Typed–Untyped Interactions: A Comparative Analysis (Supplementary Material)

BEN GREENMAN*, PLT @ Brown University, USA
CHRISTOS DIMOULAS, PLT @ Northwestern University, USA
MATTHIAS FELLEISEN, PLT @ Northeastern University, USA

This document is an appendix to section 6 of our TOPLAS manuscript. It presents the definitions that support the technical results. The proofs use basic syntactic techniques.

ACM Reference Format:
Ben Greenman, Christos Dimoulas, and Matthias Felleisen. 2022. Typed–Untyped Interactions: A Comparative Analysis (Supplementary Material). *ACM Trans. Program. Lang. Syst.* 1, 1 (November 2022), 143 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

Contents

*Research completed at Northeastern University prior to joining Brown

Authors' addresses: Ben Greenman, PLT @ Brown University, Providence, Rhode Island, USA, benjaminlgreenman@gmail.com; Christos Dimoulas, PLT @ Northwestern University, Evanston, Illinois, USA, chrdimo@northwestern.edu; Matthias Felleisen, PLT @ Northeastern University, Boston, Massachusetts, USA, matthias@ccs.neu.edu.

0164-0925/2022/11-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

6 TECHNICAL DEVELOPMENT

6.1 Surface Language, Types, and Ownership

$\boxed{\text{Surface Syntax}}$

$$
\begin{array}{lcl}
e & = & x \mid i \mid n \mid \langle e, e \rangle \mid \lambda x.\, e \mid \lambda(x : \tau).\, e \mid \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\; e\; e \mid \mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\; e \mid \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\; e\; e \mid \\
 & & \mathsf{dyn}\; b\; e \mid \mathsf{stat}\; b\; e \\
\tau & = & \mathsf{Int} \mid \mathsf{Nat} \mid \tau \Rightarrow \tau \mid \tau \times \tau \\
{}^{\tau}/_{\mathcal{U}} & = & \tau \mid \mathcal{U} \\
\Gamma & = & \cdot \mid (x : {}^{\tau}/_{\mathcal{U}}), \Gamma \\
b & = & (\ell \blacktriangleleft \tau \blacktriangleleft \ell) \\
\ell & = & \text{countable set of names} \\
\mathit{unop} & = & \mathsf{fst} \mid \mathsf{snd} \\
\mathit{binop} & = & \mathsf{sum} \mid \mathsf{quotient} \\
i & = & \mathbb{Z} \\
n & = & \mathbb{N}
\end{array}
$$

$\boxed{\Delta : \mathit{unop} \times \tau \longrightarrow \tau}$

$$
\Delta(\mathit{unop}_0, \tau_0) = \begin{cases} \tau_1 & \text{if } \mathit{unop}_0 = \mathsf{fst} \text{ and } \tau_0 = \tau_1 \times \tau_2 \\ \tau_2 & \text{if } \mathit{unop}_0 = \mathsf{snd} \text{ and } \tau_0 = \tau_1 \times \tau_2 \end{cases}
$$

$\boxed{\Delta : \mathit{binop} \times \tau \times \tau \longrightarrow \tau}$

$$
\Delta(\mathit{binop}_0, \tau_0, \tau_1) = \begin{cases} \mathsf{Nat} & \text{if } \mathit{binop}_0 = \mathsf{sum} \text{ and } \tau_0 = \mathsf{Nat} \text{ and } \tau_1 = \mathsf{Nat} \\ \mathsf{Nat} & \text{if } \mathit{binop}_0 = \mathsf{quotient} \text{ and } \tau_0 = \mathsf{Nat} \text{ and } \tau_1 = \mathsf{Nat} \\ \mathsf{Int} & \text{if } \mathit{binop}_0 = \mathsf{sum} \text{ and } \tau_0 = \mathsf{Int} \text{ and } \tau_1 = \mathsf{Int} \\ \mathsf{Int} & \text{if } \mathit{binop}_0 = \mathsf{quotient} \text{ and } \tau_0 = \mathsf{Int} \text{ and } \tau_1 = \mathsf{Int} \end{cases}
$$

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

$$\frac{(x_0 : \tau_0) \in \Gamma_0}{\Gamma_0 \vdash x_0 : \tau_0} \qquad \frac{}{\Gamma_0 \vdash n_0 : \mathsf{Nat}} \qquad \frac{}{\Gamma_0 \vdash i_0 : \mathsf{Int}} \qquad \frac{(x_0 : \tau_0), \Gamma_0 \vdash e_0 : \tau_1}{\Gamma_0 \vdash \lambda(x_0 : \tau_0).\, e_0 : \tau_0 \Rightarrow \tau_1}$$

$$\frac{\Gamma_0 \vdash e_0 : \tau_0 \qquad \Gamma_0 \vdash e_1 : \tau_1}{\Gamma_0 \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \qquad \frac{\Gamma_0 \vdash e_0 : \tau_1 \qquad \Delta(\mathit{unop}, \tau_1) \leqslant: \tau_0}{\Gamma_0 \vdash \mathit{unop}\{\tau_0\}\, e_0 : \tau_0}$$

$$\frac{\Gamma_0 \vdash e_0 : \tau_1 \qquad \Gamma_0 \vdash e_1 : \tau_2 \qquad \Delta(\mathit{binop}, \tau_1, \tau_2) \leqslant: \tau_0}{\Gamma_0 \vdash \mathit{binop}\{\tau_0\}\, e_0\, e_1 : \tau_0}$$

$$\frac{\Gamma_0 \vdash e_0 : \tau_1 \Rightarrow \tau_2 \qquad \Gamma_0 \vdash e_1 : \tau_1 \qquad \tau_2 \leqslant: \tau_0}{\Gamma_0 \vdash \mathsf{app}\{\tau_0\}\, e_0\, e_1 : \tau_0} \qquad \frac{\Gamma_0 \vdash e_0 : \mathcal{U}}{\Gamma_0 \vdash \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ e_0 : \tau_0}$$

$$\frac{\Gamma_0 \vdash e_0 : \tau_1 \qquad \tau_1 \leqslant: \tau_0}{\Gamma_0 \vdash e_0 : \tau_0}$$

$\boxed{\Gamma \vdash e : \mathcal{U}}$

$$\frac{(x_0 : \mathcal{U}) \in \Gamma_0}{\Gamma_0 \vdash x_0 : \mathcal{U}} \qquad \frac{}{\Gamma_0 \vdash i_0 : \mathcal{U}} \qquad \frac{(x_0 : \mathcal{U}), \Gamma_0 \vdash e_0 : \mathcal{U}}{\Gamma_0 \vdash \lambda x_0.\, e_0 : \mathcal{U}} \qquad \frac{\Gamma_0 \vdash e_0 : \mathcal{U} \qquad \Gamma_0 \vdash e_1 : \mathcal{U}}{\Gamma_0 \vdash \langle e_0, e_1 \rangle : \mathcal{U}}$$

$$\frac{\Gamma_0 \vdash e_0 : \mathcal{U}}{\Gamma_0 \vdash \mathit{unop}\{\mathcal{U}\}\, e_0 : \mathcal{U}} \qquad \frac{\Gamma_0 \vdash e_0 : \mathcal{U} \qquad \Gamma_0 \vdash e_1 : \mathcal{U}}{\Gamma_0 \vdash \mathit{binop}\{\mathcal{U}\}\, e_0\, e_1 : \mathcal{U}} \qquad \frac{\Gamma_0 \vdash e_0 : \mathcal{U} \qquad \Gamma_0 \vdash e_1 : \mathcal{U}}{\Gamma_0 \vdash \mathsf{app}\{\mathcal{U}\}\, e_0\, e_1 : \mathcal{U}}$$

$$\frac{\Gamma_0 \vdash e_0 : \tau_0}{\Gamma_0 \vdash \mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ e_0 : \mathcal{U}}$$

$\boxed{\tau \leqslant: \tau}$

$$\frac{}{\mathsf{Nat} \leqslant: \mathsf{Int}} \qquad \frac{\tau_0 \leqslant: \tau_2 \qquad \tau_1 \leqslant: \tau_3}{\tau_0 \times \tau_1 \leqslant: \tau_2 \times \tau_3} \qquad \frac{\tau_2 \leqslant: \tau_0 \qquad \tau_1 \leqslant: \tau_3}{\tau_0 \Rightarrow \tau_1 \leqslant: \tau_2 \Rightarrow \tau_3} \qquad \frac{}{\tau_0 \leqslant: \tau_0}$$

$\boxed{b \leqslant: b}$

$$\frac{\tau_0 \leqslant: \tau_1}{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \leqslant: (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)}$$

$\boxed{\text{Ownership Syntax}}$

$$\begin{array}{lcl} e & = & x \mid i \mid n \mid \langle e, e \rangle \mid \lambda x.\, e \mid \lambda(x : \tau).\, e \mid \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, e\; e \mid \mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\, e \mid \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, e\; e \mid \\ & & \mathsf{dyn}\; b\; (e)^{\ell} \mid \mathsf{stat}\; b\; (e)^{\ell} \mid (e)^{\ell} \\ \ell & = & \text{countable set} \\ \mathcal{L} & = & \cdot \mid (x : \ell), \mathcal{L} \end{array}$$

$\boxed{e : {}^{\tau}/_{\mathcal{U}}\ \mathbf{wf}}$

$(e_0)^{\ell_0} : \tau_0\ \mathbf{wf}$ iff $\ell_0 \Vdash (e_0)^{\ell_0}$ and $\vdash (e_0)^{\ell_0} : \tau_0$

$(e_0)^{\ell_0} : \mathcal{U}\ \mathbf{wf}$ iff $\ell_0 \Vdash (e_0)^{\ell_0}$ and $\vdash (e_0)^{\ell_0} : \mathcal{U}$

$\boxed{\Gamma \vdash e : \tau}$ additional rules for the ownership syntax

$$\frac{\Gamma_0 \vdash e_0 : \tau_0}{\Gamma_0 \vdash (e_0)^{\ell_0} : \tau_0} \qquad \frac{\Gamma_0 \vdash e_0 : \mathcal{U}}{\Gamma_0 \vdash \mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; (e_0)^{\ell_0} : \tau_0}$$

$\boxed{\Gamma \vdash e : \mathcal{U}}$ additional rules for the ownership syntax

$$\frac{\Gamma_0 \vdash e_0 : \mathcal{U}}{\Gamma_0 \vdash (e_0)^{\ell_0} : \mathcal{U}} \qquad \frac{\Gamma_0 \vdash e_0 : \tau_0}{\Gamma_0 \vdash \mathsf{stat}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; (e_0)^{\ell_0} : \mathcal{U}}$$

$\boxed{\mathcal{L}; \ell \Vdash e}$

$$\frac{\mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}} \qquad \frac{(x_0 : \ell_0) \in \mathcal{L}_0}{\mathcal{L}_0; \ell_0 \Vdash x_0} \qquad \frac{}{\mathcal{L}_0; \ell_0 \Vdash i_0} \qquad \frac{(x_0 : \ell_0), \mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \lambda x_0.\, e_0}$$

$$\frac{(x_0 : \ell_0), \mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \lambda(x_0 : \tau_0).\, e_0} \qquad \frac{\mathcal{L}_0; \ell_0 \Vdash e_0 \qquad \mathcal{L}_0; \ell_0 \Vdash e_1}{\mathcal{L}_0; \ell_0 \Vdash \langle e_0, e_1 \rangle} \qquad \frac{\mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\, e_0}$$

$$\frac{\mathcal{L}_0; \ell_0 \Vdash e_0 \qquad \mathcal{L}_0; \ell_0 \Vdash e_1}{\mathcal{L}_0; \ell_0 \Vdash \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, e_0\; e_1} \qquad \frac{\mathcal{L}_0; \ell_0 \Vdash e_0 \qquad \mathcal{L}_0; \ell_0 \Vdash e_1}{\mathcal{L}_0; \ell_0 \Vdash \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, e_0\; e_1} \qquad \frac{\mathcal{L}_0; \ell_1 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; e_0}$$

$$\frac{\mathcal{L}_0; \ell_1 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \mathsf{stat}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; e_0}$$

6.2 Three Evaluation Languages

$\boxed{\text{Common Evaluation Syntax}}$

$$
\begin{array}{lcl}
v & = & i \mid n \mid \langle v, v\rangle \mid \lambda x.\, e \mid \lambda(x:\tau).\, e \mid \mathbb{G}\, b\, v \mid \mathbb{T}\, \overline{b}\, v \\
\mathsf{Err} & = & \mathsf{InvariantErr} \mid \mathsf{TagErr} \mid \mathsf{BoundaryErr}\,(B, v) \mid \mathsf{DivErr} \\
B & = & b \mid \overline{b} \mid b^{*} \\
\overline{b} & = & \text{ordered sequence of boundaries } (b) \\
b^{*} & = & \text{set of boundaries } (b) \\
s & = & \mathsf{Int} \mid \mathsf{Nat} \mid \mathsf{Pair} \mid \mathsf{Fun} \\
E & = & [\,] \mid \mathsf{app}\{^{\tau}/_{\mathcal{U}}\}\, E\, e \mid \mathsf{app}\{^{\tau}/_{\mathcal{U}}\}\, v\, E \mid \langle E, e\rangle \mid \langle v, E\rangle \mid \mathit{unop}\{^{\tau}/_{\mathcal{U}}\}\, E \mid \mathit{binop}\{^{\tau}/_{\mathcal{U}}\}\, E\, v \mid \\
 & & \mathit{binop}\{^{\tau}/_{\mathcal{U}}\}\, v\, E \mid \mathsf{dyn}\, b\, E \mid \mathsf{stat}\, b\, E \mid \mathbb{T}\, \overline{b}\, E
\end{array}
$$

$\boxed{\lfloor\cdot\rfloor : \tau \longrightarrow s}$

$$
\lfloor \tau_0 \rfloor = \begin{cases}
\mathsf{Nat} & \text{if } \tau_0 = \mathsf{Nat} \\
\mathsf{Int} & \text{if } \tau_0 = \mathsf{Int} \\
\mathsf{Pair} & \text{if } \tau_0 \in \tau\times\tau \\
\mathsf{Fun} & \text{if } \tau_0 \in \tau \Rightarrow \tau
\end{cases}
$$

$\boxed{\mathit{shape\text{-}match} : s \times v \longrightarrow \mathcal{B}}$

$$
\mathit{shape\text{-}match}\,(s_0, v_0) = \begin{cases}
\mathsf{True} \\
\quad \text{if } \ s_0 = \mathsf{Nat} \text{ and } v_0 \in n \\
\quad \text{or } s_0 = \mathsf{Int} \text{ and } v_0 \in i \\
\quad \text{or } s_0 = \mathsf{Pair} \text{ and } v_0 \in \langle v, v\rangle \cup (\mathbb{G}\,(\ell \blacktriangleleft (\tau\times\tau) \blacktriangleleft \ell)\, v) \\
\quad \text{or } s_0 = \mathsf{Fun} \text{ and } v_0 \in (\lambda x.\, e) \cup (\lambda(x:\tau).\, e) \cup (\mathbb{G}\,(\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell)\, v) \\
\mathit{shape\text{-}match}\,(s_0, v_1) \\
\quad \text{if } \ v_0 = \mathbb{T}\, \overline{b}_0\, v_1 \\
\mathsf{False} \\
\quad \text{otherwise}
\end{cases}
$$

$\boxed{\delta : \mathit{unop} \times v \longrightarrow v}$

$$
\delta(\mathit{unop}, \langle v_0, v_1\rangle) = \begin{cases}
v_0 & \text{if } \mathit{unop} = \mathsf{fst}\{^{\tau}/_{\mathcal{U}}\} \\
v_1 & \text{if } \mathit{unop} = \mathsf{snd}\{^{\tau}/_{\mathcal{U}}\}
\end{cases}
$$

$\boxed{\delta : \mathit{binop} \times v \times v \longrightarrow v}$

$$
\delta(\mathit{binop}, i_0, i_1) = \begin{cases}
i_0 + i_1 \\
\quad \text{if } \mathit{binop} = \mathsf{sum}\{^{\tau}/_{\mathcal{U}}\} \\
\mathsf{DivErr} \\
\quad \text{if } \mathit{binop} = \mathsf{quotient}\{^{\tau}/_{\mathcal{U}}\} \text{ and } i_1 = 0 \\
\lfloor i_0 / i_1 \rfloor \\
\quad \text{if } \mathit{binop} = \mathsf{quotient}\{^{\tau}/_{\mathcal{U}}\} \text{ and } i_1 \neq 0
\end{cases}
$$

$\boxed{\mathsf{fst} : \tau\times\tau \longrightarrow \tau}$

$\mathsf{fst}\,(\tau_0\times\tau_1) = \tau_0$

$\boxed{\mathsf{snd} : \tau\times\tau \longrightarrow \tau}$

$\mathsf{snd}\,(\tau_0\times\tau_1) = \tau_1$

$\boxed{\mathsf{dom} : \tau\Rightarrow\tau \longrightarrow \tau}$

$\mathsf{dom}\,(\tau_0\Rightarrow\tau_1) = \tau_0$

$\boxed{\mathsf{cod} : \tau\Rightarrow\tau \longrightarrow \tau}$

$\mathsf{cod}\,(\tau_0\Rightarrow\tau_1) = \tau_1$

Lemma 6.1 (unique decomposition). *For all e_0 one of the following holds:*

- $e_0 \in x \cup v$
- $e_0 = E_0[\mathsf{Err}]$
- $e_0 = E_0[\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, v_0\, v_1]$
- $e_0 = E_0[\mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\, v_0]$
- $e_0 = E_0[\mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, v_0\, v_1]$
- $e_0 = E_0[\mathsf{dyn}\ b_0\ v_0]$
- $e_0 = E_0[\mathsf{stat}\ b_0\ v_0]$

Proof Sketch. By induction on the structure of e_0. □

Lemma 6.2 (δ compatibility).

- *If* $\Delta(\mathit{unop}_0, \tau_0) = \tau_1$ *and* $\vdash v_0 : \tau_0$ *and* $\delta(\mathit{unop}_0, v_0) = v_1$ *then* $\vdash v_1 : \tau_1$.
- *If* $\Delta(\mathit{binop}_0, \tau_0, \tau_1) = \tau_2$ *and* $\vdash v_0 : \tau_0$ *and* $\vdash v_1 : \tau_1$ *and* $\delta(\mathit{binop}_0, v_0, v_1) = v_2$ *then* $\vdash v_2 : \tau_2$.

Proof Sketch. By case analysis of δ. □

$\boxed{\text{Ownership Evaluation Syntax}}$

$$\begin{array}{rcl} v & = & i \mid n \mid \langle v, v\rangle \mid \lambda x.\, e \mid \lambda(x:\tau).\, e \mid \mathbb{G}\, b\, v \mid \mathbb{T}\, \overline{b}\, v \mid (v)^{\ell} \\ E & = & [\,] \mid \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, E\, e \mid \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, v\, E \mid \langle E, e\rangle \mid \langle v, E\rangle \mid \mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\, E \mid \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, E\, v \mid \\ & & \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, v\, E \mid \mathsf{dyn}\ b\ E \mid \mathsf{stat}\ b\ E \mid (E)^{\ell} \end{array}$$

$\boxed{\mathit{rev} : B \longrightarrow B}$

$$\mathit{rev}(B_0) = \begin{cases} (\ell_1 \blacktriangleleft \tau_0 \blacktriangleleft \ell_0) & \text{if } B_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \\ \mathit{rev}(b_n) \cdots \mathit{rev}(b_0) & \text{if } B_0 = b_0 \cdots b_n \\ \{\mathit{rev}(b_0) \mid b_0 \in b_0^*\} & \text{if } B_0 = b_0^* \end{cases}$$

$\boxed{\mathit{rev} : \overline{\ell} \longrightarrow \overline{\ell}}$

$$\mathit{rev}(\ell_0 \cdots \ell_n) = \ell_n \cdots \ell_0$$

$\boxed{\mathit{senders} : B \longrightarrow L}$

$$\mathit{senders}(B_0) = \begin{cases} \ell_1 & \text{if } B_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \\ \mathit{senders}(b_0) \cdots \mathit{senders}(b_n) & \text{if } B_0 = b_0 \cdots b_n \\ \{\mathit{senders}(b_0) \mid b_0 \in b_0^*\} & \text{if } B_0 = b_0^* \end{cases}$$

$\boxed{\mathit{owners} : v \longrightarrow \overline{\ell}}$

$$\mathit{owners}(v_0) = \begin{cases} \ell_0\, \mathit{owners}(v_1) & \text{if } v_0 = (v_1)^{\ell_0} \\ \mathit{owners}(v_1) & \text{if } v_0 = \mathbb{T}\, \overline{b}_0\, v_1 \\ \cdot & \text{otherwise} \end{cases}$$

$$(\!(e_0)\!)^{\ell_n \cdots \ell_1} = e_1 \quad \Longleftrightarrow \quad e_1 = (\cdots (e_0)^{\ell_n} \cdots)^{\ell_1}$$

6.2.1 *Higher-Order Language, Path-Based Ownership Consistency.*

$\boxed{\text{Higher-Order Evaluation Syntax}}$

$$
\begin{array}{lcl}
e & = & x \mid i \mid n \mid \langle e, e\rangle \mid \lambda x.\, e \mid \lambda(x:\tau).\, e \mid \mathsf{app}\{{}^{\tau}\!/_{\mathcal{U}}\}\; e\; e \mid \mathit{unop}\{{}^{\tau}\!/_{\mathcal{U}}\}\; e \mid \mathit{binop}\{{}^{\tau}\!/_{\mathcal{U}}\}\; e\; e \mid \\
 & & \mathsf{dyn}\; b\; e \mid \mathsf{stat}\; b\; e \mid \mathsf{trace}\; \overline{b}\; e \mid \mathsf{Err} \\
v & = & i \mid n \mid \langle v, v\rangle \mid \lambda x.\, e \mid \lambda(x:\tau).\, e \mid \mathbb{G}\,(\ell \blacktriangleleft \tau \Rightarrow \tau \blacktriangleleft \ell)\; v \mid \mathbb{G}\,(\ell \blacktriangleleft \tau \times \tau \blacktriangleleft \ell)\; v \mid \mathbb{T}\; \overline{b}\; v \\
\mathsf{Err} & = & \mathsf{InvariantErr} \mid \mathsf{TagErr} \mid \mathsf{BoundaryErr}\,(\overline{b}, v) \mid \mathsf{DivErr}
\end{array}
$$

$\boxed{\Gamma \vdash_1 e : \tau}$

$$
\frac{(x_0 : \tau_0) \in \Gamma_0}{\Gamma_0 \vdash_1 x_0 : \tau_0}
\qquad
\frac{}{\Gamma_0 \vdash_1 n_0 : \mathsf{Nat}}
\qquad
\frac{}{\Gamma_0 \vdash_1 i_0 : \mathsf{Int}}
\qquad
\frac{(x_0 : \tau_0), \Gamma_0 \vdash_1 e_0 : \tau_1}{\Gamma_0 \vdash_1 \lambda(x_0 : \tau_0).\, e_0 : \tau_0 \Rightarrow \tau_1}
$$

$$
\frac{\Gamma_0 \vdash_1 e_0 : \tau_0 \qquad \Gamma_0 \vdash_1 e_1 : \tau_1}{\Gamma_0 \vdash_1 \langle e_0, e_1\rangle : \tau_0 \times \tau_1}
\qquad
\frac{\Gamma_0 \vdash_1 e_0 : \tau_1 \qquad \Delta(\mathit{unop}, \tau_1) \leqslant: \tau_0}{\Gamma_0 \vdash_1 \mathit{unop}\{\tau_0\}\; e_0 : \tau_0}
$$

$$
\frac{\Gamma_0 \vdash_1 e_0 : \tau_1 \qquad \Gamma_0 \vdash_1 e_1 : \tau_2 \qquad \Delta(\mathit{binop}, \tau_1, \tau_2) \leqslant: \tau_0}{\Gamma_0 \vdash_1 \mathit{binop}\{\tau_0\}\; e_0\; e_1 : \tau_0}
$$

$$
\frac{\Gamma_0 \vdash_1 e_0 : \tau_1 \Rightarrow \tau_2 \qquad \Gamma_0 \vdash_1 e_1 : \tau_1 \qquad \tau_2 \leqslant: \tau_0}{\Gamma_0 \vdash_1 \mathsf{app}\{\tau_0\}\; e_0\; e_1 : \tau_0}
\qquad
\frac{\Gamma_0 \vdash_1 e_0 : \mathcal{U}}{\Gamma_0 \vdash_1 \mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; e_0 : \tau_0}
$$

$$
\frac{\Gamma_0 \vdash_1 e_0 : \tau_1 \qquad \tau_1 \leqslant: \tau_0}{\Gamma_0 \vdash_1 e_0 : \tau_0}
\qquad
\frac{\Gamma_0 \vdash_1 v_0 : \mathcal{U}}{\Gamma_0 \vdash_1 \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 : \tau_0}
\qquad
\frac{}{\Gamma_0 \vdash_1 \mathsf{Err} : \tau_0}
$$

