{\tau} \to \tau', f_1, f_3) \in G$;
    – $(\widetilde{\tau}, v_1, v_2) \in \overline{G_{(1)}{}^{[L_1]}}$;
    By definition of $\mathbf{S}$ and $G_{(2)}$, we have for some $\widetilde{\tau}', f_1', f_3', v_2', v_3$,
    – $e_2'' = \mathbf{I}(\widetilde{\tau}', \tau'', f_1', f_3')\ v_2'$;
    – $e_3' = f_3'\ v_3$;
    – $(\widetilde{\tau}' \to \tau'', f_1', f_3') \in G$;
    – $(\widetilde{\tau}', v_2', v_3) \in \overline{G_{(2)}{}^{[L_2]}}$.
    Since both e_2' and e_2'' get stuck, we have $n = m$ and thus
    – $K_2 = K_2'$;
    – $\mathbf{I}(\widetilde{\tau}, \tau', f_1, f_3) = \mathbf{I}(\widetilde{\tau}', \tau'', f_1', f_3')$;
    – $v_2 = v_2'$.
    Since $\mathbf{I}$ is injective, we have
    – $\widetilde{\tau} = \widetilde{\tau}'$;
    – $\tau' = \tau''$;
    – $f_1 = f_1'$;
    – $f_3 = f_3'$.
    Thus we have
    – $e_1' = f_1\ v_1$;

– $e'_3 = f_3\ v_3$;
– $(f_1, f_3) \in G(\widetilde{\tau} \to \tau') = \overline{G}(\widetilde{\tau} \to \tau')$;
– $(v_1, v_3) \in \overline{G}(\widetilde{\tau})$ by Lemmas 98 and 99 since $(\widetilde{\tau}, v_1, v_2) \in \overline{{G_{(1)}}^{[L_1]}}$, $(\widetilde{\tau}, v_2, v_3) \in \overline{{G_{(2)}}^{[L_2]}}$.
Thus it remains to show that $(\tau', \tau, K_1, K_3) \in \mathbf{K}'(G)$. By definition of $\mathbf{K}'$, this follows from
– $(\tau', \tau, K_1, K_2) \in \mathbf{K}({G_{(1)}}^{[L_1]})$; and
– $(\tau', \tau, K_2, K_3) \in \mathbf{K}({G_{(2)}}^{[L_2]})$.

- Now we need to show that
$$(\tau_2, K_1[v_1], K_3[v_3]) \in \mathbf{E}'(G)$$
for $(\tau_1, \tau_2, K_1, K_2) \in \mathbf{K}({G_{(1)}}^{[L_1]})$, $(\tau_1, \tau_2, K_2, K_3) \in \mathbf{K}({G_{(2)}}^{[L_2]})$ and $(\tau_1, v_1, v_3) \in \overline{G}$.
- By Lemmas 98 and 99, there exists v_2 such that $(\tau_1, v_1, v_2) \in \overline{{G_{(1)}}^{[L_1]}}$ and $(\tau_1, v_2, v_3) \in \overline{{G_{(2)}}^{[L_2]}}$.
- Thus we have that $(\tau_2, K_1[v_1], K_2[v_2]) \in \mathbf{E}({G_{(1)}}^{[L_1]})$ and $(\tau_2, K_2[v_2], K_3[v_3]) \in \mathbf{E}({G_{(2)}}^{[L_2]})$.
- Thus, by definition of $\mathbf{E}'$, we have $(\tau_2, K_1[v_1], K_3[v_3]) \in \mathbf{E}'(G)$.

□

Theorem 101.
$$\Gamma \vdash e_1 \sim e_2 : \tau \ \wedge\ \Gamma \vdash e_2 \sim e_3 : \tau \implies \Gamma \vdash e_1 \sim e_3 : \tau$$

Proof.
Assume $\Gamma \vdash e_1 \sim_{L_1} e_2 : \tau \ \wedge\ \Gamma \vdash e_2 \sim_{L_2} e_3 : \tau$ and let $L := L_1 \circ L_2$. We show *consistent*(L) as follows.

- Let $G \in \mathrm{GK}(L)$, $(\tau_1 \to \tau_2, f_1, f_3) \in L(G)$, $(v_1, v_3) \in \overline{G}(\tau_1)$.
- Then we need to show $(\tau_2, \mathit{beta}(f_1\ v_1), \mathit{beta}(f_3\ v_3)) \in \mathbf{E}(G)$.
- By definition of L, we have f_2 such that $(\tau_1 \to \tau_2, f_1, f_2) \in L_1({G_{(1)}}^{[L_1]})$ and $(\tau_1 \to \tau_2, f_2, f_3) \in L_2({G_{(2)}}^{[L_2]})$.
- By Lemmas 98 and 99, we have v_2 such that $(\tau_1, v_1, v_2) \in \overline{{G_{(1)}}^{[L_1]}}$ and $(\tau_1, v_2, v_3) \in \overline{{G_{(2)}}^{[L_2]}}$.
- By Lemma 100, it suffices to show
$$(\tau_2, \mathit{beta}(f_1\ v_1), \mathit{beta}(f_2\ v_2)) \in \mathbf{E}({G_{(1)}}^{[L_1]}) \wedge (\tau_2, \mathit{beta}(f_2\ v_2), \mathit{beta}(f_3\ v_3)) \in \mathbf{E}({G_{(2)}}^{[L_2]})$$
which directly follows from the assumptions.

Now we show $\forall G \in \mathrm{GK}(L).\ \forall (\gamma_1, \gamma_3) \in \mathrm{Env}(\Gamma, G).\ (\tau, \gamma_1 e_1, \gamma_3 e_3) \in \mathbf{E}(G)$.

- Let $G \in \mathrm{GK}(L)$ and $(\gamma_1, \gamma_3) \in \mathrm{Env}(\Gamma, G)$.
- By Lemmas 98 and 99 there exists γ_2 such that
$$(\gamma_1, \gamma_2) \in \mathrm{Env}(\Gamma, {G_{(1)}}^{[L_1]}) \wedge (\gamma_2, \gamma_3) \in \mathrm{Env}(\Gamma, {G_{(2)}}^{[L_2]})\ .$$
- Thus by assumption, we have
$$(\tau, \gamma_1 e_1, \gamma_2 e_2) \in \mathbf{E}({G_{(1)}}^{[L_1]})$$
$$(\tau, \gamma_2 e_2, \gamma_3 e_3) \in \mathbf{E}({G_{(2)}}^{[L_2]})$$
- Thus, by Lemma 100, we have $(\tau, \gamma_1 e_1, \gamma_3 e_3) \in \mathbf{E}(G)$.

□