$\boxed{\Gamma \vdash_1 e : \mathcal{U}}$

$$
\frac{(x_0 : \mathcal{U}) \in \Gamma_0}{\Gamma_0 \vdash_1 x_0 : \mathcal{U}}
\qquad
\frac{}{\Gamma_0 \vdash_1 i_0 : \mathcal{U}}
\qquad
\frac{(x_0 : \mathcal{U}), \Gamma_0 \vdash_1 e_0 : \mathcal{U}}{\Gamma_0 \vdash_1 \lambda x_0.\, e_0 : \mathcal{U}}
\qquad
\frac{\Gamma_0 \vdash_1 e_0 : \mathcal{U} \qquad \Gamma_0 \vdash_1 e_1 : \mathcal{U}}{\Gamma_0 \vdash_1 \langle e_0, e_1\rangle : \mathcal{U}}
$$

$$
\frac{\Gamma_0 \vdash_1 e_0 : \mathcal{U}}{\Gamma_0 \vdash_1 \mathit{unop}\{\mathcal{U}\}\; e_0 : \mathcal{U}}
\qquad
\frac{\Gamma_0 \vdash_1 e_0 : \mathcal{U} \qquad \Gamma_0 \vdash_1 e_1 : \mathcal{U}}{\Gamma_0 \vdash_1 \mathit{binop}\{\mathcal{U}\}\; e_0\; e_1 : \mathcal{U}}
\qquad
\frac{\Gamma_0 \vdash_1 e_0 : \mathcal{U} \qquad \Gamma_0 \vdash_1 e_1 : \mathcal{U}}{\Gamma_0 \vdash_1 \mathsf{app}\{\mathcal{U}\}\; e_0\; e_1 : \mathcal{U}}
$$

$$
\frac{\Gamma_0 \vdash_1 e_0 : \tau_0}{\Gamma_0 \vdash_1 \mathsf{stat}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; e_0 : \mathcal{U}}
\qquad
\frac{\Gamma_0 \vdash_1 v_0 : \tau_0}{\Gamma_0 \vdash_1 \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 : \mathcal{U}}
\qquad
\frac{\Gamma_0 \vdash_1 v_0 : \mathcal{U}}{\Gamma_0 \vdash_1 \mathbb{T}\; \overline{b_0}\; v_0 : \mathcal{U}}
$$

$$
\frac{\Gamma_0 \vdash_1 e_0 : \mathcal{U}}{\Gamma_0 \vdash_1 \mathsf{trace}\; \overline{b_0}\; e_0 : \mathcal{U}}
\qquad
\frac{}{\Gamma_0 \vdash_1 \mathsf{Err} : \mathcal{U}}
$$

$\boxed{\text{Higher-Order Evaluation Syntax, with Ownership}}$

$$
\begin{array}{lcl}
e & = & x \mid i \mid n \mid \langle e, e\rangle \mid \lambda x.\, e \mid \lambda(x : \tau).\, e \mid \mathsf{app}\{^{\tau}/_{\mathcal{U}}\}\, e\, e \mid \mathit{unop}\{^{\tau}/_{\mathcal{U}}\}\, e \mid \mathit{binop}\{^{\tau}/_{\mathcal{U}}\}\, e\, e \mid \\
& & \mathsf{dyn}\; b\; (e)^{\ell} \mid \mathsf{stat}\; b\; (e)^{\ell} \mid \mathsf{trace}\, \overline{b}\, e \mid (e)^{\ell} \mid \mathsf{Err} \\
v & = & i \mid n \mid \langle v, v\rangle \mid \lambda x.\, e \mid \lambda(x : \tau).\, e \mid \mathbb{G}\; b\; (v)^{\ell} \mid \mathbb{T}\, \overline{b}\, v \mid (v)^{\ell}
\end{array}
$$

$\boxed{\mathcal{L}; \ell \Vdash e}$

$$
\frac{\mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}}
\qquad
\frac{(x_0 : \ell_0) \in \mathcal{L}_0}{\mathcal{L}_0; \ell_0 \Vdash x_0}
\qquad
\frac{}{\mathcal{L}_0; \ell_0 \Vdash i_0}
\qquad
\frac{(x_0 : \ell_0), \mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \lambda x_0.\, e_0}
$$

$$
\frac{(x_0 : \ell_0), \mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \lambda(x_0 : \tau_0).\, e_0}
\qquad
\frac{\mathcal{L}_0; \ell_0 \Vdash e_0 \qquad \mathcal{L}_0; \ell_0 \Vdash e_1}{\mathcal{L}_0; \ell_0 \Vdash \langle e_0, e_1\rangle}
\qquad
\frac{\mathcal{L}_0; \ell_1 \Vdash v_0}{\mathcal{L}_0; \ell_0 \Vdash \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0}
$$

$$
\frac{\mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \mathit{unop}\{^{\tau}/_{\mathcal{U}}\}\, e_0}
\qquad
\frac{\mathcal{L}_0; \ell_0 \Vdash e_0 \qquad \mathcal{L}_0; \ell_0 \Vdash e_1}{\mathcal{L}_0; \ell_0 \Vdash \mathit{binop}\{^{\tau}/_{\mathcal{U}}\}\, e_0\, e_1}
\qquad
\frac{\mathcal{L}_0; \ell_0 \Vdash e_0 \qquad \mathcal{L}_0; \ell_0 \Vdash e_1}{\mathcal{L}_0; \ell_0 \Vdash \mathsf{app}\{^{\tau}/_{\mathcal{U}}\}\, e_0\, e_1}
$$

$$
\frac{\mathcal{L}_0; \ell_1 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, e_0}
\qquad
\frac{\mathcal{L}_0; \ell_1 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, e_0}
\qquad
\frac{\mathcal{L}_0; \ell_0 \Vdash v_0}{\mathcal{L}_0; \ell_0 \Vdash \mathbb{T}\, \overline{b}_0\, v_0}
$$

$$
\frac{\mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \mathsf{trace}\, \overline{b}_0\, e_0}
\qquad
\frac{}{\mathcal{L}_0; \ell_0 \Vdash \mathsf{Err}}
$$

$\boxed{\mathcal{L}; \ell \Vdash_p e}$

$$
\frac{\mathcal{L}_0; \ell_0 \Vdash_p e_0}{\mathcal{L}_0; \ell_0 \Vdash_p (e_0)^{\ell_0}}
\qquad
\frac{(x_0 : \ell_0) \in \mathcal{L}_0}{\mathcal{L}_0; \ell_0 \Vdash_p x_0}
\qquad
\frac{}{\mathcal{L}_0; \ell_0 \Vdash_p i_0}
\qquad
\frac{(x_0 : \ell_0), \mathcal{L}_0; \ell_0 \Vdash_p e_0}{\mathcal{L}_0; \ell_0 \Vdash_p \lambda x_0.\, e_0}
$$

$$
\frac{(x_0 : \ell_0), \mathcal{L}_0; \ell_0 \Vdash_p e_0}{\mathcal{L}_0; \ell_0 \Vdash_p \lambda(x_0 : \tau_0).\, e_0}
\qquad
\frac{\mathcal{L}_0; \ell_0 \Vdash_p e_0 \qquad \mathcal{L}_0; \ell_0 \Vdash_p e_1}{\mathcal{L}_0; \ell_0 \Vdash_p \langle e_0, e_1\rangle}
\qquad
\frac{\mathcal{L}_0; \ell_1 \Vdash_p v_0}{\mathcal{L}_0; \ell_0 \Vdash_p \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (v_0)^{\ell_1}}
$$

$$
\frac{\mathcal{L}_0; \ell_0 \Vdash_p e_0}{\mathcal{L}_0; \ell_0 \Vdash_p \mathit{unop}\{^{\tau}/_{\mathcal{U}}\}\, e_0}
\qquad
\frac{\mathcal{L}_0; \ell_0 \Vdash_p e_0 \qquad \mathcal{L}_0; \ell_0 \Vdash_p e_1}{\mathcal{L}_0; \ell_0 \Vdash_p \mathit{binop}\{^{\tau}/_{\mathcal{U}}\}\, e_0\, e_1}
\qquad
\frac{\mathcal{L}_0; \ell_0 \Vdash_p e_0 \qquad \mathcal{L}_0; \ell_0 \Vdash_p e_1}{\mathcal{L}_0; \ell_0 \Vdash_p \mathsf{app}\{^{\tau}/_{\mathcal{U}}\}\, e_0\, e_1}
$$

$$
\frac{\mathcal{L}_0; \ell_1 \Vdash_p e_0}{\mathcal{L}_0; \ell_0 \Vdash_p \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (e_0)^{\ell_1}}
\qquad
\frac{\mathcal{L}_0; \ell_1 \Vdash_p e_0}{\mathcal{L}_0; \ell_0 \Vdash_p \mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (e_0)^{\ell_1}}
$$

$$
\frac{\overline{b}_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \cdots (\ell_{n-1} \blacktriangleleft \tau_{n-1} \blacktriangleleft \ell_n) \qquad \mathcal{L}_0; \ell_n \Vdash_p v_0}{\mathcal{L}_0; \ell_0 \Vdash_p (\mathbb{T}\, \overline{b}_0\, (\!(v_0)\!)^{\ell_n \cdots \ell_1})^{\ell_0}}
$$

$$
\frac{\overline{b}_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \cdots (\ell_{n-1} \blacktriangleleft \tau_{n-1} \blacktriangleleft \ell_n) \qquad \mathcal{L}_0; \ell_n \Vdash_p e_0}{\mathcal{L}_0; \ell_0 \Vdash_p (\mathsf{trace}\, \overline{b}_0\, (\!(e_0)\!)^{\ell_n \cdots \ell_1})^{\ell_0}}
\qquad
\frac{}{\mathcal{L}_0; \ell_0 \Vdash_p \mathsf{Err}}
$$

LEMMA 6.3 (HIGHER-ORDER INITIALIZATION).

- *If* $(e_0)^{\ell_0} : \tau_0$ **wf** *then* $\cdot \vdash_1 (e_0)^{\ell_0} : \tau_0$ *and* $\cdot; \ell_0 \Vdash (e_0)^{\ell_0}$ *and* $\cdot; \ell_0 \Vdash_p (e_0)^{\ell_0}$.
- *If* $(e_0)^{\ell_0} : \mathcal{U}$ **wf** *then* $\cdot \vdash_1 (e_0)^{\ell_0} : \mathcal{U}$ *and* $\cdot; \ell_0 \Vdash (e_0)^{\ell_0}$ *and* $\cdot; \ell_0 \Vdash_p (e_0)^{\ell_0}$.

PROOF SKETCH. By lemma 6.4. □

LEMMA 6.4.

- *If* $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}$ *and* $\Gamma_0 \vdash (e_0)^{\ell_0} : \tau_0$ *then* $\Gamma_0 \vdash_1 (e_0)^{\ell_0} : \tau_0$ *and* $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}$ *and* $\mathcal{L}_0; \ell_0 \Vdash_p (e_0)^{\ell_0}$.
- *If* $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}$ *and* $\Gamma_0 \vdash (e_0)^{\ell_0} : \mathcal{U}$ *then* $\Gamma_0 \vdash_1 (e_0)^{\ell_0} : \mathcal{U}$ *and* $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}$ *and* $\mathcal{L}_0; \ell_0 \Vdash_p (e_0)^{\ell_0}$.

PROOF SKETCH. By induction on the surface typing and surface ownership judgments. □

6.2.2 First-Order Language.

$\boxed{\text{First-Order Evaluation Syntax}}$

$$
\begin{array}{lcl}
e & = & x \mid i \mid n \mid \lambda x.\, e \mid \lambda(x : \tau).\, e \mid \langle e, e\rangle \mid \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, e\, e \mid \mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\, e \mid \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, e\, e \mid \\
 & & \mathsf{dyn}\, b\, e \mid \mathsf{stat}\, b\, e \mid \mathsf{p} \mid \mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\, e\, \mathsf{p} \mid \mathsf{Err} \\
v & = & i \mid n \mid \mathsf{p} \\
\mathsf{w} & = & \lambda x.\, e \mid \lambda(x : \tau).\, e \mid \langle v, v\rangle \\
\mathsf{p} & = & \text{countable set of heap locations} \\
\mathsf{Err} & = & \mathsf{InvariantErr} \mid \mathsf{TagErr} \mid \mathsf{BoundaryErr}\,(b^*, v) \mid \mathsf{DivErr} \\
\mathcal{H} & = & \mathcal{P}((\mathsf{p} \mapsto \mathsf{w})) \\
\mathcal{B} & = & \mathcal{P}((\mathsf{p} \mapsto b^*)) \\
\mathcal{T} & = & \cdot \mid (\mathsf{p} : s), \mathcal{T}
\end{array}
$$

$\boxed{\cdot(\cdot) : \mathcal{H} \times v \longrightarrow \mathsf{w} \cup v}$

$$
\mathcal{H}_0(v_0) = \begin{cases} \mathsf{w}_0 & \text{if } v_0 \in \mathsf{p} \text{ and } (v_0 \mapsto \mathsf{w}_0) \in \mathcal{H}_0 \\ v_0 & \text{if } v_0 \notin \mathsf{p} \end{cases}
$$

$\boxed{\cdot(\cdot) : \mathcal{B} \times v \longrightarrow b^*}$

$$
\mathcal{B}_0(v_0) = \begin{cases} b_0^* & \text{if } v_0 \in \mathsf{p} \text{ and } (v_0 \mapsto b_0^*) \in \mathcal{B}_0 \\ \emptyset & \text{otherwise} \end{cases}
$$

$\boxed{\cdot[\cdot \mapsto \cdot] : \mathcal{B} \times v \times b^* \longrightarrow b^*}$

$$
\mathcal{B}_0[v_0 \mapsto b_0^*] = \begin{cases} \{v_0 \mapsto b_0^*\} \cup (\mathcal{B}_0 \setminus (v_0 \mapsto b_1^*)) & \\ \quad \text{if } v_0 \in \mathsf{p} \text{ and } (v_0 \mapsto b_1^*) \in \mathcal{B}_0 & \\ \mathcal{B}_0 \quad \text{otherwise} & \end{cases}
$$

$\boxed{\cdot[\cdot \cup \cdot] : \mathcal{B} \times v \times b^* \longrightarrow b^*}$

$$
\mathcal{B}_0[v_0 \cup b_0^*] = \mathcal{B}_0[v_0 \mapsto b_0^* \cup \mathcal{B}_0(v_0)]
$$

$\boxed{\mathcal{T}; \Gamma \vdash_{\mathsf{s}} e; \mathcal{H}; \mathcal{B} : s}$

$$
\frac{\mathcal{T}_0; \Gamma_0 \vdash_{\mathsf{s}} e_0 : s_0 \qquad \mathcal{T}_0 \vdash_{\mathsf{s}} \mathcal{H}_0}{\mathcal{T}_0; \Gamma_0 \vdash_{\mathsf{s}} e_0; \mathcal{H}_0; \mathcal{B}_0 : s_0}
$$

$\boxed{\mathcal{T}; \Gamma \vdash_{\mathsf{s}} e; \mathcal{H}; \mathcal{B} : \mathcal{U}}$

$$
\frac{\mathcal{T}_0; \Gamma_0 \vdash_{\mathsf{s}} e_0 : \mathcal{U} \qquad \mathcal{T}_0 \vdash_{\mathsf{s}} \mathcal{H}_0}{\mathcal{T}_0; \Gamma_0 \vdash_{\mathsf{s}} e_0; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}}
$$

$\boxed{\mathcal{T} \vdash_{\mathsf{s}} \mathcal{H}}$

$$
\frac{\forall\, (\mathsf{p}_0 \mapsto v_0) \in \mathcal{H}_0.\ \forall\, (\mathsf{p}_0 \mapsto s_0) \in \mathcal{T}_0.\ \mathcal{T}_0; \cdot \vdash_{\mathsf{s}} v_0 : s_0}{\mathcal{T}_0 \vdash_{\mathsf{s}} \mathcal{H}_0}
$$

$\boxed{\mathcal{T};\Gamma \vdash_{\mathsf{s}} e : s}$

$$\frac{(\mathsf{p}_0 : s_0) \in \mathcal{T}_0}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathsf{p}_0 : s_0} \qquad \frac{(x_0 : \tau_0) \in \Gamma_0}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} x_0 : \lfloor \tau_0 \rfloor} \qquad \frac{}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} i_0 : \mathsf{Int}} \qquad \frac{}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} n_0 : \mathsf{Nat}}$$

$$\frac{\mathcal{T}_0;(x_0 : \mathcal{U}),\Gamma_0 \vdash_{\mathsf{s}} e_0 : \mathcal{U}}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \lambda x_0.\, e_0 : \mathsf{Fun}} \qquad \frac{\mathcal{T}_0;(x_0 : \tau_0),\Gamma_0 \vdash_{\mathsf{s}} e_0 : s_0}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \lambda(x_0 : \tau_0).\, e_0 : \mathsf{Fun}} \qquad \frac{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : s_0 \qquad \mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_1 : s_1}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \langle e_0, e_1 \rangle : \mathsf{Pair}}$$

$$\frac{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : \mathsf{Fun} \qquad \mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_1 : s_0}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathsf{app}\{\tau_0\}\, e_0\, e_1 : \lfloor \tau_0 \rfloor} \qquad \frac{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : \mathsf{Pair}}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathit{unop}\{\tau_0\}\, e_0 : \lfloor \tau_0 \rfloor}$$

$$\frac{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : s_0 \qquad \mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : s_1 \qquad \Delta(\mathit{binop}, s_0, s_1) = \tau_1 \qquad \tau_1 \leqslant: \tau_0}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathit{binop}\{\tau_0\}\, e_0\, e_1 : \lfloor \tau_0 \rfloor}$$

$$\frac{\mathcal{T}_0;\Gamma_0 \vdash e_0 : \mathcal{U}}{\mathcal{T}_0;\Gamma_0 \vdash \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ e_0 : \lfloor \tau_0 \rfloor} \qquad \frac{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : \mathcal{U}}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathsf{check}\{\tau_0\}\, e_0\, \mathsf{p}_0 : \lfloor \tau_0 \rfloor}$$

$$\frac{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : s_0}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathsf{check}\{\tau_0\}\, e_0\, \mathsf{p}_0 : \lfloor \tau_0 \rfloor} \qquad \frac{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : s_1 \qquad s_1 \leqslant: s_0}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : s_0} \qquad \frac{}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathsf{Err} : s_0}$$

$\boxed{\mathcal{T};\Gamma \vdash_{\mathsf{s}} e : \mathcal{U}}$

$$\frac{(\mathsf{p}_0 : s_0) \in \mathcal{T}_0}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathsf{p}_0 : \mathcal{U}} \qquad \frac{(x_0 : \mathcal{U}) \in \Gamma_0}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} x_0 : \mathcal{U}} \qquad \frac{}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} i_0 : \mathcal{U}} \qquad \frac{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : \mathcal{U} \qquad \mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_1 : \mathcal{U}}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \langle e_0, e_1 \rangle : \mathcal{U}}$$

$$\frac{\mathcal{T}_0;(x_0 : \mathcal{U}),\Gamma_0 \vdash_{\mathsf{s}} e_0 : \mathcal{U}}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \lambda x_0.\, e_0 : \mathcal{U}} \qquad \frac{\mathcal{T}_0;(x_0 : \tau_0),\Gamma_0 \vdash_{\mathsf{s}} e_0 : s_0}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \lambda(x_0 : \tau_0).\, e_0 : \mathcal{U}} \qquad \frac{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : \mathcal{U} \qquad \mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_1 : \mathcal{U}}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathsf{app}\{\mathcal{U}\}\, e_0\, e_1 : \mathcal{U}}$$

$$\frac{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : \mathcal{U}}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathit{unop}\{\mathcal{U}\}\, e_0 : \mathcal{U}} \qquad \frac{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : \mathcal{U} \qquad \mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_1 : \mathcal{U}}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathit{binop}\{\mathcal{U}\}\, e_0\, e_1 : \mathcal{U}}$$

$$\frac{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : \lfloor \tau_0 \rfloor}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ e_0 : \mathcal{U}} \qquad \frac{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : \mathcal{U}}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathsf{check}\{\mathcal{U}\}\, e_0\, \mathsf{p}_0 : \mathcal{U}}$$

$$\frac{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} e_0 : s_0}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathsf{check}\{\mathcal{U}\}\, e_0\, \mathsf{p}_0 : \mathcal{U}} \qquad \frac{}{\mathcal{T}_0;\Gamma_0 \vdash_{\mathsf{s}} \mathsf{Err} : \mathcal{U}}$$

$\boxed{s \leqslant: s}$

$$\frac{}{\mathsf{Nat} \leqslant: \mathsf{Int}} \qquad \frac{}{s_0 \leqslant: s_0}$$

Lemma 6.5 (First-Order initialization).

- *If* $(e_0)^{\ell_0} : \tau_0$ **wf** *then* $\cdot \vdash_{\mathbf{s}} (e_0)^{\ell_0} : \lfloor \tau_0 \rfloor$ *and* $\cdot; \ell_0 \Vdash (e_0)^{\ell_0}; \emptyset; \emptyset$.
- *If* $(e_0)^{\ell_0} : \mathcal{U}$ **wf** *then* $\cdot \vdash_{\mathbf{s}} (e_0)^{\ell_0} : \mathcal{U}$ *and* $\cdot; \ell_0 \Vdash (e_0)^{\ell_0}; \emptyset; \emptyset$.

Proof Sketch. By lemma 6.6. □

Lemma 6.6.

- *If* $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}$ *and* $\Gamma_0 \vdash (e_0)^{\ell_0} : \tau_0$ *then* $\Gamma_0 \vdash_{\mathbf{s}} (e_0)^{\ell_0} : \tau_0$ *and* $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}$.
- *If* $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}$ *and* $\Gamma_0 \vdash (e_0)^{\ell_0} : \mathcal{U}$ *then* $\Gamma_0 \vdash_{\mathbf{s}} (e_0)^{\ell_0} : \mathcal{U}$ *and* $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}; \emptyset; \emptyset$.

Proof Sketch. By induction on the surface typing and surface ownership judgments. □

6.2.3 *Erased Language.*

$\boxed{\text{Erased Evaluation Syntax}}$

$$\begin{array}{lcl} e & = & x \mid i \mid n \mid \langle e, e\rangle \mid \lambda x.\, e \mid \lambda(x:\tau).\, e \mid \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\; e\; e \mid \mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\; e \mid \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\; e\; e \mid \\ & & \mathsf{dyn}\; b\; e \mid \mathsf{stat}\; b\; e \mid \mathsf{Err} \\ v & = & i \mid n \mid \langle v, v\rangle \mid \lambda x.\, e \mid \lambda(x:\tau).\, e \\ \mathsf{Err} & = & \mathsf{InvariantErr} \mid \mathsf{TagErr} \mid \mathsf{BoundaryErr}\,(b^*, v) \mid \mathsf{DivErr} \end{array}$$

$\boxed{\Gamma \vdash_{\mathbf{0}} e : \mathcal{U}}$

$$\frac{(x_0 : {}^{\tau}/_{\mathcal{U}}) \in \Gamma_0}{\Gamma_0 \vdash_{\mathbf{0}} x_0 : \mathcal{U}} \qquad \frac{}{\Gamma_0 \vdash_{\mathbf{0}} i_0 : \mathcal{U}} \qquad \frac{(x_0 : \tau_0), \Gamma_0 \vdash_{\mathbf{0}} e_0 : \mathcal{U}}{\Gamma_0 \vdash_{\mathbf{0}} \lambda(x_0 : \tau_0).\, e_0 : \mathcal{U}} \qquad \frac{(x_0 : \mathcal{U}), \Gamma_0 \vdash_{\mathbf{0}} e_0 : \mathcal{U}}{\Gamma_0 \vdash_{\mathbf{0}} \lambda x_0.\, e_0 : \mathcal{U}}$$

$$\frac{\Gamma_0 \vdash_{\mathbf{0}} e_0 : \mathcal{U} \qquad \Gamma_0 \vdash_{\mathbf{0}} e_1 : \mathcal{U}}{\Gamma_0 \vdash_{\mathbf{0}} \langle e_0, e_1\rangle : \mathcal{U}} \qquad \frac{\Gamma_0 \vdash_{\mathbf{0}} e_0 : \mathcal{U}}{\Gamma_0 \vdash_{\mathbf{0}} \mathit{unop}\{\mathcal{U}\}\; e_0 : \mathcal{U}} \qquad \frac{\Gamma_0 \vdash_{\mathbf{0}} e_0 : \mathcal{U} \qquad \Gamma_0 \vdash_{\mathbf{0}} e_1 : \mathcal{U}}{\Gamma_0 \vdash_{\mathbf{0}} \mathit{binop}\{\mathcal{U}\}\; e_0\; e_1 : \mathcal{U}}$$

$$\frac{\Gamma_0 \vdash_{\mathbf{0}} e_0 : \mathcal{U} \qquad \Gamma_0 \vdash_{\mathbf{0}} e_1 : \mathcal{U}}{\Gamma_0 \vdash_{\mathbf{0}} \mathsf{app}\{\mathcal{U}\}\; e_0\; e_1 : \mathcal{U}} \qquad \frac{\Gamma_0 \vdash_{\mathbf{0}} e_0 : \mathcal{U}}{\Gamma_0 \vdash_{\mathbf{0}} \mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; e_0 : \mathcal{U}} \qquad \frac{\Gamma_0 \vdash_{\mathbf{0}} e_0 : \mathcal{U}}{\Gamma_0 \vdash_{\mathbf{0}} \mathsf{stat}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; e_0 : \mathcal{U}}$$

$$\frac{}{\Gamma_0 \vdash_{\mathbf{0}} \mathsf{Err} : \mathcal{U}}$$

$\boxed{\text{Erased Evaluation Syntax, with Ownership}}$

$$\begin{array}{lcl} e & = & x \mid i \mid n \mid \langle e, e\rangle \mid \lambda x.\, e \mid \lambda(x:\tau).\, e \mid \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\; e\; e \mid \mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\; e \mid \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\; e\; e \mid \\ & & \mathsf{dyn}\; b\; (e)^{\ell} \mid \mathsf{stat}\; b\; (e)^{\ell} \mid (e)^{\ell} \mid \mathsf{Err} \\ v & = & i \mid n \mid \langle v, v\rangle \mid \lambda x.\, e \mid \lambda(x:\tau).\, e \mid (v)^{\ell} \end{array}$$

$\boxed{\mathcal{L}; \ell \Vdash e}$

$$\frac{\mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}} \qquad \frac{(x_0 : \ell_0) \in \mathcal{L}_0}{\mathcal{L}_0; \ell_0 \Vdash x_0} \qquad \frac{}{\mathcal{L}_0; \ell_0 \Vdash i_0} \qquad \frac{(x_0 : \ell_0), \mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \lambda x_0.\, e_0}$$

$$\frac{(x_0 : \ell_0), \mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \lambda(x_0 : \tau_0).\, e_0} \qquad \frac{\mathcal{L}_0; \ell_0 \Vdash e_0 \qquad \mathcal{L}_0; \ell_0 \Vdash e_1}{\mathcal{L}_0; \ell_0 \Vdash \langle e_0, e_1\rangle} \qquad \frac{\mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\; e_0}$$

$$\frac{\mathcal{L}_0; \ell_0 \Vdash e_0 \qquad \mathcal{L}_0; \ell_0 \Vdash e_1}{\mathcal{L}_0; \ell_0 \Vdash \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\; e_0\; e_1} \qquad \frac{\mathcal{L}_0; \ell_0 \Vdash e_0 \qquad \mathcal{L}_0; \ell_0 \Vdash e_1}{\mathcal{L}_0; \ell_0 \Vdash \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\; e_0\; e_1} \qquad \frac{\mathcal{L}_0; \ell_1 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; e_0}$$

$$\frac{\mathcal{L}_0; \ell_1 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \mathsf{stat}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; e_0} \qquad \frac{}{\mathcal{L}_0; \ell_0 \Vdash \mathsf{Err}}$$

Lemma 6.7 (Erased initialization). *If* $(e_0)^{\ell_0} : {}^{\tau}/_{\mathcal{U}}$ **wf** *then* $\cdot \vdash_{\mathbf{0}} (e_0)^{\ell_0} : \mathcal{U}$ *and* $\cdot; \ell_0 \Vdash (e_0)^{\ell_0}$.

Proof Sketch. By lemma 6.8. □

Lemma 6.8. *If* $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}$ *and* $\Gamma_0 \vdash (e_0)^{\ell_0} : {}^{\tau}/_{\mathcal{U}}$ *then* $\Gamma_0 \vdash_{\mathbf{0}} (e_0)^{\ell_0} : \mathcal{U}$ *and* $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}$.

Proof Sketch. By induction on the surface typing and surface ownership judgments. □

6.3 Properties of Interest

Definition 6.9 (F-type soundness). *A semantics X satisfies* $\mathbf{TS}(F)$ *(for $F \in \{\mathbf{1}, \mathbf{s}, \mathbf{0}\}$) if for all $e_0 : {}^{\tau}/_{\mathcal{U}}\ \mathbf{wf}$ one of the following holds:*

- $e_0 \rightarrow^*_{\mathsf{X}} v_0$ *and* $\vdash_F v_0 : F({}^{\tau}/_{\mathcal{U}})$
- $e_0 \rightarrow^*_{\mathsf{X}} \{\mathsf{TagErr}, \mathsf{DivErr}\} \cup \mathsf{BoundaryErr}\,(b^*, v)$
- e_0 *diverges*

$\boxed{\mathbf{1} : {}^{\tau}/_{\mathcal{U}} \longrightarrow {}^{\tau}/_{\mathcal{U}}}$

$\mathbf{1}({}^{\tau}/_{\mathcal{U}}) = {}^{\tau}/_{\mathcal{U}}$

$\boxed{\mathbf{s} : {}^{\tau}/_{\mathcal{U}} \longrightarrow s \cup \mathcal{U}}$

$$\mathbf{s}({}^{\tau}/_{\mathcal{U}}) = \begin{cases} \mathcal{U} & \text{if } {}^{\tau}/_{\mathcal{U}} = \mathcal{U} \\ \lfloor \tau_0 \rfloor & \text{if } {}^{\tau}/_{\mathcal{U}} = \tau_0 \end{cases}$$

$\boxed{\mathbf{0} : {}^{\tau}/_{\mathcal{U}} \longrightarrow \mathcal{U}}$

$\mathbf{0}({}^{\tau}/_{\mathcal{U}}) = \mathcal{U}$

Definition 6.10 (complete monitoring). *A semantics X satisfies* $\mathbf{CM}$ *if for all $(e_0)^{\ell_0} : {}^{\tau}/_{\mathcal{U}}\ \mathbf{wf}$ and all e_1 such that $e_0 \rightarrow^*_{\mathsf{X}} e_1$, the contractum is single-owner consistent: $\ell_0 \Vdash e_1$.*

Definition 6.11 (path-based blame soundness and blame completeness). *For all well-formed e_0 such that $e_0 \rightarrow^*_{\mathsf{X}} \mathsf{BoundaryErr}\,(b_0^*, v_0)$:*

- *X satisfies* $\mathbf{BS}$ *iff $senders\,(b_0^*) \subseteq owners\,(v_0)$*
- *X satisfies* $\mathbf{BC}$ *iff $senders\,(b_0^*) \supseteq owners\,(v_0)$*

Definition 6.12 (error preorder). *$X \lesssim Y$ iff $e_0 \rightarrow^*_{\mathsf{Y}} \mathsf{Err}$ implies $e_0 \rightarrow^*_{\mathsf{X}} \mathsf{Err}$ for all well-formed expressions e_0.*

Definition 6.13 (error equivalence). *$X \approx Y$ iff $X \lesssim Y$ and $Y \lesssim X$.*

6.4 Common Higher-Order Notions of Reduction

This section is intentionally left blank. The common notions of reduction are inlined into the definitions that require them.

6.5 Natural and its Properties

6.5.1 Semantics, Type Soundness.

$\boxed{e \rhd_{\mathsf{N}} e}$

$$
\begin{array}{lll}
\mathit{unop}\{\tau_0\}\ v_0 & \rhd_{\mathsf{N}} & \mathsf{InvariantErr} \\
\quad \text{if } \delta(\mathit{unop}, v_0) \text{ is undefined} & & \\
\mathit{unop}\{\tau_0\}\ v_0 & \rhd_{\mathsf{N}} & \delta(\mathit{unop}, v_0) \\
\quad \text{if } \delta(\mathit{unop}, v_0) \text{ is defined} & & \\
\mathit{binop}\{\tau_0\}\ v_0\ v_1 & \rhd_{\mathsf{N}} & \mathsf{InvariantErr} \\
\quad \text{if } \delta(\mathit{binop}, v_0, v_1) \text{ is undefined} & & \\
\mathit{binop}\{\tau_0\}\ v_0\ v_1 & \rhd_{\mathsf{N}} & \delta(\mathit{binop}, v_0, v_1) \\
\quad \text{if } \delta(\mathit{binop}, v_0, v_1) \text{ is defined} & & \\
\mathsf{app}\{\tau_0\}\ v_0\ v_1 & \rhd_{\mathsf{N}} & \mathsf{InvariantErr} \\
\quad \text{if } v_0 \notin (\lambda(x:\tau).\, e) \cup (\mathbb{G}\ b\ v) & & \\
\mathsf{app}\{\tau_0\}\ (\lambda(x_0:\tau_1).\, e_0)\ v_0 & \rhd_{\mathsf{N}} & e_0[x_0 \leftarrow v_0] \\
\mathsf{app}\{\tau_0\}\ (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_0)\ v_1 & \rhd_{\mathsf{N}} & \mathsf{dyn}\ b_0\ (\mathsf{app}\{\mathcal{U}\}\ v_0\ (\mathsf{stat}\ b_1\ v_1)) \\
\quad \text{where } b_0 = (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1) \text{ and } b_1 = (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0) & & \\
\mathsf{dyn}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ v_0 & \rhd_{\mathsf{N}} & \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ v_0 \\
\quad \text{if } \mathit{shape\text{-}match}(\lfloor \tau_0 \Rightarrow \tau_1 \rfloor, v_0) & & \\
\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \langle v_0, v_1 \rangle & \rhd_{\mathsf{N}} & \langle \mathsf{dyn}\ b_0\ v_0, \mathsf{dyn}\ b_1\ v_1 \rangle \\
\quad \text{if } \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \langle v_0, v_1 \rangle) \text{ and } b_0 = (\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1) \text{ and } b_1 = (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1) & & \\
\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ i_0 & \rhd_{\mathsf{N}} & i_0 \\
\quad \text{if } \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, i_0) & & \\
\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 & \rhd_{\mathsf{N}} & \mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), v_0) \\
\quad \text{if } \neg\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0) & &
\end{array}
$$

$\boxed{e \blacktriangleright_{\mathsf{N}} e}$

$$\begin{array}{lll}
\mathit{unop}\{\mathcal{U}\}\ v_0 & \blacktriangleright_{\mathsf{N}} & \mathsf{TagErr} \\
\quad \text{if } \delta(\mathit{unop}, v_0) \text{ is undefined} & & \\
\mathit{unop}\{\mathcal{U}\}\ v_0 & \blacktriangleright_{\mathsf{N}} & \delta(\mathit{unop}, v_0) \\
\quad \text{if } \delta(\mathit{unop}, v_0) \text{ is defined} & & \\
\mathit{binop}\{\mathcal{U}\}\ v_0\ v_1 & \blacktriangleright_{\mathsf{N}} & \mathsf{TagErr} \\
\quad \text{if } \delta(\mathit{binop}, v_0, v_1) \text{ is undefined} & & \\
\mathit{binop}\{\mathcal{U}\}\ v_0\ v_1 & \blacktriangleright_{\mathsf{N}} & \delta(\mathit{binop}, v_0, v_1) \\
\quad \text{if } \delta(\mathit{binop}, v_0, v_1) \text{ is defined} & & \\
\mathsf{app}\{\mathcal{U}\}\ v_0\ v_1 & \blacktriangleright_{\mathsf{N}} & \mathsf{TagErr} \\
\quad \text{if } v_0 \notin (\lambda x.\, e) \cup (\mathbb{G}\ b\ v) & & \\
\mathsf{app}\{\mathcal{U}\}\ (\lambda x_0.\, e_0)\ v_0 & \blacktriangleright_{\mathsf{N}} & e_0[x_0 \leftarrow v_0] \\
\mathsf{app}\{\mathcal{U}\}\ (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)\ v_1 & \blacktriangleright_{\mathsf{N}} & \mathsf{stat}\ b_0\ (\mathsf{app}\{\mathit{cod}(\tau_0)\}\ v_0\ (\mathsf{dyn}\ b_1\ v_1)) \\
\quad \text{where } b_0 = (\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1) \text{ and } b_1 = (\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0) & & \\
\mathsf{stat}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ v_0 & \blacktriangleright_{\mathsf{N}} & \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ v_0 \\
\quad \text{if } \mathit{shape\text{-}match}(\lfloor \tau_0 \Rightarrow \tau_1 \rfloor, v_0) \text{ and } v_0 \in (\lambda(x:\tau).\, e) \cup (\mathbb{G}\ b\ v) & & \\
\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \langle v_0, v_1 \rangle & \blacktriangleright_{\mathsf{N}} & \langle \mathsf{stat}\ b_0\ v_0, \mathsf{stat}\ b_1\ v_1 \rangle \\
\quad \text{if } \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \langle v_0, v_1 \rangle) \text{ and } b_0 = (\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1) \text{ and } b_1 = (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1) & & \\
\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ i_0 & \blacktriangleright_{\mathsf{N}} & i_0 \\
\quad \text{if } \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, i_0) & & \\
\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 & \blacktriangleright_{\mathsf{N}} & \mathsf{InvariantErr} \\
\quad \text{if } \neg \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0) & &
\end{array}$$

$\boxed{e \rightarrow^*_{\mathsf{N}} e}$ is the transitive, reflexive, compatible (with respect to evaluation contexts E, section 6.2) closure of the relation $\bigcup\{\rhd_{\mathsf{N}}, \blacktriangleright_{\mathsf{N}}\}$

$\boxed{N(e)}$ holds for expressions that contain no subterms of the form $(\mathbb{T}\ \overline{b}\ v)$, $(\mathsf{trace}\ \overline{b}\ e)$, or $(\mathbb{G}\ \tau\ v)$ where τ is not a function type.

$$\frac{}{N(x_0)} \qquad \frac{}{N(i_0)} \qquad \frac{}{N(\mathsf{Err})} \qquad \frac{N(e_0)}{N(\lambda x_0.\, e_0)} \qquad \frac{N(e_0)}{N(\lambda(x_0 : \tau_0).\, e_0)}$$

$$\frac{N(e_0)}{N(\mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ e_0)} \qquad \frac{N(e_0)}{N(\mathit{unop}\{^{\tau}/_{\mathcal{U}}\}\ e_0)} \qquad \frac{N(e_0)}{N(\mathsf{dyn}\ b_0\ e_0)} \qquad \frac{N(e_0)}{N(\mathsf{stat}\ b_0\ e_0)}$$

$$\frac{N(e_0) \qquad N(e_1)}{N(\mathsf{app}\{^{\tau}/_{\mathcal{U}}\}\ e_0\ e_1)} \qquad \frac{N(e_0) \qquad N(e_1)}{N(\mathit{binop}\{^{\tau}/_{\mathcal{U}}\}\ e_0\ e_1)}$$

Theorem 6.14 (Natural type soundness). *Natural satisfies* **TS (1)**

Proof. By lemma 6.15, progress (lemma 6.16), and preservation (lemma 6.17). □

Lemma 6.15. *If* $e_0 : {}^{\tau}/_{\mathcal{U}}\ \mathbf{wf}$ *then* $N(e_0)$.

Proof. Wrappers and trace expressions are not part of the surface language. □

Lemma 6.16 (Natural type progress). *If* $\cdot \vdash_1 E_0[e_0] : {}^{\tau}/_{\mathcal{U}}$ *and* $N(E_0[e_0])$ *then one of the following holds:*

- $e_0 \in v \cup \mathsf{Err}$
- ${}^{\tau}/_{\mathcal{U}} \in \tau$ *and* $\exists\, e_1.\ e_0 \rhd_{\mathsf{N}} e_1$
- ${}^{\tau}/_{\mathcal{U}} \in \mathcal{U}$ *and* $\exists\, e_1.\ e_0 \blacktriangleright_{\mathsf{N}} e_1$

Proof Sketch. By unique decomposition (lemma 6.1) and case analysis. More details in appendix: lemma A.1. □

Lemma 6.17 (Natural type preservation).
If $\cdot \vdash_1 E_0[e_0] : {}^{\tau}/_{\mathcal{U}}$ *and* $N(E_0[e_0])$ *and* $e_0(\rhd_{\mathsf{N}} \cup \blacktriangleright_{\mathsf{N}})e_1$ *then* $\cdot \vdash_1 E_0[e_1] : {}^{\tau}/_{\mathcal{U}}$ *and* $N(E_0[e_1])$.

Proof Sketch. By case analysis of each reduction relation. More details in appendix: lemma A.2. □

Lemma 6.18.

- *If* $N(E_0[e_0])$ *then* $N(e_0)$
- *If* $N(E_0[e_0])$ *and* $N(e_1)$ *then* $N(E_0[e_1])$

Proof Sketch. By induction on the structure of E_0. □

6.5.2 *Lifted Semantics, Complete Monitoring, Blame.*

$\boxed{(e)^{\ell} \rhd_{\overline{\mathsf{N}}} (e)^{\ell}}$ lifted version of $\rhd_{\mathsf{N}}$

$$(\mathit{unop}\{\tau_0\}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}})^{\ell_0} \quad \rhd_{\overline{\mathsf{N}}} \quad (\mathsf{InvariantErr})^{\ell_0}$$
if $v_0 \notin (v)^{\ell}$ and $\delta(\mathit{unop}, v_0)$ is undefined

$$(\mathit{unop}\{\tau_0\}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}})^{\ell_0} \quad \rhd_{\overline{\mathsf{N}}} \quad (\delta(\mathit{unop}, v_0))^{\overline{\ell_0}\ell_0}$$
if $\delta(\mathit{unop}, v_0)$ is defined

$$(\mathit{binop}\{\tau_0\}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}}\, \llparenthesis v_1 \rrparenthesis^{\overline{\ell_1}})^{\ell_0} \quad \rhd_{\overline{\mathsf{N}}} \quad (\mathsf{InvariantErr})^{\ell_0}$$
if $v_0 \notin (v)^{\ell}$ and $v_1 \notin (v)^{\ell}$ and $\delta(\mathit{binop}, v_0, v_1)$ is undefined

$$(\mathit{binop}\{\tau_0\}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}}\, \llparenthesis v_1 \rrparenthesis^{\overline{\ell_1}})^{\ell_0} \quad \rhd_{\overline{\mathsf{N}}} \quad (\delta(\mathit{binop}, v_0, v_1))^{\ell_0}$$
if $\delta(\mathit{binop}, v_0, v_1)$ is defined

$$(\mathsf{app}\{\tau_0\}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}}\; v_1)^{\ell_0} \quad \rhd_{\overline{\mathsf{N}}} \quad (\mathsf{InvariantErr})^{\ell_0}$$
if $v_0 \notin (v)^{\ell} \cup (\lambda x.\, e) \cup (\mathbb{G}\; b\; v)$

$$(\mathsf{app}\{\tau_0\}\, \llparenthesis \lambda(x_0 : \tau_1).\, e_0 \rrparenthesis^{\overline{\ell_0}}\; v_1)^{\ell_0} \quad \rhd_{\overline{\mathsf{N}}} \quad \llparenthesis e_0[x_0 \leftarrow \llparenthesis v_1 \rrparenthesis^{\ell_0 \mathit{rev}(\overline{\ell_0})}] \rrparenthesis^{\overline{\ell_0}\ell_0}$$

$$(\mathsf{app}\{\tau_0\}\, \llparenthesis \mathbb{G}\; (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell_0}}\; v_1)^{\ell_3} \quad \rhd_{\overline{\mathsf{N}}}$$
$$\llparenthesis (\mathsf{dyn}\; b_0\; (\mathsf{app}\{\mathcal{U}\}\; v_0\; (\mathsf{stat}\; b_1\; \llparenthesis v_1 \rrparenthesis^{\ell_3 \mathit{rev}(\overline{\ell_0})})))^{\ell_2} \rrparenthesis^{\overline{\ell_0}\ell_3}$$
where $b_0 = (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)$

$$(\mathsf{dyn}\; (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\; \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}})^{\ell_2} \quad \rhd_{\overline{\mathsf{N}}} \quad (\mathbb{G}\; (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\; \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}})^{\ell_2}$$
if $\mathit{shape\text{-}match}(\lfloor \tau_0 \Rightarrow \tau_1 \rfloor, v_0)$ and $v_0 \in (\lambda x.\, e) \cup (\mathbb{G}\; b\; v)$

$$(\mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; \llparenthesis \langle v_0, v_1 \rangle \rrparenthesis^{\overline{\ell_0}})^{\ell_2} \quad \rhd_{\overline{\mathsf{N}}} \quad (\langle \mathsf{dyn}\; b_0\; \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}}, \mathsf{dyn}\; b_1\; \llparenthesis v_1 \rrparenthesis^{\overline{\ell_0}} \rangle)^{\ell_2}$$
if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \langle v_0, v_1 \rangle)$ and $b_0 = (\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)$

$$(\mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; \llparenthesis i_0 \rrparenthesis^{\overline{\ell_0}})^{\ell_2} \quad \rhd_{\overline{\mathsf{N}}} \quad (i_0)^{\ell_2}$$
if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, i_0)$

$$(\mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}})^{\ell_2} \quad \rhd_{\overline{\mathsf{N}}} \quad (\mathsf{BoundaryErr}\, ((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}}))^{\ell_2}$$
if $\neg\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$

$\boxed{(e)^{\ell} \blacktriangleright_{\overline{\mathsf{N}}} (e)^{\ell}}$ lifted version of $\blacktriangleright_{\mathsf{N}}$

$$(unop\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}})^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{N}}} \quad (\mathsf{TagErr})^{\ell_0}$$

if $v_0 \notin (v)^{\ell}$ and $\delta(unop, v_0)$ is undefined

$$(unop\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}})^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{N}}} \quad (\delta(unop, v_0))^{\overline{\ell_0}\ell_0}$$

if $\delta(unop, v_0)$ is defined

$$(binop\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ (\!(v_1)\!)^{\overline{\ell_1}})^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{N}}} \quad (\mathsf{TagErr})^{\ell_0}$$

if $v_0 \notin (v)^{\ell}$ and $v_1 \notin (v)^{\ell}$ and $\delta(binop, v_0, v_1)$ is undefined

$$(binop\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ (\!(v_1)\!)^{\overline{\ell_1}})^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{N}}} \quad (\delta(binop, v_0, v_1))^{\ell_0}$$

if $\delta(binop, v_0, v_1)$ is defined

$$(\mathsf{app}\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ v_1)^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{N}}} \quad (\mathsf{TagErr})^{\ell_0}$$

if $v_0 \notin (v)^{\ell} \cup (\lambda x.\, e) \cup (\mathbb{G}\ b\ v)$

$$(\mathsf{app}\{\mathcal{U}\}\ (\!(\lambda x_0.\, e_0)\!)^{\overline{\ell_0}}\ v_1)^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{N}}} \quad (\!(e_0[x_0 \leftarrow (\!(v_1)\!)^{\ell_0\, rev(\overline{\ell_0})}])\!)^{\overline{\ell_0}\ell_0}$$

$$(\mathsf{app}\{\mathcal{U}\}\ (\!(\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2})\!)^{\overline{\ell_0}}\ v_1)^{\ell_3} \quad \blacktriangleright_{\overline{\mathsf{N}}}$$

$$(\!(\mathsf{stat}\ b_0\ (\mathsf{app}\{\tau_1\}\ v_0\ (\mathsf{dyn}\ b_1\ (\!(v_1)\!)^{\ell_3\, rev(\overline{\ell_0})}))^{\ell_2})\!)^{\overline{\ell_0}\ell_3}$$

where $b_0 = (\ell_0 \blacktriangleleft cod(\tau_0) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft dom(\tau_0) \blacktriangleleft \ell_0)$ and $\tau_1 = cod(\tau_0)$

$$(\mathsf{stat}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell_0}})^{\ell_2} \quad \blacktriangleright_{\overline{\mathsf{N}}} \quad (\mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell_0}})^{\ell_2}$$

if $shape\text{-}match(\lfloor \tau_0 \Rightarrow \tau_1 \rfloor, v_0)$ and $v_0 \in (\lambda x.\, e) \cup (\mathbb{G}\ b\ v)$

$$(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(\langle v_0, v_1 \rangle)\!)^{\overline{\ell_0}})^{\ell_2} \quad \blacktriangleright_{\overline{\mathsf{N}}} \quad (\langle \mathsf{dyn}\ b_0\ (\!(v_0)\!)^{\overline{\ell_0}}, \mathsf{dyn}\ b_1\ (\!(v_1)\!)^{\overline{\ell_0}} \rangle)^{\ell_2}$$

if $shape\text{-}match(\langle v_0, v_1 \rangle, \tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft fst(\tau_0) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_0 \blacktriangleleft snd(\tau_0) \blacktriangleleft \ell_1)$

$$(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(i_0)\!)^{\overline{\ell_2}})^{\ell_3} \quad \blacktriangleright_{\overline{\mathsf{N}}} \quad (i_0)^{\ell_3}$$

if $shape\text{-}match(i_0, \tau_0)$

$$(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell_2}})^{\ell_2} \quad \blacktriangleright_{\overline{\mathsf{N}}} \quad (\mathsf{InvariantErr})^{\ell_2}$$

if $\neg shape\text{-}match(v_0, \tau_0)$

Theorem 6.19 (Natural complete monitoring). *Natural satisfies* **CM**

Proof Sketch. By preservation of single-owner consistency ($\Vdash$) for $\triangleright_{\overline{\mathsf{N}}}$ and $\blacktriangleright_{\overline{\mathsf{N}}}$. More details in appendix: theorem A.3. $\square$

Lemma 6.20 (Natural blame soundness and completeness). *If e_0 is well-formed and $e_0 \rightarrow^*_{\mathsf{N}}$ $\mathsf{BoundaryErr}\,(\bar{b}_0, v_0)$, then $senders\,(\bar{b}_0) = owners\,(v_0)$ and furthermore $\bar{b}_0$ contains exactly one boundary specification.*

Proof. By complete monitoring (theorem 6.19) and the definition of $\rightarrow^*_{\mathsf{N}}$. There is only one rule that produces a boundary error. It blames a single boundary, and complete monitoring guarantees that the component names (*senders*) and labels (*owners*) match. $\square$

Corollary 6.21. *Natural satisfies* **BS** *and* **BC**

6.6 Co-Natural and its Properties

6.6.1 *Semantics, Type Soundness.*

$\boxed{e \rhd_{\mathsf{C}} e}$

$unop\{\tau_0\}\, v_0 \quad \rhd_{\mathsf{C}} \quad \mathsf{InvariantErr}$
  if $v_0 \notin (\mathbb{G}\,(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell)\ v)$ and $\delta(unop, v_0)$ is undefined

$unop\{\tau_0\}\, v_0 \quad \rhd_{\mathsf{C}} \quad \delta(unop, v_0)$
  if $\delta(unop, v_0)$ is defined

$\mathsf{fst}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_0) \quad \rhd_{\mathsf{C}} \quad \mathsf{dyn}\ b_0\ (\mathsf{fst}\{\mathcal{U}\}\ v_0)$
  where $\tau_2 = fst(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$

$\mathsf{snd}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_0 \quad \rhd_{\mathsf{C}} \quad \mathsf{dyn}\ b_0\ (\mathsf{snd}\{\mathcal{U}\}\ v_0)$
  where $\tau_2 = snd(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$

$binop\{\tau_0\}\, v_0\, v_1 \quad \rhd_{\mathsf{C}} \quad \mathsf{InvariantErr}$
  if $\delta(binop, v_0, v_1)$ is undefined

$binop\{\tau_0\}\, v_0\, v_1 \quad \rhd_{\mathsf{C}} \quad \delta(binop, v_0, v_1)$
  if $\delta(binop, v_0, v_1)$ is defined

$\mathsf{app}\{\tau_0\}\ v_0\ v_1 \quad \rhd_{\mathsf{C}} \quad \mathsf{InvariantErr}$
  if $v_0 \notin (\lambda(x : \tau).\, e) \cup (\mathbb{G}\ b\ v)$

$\mathsf{app}\{\tau_0\}\,(\lambda(x_0 : \tau_1).\, e_0)\ v_0 \quad \rhd_{\mathsf{C}} \quad e_0[x_0 \leftarrow v_0]$

$\mathsf{app}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_0)\ v_1 \quad \rhd_{\mathsf{C}} \quad \mathsf{dyn}\ b_0\ (\mathsf{app}\{\mathcal{U}\}\ v_0\ (\mathsf{stat}\ b_1\ v_1))$
  where $b_0 = (\ell_0 \blacktriangleleft cod(\tau_1) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)$

$\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \quad \rhd_{\mathsf{C}} \quad \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0$
  if $shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$ and $v_0 \in \langle v, v \rangle \cup (\lambda x.\, e) \cup (\mathbb{G}\ b\ v)$

$\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ i_0 \quad \rhd_{\mathsf{C}} \quad i_0$
  if $shape\text{-}match(\lfloor \tau_0 \rfloor, i_0)$

$\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \quad \rhd_{\mathsf{C}} \quad \mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), v_0)$
  if $\neg shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$

$\boxed{e \blacktriangleright_{\mathsf{C}} e}$

$unop\{\mathcal{U}\}\, v_0 \quad \blacktriangleright_{\mathsf{C}} \quad \mathsf{TagErr}$
  if $v_0 \notin (\mathbb{G}\,(\ell \blacktriangleleft (\tau{\times}\tau) \blacktriangleleft \ell)\; v)$ and $\delta(unop, v_0)$ is undefined

$unop\{\mathcal{U}\}\, v_0 \quad \blacktriangleright_{\mathsf{C}} \quad \delta(unop, v_0)$
  if $\delta(unop, v_0)$ is defined

$\mathsf{fst}\{\mathcal{U}\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0) \quad \blacktriangleright_{\mathsf{C}} \quad \mathsf{stat}\; b_0\; (\mathsf{fst}\{\tau_1\}\; v_0)$
  where $\tau_1 = \mathit{fst}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$

$\mathsf{snd}\{\mathcal{U}\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \quad \blacktriangleright_{\mathsf{C}} \quad \mathsf{stat}\; b_0\; (\mathsf{snd}\{\tau_1\}\; v_0)$
  where $\tau_1 = \mathit{snd}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$

$binop\{\mathcal{U}\}\, v_0\, v_1 \quad \blacktriangleright_{\mathsf{C}} \quad \mathsf{TagErr}$
  if $\delta(binop, v_0, v_1)$ is undefined

$binop\{\mathcal{U}\}\, v_0\, v_1 \quad \blacktriangleright_{\mathsf{C}} \quad \delta(binop, v_0, v_1)$
  if $\delta(binop, v_0, v_1)$ is defined

$\mathsf{app}\{\mathcal{U}\}\; v_0\; v_1 \quad \blacktriangleright_{\mathsf{C}} \quad \mathsf{TagErr}$
  if $v_0 \notin (\lambda x.\, e) \cup (\mathbb{G}\; b\; v)$

$\mathsf{app}\{\mathcal{U}\}\; (\lambda x_0.\, e_0)\; v_0 \quad \blacktriangleright_{\mathsf{C}} \quad e_0[x_0 \leftarrow v_0]$

$\mathsf{app}\{\mathcal{U}\}\; (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0)\; v_1 \quad \blacktriangleright_{\mathsf{C}} \quad \mathsf{stat}\; b_0\; (\mathsf{app}\{\mathit{cod}(\tau_0)\}\; v_0\; (\mathsf{dyn}\; b_1\; v_1))$
  where $b_0 = (\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)$

$\mathsf{stat}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \quad \blacktriangleright_{\mathsf{C}} \quad \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0$
  if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$ and $v_0 \in \langle v, v\rangle \cup (\lambda(x : \tau).\, e) \cup (\mathbb{G}\; b\; v)$

$\mathsf{stat}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; i_0 \quad \blacktriangleright_{\mathsf{C}} \quad i_0$
  if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, i_0)$

$\mathsf{stat}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \quad \blacktriangleright_{\mathsf{C}} \quad \mathsf{InvariantErr}$
  if $\neg\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$

$\boxed{e \rightarrow^*_{\mathsf{C}} e}$ is the transitive, reflexive, compatible (with respect to evaluation contexts E, section 6.2) closure of the relation $\bigcup\{\triangleright_{\mathsf{C}}, \blacktriangleright_{\mathsf{C}}\}$

$\boxed{C(e)}$ holds for expressions that contain no subterms of the form $(\mathbb{T}\; \bar{b}\; v)$, $(\mathsf{trace}\; \bar{b}\; e)$, or $(\mathbb{G}\; \tau\; v)$ where τ is not a pair or function type.

$$\frac{}{C(x_0)} \qquad \frac{}{C(i_0)} \qquad \frac{}{C(\mathsf{Err})} \qquad \frac{C(e_0)}{C(\lambda x_0.\, e_0)} \qquad \frac{C(e_0)}{C(\lambda(x_0 : \tau_0).\, e_0)} \qquad \frac{C(e_0)}{C(\mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\; e_0)}$$

$$\frac{C(e_0)}{C(\mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_0{\times}\tau_1) \blacktriangleleft \ell_1)\; e_0)} \qquad \frac{C(e_0)}{C(unop\{{}^{\tau}/_{\mathcal{U}}\}\; e_0)} \qquad \frac{C(e_0)}{C(\mathsf{dyn}\; b_0\; e_0)} \qquad \frac{C(e_0)}{C(\mathsf{stat}\; b_0\; e_0)}$$

$$\frac{C(e_0) \qquad C(e_1)}{C(\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\; e_0\; e_1)} \qquad \frac{C(e_0) \qquad C(e_1)}{C(binop\{{}^{\tau}/_{\mathcal{U}}\}\; e_0\; e_1)}$$

THEOREM 6.22 (CO-NATURAL TYPE SOUNDNESS). *Co-Natural satisfies* **TS (1)**

PROOF. By lemma 6.23, progress (lemma 6.24), and preservation (lemma 6.25). □

LEMMA 6.23. *If* $e_0 : {}^{\tau}/_{\mathcal{U}}$ **wf** *then* $C(e_0)$.

PROOF. Wrappers and trace expressions are not part of the surface language. □

LEMMA 6.24 (CO-NATURAL TYPE PROGRESS).
If $\cdot \vdash_1 E_0[e_0] : {}^{\tau}/_{\mathcal{U}}$ *and* $C(E_0[e_0])$ *then one of the following holds:*

- $e_0 \in v \cup \mathsf{Err}$
- ${}^{\tau}/_{\mathcal{U}} \in \tau$ *and* $\exists\, e_1.\ e_0 \rhd_{\mathrm{C}} e_1$
- ${}^{\tau}/_{\mathcal{U}} \in \mathcal{U}$ *and* $\exists\, e_1.\ e_0 \blacktriangleright_{\mathrm{C}} e_1$

PROOF SKETCH. By unique decomposition (lemma 6.1) and case analysis. More details in appendix: lemma A.4. □

LEMMA 6.25. *[Co-Natural type preservation]*
If $\cdot \vdash_1 E_0[e_0] : {}^{\tau}/_{\mathcal{U}}$ *and* $C(E_0[e_0])$ *and* $e_0(\rhd_{\mathrm{C}} \cup \blacktriangleright_{\mathrm{C}})e_1$ *then* $\cdot \vdash_1 E_0[e_1] : {}^{\tau}/_{\mathcal{U}}$ *and* $C(E_0[e_1])$.

PROOF SKETCH. By case analysis of each reduction relation. More details in appendix: lemma A.5. □

LEMMA 6.26.

- *If* $C(E_0[e_0])$ *then* $C(e_0)$
- *If* $C(E_0[e_0])$ *and* $C(e_1)$ *then* $C(E_0[e_1])$

PROOF SKETCH. By induction on the structure of E_0. □

6.6.2 *Lifted Semantics, Complete Monitoring, Blame.*

$\boxed{(e)^{\ell} \rhd_{\overline{\mathsf{C}}} (e)^{\ell}}$ lifted version of $\rhd_{\mathsf{C}}$

$$(\mathit{unop}\{\tau_0\}\ (\!(v_0)\!)^{\overline{\ell}_0})^{\ell_0} \quad \rhd_{\overline{\mathsf{C}}} \quad (\mathsf{InvariantErr})^{\ell_0}$$
if $v_0 \notin (v)^{\ell} \cup (\mathbb{G}\ (\ell \blacktriangleleft (\tau{\times}\tau) \blacktriangleleft \ell)\ v)$ and $\delta(\mathit{unop}, v_0)$ is undefined

$$(\mathit{unop}\{\tau_0\}\ (\!(v_0)\!)^{\overline{\ell}_0})^{\ell_0} \quad \rhd_{\overline{\mathsf{C}}} \quad (\delta(\mathit{unop}, v_0))^{\overline{\ell}_0 \ell_0}$$
if $\delta(\mathit{unop}, v_0)$ is defined

$$(\mathsf{fst}\{\tau_0\}\ (\!(\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2})\!)^{\overline{\ell}_0})^{\ell_3} \quad \rhd_{\overline{\mathsf{C}}} \quad (\mathsf{dyn}\ b_0\ (\mathsf{fst}\{\mathcal{U}\}\ (v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$$
where $\tau_2 = \mathit{fst}(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$

$$(\mathsf{snd}\{\tau_0\}\ (\!(\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2})\!)^{\overline{\ell}_0})^{\ell_3} \quad \rhd_{\overline{\mathsf{C}}} \quad (\mathsf{dyn}\ b_0\ (\mathsf{snd}\{\mathcal{U}\}\ (v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$$
where $\tau_2 = \mathit{snd}(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$

$$(\mathit{binop}\{\tau_0\}\ (\!(v_0)\!)^{\overline{\ell}_0}\ (\!(v_1)\!)^{\overline{\ell}_1})^{\ell_0} \quad \rhd_{\overline{\mathsf{C}}} \quad (\mathsf{InvariantErr})^{\ell_0}$$
if $v_0 \notin (v)^{\ell}$ and $v_1 \notin (v)^{\ell}$ and $\delta(\mathit{binop}, v_0, v_1)$ is undefined

$$(\mathit{binop}\{\tau_0\}\ (\!(v_0)\!)^{\overline{\ell}_0}\ (\!(v_1)\!)^{\overline{\ell}_1})^{\ell_0} \quad \rhd_{\overline{\mathsf{C}}} \quad (\delta(\mathit{binop}, v_0, v_1))^{\ell_0}$$
if $\delta(\mathit{binop}, v_0, v_1)$ is defined

$$(\mathsf{app}\{\tau_0\}\ (\!(v_0)\!)^{\overline{\ell}_0}\ v_1)^{\ell_0} \quad \rhd_{\overline{\mathsf{C}}} \quad (\mathsf{InvariantErr})^{\ell_0}$$
if $v_0 \notin (v)^{\ell} \cup (\lambda(x:\tau).\, e) \cup (\mathbb{G}\ b\ v)$

$$(\mathsf{app}\{\tau_0\}\ (\!(\lambda(x_0:\tau_1).\, e_0)\!)^{\overline{\ell}_0}\ v_0)^{\ell_0} \quad \rhd_{\overline{\mathsf{C}}} \quad (\!(e_0[x_0 \leftarrow (\!(v_0)\!)^{\ell_0 \mathit{rev}(\overline{\ell}_0)}])\!)^{\overline{\ell}_0 \ell_0}$$

$$(\mathsf{app}\{\tau_0\}\ (\!(\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2})\!)^{\overline{\ell}_0}\ v_1)^{\ell_3} \quad \rhd_{\overline{\mathsf{C}}}$$
$$(\!(\mathsf{dyn}\ b_0\ (\mathsf{app}\{\mathcal{U}\}\ v_0\ (\mathsf{stat}\ b_1\ (\!(v_1)\!)^{\ell_3 \mathit{rev}(\overline{\ell}_0)}))^{\ell_2})\!)^{\overline{\ell}_0 \ell_3}$$
where $b_0 = (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)$

$$(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell}_0})^{\ell_2} \quad \rhd_{\overline{\mathsf{C}}} \quad (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell}_0})^{\ell_2}$$
if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$ and $v_0 \in \langle v, v\rangle \cup (\lambda x.\, e) \cup (\mathbb{G}\ b\ v)$

$$(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(i_0)\!)^{\overline{\ell}_0})^{\ell_2} \quad \rhd_{\overline{\mathsf{C}}} \quad (i_0)^{\ell_2}$$
if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, i_0)$

$$(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell}_0})^{\ell_2} \quad \rhd_{\overline{\mathsf{C}}} \quad (\mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), (\!(v_0)\!)^{\overline{\ell}_0}))^{\ell_2}$$
if $\neg\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$

$\boxed{(e)^{\ell} \blacktriangleright_{\overline{\mathsf{C}}} (e)^{\ell}}$ lifted version of $\blacktriangleright_{\mathsf{C}}$

$$(unop\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}})^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{C}}} \quad (\mathsf{TagErr})^{\ell_0}$$

if $v_0 \notin (v)^{\ell} \cup (\mathbb{G}\ (\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell)\ v)$ and $\delta(unop, v_0)$ is undefined

$$(unop\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}})^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{C}}} \quad (\delta(unop, v_0))^{\overline{\ell_0}\ell_0}$$

if $\delta(unop, v_0)$ is defined

$$(\mathsf{fst}\{\mathcal{U}\}\ (\!(\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2})\!)^{\overline{\ell_0}})^{\ell_3} \quad \blacktriangleright_{\overline{\mathsf{C}}} \quad (\mathsf{stat}\ b_0\ (\mathsf{fst}\{\tau_1\}\ (v_0)^{\ell_2}))^{\overline{\ell_0}\ell_3}$$

where $\tau_1 = fst(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$

$$(\mathsf{snd}\{\mathcal{U}\}\ (\!(\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2})\!)^{\overline{\ell_0}})^{\ell_3} \quad \blacktriangleright_{\overline{\mathsf{C}}} \quad (\mathsf{stat}\ b_0\ (\mathsf{snd}\{\tau_1\}\ (v_0)^{\ell_2}))^{\overline{\ell_0}\ell_3}$$

where $\tau_1 = snd(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$

$$(binop\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ (\!(v_1)\!)^{\overline{\ell_1}})^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{C}}} \quad (\mathsf{TagErr})^{\ell_0}$$

if $v_0 \notin (v)^{\ell}$ and $v_1 \notin (v)^{\ell}$ and $\delta(binop, v_0, v_1)$ is undefined

$$(binop\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ (\!(v_1)\!)^{\overline{\ell_1}})^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{C}}} \quad (\delta(binop, v_0, v_1))^{\ell_0}$$

if $\delta(binop, v_0, v_1)$ is defined

$$(\mathsf{app}\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ v_1)^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{C}}} \quad (\mathsf{TagErr})^{\ell_0}$$

if $v_0 \notin (\lambda x.\, e) \cup (\mathbb{G}\ b\ v)$

$$(\mathsf{app}\{\mathcal{U}\}\ (\!(\lambda x_0.\, e_0)\!)^{\overline{\ell_0}}\ v_1)^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{C}}} \quad (\!(e_0[x_0 \leftarrow (\!(v_1)\!)^{\ell_0 rev(\overline{\ell_0})}])\!)^{\overline{\ell_0}\ell_0}$$

$$(\mathsf{app}\{\mathcal{U}\}\ (\!(\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2})\!)^{\overline{\ell_0}}\ v_1)^{\ell_3} \quad \blacktriangleright_{\overline{\mathsf{C}}}$$

$$(\!(\mathsf{stat}\ b_0\ (\mathsf{app}\{\tau_1\}\ v_0\ (\mathsf{dyn}\ b_1\ (\!(v_1)\!)^{\ell_3 rev(\overline{\ell_0})}))^{\ell_2})\!)^{\overline{\ell_0}\ell_3}$$

where $b_0 = (\ell_0 \blacktriangleleft cod(\tau_0) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft dom(\tau_0) \blacktriangleleft \ell_0)$ and $\tau_1 = cod(\tau_0)$

$$(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell_0}})^{\ell_2} \quad \blacktriangleright_{\overline{\mathsf{C}}} \quad (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell_0}})^{\ell_2}$$

if $shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$ and $v_0 \in \langle v, v \rangle \cup (\lambda(x : \tau).\, e) \cup (\mathbb{G}\ b\ v)$

$$(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(i_0)\!)^{\overline{\ell_2}})^{\ell_3} \quad \blacktriangleright_{\overline{\mathsf{C}}} \quad (i_0)^{\ell_3}$$

if $shape\text{-}match(\lfloor \tau_0 \rfloor, i_0)$

$$(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell_2}})^{\ell_2} \quad \blacktriangleright_{\overline{\mathsf{C}}} \quad (\mathsf{InvariantErr})^{\ell_2}$$

if $\neg shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$

Theorem 6.27 (Co-Natural complete monitoring). *Co-Natural satisfies* **CM**

Proof Sketch. By preservation of single-owner consistency ($\Vdash$) for $\rhd_{\overline{C}}$ and $\blacktriangleright_{\overline{C}}$. More details in appendix: lemma A.6. □

Lemma 6.28 (Co-Natural blame soundness and completeness). *If* e_0 *is well-formed and* $e_0 \rightarrow^*_{C} \mathsf{BoundaryErr}\,(\overline{b}_0, v_0)$*, then* $senders\,(\overline{b}_0) = owners\,(v_0)$ *and furthermore* $\overline{b}_0$ *contains exactly one boundary specification.*

Proof. By complete monitoring (theorem 6.27) and the definition of $\rightarrow^*_{C}$. There is one rule that produces a boundary error; it blames a single boundary. Complete monitoring guarantees that the component names and labels match. □

Corollary 6.29. *Co-Natural satisfies* **BS** *and* **BC**

6.6.3 Relation to Natural.

$\boxed{v \lesssim v}$

$$\frac{}{i_0 \lesssim i_0} \qquad \frac{v_0 \lesssim v_2 \qquad v_1 \lesssim v_3}{\langle v_0, v_1\rangle \lesssim \langle v_2, v_3\rangle} \qquad \frac{v_0 \lesssim \mathbb{G}^{+?}\,\mathsf{fst}\,(\overline{b}_0)\; v_2 \qquad v_1 \lesssim \mathbb{G}^{+?}\,\mathsf{snd}\,(\overline{b}_0)\; v_3}{\langle v_0, v_1\rangle \lesssim \mathbb{G}^{+}\,\overline{b}_0\,\langle v_2, v_3\rangle}$$

$$\frac{e_0 \lesssim e_1}{\lambda x_0.\, e_0 \lesssim \lambda x_0.\, e_1} \qquad \frac{e_0 \lesssim e_1}{\lambda (x_0 : \tau_0).\, e_0 \lesssim \lambda (x_0 : \tau_0).\, e_1} \qquad \frac{v_0 \lesssim v_1}{\mathbb{G}\; b_0\; v_0 \lesssim \mathbb{G}\; b_0\; v_1}$$

$\boxed{e \lesssim e}$

$$\frac{}{x_0 \lesssim x_0} \qquad \frac{e_0 \lesssim e_2 \qquad e_1 \lesssim e_3}{\langle e_0, e_1\rangle \lesssim \langle e_2, e_3\rangle} \qquad \frac{e_0 \lesssim e_2 \qquad e_1 \lesssim e_3}{\mathsf{app}\{{}^{\tau}\!/\mathcal{U}\}\; e_0\; e_1 \lesssim \mathsf{app}\{{}^{\tau}\!/\mathcal{U}\}\; e_2\; e_3}$$

$$\frac{e_0 \lesssim e_1}{\mathit{unop}\{{}^{\tau}\!/\mathcal{U}\}\; e_0 \lesssim \mathit{unop}\{{}^{\tau}\!/\mathcal{U}\}\; e_1} \qquad \frac{e_0 \lesssim e_2 \qquad e_1 \lesssim e_3}{\mathit{binop}\{{}^{\tau}\!/\mathcal{U}\}\; e_0\; e_1 \lesssim \mathit{binop}\{{}^{\tau}\!/\mathcal{U}\}\; e_2\; e_3} \qquad \frac{e_0 \lesssim e_1}{\mathsf{dyn}\; b_0\; e_0 \lesssim \mathsf{dyn}\; b_1\; e_1}$$

$$\frac{e_0 \lesssim e_1}{\mathsf{stat}\; b_0\; e_0 \lesssim \mathsf{stat}\; b_1\; e_1} \qquad \frac{}{\mathsf{InvariantErr} \lesssim \mathsf{InvariantErr}} \qquad \frac{}{\mathsf{TagErr} \lesssim \mathsf{TagErr}}$$

$$\frac{}{\mathsf{DivErr} \lesssim \mathsf{DivErr}} \qquad \frac{}{\mathsf{BoundaryErr}\,(b_0, v_0) \lesssim e_1}$$

$\boxed{E \lesssim E}$

$$\frac{}{[\,] \lesssim [\,]} \qquad \frac{E_0 \lesssim E_2 \qquad e_1 \lesssim e_3}{\langle E_0, e_1\rangle \lesssim \langle E_2, e_3\rangle} \qquad \frac{v_0 \lesssim v_2 \qquad E_1 \lesssim E_3}{\langle v_0, E_1\rangle \lesssim \langle v_2, E_3\rangle} \qquad \frac{E_0 \lesssim E_2 \qquad e_1 \lesssim e_3}{\mathsf{app}\{{}^{\tau}\!/\mathcal{U}\}\; E_0\; e_1 \lesssim \mathsf{app}\{{}^{\tau}\!/\mathcal{U}\}\; E_2\; e_3}$$

$$\frac{v_0 \lesssim v_2 \qquad E_1 \lesssim E_3}{\mathsf{app}\{{}^{\tau}\!/\mathcal{U}\}\; v_0\; E_1 \lesssim \mathsf{app}\{{}^{\tau}\!/\mathcal{U}\}\; v_2\; E_3} \qquad \frac{E_0 \lesssim E_1}{\mathit{unop}\{{}^{\tau}\!/\mathcal{U}\}\; E_0 \lesssim \mathit{unop}\{{}^{\tau}\!/\mathcal{U}\}\; E_1}$$

$$\frac{E_0 \lesssim E_2 \qquad e_1 \lesssim e_3}{\mathit{binop}\{{}^{\tau}\!/\mathcal{U}\}\; E_0\; e_1 \lesssim \mathit{binop}\{{}^{\tau}\!/\mathcal{U}\}\; E_2\; e_3} \qquad \frac{v_0 \lesssim v_2 \qquad E_1 \lesssim E_3}{\mathit{binop}\{{}^{\tau}\!/\mathcal{U}\}\; v_0\; E_1 \lesssim \mathit{binop}\{{}^{\tau}\!/\mathcal{U}\}\; v_2\; E_3}$$

$$\frac{b_0 \leqslant: b_1 \qquad E_0 \lesssim E_1}{\mathsf{dyn}\; b_0\; E_0 \lesssim \mathsf{dyn}\; b_1\; E_1} \qquad \frac{b_0 \leqslant: b_1 \qquad E_0 \lesssim E_1}{\mathsf{stat}\; b_0\; E_0 \lesssim \mathsf{stat}\; b_1\; E_1} \qquad \frac{b_0 \leqslant: b_2 \qquad b_1 \leqslant: b_3 \qquad E_0 \lesssim \mathsf{trace}\; \overline{b}_4\; E_1}{\mathsf{stat}\; b_0\; (\mathsf{dyn}\; b_1\; E_0) \lesssim \mathsf{trace}\; b_2 b_3 \overline{b}_4\; E_1}$$

$\boxed{\mathsf{fst} : \overline{b} \longrightarrow \overline{b}}$

$\mathsf{fst}\,((\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1) \cdots (\ell_n \blacktriangleleft (\tau_n \times \tau_{n+1}) \blacktriangleleft \ell_{n+1})) = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \cdots (\ell_n \blacktriangleleft \tau_n) \blacktriangleleft \ell_{n+1})$

$\boxed{\mathsf{snd} : \overline{b} \longrightarrow \overline{b}}$

$\mathsf{snd}\,((\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1) \cdots (\ell_n \blacktriangleleft (\tau_n \times \tau_{n+1}) \blacktriangleleft \ell_{n+1})) = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) \cdots (\ell_n \blacktriangleleft \tau_{n+1}) \blacktriangleleft \ell_{n+1})$

$\boxed{\mathbb{G}^{?}\;\cdot\;\cdot : b \times v \longrightarrow v}$

$$\mathbb{G}^{?}\; b_0\; v_0 = \begin{cases} v_0 & \text{if } v_0 \in i \\ \mathbb{G}\; b_0\; v_0 & \text{otherwise} \end{cases}$$

$$\mathbb{G}^{+}\; b_0 \cdots b_n\; v_0 = v_1 \iff v_1 = \mathbb{G}\; b_0\; (\cdots (\mathbb{G}\; b_n\; v_0) \cdots)$$

Theorem 6.30 (Natural Co-Natural error preorder). $N \lesssim C$

Proof. By lemma 6.32 and that $e_0 \lesssim \text{BoundaryErr}\,(\overline{b}_1, v_1)$ implies $e_0 \in \text{BoundaryErr}\,(b, v)$. □

Theorem 6.31. $C \not\lesssim N$

Proof. Let e_0 import an untyped pair into a typed context.

$e_0 = \text{dyn}\,(\ell_0 \blacktriangleleft \text{Nat}{\times}\text{Nat} \blacktriangleleft \ell_1)\,\langle -2, 2\rangle$

Natural raises a boundary error and Co-Natural computes a natural number. □

Lemma 6.32.

- *If* $e_0 \lesssim e_2$ *and* $e_0 \rightarrow_{\text{N}} e_1$ *then* $\exists\, e_3, e_4$ *such that* $e_1 \rightarrow^*_{\text{N}} e_3$ *and* $e_2 \rightarrow^*_{\text{C}} e_4$ *and* $e_3 \lesssim e_4$*.*
- *If* $e_0 \lesssim e_2$ *and* $e_2 \rightarrow_{\text{C}} e_3$ *then* $\exists\, e_1, e_4$ *such that* $e_3 \rightarrow^*_{\text{C}} e_4$ *and* $e_0 \rightarrow^*_{\text{N}} e_1$ *and* $e_1 \lesssim e_4$

Proof Sketch. For the most part, both move in lock-step. Natural takes additional steps when a pair reaches a boundary and Co-Natural simply creates a wrapper. Co-Natural takes additional steps (to catch up) when eliminating a wrapped pair. The $\lesssim$ relation shows how unwrapped pairs match wrapped pairs in a controlled way. More details in appendix: lemma A.7. □

6.7 Forgetful and its Properties

Unlike the paper, this forgetful semantics uses trace wrappers in the same way as the Amnesic semantics to satisfy (path-based) blame completeness.

6.7.1 Semantics, Type Soundness.

$\boxed{e \rhd_{\mathsf{F}} e}$

$unop\{\tau_0\}\, v_0 \quad \rhd_{\mathsf{F}} \quad \mathsf{InvariantErr}$
  if $v_0 \notin (\mathbb{G}\, (\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell)\, v)$ and $\delta(unop, v_0)$ is undefined

$unop\{\tau_0\}\, v_0 \quad \rhd_{\mathsf{F}} \quad \delta(unop, v_0)$
  if $\delta(unop, v_0)$ is defined

$\mathsf{fst}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0) \quad \rhd_{\mathsf{F}} \quad \mathsf{dyn}\; b_0\; (\mathsf{fst}\{\mathcal{U}\}\, v_0)$
  where $\tau_2 = \mathit{fst}(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$

$\mathsf{snd}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0 \quad \rhd_{\mathsf{F}} \quad \mathsf{dyn}\; b_0\; (\mathsf{snd}\{\mathcal{U}\}\, v_0)$
  where $\tau_2 = \mathit{snd}(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$

$binop\{\tau_0\}\, v_0\, v_1 \quad \rhd_{\mathsf{F}} \quad \mathsf{InvariantErr}$
  if $\delta(binop, v_0, v_1)$ is undefined

$binop\{\tau_0\}\, v_0\, v_1 \quad \rhd_{\mathsf{F}} \quad \delta(binop, v_0, v_1)$
  if $\delta(binop, v_0, v_1)$ is defined

$\mathsf{app}\{\tau_0\}\, v_0\, v_1 \quad \rhd_{\mathsf{F}} \quad \mathsf{InvariantErr}$
  if $v_0 \notin (\lambda(x : \tau).\, e) \cup (\mathbb{G}\, (\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell)\, v)$

$\mathsf{app}\{\tau_0\}\, (\lambda(x_0 : \tau_1).\, e_0)\, v_0 \quad \rhd_{\mathsf{F}} \quad e_0[x_0 \leftarrow v_0]$

$\mathsf{app}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0)\, v_1 \quad \rhd_{\mathsf{F}} \quad \mathsf{dyn}\; b_0\; (\mathsf{app}\{\mathcal{U}\}\, v_0\, (\mathsf{stat}\; b_1\; v_1))$
  where $b_0 = (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)$

$\mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \quad \rhd_{\mathsf{F}} \quad \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0$
  if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
  and $v_0 \in (\mathbb{T}_?\, \overline{b}\, (\lambda(x : \tau).\, e)) \cup (\mathbb{T}_?\, \overline{b}\, \langle v, v \rangle) \cup (\mathbb{T}_?\, \overline{b}\, (\mathbb{G}\, (\ell \blacktriangleleft \tau \blacktriangleleft \ell)\, v))$

$\mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; (\mathbb{T}_?\, \overline{b_0}\, i_0) \quad \rhd_{\mathsf{F}} \quad i_0$
  if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, i_0)$

$\mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \quad \rhd_{\mathsf{F}} \quad \mathsf{BoundaryErr}\, ((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b}_0, v_0)$
  if $\neg \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$ and $\overline{b}_0 = \mathit{get\text{-}trace}(v_0)$

$\boxed{e \blacktriangleright_{\mathsf{F}} e}$

$unop\{\mathcal{U}\}\ v_0 \quad \blacktriangleright_{\mathsf{F}}\ \mathsf{TagErr}$
  if $v_1 = \textit{rem-trace}(v_0)$ and $v_1 \notin (\mathbb{G}\,(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell)\ v)$ and $\delta(unop, v_1)$ is undefined

$unop\{\mathcal{U}\}\ v_0 \quad \blacktriangleright_{\mathsf{F}}\ \textit{add-trace}(\textit{get-trace}(v_0), \delta(unop, v_1))$
  if $v_1 = \textit{rem-trace}(v_0)$ and $\delta(unop, v_1)$ is defined

$\mathsf{fst}\{\mathcal{U}\}\ (\mathbb{T}_?\,\overline{b_0}\ (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)) \quad \blacktriangleright_{\mathsf{F}}\ \mathsf{trace}\,\overline{b_0}\ (\mathsf{stat}\ b_0\ (\mathsf{fst}\{\tau_1\}\ v_0))$
  where $\tau_1 = \textit{fst}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$

$\mathsf{snd}\{\mathcal{U}\}\ (\mathbb{T}_?\,\overline{b_0}\ (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)) \quad \blacktriangleright_{\mathsf{F}}\ \mathsf{trace}\,\overline{b_0}\ (\mathsf{stat}\ b_0\ (\mathsf{snd}\{\tau_1\}\ v_0))$
  where $\tau_1 = \textit{snd}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$

$binop\{\mathcal{U}\}\ v_0\ v_1 \quad \blacktriangleright_{\mathsf{F}}\ \mathsf{TagErr}$
  if $v_2 = \textit{rem-trace}(v_0)$ and $v_3 = \textit{rem-trace}(v_1)$ and $\delta(binop, v_2, v_3)$ is undefined

$binop\{\mathcal{U}\}\ v_0\ v_1 \quad \blacktriangleright_{\mathsf{F}}\ \delta(binop, v_2, v_3)$
  if $v_2 = \textit{rem-trace}(v_0)$ and $v_3 = \textit{rem-trace}(v_1)$ and $\delta(binop, v_2, v_3)$ is defined

$\mathsf{app}\{\mathcal{U}\}\ v_0\ v_1 \quad \blacktriangleright_{\mathsf{F}}\ \mathsf{TagErr}$
  if $v_0 \notin (\mathbb{T}_?\,\overline{b}\,(\lambda x.\, e)) \cup (\mathbb{T}_?\,\overline{b}\,(\mathbb{G}\,(\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell)\ v))$

$\mathsf{app}\{\mathcal{U}\}\ (\mathbb{T}_?\,\overline{b_0}\ (\lambda x_0.\, e_0))\ v_0 \quad \blacktriangleright_{\mathsf{F}}\ \mathsf{trace}\,\overline{b_0}\ (e_0[x_0 \leftarrow v_1])$
  where $v_1 = \textit{add-trace}(\textit{rev}(\overline{b_0}), v_0)$

$\mathsf{app}\{\mathcal{U}\}\ (\mathbb{T}_?\,\overline{b_0}\ (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0))\ v_1 \quad \blacktriangleright_{\mathsf{F}}\ \mathsf{trace}\,\overline{b_0}\ (\mathsf{stat}\ b_0\ (\mathsf{app}\{\tau_1\}\ v_0\ (\mathsf{dyn}\ b_1\ v_2)))$
  where $\tau_1 = \textit{cod}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft \textit{dom}(\tau_0) \blacktriangleleft \ell_0)$
  and $v_2 = \textit{add-trace}(\textit{rev}(\overline{b_0}), v_1)$

$\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \quad \blacktriangleright_{\mathsf{F}}\ \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0$
  if $\textit{shape-match}(\lfloor \tau_0 \rfloor, v_0)$ and $v_0 \in (\lambda(x : \tau).\, e) \cup \langle v, v \rangle$

$\mathsf{stat}\ b_0\ (\mathbb{G}\,b_1\ (\mathbb{T}_?\,\overline{b_0}\ v_0)) \quad \blacktriangleright_{\mathsf{F}}\ \mathsf{trace}\,(b_0 b_1 \overline{b_0})\ v_0$
  if $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$ and $\textit{shape-match}(\lfloor \tau_0 \rfloor, v_0)$
  and $v_0 \in (\lambda x.\, e) \cup \langle v, v \rangle \cup (\mathbb{G}\,b\ (\lambda(x : \tau).\, e)) \cup (\mathbb{G}\,b\ \langle v, v \rangle)$

$\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ i_0 \quad \blacktriangleright_{\mathsf{F}}\ i_0$
  if $\textit{shape-match}(\lfloor \tau_0 \rfloor, i_0)$

$\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \quad \blacktriangleright_{\mathsf{F}}\ \mathsf{InvariantErr}$
  if $\neg\textit{shape-match}(\lfloor \tau_0 \rfloor, v_0)$

$\mathsf{trace}\,\overline{b_0}\ v_0 \quad \blacktriangleright_{\mathsf{F}}\ v_1$
  where $v_1 = \textit{add-trace}(\overline{b_0}, v_0)$

$\boxed{e \rightarrow^*_{\mathsf{F}} e}$ is the transitive, reflexive, compatible (with respect to evaluation contexts E, section 6.2) closure of the relation $\bigcup\{\rhd_{\mathsf{F}}, \blacktriangleright_{\mathsf{F}}\}$

$\boxed{F(e)}$ holds for typed expressions with at most two guard wrappers and for untyped expressions with at most one guard wrapper. More precisely:

$$F(e_0) = \begin{cases} \mathsf{True} \ \text{ if } \cdot \vdash_1 e_0 : \tau_0 \text{ and } \cdot \vdash_{FS} e_0 : \tau_0 \\ \mathsf{True} \ \text{ if } \cdot \vdash_1 e_0 : \mathcal{U} \text{ and } \cdot \vdash_{FD} e_0 : \mathcal{U} \\ \mathsf{False} \text{ otherwise} \end{cases}$$

$\boxed{\Gamma \vdash_{FS} e : \tau}$

$$\frac{}{\Gamma_0 \vdash_{FS} x_0 : \tau_0} \qquad \frac{}{\Gamma_0 \vdash_{FS} n_0 : \mathsf{Nat}} \qquad \frac{}{\Gamma_0 \vdash_{FS} i_0 : \mathsf{Int}} \qquad \frac{(x_0 : \tau_0), \Gamma_0 \vdash_{FS} e_0 : \tau_1}{\Gamma_0 \vdash_{FS} \lambda(x_0 : \tau_0).\, e_0 : \tau_0 \Rightarrow \tau_1}$$

$$\frac{\Gamma_0 \vdash_{FS} e_0 : \tau_0 \qquad \Gamma_0 \vdash_{FS} e_1 : \tau_1}{\Gamma_0 \vdash_{FS} \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \qquad \frac{\Gamma_0 \vdash_{FS} e_0 : \tau_1}{\Gamma_0 \vdash_{FS} \mathit{unop}\{\tau_0\}\, e_0 : \tau_0} \qquad \frac{\Gamma_0 \vdash_{FS} e_0 : \tau_1 \qquad \Gamma_0 \vdash_{FS} e_1 : \tau_2}{\Gamma_0 \vdash_{FS} \mathit{binop}\{\tau_0\}\, e_0\, e_1 : \tau_0}$$

$$\frac{\Gamma_0 \vdash_{FS} e_0 : \tau_1 \Rightarrow \tau_2 \qquad \Gamma_0 \vdash_{FS} e_1 : \tau_1}{\Gamma_0 \vdash_{FS} \mathsf{app}\{\tau_0\}\, e_0\, e_1 : \tau_0} \qquad \frac{\Gamma_0 \vdash_{FD} e_0 : \mathcal{U}}{\Gamma_0 \vdash_{FS} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, e_0 : \tau_0}$$

$$\frac{\Gamma_0 \vdash_{FS} e_0 : \tau_1 \qquad \tau_1 \leqslant: \tau_0}{\Gamma_0 \vdash_{FS} e_0 : \tau_0} \qquad \frac{\Gamma_0 \vdash_{FD} \langle v_0, v_1 \rangle : \mathcal{U}}{\Gamma_0 \vdash_{FS} \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1)\, \langle v_0, v_1 \rangle : \tau_0 \times \tau_1}$$

$$\frac{\Gamma_0 \vdash_{FD} \lambda x_0.\, e_0 : \mathcal{U}}{\Gamma_0 \vdash_{FS} \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\, (\lambda x_0.\, e_0) : \tau_0 \Rightarrow \tau_1}$$

$$\frac{\Gamma_0 \vdash_{FS} \langle v_0, v_1 \rangle : \tau_2 \times \tau_3}{\Gamma_0 \vdash_{FS} \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1)\, (\mathbb{G}\, (\ell_2 \blacktriangleleft (\tau_2 \times \tau_3) \blacktriangleleft \ell_3)\, \langle v_0, v_1 \rangle) : \tau_0 \times \tau_1}$$

$$\frac{\Gamma_0 \vdash_{FS} \lambda(x_0 : \tau_4).\, e_0 : \tau_2 \Rightarrow \tau_3}{\Gamma_0 \vdash_{FS} \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\, (\mathbb{G}\, (\ell_2 \blacktriangleleft (\tau_2 \Rightarrow \tau_3) \blacktriangleleft \ell_3)\, (\lambda(x_0 : \tau_4).\, e_0)) : (\tau_0 \Rightarrow \tau_1)} \qquad \frac{}{\Gamma_0 \vdash_{FS} \mathsf{Err} : \tau_0}$$

$\boxed{\Gamma \vdash_{FD} e : \mathcal{U}}$

$$\frac{}{\Gamma_0 \vdash_{FD} x_0 : \mathcal{U}} \qquad \frac{}{\Gamma_0 \vdash_{FD} i_0 : \mathcal{U}} \qquad \frac{(x_0 : \mathcal{U}), \Gamma_0 \vdash_{FD} e_0 : \mathcal{U}}{\Gamma_0 \vdash_{FD} \lambda x_0.\, e_0 : \mathcal{U}} \qquad \frac{\Gamma_0 \vdash_{FD} e_0 : \mathcal{U} \qquad \Gamma_0 \vdash_{FD} e_1 : \mathcal{U}}{\Gamma_0 \vdash_{FD} \langle e_0, e_1 \rangle : \mathcal{U}}$$

$$\frac{\Gamma_0 \vdash_{FD} e_0 : \mathcal{U}}{\Gamma_0 \vdash_{FD} \mathit{unop}\{\mathcal{U}\}\, e_0 : \mathcal{U}} \qquad \frac{\Gamma_0 \vdash_{FD} e_0 : \mathcal{U} \qquad \Gamma_0 \vdash_{FD} e_1 : \mathcal{U}}{\Gamma_0 \vdash_{FD} \mathit{binop}\{\mathcal{U}\}\, e_0\, e_1 : \mathcal{U}}$$

$$\frac{\Gamma_0 \vdash_{FD} e_0 : \mathcal{U} \qquad \Gamma_0 \vdash_{FD} e_1 : \mathcal{U}}{\Gamma_0 \vdash_{FD} \mathsf{app}\{\mathcal{U}\}\, e_0\, e_1 : \mathcal{U}} \qquad \frac{\Gamma_0 \vdash_{FS} e_0 : \tau_0}{\Gamma_0 \vdash_{FD} \mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, e_0 : \mathcal{U}}$$

$$\frac{\Gamma_0 \vdash_{FS} \langle v_0, v_1 \rangle : \tau_0 \times \tau_1}{\Gamma_0 \vdash_{FD} \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1)\, \langle v_0, v_1 \rangle : \mathcal{U}} \qquad \frac{\Gamma_0 \vdash_{FS} \lambda(x_0 : \tau_2).\, e_0 : \tau_0 \Rightarrow \tau_1}{\Gamma_0 \vdash_{FD} \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\, (\lambda(x_0 : \tau_2).\, e_0) : \mathcal{U}}$$

$$\frac{\Gamma_0 \vdash_{FD} v_0 : \mathcal{U}}{\Gamma_0 \vdash_{FD} \mathbb{T}\, \overline{b}_0\, v_0 : \mathcal{U}} \qquad \frac{\Gamma_0 \vdash_{FD} e_0 : \mathcal{U}}{\Gamma_0 \vdash_{FD} \mathsf{trace}\, \overline{b}_0\, e_0 : \mathcal{U}} \qquad \frac{}{\Gamma_0 \vdash_{FD} \mathsf{Err} : \mathcal{U}}$$

Theorem 6.33 (Forgetful type soundness). *Forgetful satisfies* **TS (1)**

Proof. By lemma 6.34, progress (lemma 6.35), and preservation (lemma 6.36). □

Lemma 6.34. *If* $e_0 : {}^{\tau}/_{\mathcal{U}}$ **wf** *then* $F(e_0)$.

Proof. Wrappers are not part of the surface language. □

Lemma 6.35 (Forgetful type progress). *If* $\cdot \vdash_1 E_0[e_0] : {}^{\tau}/_{\mathcal{U}}$ *and* $F(E_0[e_0])$ *then one of the following holds:*

- $e_0 \in v \cup \mathsf{Err}$
- ${}^{\tau}/_{\mathcal{U}} \in \tau$ *and* $\exists\, e_1.\ e_0 \vartriangleright_{\mathsf{F}} e_1$
- ${}^{\tau}/_{\mathcal{U}} \in \mathcal{U}$ *and* $\exists\, e_1.\ e_0 \blacktriangleright_{\mathsf{F}} e_1$

Proof Sketch. By unique decomposition (lemma 6.1) and case analysis. More details in appendix: lemma A.14. □

Lemma 6.36 (Forgetful type preservation).
If $\cdot \vdash_1 E_0[e_0] : {}^{\tau}/_{\mathcal{U}}$ *and* $F(E_0[e_0])$ *and* $e_0(\vartriangleright_{\mathsf{F}} \cup \blacktriangleright_{\mathsf{F}})e_1$ *then* $\cdot \vdash_1 E_0[e_1] : {}^{\tau}/_{\mathcal{U}}$ *and* $F(E_0[e_1])$.

Proof Sketch. By case analysis of each reduction relation. An interesting case is the $\blacktriangleright_{\mathsf{F}}$ rule that removes a guard wrapper; the rule preserves soundness because it unwraps an untyped value in an untyped context. More details in appendix: lemma A.15. □

Lemma 6.37.

- *If* $F(E_0[e_0])$ *then* $F(e_0)$
- *If* $F(E_0[e_0])$ *and* $F(e_1)$ *then* $F(E_0[e_1])$

Proof Sketch. By induction on the structure of E_0. □

6.7.2 *Lifted Semantics, Complete Monitoring, Blame.*

$\boxed{(e)^{\ell} \rhd_{\overline{\mathsf{F}}} (e)^{\ell}}$ lifted version of $\rhd_{\mathsf{F}}$

$$(\mathit{unop}\{\tau_0\}\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_0} \quad \rhd_{\overline{\mathsf{F}}} \quad (\mathsf{InvariantErr})^{\ell_0}$$
if $v_0 \notin (v)^{\ell} \cup (\mathbb{G}\ (\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell)\ v)$ and $\delta(\mathit{unop}, v_0)$ is undefined

$$(\mathit{unop}\{\tau_0\}\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_0} \quad \rhd_{\overline{\mathsf{F}}} \quad (\delta(\mathit{unop}, v_0))^{\overline{\ell}_0 \ell_0}$$
if $\delta(\mathit{unop}, v_0)$ is defined

$$(\mathsf{fst}\{\tau_0\}\ \llparenthesis \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_0})^{\ell_3} \quad \rhd_{\overline{\mathsf{F}}} \quad (\mathsf{dyn}\ b_0\ (\mathsf{fst}\{\mathcal{U}\}\ (v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$$
where $\tau_2 = \mathit{fst}(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$

$$(\mathsf{snd}\{\tau_0\}\ \llparenthesis \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_0})^{\ell_3} \quad \rhd_{\overline{\mathsf{F}}} \quad (\mathsf{dyn}\ b_0\ (\mathsf{snd}\{\mathcal{U}\}\ (v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$$
where $\tau_2 = \mathit{snd}(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$

$$(\mathit{binop}\{\tau_0\}\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}\ \llparenthesis v_1 \rrparenthesis^{\overline{\ell}_1})^{\ell_0} \quad \rhd_{\overline{\mathsf{F}}} \quad (\mathsf{InvariantErr})^{\ell_0}$$
if $v_0 \notin (v)^{\ell}$ and $v_1 \notin (v)^{\ell}$ and $\delta(\mathit{binop}, v_0, v_1)$ is undefined

$$(\mathit{binop}\{\tau_0\}\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}\ \llparenthesis v_1 \rrparenthesis^{\overline{\ell}_1})^{\ell_0} \quad \rhd_{\overline{\mathsf{F}}} \quad (\delta(\mathit{binop}, v_0, v_1))^{\ell_0}$$
if $\delta(\mathit{binop}, v_0, v_1)$ is defined

$$(\mathsf{app}\{\tau_0\}\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}\ v_1)^{\ell_0} \quad \rhd_{\overline{\mathsf{F}}} \quad (\mathsf{InvariantErr})^{\ell_0}$$
if $v_0 \notin (v)^{\ell} \cup (\lambda(x : \tau).\, e) \cup (\mathbb{G}\ b\ v)$

$$(\mathsf{app}\{\tau_0\}\ \llparenthesis \lambda(x_0 : \tau_1).\, e_0 \rrparenthesis^{\overline{\ell}_0}\ v_0)^{\ell_0} \quad \rhd_{\overline{\mathsf{F}}} \quad \llparenthesis e_0[x_0 \leftarrow \llparenthesis v_0 \rrparenthesis^{\ell_0 \mathit{rev}(\overline{\ell}_0)}] \rrparenthesis^{\overline{\ell}_0 \ell_0}$$

$$(\mathsf{app}\{\tau_0\}\ \llparenthesis \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_0}\ v_1)^{\ell_3} \quad \rhd_{\overline{\mathsf{F}}}$$
$$\llparenthesis (\mathsf{dyn}\ b_0\ (\mathsf{app}\{\mathcal{U}\}\ v_0\ (\mathsf{stat}\ b_1\ \llparenthesis v_1 \rrparenthesis^{\ell_3 \mathit{rev}(\overline{\ell}_0)})))^{\ell_2} \rrparenthesis^{\overline{\ell}_0 \ell_3}$$
where $b_0 = (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)$

$$(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_2} \quad \rhd_{\overline{\mathsf{F}}} \quad (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_2}$$
if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
and $v_0 \in (\mathbb{T}_?\ \overline{b}\ (\lambda(x : \tau).\, e)) \cup (\mathbb{T}_?\ \overline{b}\ \langle v, v \rangle) \cup (\mathbb{T}_?\ \overline{b}\ (\mathbb{G}\ (\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell)\ v))$

$$(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis \mathbb{T}_?\ \overline{b}_0\ \llparenthesis i_0 \rrparenthesis^{\overline{\ell}_0} \rrparenthesis^{\overline{\ell}_1})^{\ell_2} \quad \rhd_{\overline{\mathsf{F}}} \quad (i_0)^{\ell_2}$$
if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, i_0)$

$$(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_2})^{\ell_3} \quad \rhd_{\overline{\mathsf{F}}} \quad (\mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b}_0, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_2}))^{\ell_3}$$
if $\neg \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$ and $\overline{b}_0 = \mathit{get\text{-}trace}(v_0)$

$\boxed{(e)^{\ell} \blacktriangleright_{\overline{\mathsf{F}}} (e)^{\ell}}$ lifted version of $\blacktriangleright_{\mathsf{F}}$

$$(\mathit{unop}\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}})^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{F}}} \quad (\mathsf{TagErr})^{\ell_0}$$
if $v_0 \notin (v)^{\ell} \cup (\mathbb{G}\ (\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell)\ v)$ and $\delta(\mathit{unop}, v_0)$ is undefined

$$(\mathit{unop}\{\mathcal{U}\}\ v_0)^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{F}}}$$
$$(\mathit{add\text{-}trace}(\mathit{get\text{-}trace}(v_0), \delta(\mathit{unop}, v_1)))^{\ell_0}$$
if $v_1 = \mathit{rem\text{-}trace}(v_0)$ and $\delta(\mathit{unop}, v_1)$ is defined

$$(\mathsf{fst}\{\mathcal{U}\}\ (\!(\mathbb{T}_?\ \overline{b_0}\ (\!(\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2})\!)^{\overline{\ell_3}})\!)^{\overline{\ell_4}})^{\ell_5} \quad \blacktriangleright_{\overline{\mathsf{F}}} \quad (\mathsf{trace}\ \overline{b_0}\ (\!(\mathsf{stat}\ b_0\ (\mathsf{fst}\{\tau_1\}\ v_0)^{\ell_2})\!)^{\overline{\ell_3}})^{\overline{\ell_4}\ell_5}$$
where $\tau_1 = \mathit{fst}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$

$$(\mathsf{snd}\{\mathcal{U}\}\ (\!(\mathbb{T}_?\ \overline{b_0}\ (\!(\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2})\!)^{\overline{\ell_3}})\!)^{\overline{\ell_4}})^{\ell_5} \quad \blacktriangleright_{\overline{\mathsf{F}}} \quad (\mathsf{trace}\ \overline{b_0}\ (\!(\mathsf{stat}\ b_0\ (\mathsf{snd}\{\tau_1\}\ v_0)^{\ell_2})\!)^{\overline{\ell_3}})^{\overline{\ell_4}\ell_5}$$
where $\tau_1 = \mathit{snd}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$

$$(\mathit{binop}\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ (\!(v_1)\!)^{\overline{\ell_1}})^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{F}}} \quad (\mathsf{TagErr})^{\ell_0}$$
if $v_2 = \mathit{rem\text{-}trace}(v_0)$ and $v_3 = \mathit{rem\text{-}trace}(v_1)$ and $\delta(\mathit{binop}, v_2, v_3)$ is undefined

$$(\mathit{binop}\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ (\!(v_1)\!)^{\overline{\ell_1}})^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{F}}} \quad \delta(\mathit{binop}, v_2, v_3)$$
if $v_2 = \mathit{rem\text{-}trace}(v_0)$ and $v_3 = \mathit{rem\text{-}trace}(v_1)$ and $\delta(\mathit{binop}, v_2, v_3)$ is defined

$$(\mathsf{app}\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ v_1)^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{F}}} \quad (\mathsf{TagErr})^{\ell_0}$$
if $v_0 \notin (\mathbb{T}_?\ \overline{b}\ (\lambda x.\, e)) \cup (\mathbb{T}_?\ \overline{b}\ (\mathbb{G}\ (\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell)\ v))$

$$(\mathsf{app}\{\mathcal{U}\}\ (\!(\mathbb{T}_?\ \overline{b_0}\ (\!(\lambda x_0.\, e_0)\!)^{\overline{\ell_0}})\!)^{\overline{\ell_1}}\ v_0)^{\ell_2} \quad \blacktriangleright_{\overline{\mathsf{F}}} \quad (\mathsf{trace}\ \overline{b_0}\ (\!(e_0[x_0 \leftarrow v_1])\!)^{\overline{\ell_0}})^{\overline{\ell_1}\ell_2}$$
where $v_1 = \mathit{add\text{-}trace}(\mathit{rev}(\overline{b_0}), (\!(v_0)\!)^{\ell_2 \mathit{rev}(\overline{\ell_1}) \mathit{rev}(\overline{\ell_0})})$

$$(\mathsf{app}\{\mathcal{U}\}\ (\!(\mathbb{T}_?\ \overline{b_0}\ (\!(\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2})\!)^{\overline{\ell_3}})\!)^{\overline{\ell_4}}\ v_1)^{\ell_5} \quad \blacktriangleright_{\overline{\mathsf{F}}}$$
$$(\!(\mathsf{trace}\ \overline{b_0}\ (\!(\mathsf{stat}\ b_0\ (\mathsf{app}\{\tau_1\}\ v_0\ (\mathsf{dyn}\ b_1\ v_2))^{\ell_2})\!)^{\overline{\ell_3}})\!)^{\overline{\ell_4}\ell_5}$$
where $\tau_1 = \mathit{cod}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)$
and $v_2 = \mathit{add\text{-}trace}(\mathit{rev}(\overline{b_0}), (\!(v_1)\!)^{\ell_5 \mathit{rev}(\overline{\ell_3}\overline{\ell_4})})$

$$(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)^{\ell_2} \quad \blacktriangleright_{\overline{\mathsf{F}}} \quad (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)^{\ell_2}$$
if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$ and $v_0 \in (\!(\lambda(x : \tau).\, e)\!)^{\overline{\ell}} \cup (\!(\langle v, v \rangle)\!)^{\overline{\ell}}$

$$(\mathsf{stat}\ b_0\ (\!(\mathbb{G}\ b_1\ (\!(\mathbb{T}_?\ \overline{b_2}\ v_0)\!)^{\overline{\ell_0}})\!)^{\overline{\ell_1}})^{\ell_2} \quad \blacktriangleright_{\overline{\mathsf{F}}} \quad (\mathsf{trace}\ (b_0 b_1 \overline{b_2})\ (\!(v_0)\!)^{\overline{\ell_0}\overline{\ell_1}\ell_2})^{\ell_2}$$
if $b_0 = (\ell_3 \blacktriangleleft \tau_0 \blacktriangleleft \ell_4)$ and $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
and $v_0 \in (\!(\lambda x.\, e)\!)^{\overline{\ell}} \cup (\!(\langle v, v \rangle)\!)^{\overline{\ell}} \cup (\!(\mathbb{G}\ b\ (\lambda(x : \tau).\, e))\!)^{\overline{\ell}} \cup (\!(\mathbb{G}\ b\ \langle v, v \rangle)\!)^{\overline{\ell}}$

$$(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(i_0)\!)^{\overline{\ell_2}})^{\ell_3} \quad \blacktriangleright_{\overline{\mathsf{F}}} \quad (i_0)^{\ell_3}$$
if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, i_0)$

$$(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell_2}})^{\ell_3} \quad \blacktriangleright_{\overline{\mathsf{F}}} \quad (\mathsf{InvariantErr})^{\ell_3}$$
if $\neg\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$

$$(\mathsf{trace}\ \overline{b_0}\ v_0)^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{F}}} \quad (v_1)^{\ell_0}$$
where $v_1 = \mathit{add\text{-}trace}(\overline{b_0}, v_0)$

Theorem 6.38 (Forgetful incomplete monitoring). *Forgetful does not satisfy* **CM**

Proof. The stat rule that removes an outer guard breaks single-owner consistency. One way to exercise this rule is to send an untyped function into typed code and back out again; on the way out, the function loses a wrapper and gains an owner. □

Theorem 6.39 (Forgetful blame soundness and completeness). *Forgetful satisfies* **BS** *and* **BC**

Proof Sketch. By preservation of path-owner consistency ($\Vdash_p$) for $\triangleright_{\overline{\mathsf{F}}}$ and $\blacktriangleright_{\overline{\mathsf{F}}}$. More details in appendix: lemma A.16. □

6.7.3 Relation to Co-Natural.

$\boxed{v \lesssim v}$

$$\frac{}{i_0 \lesssim i_0} \qquad \frac{}{i_0 \lesssim \mathbb{T}\,\overline{b_0}\,i_0} \qquad \frac{v_0 \lesssim v_2 \qquad v_1 \lesssim v_3}{\langle v_0, v_1\rangle \lesssim \langle v_2, v_3\rangle} \qquad \frac{e_0 \lesssim e_1}{\lambda x_0.\, e_0 \lesssim \lambda x_0.\, e_1}$$

$$\frac{e_0 \lesssim e_1}{\lambda(x_0 : \tau_0).\, e_0 \lesssim \lambda(x_0 : \tau_0).\, e_1} \qquad \frac{b_0 \leqslant: b_2 \qquad b_1 \leqslant: b_3 \qquad v_0 \lesssim v_1}{\mathbb{G}\,b_0\,(\mathbb{G}\,b_1\,v_0) \lesssim \mathbb{T}\,b_2 b_3\,v_1}$$

$$\frac{b_0 \leqslant: b_2 \qquad b_1 \leqslant: b_3 \qquad v_0 \lesssim \mathbb{T}\,\overline{b_4}\,v_1}{\mathbb{G}\,b_0\,(\mathbb{G}\,b_1\,v_0) \lesssim \mathbb{T}\,b_2 b_3 \overline{b_4}\,v_1} \qquad \frac{b_0 \leqslant: b_1 \qquad v_0 \lesssim v_1}{\mathbb{G}\,b_0\,v_0 \lesssim \mathbb{G}\,b_1\,v_1}$$

$\boxed{e \lesssim e}$

$$\frac{}{x_0 \lesssim x_0} \qquad \frac{e_0 \lesssim e_2 \qquad e_1 \lesssim e_3}{\langle e_0, e_1\rangle \lesssim \langle e_2, e_3\rangle} \qquad \frac{e_0 \lesssim e_2 \qquad e_1 \lesssim e_3}{\mathsf{app}\{^{\tau}/_{\mathcal{U}}\}\,e_0\,e_1 \lesssim \mathsf{app}\{^{\tau}/_{\mathcal{U}}\}\,e_2\,e_3}$$

$$\frac{e_0 \lesssim e_1}{\mathit{unop}\{^{\tau}/_{\mathcal{U}}\}\,e_0 \lesssim \mathit{unop}\{^{\tau}/_{\mathcal{U}}\}\,e_1} \qquad \frac{e_0 \lesssim e_2 \qquad e_1 \lesssim e_3}{\mathit{binop}\{^{\tau}/_{\mathcal{U}}\}\,e_0\,e_1 \lesssim \mathit{binop}\{^{\tau}/_{\mathcal{U}}\}\,e_2\,e_3} \qquad \frac{b_0 \leqslant: b_1 \qquad e_0 \lesssim e_1}{\mathsf{dyn}\,b_0\,e_0 \lesssim \mathsf{dyn}\,b_1\,e_1}$$

$$\frac{b_0 \leqslant: b_1 \qquad e_0 \lesssim e_1}{\mathsf{stat}\,b_0\,e_0 \lesssim \mathsf{stat}\,b_1\,e_1} \qquad \frac{b_0 \leqslant: b_2 \qquad b_1 \leqslant: b_3 \qquad e_0 \lesssim \mathsf{trace}\,\overline{b_4}\,e_1}{\mathsf{stat}\,b_0\,(\mathsf{dyn}\,b_1\,e_0) \lesssim \mathsf{trace}\,b_2 b_3 \overline{b_4}\,e_1}$$

$$\frac{}{\mathsf{InvariantErr} \lesssim \mathsf{InvariantErr}} \qquad \frac{}{\mathsf{TagErr} \lesssim \mathsf{TagErr}} \qquad \frac{}{\mathsf{DivErr} \lesssim \mathsf{DivErr}}$$

$$\frac{}{\mathsf{BoundaryErr}\,(b_0, v_0) \lesssim e_1}$$

$\boxed{E \lesssim E}$

$$\frac{}{[\,] \lesssim [\,]} \qquad \frac{E_0 \lesssim E_2 \qquad e_1 \lesssim e_3}{\langle E_0, e_1\rangle \lesssim \langle E_2, e_3\rangle} \qquad \frac{v_0 \lesssim v_2 \qquad E_1 \lesssim E_3}{\langle v_0, E_1\rangle \lesssim \langle v_2, E_3\rangle} \qquad \frac{E_0 \lesssim E_2 \qquad e_1 \lesssim e_3}{\mathsf{app}\{^{\tau}/_{\mathcal{U}}\}\,E_0\,e_1 \lesssim \mathsf{app}\{^{\tau}/_{\mathcal{U}}\}\,E_2\,e_3}$$

$$\frac{v_0 \lesssim v_2 \qquad E_1 \lesssim E_3}{\mathsf{app}\{^{\tau}/_{\mathcal{U}}\}\,v_0\,E_1 \lesssim \mathsf{app}\{^{\tau}/_{\mathcal{U}}\}\,v_2\,E_3} \qquad \frac{E_0 \lesssim E_1}{\mathit{unop}\{^{\tau}/_{\mathcal{U}}\}\,E_0 \lesssim \mathit{unop}\{^{\tau}/_{\mathcal{U}}\}\,E_1}$$

$$\frac{E_0 \lesssim E_2 \qquad e_1 \lesssim e_3}{\mathit{binop}\{^{\tau}/_{\mathcal{U}}\}\,E_0\,e_1 \lesssim \mathit{binop}\{^{\tau}/_{\mathcal{U}}\}\,E_2\,e_3} \qquad \frac{v_0 \lesssim v_2 \qquad E_1 \lesssim E_3}{\mathit{binop}\{^{\tau}/_{\mathcal{U}}\}\,v_0\,E_1 \lesssim \mathit{binop}\{^{\tau}/_{\mathcal{U}}\}\,v_2\,E_3}$$

$$\frac{b_0 \leqslant: b_1 \qquad E_0 \lesssim E_1}{\mathsf{dyn}\,b_0\,E_0 \lesssim \mathsf{dyn}\,b_1\,E_1} \qquad \frac{b_0 \leqslant: b_1 \qquad E_0 \lesssim E_1}{\mathsf{stat}\,b_0\,E_0 \lesssim \mathsf{stat}\,b_1\,E_1} \qquad \frac{b_0 \leqslant: b_2 \qquad b_1 \leqslant: b_3 \qquad E_0 \lesssim \mathsf{trace}\,\overline{b_4}\,E_1}{\mathsf{stat}\,b_0\,(\mathsf{dyn}\,b_1\,E_0) \lesssim \mathsf{trace}\,b_2 b_3 \overline{b_4}\,E_1}$$

Theorem 6.40 (Co-Natural Forgetful error preorder). $C \lesssim F$

Proof. By lemma 6.42 and that $e_0 \lesssim \mathsf{BoundaryErr}\,(\overline{b_1}, v_1)$ implies $e_0 \in \mathsf{BoundaryErr}\,(b, v)$. □

Theorem 6.41. $F \not\lesssim C$

Proof. If an untyped value travels to typed code and back again, Forgetful unwraps it but Co-Natural continues to enforce the type.

Let:

$e_0 = \mathsf{stat}\ b_0\ (\mathsf{dyn}\ (\ell_0 \blacktriangleleft (\mathsf{Nat} \Rightarrow \mathsf{Nat}) \blacktriangleleft \ell_1)\ (\lambda x_0.\, x_0))$

$e_1 = \mathsf{app}\{\mathcal{U}\}\ e_0\ \langle 2, 8\rangle$

Then $e_1 \rightarrow^*_{\mathsf{F}} \langle 2, 8\rangle$ and $e_1 \rightarrow^*_{\mathsf{C}} \mathsf{BoundaryErr}\,(\ldots)$. □

Lemma 6.42.

- *If $e_0 \lesssim e_2$ and $e_0 \rightarrow_{\mathsf{C}} e_1$ then $\exists\, e_3, e_4$ such that $e_1 \rightarrow^*_{\mathsf{C}} e_3$ and $e_2 \rightarrow^*_{\mathsf{F}} e_4$ and $e_3 \lesssim e_4$.*
- *If $e_0 \lesssim e_2$ and $e_2 \rightarrow_{\mathsf{F}} e_3$ then $\exists\, e_1, e_4$ such that $e_3 \rightarrow^*_{\mathsf{F}} e_4$ and $e_0 \rightarrow^*_{\mathsf{C}} e_1$ and $e_1 \lesssim e_4$*

Proof Sketch. Co-Natural may take extra steps at elimination forms, to unwrap several layers. Forgetful takes extra steps to combine boundaries in a trace wrapper. Otherwise, the two are in sync modulo extra guard wrappers on the Co-Natural side of the $\lesssim$ relation More details in appendix: lemma A.17. □

6.8 Transient and its Properties

6.8.1 Semantics, Type Soundness.

$\boxed{e; \mathcal{H}; \mathcal{B} \vartriangleright_{\mathsf{T}} e; \mathcal{H}; \mathcal{B}}$

$\mathsf{w}_0; \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad \mathsf{p}_0; (\{\mathsf{p}_0 \mapsto \mathsf{w}_0\} \cup \mathcal{H}_0); (\{\mathsf{p}_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$
  where p_0 fresh in $\mathcal{H}_0$ and $\mathcal{B}_0$

$(\mathit{unop}\{\tau_0\}\ v_0); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad \mathsf{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$
  if $\delta(\mathit{unop}, \mathcal{H}_0(v_0))$ is undefined

$(\mathit{unop}\{\mathcal{U}\}\ v_0); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad \mathsf{TagErr}; \mathcal{H}_0; \mathcal{B}_0$
  if $\delta(\mathit{unop}, \mathcal{H}_0(v_0))$ is undefined

$(\mathit{unop}\{{}^{\tau}\!/\!_{\mathcal{U}}\}\ \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad (\mathsf{check}\{{}^{\tau}\!/\!_{\mathcal{U}}\}\ \delta(\mathit{unop}, \mathcal{H}_0(\mathsf{p}_0))\ \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0$
  if $\delta(\mathit{unop}, \mathcal{H}_0(\mathsf{p}_0))$ is defined

$(\mathit{binop}\{\tau_0\}\ v_0\ v_1); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad \mathsf{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$
  if $\delta(\mathit{binop}, v_0, v_1)$ is undefined

$(\mathit{binop}\{\mathcal{U}\}\ v_0\ v_1); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad \mathsf{TagErr}; \mathcal{H}_0; \mathcal{B}_0$
  if $\delta(\mathit{binop}, v_0, v_1)$ is undefined

$(\mathit{binop}\{{}^{\tau}\!/\!_{\mathcal{U}}\}\ i_0\ i_1); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad \delta(\mathit{binop}, i_0, i_1); \mathcal{H}_0; \mathcal{B}_0$
  if $\delta(\mathit{binop}, i_0, i_1)$ is defined

$(\mathsf{app}\{\tau_0\}\ v_0\ v_1); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad \mathsf{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$
  if $\mathcal{H}_0(v_0) \notin (\lambda x.\, e) \cup (\lambda(x : \tau).\, e)$

$(\mathsf{app}\{\mathcal{U}\}\ v_0\ v_1); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad \mathsf{TagErr}; \mathcal{H}_0; \mathcal{B}_0$
  if $\mathcal{H}_0(v_0) \notin (\lambda x.\, e) \cup (\lambda(x : \tau).\, e)$

$(\mathsf{app}\{{}^{\tau}\!/\!_{\mathcal{U}}\}\ \mathsf{p}_0\ v_0); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad (\mathsf{check}\{{}^{\tau}\!/\!_{\mathcal{U}}\}\ e_0[x_0 \leftarrow v_0]\ \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_1$
  if $\mathcal{H}_0(\mathsf{p}_0) = \lambda(x_0 : \tau_0).\, e_0$ and $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$
  and $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \mathit{rev}(\mathcal{B}_0(\mathsf{p}_0))]$

$(\mathsf{app}\{{}^{\tau}\!/\!_{\mathcal{U}}\}\ \mathsf{p}_0\ v_0); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad \mathsf{BoundaryErr}\,(\mathcal{B}_0(v_0) \cup \mathit{rev}(\mathcal{B}_0(\mathsf{p}_0)), v_0); \mathcal{H}_0; \mathcal{B}_1$
  if $\mathcal{H}_0(\mathsf{p}_0) = \lambda(x_0 : \tau_0).\, e_0$ and $\neg\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$
  where $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \mathit{rev}(\mathcal{B}_0(\mathsf{p}_0))]$

$(\mathsf{app}\{\tau_0\}\ \mathsf{p}_0\ v_0); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad (\mathsf{check}\{\tau_0\}\ e_0[x_0 \leftarrow v_0]\ \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_1$
  if $\mathcal{H}_0(\mathsf{p}_0) = \lambda x_0.\, e_0$
  and $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \mathit{rev}(\mathcal{B}_0(\mathsf{p}_0))]$

$(\mathsf{app}\{\mathcal{U}\}\ \mathsf{p}_0\ v_0); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad (e_0[x_0 \leftarrow v_0]); \mathcal{H}_0; \mathcal{B}_0$
  if $\mathcal{H}_0(\mathsf{p}_0) = \lambda x_0.\, e_0$

$(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}])$
  if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$

$(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad \mathsf{BoundaryErr}\,(\{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}, v_0); \mathcal{H}_0; \mathcal{B}_0$
  if $\neg\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$

$(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}])$
  if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$

$(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0); \mathcal{H}_0; \mathcal{B}_0 \quad \vartriangleright_{\mathsf{T}} \quad \mathsf{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$
  if $\neg\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$

$$(\mathsf{check}\{\mathcal{U}\}\ v_0\ \mathrm{p}_0); \mathcal{H}_0; \mathcal{B}_0 \ \rhd_{\mathsf{T}}\ v_0; \mathcal{H}_0; \mathcal{B}_0$$

$$(\mathsf{check}\{\tau_0\}\ v_0\ \mathrm{p}_0); \mathcal{H}_0; \mathcal{B}_0 \ \rhd_{\mathsf{T}}\ v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \mathcal{B}_0(\mathrm{p}_0)])$$
$$\quad \text{if } \textit{shape-match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$$

$$(\mathsf{check}\{\tau_0\}\ v_0\ \mathrm{p}_0); \mathcal{H}_0; \mathcal{B}_0 \ \rhd_{\mathsf{T}}\ \mathsf{BoundaryErr}(\mathcal{B}_0(v_0) \cup \mathcal{B}_0(\mathrm{p}_0), v_0); \mathcal{H}_0; \mathcal{B}_0$$
$$\quad \text{if } \neg\textit{shape-match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$$

$\boxed{e; \mathcal{H}; \mathcal{B} \rightarrow_{\mathsf{T}} e; \mathcal{H}; \mathcal{B}}$ is the compatible closure of the relation $\rhd_{\mathsf{T}}$. More precisely:

$$\begin{array}{lll} \text{if} & e_0; \mathcal{H}_0; \mathcal{B}_0 & \rhd_{\mathsf{T}}\ e_1; \mathcal{H}_1; \mathcal{B}_1 \\ \text{then} & E[e_0]; \mathcal{H}_0; \mathcal{B}_0 & \rightarrow_{\mathsf{T}}\ E[e_1]; \mathcal{H}_1; \mathcal{B}_1 \end{array}$$

$\boxed{e; \mathcal{H}; \mathcal{B} \rightarrow^*_{\mathsf{T}} e; \mathcal{H}; \mathcal{B}}$ is the transitive, reflexive closure of the relation $\rightarrow_{\mathsf{T}}$

Theorem 6.43 (Transient unsoundness). *Transient does not satisfy* **TS (1)**

Proof. Let $e_0 = \mathsf{dyn}\,(\ell_0 \blacktriangleleft (\mathsf{Nat} \Rightarrow \mathsf{Nat}) \blacktriangleleft \ell_1)\ (\lambda x_0.\, -4)$.

- $\vdash e_0 : \mathsf{Nat} \Rightarrow \mathsf{Nat}$ in the surface language, but
- $e_0; \emptyset; \emptyset \rightarrow^*_{\mathsf{T}} \mathsf{p}_0; \mathcal{H}_0; \mathcal{B}_0$, where $\mathcal{H}_0(\mathsf{p}_0) = (\lambda x_0.\, -4)$

and $\nvdash_1 (\lambda x_0.\, -4) : \mathsf{Nat} \Rightarrow \mathsf{Nat}$. □

Theorem 6.44 (Transient shape soundness). *Transient satisfies* **TS (s)**

Proof. By progress (lemma 6.45) and preservation (lemma 6.46). □

Lemma 6.45 (Transient type progress).
If $\mathcal{T}_0; \cdot \vdash_{\mathsf{s}} E_0[e_0]; \mathcal{H}_0; \mathcal{B}_0 : s \cup \mathcal{U}$ then one of the following holds:

- $e_0 \in v \cup \mathsf{Err}$
- $\exists\, e_1, \mathcal{H}_1, \mathcal{B}_1.\ e_0; \mathcal{H}_0; \mathcal{B}_0 \vartriangleright_{\mathsf{T}} e_1; \mathcal{H}_1; \mathcal{B}_1$

Proof Sketch. By unique decomposition (lemma 6.1) and case analysis. More details in appendix: lemma A.24. □

Lemma 6.46 (Transient type preservation).
If $\mathcal{T}_0; \cdot \vdash_{\mathsf{s}} e_0; \mathcal{H}_0; \mathcal{B}_0 : {}^{\tau}\!/\!_{\mathcal{U}}$ and $e_0; \mathcal{H}_0; \mathcal{B}_0 \vartriangleright_{\mathsf{T}} e_1; \mathcal{H}_1; \mathcal{B}_1$ then $\exists\, \mathcal{T}_1.\ \mathcal{T}_0 \subseteq \mathcal{T}_1$ and $\mathcal{T}_1; \cdot \vdash_{\mathsf{s}} e_1; \mathcal{H}_1; \mathcal{B}_1 : {}^{\tau}\!/\!_{\mathcal{U}}$.

Proof Sketch. By case analysis of the reduction relation. The new heap typing $\mathcal{T}_1$ gains an entry only when the value heap does; if $\mathcal{H}_1 = \{\mathsf{p}_0 \mapsto \mathsf{w}_0\} \cup \mathcal{H}_0$ then $\mathcal{T}_1 = \{(\mathsf{p}_0 : s_0)\} \cup \mathcal{T}_0$, where s_0 is the shape of the pre-value (lemma 6.47). More details in appendix: lemma A.25. □

Lemma 6.47 (Transient shape inference).
If $\mathcal{T}_0; \cdot \vdash_{\mathsf{s}} \mathsf{w}_0; \mathcal{H}_0; \mathcal{B}_0 : {}^{\tau}\!/\!_{\mathcal{U}}$ then $\exists\, s_0.\ \mathcal{T}_0; \cdot \vdash_{\mathsf{s}} \mathsf{w}_0; \mathcal{H}_0; \mathcal{B}_0 : s_0$.

Proof. By induction on the structure of the closed pre-value w_0. Note that lambdas are a base case, thus the induction does not need to consider type environments (Γ). □

6.8.2 *Lifted Semantics, Complete Monitoring, Blame.*

$\boxed{(e)^{\ell}; \mathcal{H}; \mathcal{B}; O \rhd_{\overline{\mathsf{T}}} (e)^{\ell}; \mathcal{H}; \mathcal{B}; O}$

$(\mathsf{w}_0)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0 \quad \rhd_{\overline{\mathsf{T}}} \quad (\mathsf{p}_0)^{\ell_0}; \mathcal{H}_1; \mathcal{B}_1; O_1$
where p_0 fresh in $\mathcal{H}_0$ and $\mathcal{B}_0$ and O_0
and $\mathcal{H}_1 = \{\mathsf{p}_0 \mapsto \mathsf{w}_0\} \cup \mathcal{H}_0$ and $\mathcal{B}_1 = \{\mathsf{p}_0 \mapsto \emptyset\} \cup \mathcal{B}_0$ and $O_1 = (\{\mathsf{p}_0 \mapsto \{\ell_0\}\} \cup O_0)$

$(\mathit{unop}\{\tau_0\}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0 \quad \rhd_{\overline{\mathsf{T}}} \quad (\mathsf{InvariantErr})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$
if $v_0 \notin (v)^{\ell}$ and $\delta(\mathit{unop}, \mathcal{H}_0(v_0))$ is undefined

$(\mathit{unop}\{\mathcal{U}\}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0 \quad \rhd_{\overline{\mathsf{T}}} \quad (\mathsf{TagErr})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$
if $v_0 \notin (v)^{\ell}$ and $\delta(\mathit{unop}, \mathcal{H}_0(v_0))$ is undefined

$(\mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\, \llparenthesis \mathsf{p}_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0 \quad \rhd_{\overline{\mathsf{T}}}$
$\qquad (\mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\, \llparenthesis \delta(\mathit{unop}, \mathcal{H}_0(\mathsf{p}_0)) \rrparenthesis^{\overline{\ell}_0}\, \mathsf{p}_0)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0[\mathsf{p}_0 \cup \overline{\ell}_0]$
if $\delta(\mathit{unop}, \mathcal{H}_0(\mathsf{p}_0))$ is defined

$(\mathit{binop}\{\tau_0\}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}\, \llparenthesis v_1 \rrparenthesis^{\overline{\ell}_1})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0 \quad \rhd_{\overline{\mathsf{T}}} \quad (\mathsf{InvariantErr})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$
if $v_0 \notin (v)^{\ell}$ and $v_1 \notin (v)^{\ell}$ and $\delta(\mathit{binop}, v_0, v_1)$ is undefined

$(\mathit{binop}\{\mathcal{U}\}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}\, \llparenthesis v_1 \rrparenthesis^{\overline{\ell}_1})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0 \quad \rhd_{\overline{\mathsf{T}}} \quad (\mathsf{TagErr})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$
if $v_0 \notin (v)^{\ell}$ and $v_1 \notin (v)^{\ell}$ and $\delta(\mathit{binop}, v_0, v_1)$ is undefined

$(\mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, \llparenthesis i_0 \rrparenthesis^{\overline{\ell}_0}\, \llparenthesis i_1 \rrparenthesis^{\overline{\ell}_1})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0 \quad \rhd_{\overline{\mathsf{T}}} \quad (\delta(\mathit{binop}, i_0, i_1))^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$
if $\delta(\mathit{binop}, i_0, i_1)$ is defined

$(\mathsf{app}\{\tau_0\}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}\, v_1)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0 \quad \rhd_{\overline{\mathsf{T}}} \quad (\mathsf{InvariantErr})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$
if $v_0 \notin (v)^{\ell}$ and $\mathcal{H}_0(v_0) \notin (\lambda x.\, e) \cup (\lambda(x : \tau).\, e)$

$(\mathsf{app}\{\mathcal{U}\}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}\, v_1)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0 \quad \rhd_{\overline{\mathsf{T}}} \quad (\mathsf{TagErr})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$
if $v_0 \notin (v)^{\ell}$ and $\mathcal{H}_0(v_0) \notin (\lambda x.\, e) \cup (\lambda(x : \tau).\, e)$

$(\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, \llparenthesis \mathsf{p}_0 \rrparenthesis^{\overline{\ell}_0}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_1})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0 \quad \rhd_{\overline{\mathsf{T}}}$
$\qquad (\mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\, \llparenthesis e_0[x_0 \leftarrow \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_1 \ell_0 \mathit{rev}(\overline{\ell}_0)}] \rrparenthesis^{\overline{\ell}_0}\, \mathsf{p}_0)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_1; O_1$
if $\mathcal{H}_0(\mathsf{p}_0) = \lambda(x_0 : \tau_0).\, e_0$ and $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$
where $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \mathit{rev}(\mathcal{B}_0(\mathsf{p}_0))]$ and $O_1 = O_0[\mathsf{p}_0 \cup \overline{\ell}_0 \ell_0][v_0 \cup \overline{\ell}_1 O_0(\mathsf{p}_0) \cup \ell_0 \mathit{rev}(\overline{\ell}_0)]$

$(\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, \llparenthesis \mathsf{p}_0 \rrparenthesis^{\overline{\ell}_0}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_1})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0 \quad \rhd_{\overline{\mathsf{T}}}$
$\qquad (\mathsf{BoundaryErr}\,(\mathcal{B}_0(v_0) \cup \mathit{rev}(\mathcal{B}_0(\mathsf{p}_0)), \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_1 \ell_0 \mathit{rev}(\overline{\ell}_0)}))^{\ell_0}; \mathcal{H}_0; \mathcal{B}_1; O_1$
if $\mathcal{H}_0(\mathsf{p}_0) = \lambda(x_0 : \tau_0).\, e_0$ and $v_0 \notin (v)^{\ell}$ and $\neg\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$
where $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \mathit{rev}(\mathcal{B}_0(\mathsf{p}_0))]$ and $O_1 = O_0[\mathsf{p}_0 \cup \overline{\ell}_0 \ell_0][v_0 \cup O_0(\mathsf{p}_0) \cup \overline{\ell}_1 \ell_0 \mathit{rev}(\overline{\ell}_0)]$

$(\mathsf{app}\{\tau_0\}\, \llparenthesis \mathsf{p}_0 \rrparenthesis^{\overline{\ell}_0}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_1})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0 \quad \rhd_{\overline{\mathsf{T}}}$
$\qquad (\mathsf{check}\{\tau_0\}\, \llparenthesis e_0[x_0 \leftarrow \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_1 \ell_0 \mathit{rev}(\overline{\ell}_0)}] \rrparenthesis^{\overline{\ell}_0}\, \mathsf{p}_0)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_1; O_1$
if $\mathcal{H}_0(\mathsf{p}_0) = \lambda x_0.\, e_0$ and $v_0 \notin (v)^{\ell}$
where $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \mathit{rev}(\mathcal{B}_0(\mathsf{p}_0))]$
and $O_1 = O_0[\mathsf{p}_0 \cup \overline{\ell}_0 \ell_0][v_0 \cup O_0(\mathsf{p}_0) \cup \overline{\ell}_1 \ell_0 \mathit{rev}(\overline{\ell}_0)]$

$$
\begin{array}{l}
(\mathsf{app}\{\mathcal{U}\}\ \llparenthesis \mathrm{p}_0 \rrparenthesis^{\overline{\ell}_0}\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_1})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \ \ \rhd_{\overline{\top}} \ \ \llparenthesis e_0[x_0 \leftarrow \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_1 \ell_0 rev(\overline{\ell}_0)}] \rrparenthesis^{\overline{\ell}_0 \ell_0}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_1 \\
\quad \text{if } \mathcal{H}_0(\mathrm{p}_0) = \lambda x_0.\, e_0 \text{ and } v_0 \notin (v)^{\ell} \\
\quad \text{and } \mathcal{O}_1 = \mathcal{O}_0[\mathrm{p}_0 \cup \overline{\ell}_0 \ell_0][v_0 \cup \mathcal{O}_0(\mathrm{p}_0) \cup \overline{\ell}_1 \ell_0 rev(\overline{\ell}_0)] \\
(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_2}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \ \ \rhd_{\overline{\top}} \ \ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0 \ell_2}; \mathcal{H}_0; \mathcal{B}_1; \mathcal{O}_1 \\
\quad \text{if } \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0)) \\
\quad \text{where } \mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}] \text{ and } \mathcal{O}_1 = \mathcal{O}_0[v_0 \cup \overline{\ell}_0 \ell_2] \\
(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_2}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \ \ \rhd_{\overline{\top}} \\
\qquad\qquad (\mathsf{BoundaryErr}\,(\{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}))^{\ell_2}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \\
\quad \text{if } v_0 \notin (v)^{\ell} \text{ and } \neg \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0)) \\
(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_2}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \ \ \rhd_{\overline{\top}} \ \ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0 \ell_2}; \mathcal{H}_0; \mathcal{B}_1; \mathcal{O}_1 \\
\quad \text{if } \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0)) \\
\quad \text{where } \mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}] \text{ and } \mathcal{O}_1 = \mathcal{O}_0[v_0 \cup \overline{\ell}_0 \ell_2] \\
(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_2}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \ \ \rhd_{\overline{\top}} \ \ (\mathsf{InvariantErr})^{\ell_2}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \\
\quad \text{if } v_0 \notin (v)^{\ell} \text{ and } \neg \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0)) \\
\llparenthesis \mathsf{check}\{\mathcal{U}\}\ v_0\ \mathrm{p}_0 \rrparenthesis^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \ \ \rhd_{\overline{\top}} \ \ \llparenthesis v_0 \rrparenthesis^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \\
(\mathsf{check}\{\tau_0\}\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}\ \mathrm{p}_0)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \ \ \rhd_{\overline{\top}} \ \ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0 \ell_0}; \mathcal{H}_0; \mathcal{B}_1; \mathcal{O}_1 \\
\quad \text{if } v_0 \notin (v)^{\ell} \text{ and } \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0)) \\
\quad \text{where } \mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \mathcal{B}_0(\mathrm{p}_0)] \text{ and } \mathcal{O}_1 = \mathcal{O}_0[v_0 \cup \mathcal{O}_0(\mathrm{p}_0) \cup \overline{\ell}_0 \ell_0] \\
(\mathsf{check}\{\tau_0\}\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}\ \mathrm{p}_0)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \ \ \rhd_{\overline{\top}} \\
\qquad\qquad (\mathsf{BoundaryErr}\,(\mathcal{B}_0(v_0) \cup \mathcal{B}_0(\mathrm{p}_0), \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}))^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_1 \\
\quad \text{if } v_0 \notin (v)^{\ell} \text{ and } \neg \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0)) \\
\quad \text{where } \mathcal{O}_1 = \mathcal{O}_0[v_0 \cup \mathcal{O}_0(\mathrm{p}_0)]
\end{array}
$$

Theorem 6.48 (Transient incomplete monitoring). *Transient does not satisfy* **CM**

Proof. Whenever a pair or function crosses a boundary, Transient lets it across without adding a guard wrapper. Thus, the value gains an additional ownership label. □

Theorem 6.49 (Transient blame unsoundness). *Transient does not satisfy* **BS**

Proof. Let component ℓ_0 define a function f_0 and export it to components ℓ_1 and ℓ_2. If component ℓ_2 triggers a type mismatch, then component ℓ_1 gets blamed even though there is no direct channel from ℓ_1 to ℓ_2.

The following term expresses the scenario above, using a let-expression to abbreviate untyped function application:

$$\begin{array}{l}(\mathsf{let}\ f_0 = (\lambda x_0.\, \langle x_0, x_0\rangle)\ \mathsf{in} \\ \ \mathsf{let}\ f_1 = (\mathsf{stat}\ (\ell_0 \blacktriangleleft (\mathsf{Int} \Rightarrow \mathsf{Int}) \blacktriangleleft \ell_1)\ (\mathsf{dyn}\ (\ell_1 \blacktriangleleft (\mathsf{Int} \Rightarrow \mathsf{Int}) \blacktriangleleft \ell_0)\ (f_0)^{\ell_0})^{\ell_1})\ \mathsf{in} \\ \ \mathsf{stat}\ (\ell_0 \blacktriangleleft \mathsf{Int} \blacktriangleleft \ell_2)\ (\mathsf{app}\{\mathsf{Int}\}\ (\mathsf{dyn}\ (\ell_2 \blacktriangleleft (\mathsf{Int} \Rightarrow \mathsf{Int}) \blacktriangleleft \ell_0)\ (f_0)^{\ell_0})\ 5)^{\ell_2})^{\ell_0}; \emptyset; \emptyset; \emptyset\end{array}$$

Reduction ends in a boundary error that blames all three components. □

Theorem 6.50 (Transient blame incompleteness). *Transient does not satisfy* **BC**.

Proof. The rule for untyped function application does not update the blame map. The following term illustrates the problem by using an untyped identity function f_1 to coerce the type of another function (f_0). After the coercion, an application leads to type mismatch.

$$\begin{array}{l}(\mathsf{let}\ f_0 = \mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\mathsf{dyn}\ (\ell_1 \blacktriangleleft \tau_0 \blacktriangleleft \ell_2)\ (\lambda x_0.\, x_0))\ \mathsf{in} \\ \ \mathsf{let}\ f_1 = \mathsf{stat}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_3)\ (\mathsf{dyn}\ (\ell_3 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_4)\ (\lambda x_1.\, x_1))\ \mathsf{in} \\ \ \mathsf{stat}\ (\ell_0 \blacktriangleleft (\mathsf{Int} \times \mathsf{Int}) \blacktriangleleft \ell_5) \\ \qquad (\mathsf{app}\{\mathsf{Int} \times \mathsf{Int}\}\ (\mathsf{dyn}\ (\ell_5 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\ (\mathsf{app}\{\mathcal{U}\}\ f_1\ f_0)^{\ell_0})\ 42)^{\ell_5})^{\ell_0}; \emptyset; \emptyset; \emptyset\end{array}$$

Reduction ends in a boundary error that does not report the crucial labels ℓ_3 and ℓ_4. □

6.8.3 Relation to Forgetful.

Theorem 6.51. $F \lesssim T$.

Proof. Indirectly, via $T \approx A$ (theorem 6.59) and $F \lesssim A$ (theorem 6.61). Both appear in the next section. □

6.9 Amnesic and its Properties

6.9.1 Semantics, Type Soundness.

$\boxed{e \rhd_{\mathsf{A}} e}$

$$
\begin{array}{ll}
\mathit{unop}\{\tau_0\}\, v_0 & \rhd_{\mathsf{A}}\ \mathsf{InvariantErr} \\
\quad \text{if } v_0 \notin (\mathbb{G}\,(\ell \blacktriangleleft (\tau{\times}\tau) \blacktriangleleft \ell)\, v) \text{ and } \delta(\mathit{unop}, v_0) \text{ is undefined} & \\
\mathit{unop}\{\tau_0\}\, v_0 & \rhd_{\mathsf{A}}\ \delta(\mathit{unop}, v_0) \\
\quad \text{if } \delta(\mathit{unop}, v_0) \text{ is defined} & \\
\mathsf{fst}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0) & \rhd_{\mathsf{A}}\ \mathsf{dyn}\ b_0\ (\mathsf{fst}\{\mathcal{U}\}\, v_0) \\
\quad \text{where } b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) & \\
\mathsf{snd}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0 & \rhd_{\mathsf{A}}\ \mathsf{dyn}\ b_0\ (\mathsf{snd}\{\mathcal{U}\}\, v_0) \\
\quad \text{where } b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) & \\
\mathit{binop}\{\tau_0\}\, v_0\, v_1 & \rhd_{\mathsf{A}}\ \mathsf{InvariantErr} \\
\quad \text{if } \delta(\mathit{binop}, v_0, v_1) \text{ is undefined} & \\
\mathit{binop}\{\tau_0\}\, v_0\, v_1 & \rhd_{\mathsf{A}}\ \delta(\mathit{binop}, v_0, v_1) \\
\quad \text{if } \delta(\mathit{binop}, v_0, v_1) \text{ is defined} & \\
\mathsf{app}\{\tau_0\}\, v_0\, v_1 & \rhd_{\mathsf{A}}\ \mathsf{InvariantErr} \\
\quad \text{if } v_0 \notin (\lambda(x:\tau).\, e) \cup (\mathbb{G}\,(\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell)\, v) & \\
\mathsf{app}\{\tau_0\}\,(\lambda(x_0:\tau_1).\, e_0)\, v_0 & \rhd_{\mathsf{A}}\ e_0[x_0 \leftarrow v_0] \\
\mathsf{app}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0)\, v_1 & \rhd_{\mathsf{A}}\ \mathsf{dyn}\ b_0\ (\mathsf{app}\{\mathcal{U}\}\, v_0\ (\mathsf{stat}\ b_1\ v_1)) \\
\quad \text{where } b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \text{ and } b_1 = (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0) & \\
\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 & \rhd_{\mathsf{A}}\ \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \\
\quad \text{if } \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0) & \\
\quad \text{and } v_0 \in (\mathbb{T}_?\, \overline{b}\,(\lambda(x:\tau).\, e)) \cup (\mathbb{T}_?\, \overline{b}\,\langle v, v\rangle) \cup (\mathbb{T}_?\, \overline{b}\,(\mathbb{G}\,(\ell \blacktriangleleft \tau \blacktriangleleft \ell)\, v)) & \\
\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathbb{T}_?\, \overline{b_0}\, i_0) & \rhd_{\mathsf{A}}\ i_0 \\
\quad \text{if } \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, i_0) & \\
\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 & \rhd_{\mathsf{A}}\ \mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b}_0, v_0) \\
\quad \text{if } \neg \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0) \text{ and } \overline{b}_0 = \mathit{get\text{-}trace}(v_0) &
\end{array}
$$

$\boxed{e \blacktriangleright_{\mathsf{A}} e}$

$unop\{\mathcal{U}\}\ v_0 \quad \blacktriangleright_{\mathsf{A}} \quad \mathsf{TagErr}$
  if $v_1 = \mathit{rem\text{-}trace}(v_0)$ and $v_1 \notin \mathbb{G}\,(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell)\ v$ and $\delta(unop, v_1)$ is undefined

$unop\{\mathcal{U}\}\ v_0 \quad \blacktriangleright_{\mathsf{A}} \quad \mathit{add\text{-}trace}(\mathit{get\text{-}trace}(v_0), \delta(unop, v_1))$
  if $v_1 = \mathit{rem\text{-}trace}(v_0)$ and $\delta(unop, v_1)$ is defined

$\mathsf{fst}\{\mathcal{U}\}\ (\mathbb{T}_?\,\overline{b_0}\ (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)) \quad \blacktriangleright_{\mathsf{A}} \quad \mathsf{trace}\,\overline{b_0}\ (\mathsf{stat}\ b_0\ (\mathsf{fst}\{\tau_1\}\ v_0))$
  where $\tau_1 = \mathit{fst}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$

$\mathsf{snd}\{\mathcal{U}\}\ (\mathbb{T}_?\,\overline{b_0}\ (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)) \quad \blacktriangleright_{\mathsf{A}} \quad \mathsf{trace}\,\overline{b_0}\ (\mathsf{stat}\ b_0\ (\mathsf{snd}\{\tau_1\}\ v_0))$
  where $\tau_1 = \mathit{snd}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$

$binop\{\mathcal{U}\}\ v_0\ v_1 \quad \blacktriangleright_{\mathsf{A}} \quad \mathsf{TagErr}$
  if $v_2 = \mathit{rem\text{-}trace}(v_0)$ and $v_3 = \mathit{rem\text{-}trace}(v_1)$ and $\delta(binop, v_2, v_3)$ is undefined

$binop\{\mathcal{U}\}\ v_0\ v_1 \quad \blacktriangleright_{\mathsf{A}} \quad \delta(binop, v_2, v_3)$
  if $v_2 = \mathit{rem\text{-}trace}(v_0)$ and $v_3 = \mathit{rem\text{-}trace}(v_1)$ and $\delta(binop, v_2, v_3)$ is defined

$\mathsf{app}\{\mathcal{U}\}\ v_0\ v_1 \quad \blacktriangleright_{\mathsf{A}} \quad \mathsf{TagErr}$
  if $v_0 \notin (\mathbb{T}_?\,\overline{b}\,(\lambda x.\,e)) \cup (\mathbb{T}_?\,\overline{b}\,(\mathbb{G}\,(\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell)\ v))$

$\mathsf{app}\{\mathcal{U}\}\ (\mathbb{T}_?\,\overline{b_0}\ (\lambda x_0.\,e_0))\ v_0 \quad \blacktriangleright_{\mathsf{A}} \quad \mathsf{trace}\,\overline{b_0}\ (e_0[x_0 \leftarrow v_1])$
  where $v_1 = \mathit{add\text{-}trace}(\mathit{rev}(\overline{b_0}), v_0)$

$\mathsf{app}\{\mathcal{U}\}\ (\mathbb{T}_?\,\overline{b_0}\ (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0))\ v_1 \quad \blacktriangleright_{\mathsf{A}} \quad \mathsf{trace}\,\overline{b_0}\ (\mathsf{stat}\ b_0\ (\mathsf{app}\{\tau_2\}\ v_0\ (\mathsf{dyn}\ b_1\ v_2)))$
  where $\tau_2 = \mathit{cod}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)$
  and $v_2 = \mathit{add\text{-}trace}(\mathit{rev}(\overline{b_0}), v_1)$

$\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \quad \blacktriangleright_{\mathsf{A}} \quad \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0$
  if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$ and $v_0 \in (\lambda(x : \tau).\,e) \cup \langle v, v \rangle$

$\mathsf{stat}\ b_0\ (\mathbb{G}\,b_1\ (\mathbb{T}_?\,\overline{b_0}\ v_0)) \quad \blacktriangleright_{\mathsf{A}} \quad \mathsf{trace}\,(b_0 b_1 \overline{b_0})\ v_0$
  if $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$ and $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
  and $v_0 \in (\lambda x.\,e) \cup \langle v, v \rangle \cup (\mathbb{G}\,b\ (\lambda(x : \tau).\,e)) \cup (\mathbb{G}\,b\ \langle v, v \rangle)$

$\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ i_0 \quad \blacktriangleright_{\mathsf{A}} \quad i_0$
  if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, i_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$

$\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \quad \blacktriangleright_{\mathsf{A}} \quad \mathsf{InvariantErr}$
  if $\neg \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$

$\mathsf{trace}\,\overline{b_0}\ v_0 \quad \blacktriangleright_{\mathsf{A}} \quad v_1$
  where $v_1 = \mathit{add\text{-}trace}(\overline{b_0}, v_0)$

$\boxed{e \rightarrow^*_{\mathsf{A}} e}$ is the transitive, reflexive, compatible (with respect to evaluation contexts E, section 6.2) closure of the relation $\bigcup\{\rhd_{\mathsf{A}}, \blacktriangleright_{\mathsf{A}}\}$

$\boxed{A(e)} = F(e)$

holds for typed expressions with at most two guard wrappers and for untyped expressions with at most one guard wrapper.

Theorem 6.52 (Amnesic type soundness). *Amnesic satisfies* **TS (1)**

Proof. By lemma 6.53, progress (lemma 6.54), and preservation (lemma 6.55). □

Lemma 6.53. *If* $e_0 : {}^{\tau}/_{\mathcal{U}}$ **wf** *then* $A(e_0)$.

Proof. Wrappers are not part of the surface language. □

Lemma 6.54 (Amnesic type progress). *If* $\cdot \vdash_1 E_0[e_0] : {}^{\tau}/_{\mathcal{U}}$ *and* $A(E_0[e_0])$ *then one of the following holds:*

- $e_0 \in v \cup \mathsf{Err}$
- ${}^{\tau}/_{\mathcal{U}} \in \tau$ *and* $\exists\, e_1.\ e_0 \rhd_{\mathsf{A}} e_1$
- ${}^{\tau}/_{\mathcal{U}} \in \mathcal{U}$ *and* $\exists\, e_1.\ e_0 \blacktriangleright_{\mathsf{A}} e_1$

Proof Sketch. By unique decomposition (lemma 6.1) and case analysis. More details in appendix: lemma A.26. □

Lemma 6.55 (Amnesic type preservation).
If $\cdot \vdash_1 E_0[e_0] : {}^{\tau}/_{\mathcal{U}}$ *and* $A(E_0[e_0])$ *and* $e_0(\rhd_{\mathsf{A}} \cup \blacktriangleright_{\mathsf{A}})e_1$ *then* $\cdot \vdash_1 E_0[e_1] : {}^{\tau}/_{\mathcal{U}}$ *and* $A(E_0[e_1])$.

Proof Sketch. By case analysis of each reduction relation. More details in appendix: lemma A.27. □

Lemma 6.56.

- *If* $A(E_0[e_0])$ *then* $A(e_0)$
- *If* $A(E_0[e_0])$ *and* $A(e_1)$ *then* $A(E_0[e_1])$

Proof Sketch. By lemma 6.37. □

6.9.2 *Lifted Semantics, Complete Monitoring, Blame.*

$\boxed{(e)^{\ell} \rhd_{\underline{\mathsf{A}}} (e)^{\ell}}$ lifted version of $\rhd_{\mathsf{A}}$

$$(\mathit{unop}\{\tau_0\}\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}})^{\ell_0} \rhd_{\underline{\mathsf{A}}} (\mathsf{InvariantErr})^{\ell_0}$$
if $v_0 \notin (v)^{\ell} \cup (\mathbb{G}\ (\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell)\ v)$ and $\delta(\mathit{unop}, v_0)$ is undefined

$$(\mathit{unop}\{\tau_0\}\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}})^{\ell_0} \rhd_{\underline{\mathsf{A}}} (\delta(\mathit{unop}, v_0))^{\overline{\ell_0}\ell_0}$$
if $\delta(\mathit{unop}, v_0)$ is defined

$$(\mathsf{fst}\{\tau_0\}\ \llparenthesis \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell_0}})^{\ell_3} \rhd_{\underline{\mathsf{A}}} (\mathsf{dyn}\ b_0\ (\mathsf{fst}\{\mathcal{U}\}\ (v_0)^{\ell_2}))^{\overline{\ell_0}\ell_3}$$
where $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$

$$(\mathsf{snd}\{\tau_0\}\ \llparenthesis \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell_0}})^{\ell_3} \rhd_{\underline{\mathsf{A}}} (\mathsf{dyn}\ b_0\ (\mathsf{snd}\{\mathcal{U}\}\ (v_0)^{\ell_2}))^{\overline{\ell_0}\ell_3}$$
where $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$

$$(\mathit{binop}\{\tau_0\}\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}}\ \llparenthesis v_1 \rrparenthesis^{\overline{\ell_1}})^{\ell_0} \rhd_{\underline{\mathsf{A}}} (\mathsf{InvariantErr})^{\ell_0}$$
if $v_0 \notin (v)^{\ell}$ and $v_1 \notin (v)^{\ell}$ and $\delta(\mathit{binop}, v_0, v_1)$ is undefined

$$(\mathit{binop}\{\tau_0\}\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}}\ \llparenthesis v_1 \rrparenthesis^{\overline{\ell_1}})^{\ell_0} \rhd_{\underline{\mathsf{A}}} (\delta(\mathit{binop}, v_0, v_1))^{\ell_0}$$
if $\delta(\mathit{binop}, v_0, v_1)$ is defined

$$(\mathsf{app}\{\tau_0\}\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}}\ v_1)^{\ell_0} \rhd_{\underline{\mathsf{A}}} (\mathsf{InvariantErr})^{\ell_0}$$
if $v_0 \notin (v)^{\ell} \cup (\lambda(x : \tau).\ e) \cup (\mathbb{G}\ b\ v)$

$$(\mathsf{app}\{\tau_0\}\ \llparenthesis \lambda(x_0 : \tau_1).\ e_0 \rrparenthesis^{\overline{\ell_0}}\ v_0)^{\ell_0} \rhd_{\underline{\mathsf{A}}} \llparenthesis e_0[x_0 \leftarrow \llparenthesis v_0 \rrparenthesis^{\ell_0 \mathit{rev}(\overline{\ell_0})}] \rrparenthesis^{\overline{\ell_0}\ell_0}$$

$$(\mathsf{app}\{\tau_0\}\ \llparenthesis \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell_0}}\ v_1)^{\ell_3} \rhd_{\underline{\mathsf{A}}}$$
$$\llparenthesis (\mathsf{dyn}\ b_0\ (\mathsf{app}\{\mathcal{U}\}\ v_0\ (\mathsf{stat}\ b_1\ \llparenthesis v_1 \rrparenthesis^{\ell_3 \mathit{rev}(\overline{\ell_0})})))^{\ell_2} \rrparenthesis^{\overline{\ell_0}\ell_3}$$
where $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)$

$$(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}})^{\ell_2} \rhd_{\underline{\mathsf{A}}} (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}})^{\ell_2}$$
if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
and $v_0 \in (\mathbb{T}_?\ \overline{b}\ (\lambda(x : \tau).\ e)) \cup (\mathbb{T}_?\ \overline{b}\ \langle v, v \rangle) \cup (\mathbb{T}_?\ \overline{b}\ (\mathbb{G}\ (\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell)\ v))$

$$(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis \mathbb{T}_?\ \overline{b_0}\ \llparenthesis i_0 \rrparenthesis^{\overline{\ell_0}} \rrparenthesis^{\overline{\ell_1}})^{\ell_2} \rhd_{\underline{\mathsf{A}}} (i_0)^{\ell_2}$$
if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, i_0)$

$$(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell_2}})^{\ell_3} \rhd_{\underline{\mathsf{A}}} (\mathsf{BoundaryErr}\ ((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b_0}, \llparenthesis v_0 \rrparenthesis^{\overline{\ell_2}}))^{\ell_3}$$
if $\neg \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$ and $\overline{b_0} = \mathit{get\text{-}trace}(v_0)$

$\boxed{(e)^{\ell} \blacktriangleright_{\overline{\mathsf{A}}} (e)^{\ell}}$ lifted version of $\blacktriangleright_{\mathsf{A}}$

$(\mathit{unop}\{\mathcal{U}\}\ \llparenthesis (v_0) \rrparenthesis^{\overline{\ell}_0})^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{A}}} \quad (\mathsf{TagErr})^{\ell_0}$
  if $v_0 \notin (v)^{\ell} \cup (\mathbb{G}\ (\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell)\ v)$ and $\delta(\mathit{unop}, v_0)$ is undefined

$(\mathit{unop}\{\mathcal{U}\}\ v_0)^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{A}}}$
    $(\mathit{add\text{-}trace}(\mathit{get\text{-}trace}(v_0), \delta(\mathit{unop}, v_1)))^{\ell_0}$
  if $v_1 = \mathit{rem\text{-}trace}(v_0)$ and $\delta(\mathit{unop}, v_1)$ is defined

$(\mathsf{fst}\{\mathcal{U}\}\ \llparenthesis (\mathbb{T}_?\ \overline{b}_0\ \llparenthesis (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2}) \rrparenthesis^{\overline{\ell}_3}) \rrparenthesis^{\overline{\ell}_4})^{\ell_5} \quad \blacktriangleright_{\overline{\mathsf{A}}} \quad (\mathsf{trace}\ \overline{b}_0\ \llparenthesis (\mathsf{stat}\ b_0\ (\mathsf{fst}\{\tau_1\}\ v_0)^{\ell_2}) \rrparenthesis^{\overline{\ell}_3})^{\overline{\ell}_4 \ell_5}$
  where $\tau_1 = \mathit{fst}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$

$(\mathsf{snd}\{\mathcal{U}\}\ \llparenthesis (\mathbb{T}_?\ \overline{b}_0\ \llparenthesis (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2}) \rrparenthesis^{\overline{\ell}_3}) \rrparenthesis^{\overline{\ell}_4})^{\ell_5} \quad \blacktriangleright_{\overline{\mathsf{A}}} \quad (\mathsf{trace}\ \overline{b}_0\ \llparenthesis (\mathsf{stat}\ b_0\ (\mathsf{snd}\{\tau_1\}\ v_0)^{\ell_2}) \rrparenthesis^{\overline{\ell}_3})^{\overline{\ell}_4 \ell_5}$
  where $\tau_1 = \mathit{snd}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$

$(\mathit{binop}\{\mathcal{U}\}\ \llparenthesis (v_0) \rrparenthesis^{\overline{\ell}_0}\ \llparenthesis (v_1) \rrparenthesis^{\overline{\ell}_1})^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{A}}} \quad (\mathsf{TagErr})^{\ell_0}$
  if $v_2 = \mathit{rem\text{-}trace}(v_0)$ and $v_3 = \mathit{rem\text{-}trace}(v_1)$ and $\delta(\mathit{binop}, v_2, v_3)$ is undefined

$(\mathit{binop}\{\mathcal{U}\}\ \llparenthesis (v_0) \rrparenthesis^{\overline{\ell}_0}\ \llparenthesis (v_1) \rrparenthesis^{\overline{\ell}_1})^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{A}}} \quad \delta(\mathit{binop}, v_2, v_3)$
  if $v_2 = \mathit{rem\text{-}trace}(v_0)$ and $v_3 = \mathit{rem\text{-}trace}(v_1)$ and $\delta(\mathit{binop}, v_2, v_3)$ is defined

$(\mathsf{app}\{\mathcal{U}\}\ \llparenthesis (v_0) \rrparenthesis^{\overline{\ell}_0}\ v_1)^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{A}}} \quad (\mathsf{TagErr})^{\ell_0}$
  if $v_0 \notin (\mathbb{T}_?\ \overline{b}\ (\lambda x.\, e)) \cup (\mathbb{T}_?\ \overline{b}\ (\mathbb{G}\ (\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell)\ v))$

$(\mathsf{app}\{\mathcal{U}\}\ \llparenthesis (\mathbb{T}_?\ \overline{b}_0\ \llparenthesis (\lambda x_0.\, e_0) \rrparenthesis^{\overline{\ell}_0}) \rrparenthesis^{\overline{\ell}_1}\ v_0)^{\ell_2} \quad \blacktriangleright_{\overline{\mathsf{A}}} \quad (\mathsf{trace}\ \overline{b}_0\ \llparenthesis (e_0[x_0 \leftarrow v_1]) \rrparenthesis^{\overline{\ell}_0})^{\overline{\ell}_1 \ell_2}$
  where $v_1 = \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), \llparenthesis (v_0) \rrparenthesis^{\ell_2 \mathit{rev}(\overline{\ell}_1) \mathit{rev}(\overline{\ell}_0)})$

$(\mathsf{app}\{\mathcal{U}\}\ \llparenthesis (\mathbb{T}_?\ \overline{b}_0\ \llparenthesis (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2}) \rrparenthesis^{\overline{\ell}_3}) \rrparenthesis^{\overline{\ell}_4}\ v_1)^{\ell_5} \quad \blacktriangleright_{\overline{\mathsf{A}}}$
    $\llparenthesis (\mathsf{trace}\ \overline{b}_0\ \llparenthesis (\mathsf{stat}\ b_0\ (\mathsf{app}\{\tau_1\}\ v_0\ (\mathsf{dyn}\ b_1\ v_2))^{\ell_2}) \rrparenthesis^{\overline{\ell}_3}) \rrparenthesis^{\overline{\ell}_4 \ell_5}$
  where $\tau_1 = \mathit{cod}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)$
  and $v_2 = \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), \llparenthesis (v_1) \rrparenthesis^{\ell_5 \mathit{rev}(\overline{\ell}_3 \overline{\ell}_4)})$

$(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)^{\ell_2} \quad \blacktriangleright_{\overline{\mathsf{A}}} \quad (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)^{\ell_2}$
  if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$ and $v_0 \in \llparenthesis \lambda(x : \tau).\, e \rrparenthesis^{\overline{\ell}} \cup \llparenthesis \langle v, v \rangle \rrparenthesis^{\overline{\ell}}$

$(\mathsf{stat}\ b_0\ \llparenthesis (\mathbb{G}\ b_1\ \llparenthesis (\mathbb{T}_?\ \overline{b}_2\ v_0) \rrparenthesis^{\overline{\ell}_0}) \rrparenthesis^{\overline{\ell}_1})^{\ell_2} \quad \blacktriangleright_{\overline{\mathsf{A}}} \quad (\mathsf{trace}\ (b_0 b_1 \overline{b}_2)\ \llparenthesis (v_0) \rrparenthesis^{\overline{\ell}_0 \overline{\ell}_1 \ell_2})^{\ell_2}$
  if $b_0 = (\ell_3 \blacktriangleleft \tau_0 \blacktriangleleft \ell_4)$ and $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
  and $v_0 \in \llparenthesis \lambda x.\, e \rrparenthesis^{\overline{\ell}} \cup \llparenthesis \langle v, v \rangle \rrparenthesis^{\overline{\ell}} \cup \llparenthesis \mathbb{G}\ b\ (\lambda(x : \tau).\, e) \rrparenthesis^{\overline{\ell}} \cup \llparenthesis \mathbb{G}\ b\ \langle v, v \rangle \rrparenthesis^{\overline{\ell}}$

$(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis (i_0) \rrparenthesis^{\overline{\ell}_2})^{\ell_3} \quad \blacktriangleright_{\overline{\mathsf{A}}} \quad (i_0)^{\ell_3}$
  if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, i_0)$

$(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis (v_0) \rrparenthesis^{\overline{\ell}_2})^{\ell_3} \quad \blacktriangleright_{\overline{\mathsf{A}}} \quad (\mathsf{InvariantErr})^{\ell_3}$
  if $\neg \mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$

$(\mathsf{trace}\ \overline{b}_0\ v_0)^{\ell_0} \quad \blacktriangleright_{\overline{\mathsf{A}}} \quad (v_1)^{\ell_0}$
  where $v_1 = \mathit{add\text{-}trace}(\overline{b}_0, v_0)$

Theorem 6.57 (Amnesic incomplete monitoring). *Amnesic does not satisfy* **CM**

Proof. When an untyped function crosses two boundaries, it loses a guard wrapper at the second boundary and gains a second ownership label.

$$
\begin{array}{ll}
\multicolumn{2}{l}{(\mathsf{stat}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ (\mathsf{dyn}\ (\ell_1 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_2)\ (\lambda x_0.\, x_0)^{\ell_2})^{\ell_1})^{\ell_0}} \\
\rightarrow_{\mathsf{A}} & (\mathsf{stat}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ (\mathbb{G}\ (\ell_1 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_2)\ (\lambda x_0.\, x_0)^{\ell_2})^{\ell_1})^{\ell_0} \\
\rightarrow_{\mathsf{A}} & (\!(\mathsf{trace}\ ((\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)(\ell_1 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_2)\ (\lambda x_0.\, x_0)^{\ell_2})\!)^{\ell_2 \ell_1 \ell_0}
\end{array}
$$

□

Theorem 6.58 (Amnesic blame soundness and completeness). *Amnesic satisfies* **BS** *and* **BC**

Proof Sketch. By preservation of path-owner consistency ($\Vdash_p$) for $\triangleright_{\overline{\mathsf{A}}}$ and $\blacktriangleright_{\overline{\mathsf{A}}}$. More details in appendix: lemma A.28. □

6.9.3 *Relation to Transient.*

$\boxed{e \approx e; \mathcal{H}; \mathcal{B}}$

$$\frac{v_0 \approx v_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{trace}\, \overline{b}_0\, v_0 \approx v_1; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{v_0 \approx \mathcal{H}_0(\mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0}{v_0 \approx \mathsf{p}_0; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{}{i_0 \approx i_0; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{}{\mathbb{T}\, \overline{b}_0\, i_0 \approx i_0; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{v_0 \approx v_2; \mathcal{H}_0; \mathcal{B}_0 \qquad v_1 \approx v_3; \mathcal{H}_0; \mathcal{B}_0}{\mathbb{T}_?\, \overline{b}_0\, \langle v_0, v_1 \rangle \approx \langle v_2, v_3 \rangle; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{v_0 \approx v_2; \mathcal{H}_0; \mathcal{B}_0 \qquad v_1 \approx v_3; \mathcal{H}_0; \mathcal{B}_0}{\mathbb{T}_?\, \overline{b}_0\, (\mathbb{G}\, b_0\, (\mathbb{T}_?\, \overline{b}_1\, \langle v_0, v_1 \rangle)) \approx \langle v_2, v_3 \rangle; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{v_0 \approx v_2; \mathcal{H}_0; \mathcal{B}_0 \qquad v_1 \approx v_3; \mathcal{H}_0; \mathcal{B}_0}{\mathbb{G}\, b_0\, (\mathbb{T}_?\, \overline{b}_0\, (\mathbb{G}\, b_1\, \langle v_0, v_1 \rangle)) \approx \langle v_2, v_3 \rangle; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\mathbb{T}_?\, \overline{b}_0\, (\lambda x_0.\, e_0) \approx \lambda x_0.\, e_1; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\mathbb{G}\, b_0\, (\mathbb{T}_?\, \overline{b}_0\, (\lambda x_0.\, e_0)) \approx \lambda x_0.\, e_1; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\mathbb{T}_?\, \overline{b}_0\, (\lambda (x_0 : \tau_0).\, e_0) \approx \lambda (x_0 : \tau_0).\, e_1; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\mathbb{T}_?\, \overline{b}_0\, (\mathbb{G}\, b_0\, (\lambda (x_0 : \tau_0).\, e_0)) \approx \lambda (x_0 : \tau_0).\, e_1; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\mathbb{G}\, b_0\, (\mathbb{T}_?\, \overline{b}_0\, (\mathbb{G}\, b_1\, (\lambda (x_0 : \tau_0).\, e_0))) \approx \lambda (x_0 : \tau_0).\, e_1; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{}{x_0 \approx x_0; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{e_0 \approx e_2; \mathcal{H}_0; \mathcal{B}_0 \qquad e_1 \approx e_3; \mathcal{H}_0; \mathcal{B}_0}{\langle e_0, e_1 \rangle \approx \langle e_2, e_3 \rangle; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{e_0 \approx e_2; \mathcal{H}_0; \mathcal{B}_0 \qquad e_1 \approx e_3; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, e_0\, e_1 \approx \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, e_2\, e_3; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\, e_0 \approx \mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\, e_1; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{e_0 \approx e_2; \mathcal{H}_0; \mathcal{B}_0 \qquad e_1 \approx e_3; \mathcal{H}_0; \mathcal{B}_0}{\mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, e_0\, e_1 \approx \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, e_2\, e_3; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{dyn}\, b_0\, e_0 \approx \mathsf{dyn}\, b_0\, e_1; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{stat}\, b_0\, e_0 \approx \mathsf{stat}\, b_0\, e_1; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, e_0 \approx \mathsf{check}\{\tau_0\}\, e_1\, \mathsf{p}_0; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, e_0 \approx \mathsf{check}\{\mathcal{U}\}\, e_1\, \mathsf{p}_0; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{\tau_1 \leqslant: \tau_0 \qquad e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{stat}\, (\ell_2 \blacktriangleleft \tau_1 \blacktriangleleft \ell_3)\, e_0) \approx \mathsf{check}\{\tau_0\}\, e_1\, \mathsf{p}_0; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\, e_0 \bullet \approx \mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\, e_1\, \mathsf{p}_0; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{}{\mathsf{InvariantErr} \approx \mathsf{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{}{\mathsf{TagErr} \approx \mathsf{TagErr}; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{}{\mathsf{DivErr} \approx \mathsf{DivErr}; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{v_0 \approx v_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{BoundaryErr}\, (b_0, v_0) \approx \mathsf{BoundaryErr}\, (b_0, v_1); \mathcal{H}_0; \mathcal{B}_0}$$

$\boxed{E \approx E; \mathcal{H}; \mathcal{B}}$

$$\frac{E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{trace}\ \overline{b}_0\ E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{}{[\,] \approx [\,]; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{E_0 \approx E_2; \mathcal{H}_0; \mathcal{B}_0 \qquad e_1 \approx e_3; \mathcal{H}_0; \mathcal{B}_0}{\langle E_0, e_1\rangle \approx \langle E_2, e_3\rangle; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{v_0 \approx v_2; \mathcal{H}_0; \mathcal{B}_0 \qquad E_1 \approx E_3; \mathcal{H}_0; \mathcal{B}_0}{\langle v_0, E_1\rangle \approx \langle v_2, E_3\rangle; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{E_0 \approx E_2; \mathcal{H}_0; \mathcal{B}_0 \qquad e_1 \approx e_3; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\ E_0\ e_1 \approx \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\ E_2\ e_3; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{v_0 \approx v_2; \mathcal{H}_0; \mathcal{B}_0 \qquad E_1 \approx E_3; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\ v_0\ E_1 \approx \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\ v_2\ E_3; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0}{\mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\ E_0 \approx \mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\ E_1; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{E_0 \approx E_2; \mathcal{H}_0; \mathcal{B}_0 \qquad e_1 \approx e_3; \mathcal{H}_0; \mathcal{B}_0}{\mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\ E_0\ e_1 \approx \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\ E_2\ e_3; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{v_0 \approx v_2; \mathcal{H}_0; \mathcal{B}_0 \qquad E_1 \approx E_3; \mathcal{H}_0; \mathcal{B}_0}{\mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\ v_0\ E_1 \approx \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\ v_2\ E_3; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{dyn}\ b_0\ E_0 \approx \mathsf{dyn}\ b_0\ E_1; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{stat}\ b_0\ E_0 \approx \mathsf{stat}\ b_0\ E_1; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{E_0 \notin \mathsf{stat}\ b\ E \qquad E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ E_0 \approx \mathsf{check}\{\tau_0\}\ E_1\ \mathsf{p}_0; \mathcal{H}_0; \mathcal{B}_0} \qquad \frac{E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ E_0 \approx \mathsf{check}\{\mathcal{U}\}\ E_1\ \mathsf{p}_0; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{\tau_1 \leqslant: \tau_0 \qquad E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\mathsf{stat}\ (\ell_2 \blacktriangleleft \tau_1 \blacktriangleleft \ell_3)\ E_0) \approx \mathsf{check}\{\tau_0\}\ E_1\ \mathsf{p}_0; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0}{\mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\ E_0\ \bullet \approx \mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\ E_1\ \mathsf{p}_0; \mathcal{H}_0; \mathcal{B}_0}$$

Theorem 6.59 (Transient Amnesic error equivalence). $T \approx A$

Proof. By lemma 6.60. □

Lemma 6.60. *If* $e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0$ *then:*

- *if* $e_0 \rightarrow_{\mathsf{A}} e_2$ *then* $e_2 \rightarrow^*_{\mathsf{A}} e_3$ *and* $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} e_4; \mathcal{H}_1; \mathcal{B}_1$ *and* $e_3 \approx e_4; \mathcal{H}_1; \mathcal{B}_1$
- *if* $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\mathsf{T}} e_3; \mathcal{H}_1; \mathcal{B}_1$ *then* $e_0 \rightarrow^*_{\mathsf{A}} e_2$ *and* $e_2 \approx e_3; \mathcal{H}_1; \mathcal{B}_1$

Proof Sketch. Amnesic may take extra steps at an elimination form and to combine traces into one wrapper. Transient takes extra steps to place pre-values on the heap and to conservatively check the result of elimination forms. The extra checks in Transient are problematic, however, because they may appear alongside any expression on the Amnesic side. A direct simulation would be messy; thus the $\approx$ relations above assume a variant of Amnesic that inserts check expressions after the application of an unwrapped function. Type preservation guarantees that such checks never fail. More details in appendix: lemma A.29. □

6.9.4 Relation to Forgetful.

$\boxed{v \lesssim v}$

$$\frac{}{i_0 \lesssim i_0} \qquad \frac{v_0 \lesssim v_2}{\langle v_0, v_1\rangle \lesssim \langle v_2, v_3\rangle} \qquad \frac{e_0 \lesssim e_1}{\lambda x_0.\, e_0 \lesssim \lambda x_0.\, e_1} \qquad \frac{e_0 \lesssim e_1}{\lambda(x_0 : \tau_0).\, e_0 \lesssim \lambda(x_0 : \tau_0).\, e_1}$$

$$\frac{b_0 \leqslant: b_1 \qquad v_0 \lesssim v_1}{\mathbb{G}\, b_0\, v_0 \lesssim \mathbb{G}\, b_1\, v_1} \qquad \frac{b_0 \leqslant: b_1 \qquad v_0 \lesssim v_1}{\mathbb{T}\, b_0\, v_0 \lesssim \mathbb{T}\, b_1\, v_1} \qquad \frac{b_0 \leqslant: b_1 \qquad \mathbb{T}\, \overline{b}_0\, v_0 \lesssim \mathbb{T}\, \overline{b}_1\, v_1}{\mathbb{T}\, b_0\overline{b}_0\, v_0 \lesssim \mathbb{T}\, b_1\overline{b}_1\, v_1}$$

$\boxed{e \lesssim e}$

$$\frac{}{x_0 \lesssim x_0} \qquad \frac{e_0 \lesssim e_2 \qquad e_1 \lesssim e_3}{\langle e_0, e_1\rangle \lesssim \langle e_2, e_3\rangle} \qquad \frac{e_0 \lesssim e_2 \qquad e_1 \lesssim e_3}{\mathsf{app}\{^{\tau}/_{\mathcal{U}}\}\, e_0\, e_1 \lesssim \mathsf{app}\{^{\tau}/_{\mathcal{U}}\}\, e_2\, e_3}$$

$$\frac{e_0 \lesssim e_1}{unop\{^{\tau}/_{\mathcal{U}}\}\, e_0 \lesssim unop\{^{\tau}/_{\mathcal{U}}\}\, e_1} \qquad \frac{e_0 \lesssim e_2 \qquad e_1 \lesssim e_3}{binop\{^{\tau}/_{\mathcal{U}}\}\, e_0\, e_1 \lesssim binop\{^{\tau}/_{\mathcal{U}}\}\, e_2\, e_3} \qquad \frac{b_0 \leqslant: b_1 \qquad e_0 \lesssim e_1}{\mathsf{dyn}\, b_0\, e_0 \lesssim \mathsf{dyn}\, b_1\, e_1}$$

$$\frac{b_0 \leqslant: b_1 \qquad e_0 \lesssim e_1}{\mathsf{stat}\, b_0\, e_0 \lesssim \mathsf{stat}\, b_1\, e_1} \qquad \frac{b_0 \leqslant: b_1 \qquad e_0 \lesssim e_1}{\mathsf{trace}\, b_0\, e_0 \lesssim \mathsf{trace}\, b_1\, e_1} \qquad \frac{b_0 \leqslant: b_1 \qquad \mathsf{trace}\, \overline{b}_0\, e_0 \lesssim \mathsf{trace}\, \overline{b}_1\, e_1}{\mathsf{trace}\, b_0\overline{b}_0\, e_0 \lesssim \mathsf{trace}\, b_1\overline{b}_1\, e_1}$$

$$\frac{}{\mathsf{TagErr} \lesssim \mathsf{TagErr}} \qquad \frac{}{\mathsf{DivErr} \lesssim \mathsf{DivErr}} \qquad \frac{}{\mathsf{BoundaryErr}\,(b_0, v_0) \lesssim e_1}$$

$\boxed{E \lesssim E}$

$$\frac{}{[\,] \lesssim [\,]} \qquad \frac{E_0 \lesssim E_2 \qquad e_1 \lesssim e_3}{\langle E_0, e_1\rangle \lesssim \langle E_2, e_3\rangle} \qquad \frac{v_0 \lesssim v_2 \qquad E_1 \lesssim E_3}{\langle v_0, E_1\rangle \lesssim \langle v_2, E_3\rangle}$$

$$\frac{E_0 \lesssim E_2 \qquad e_1 \lesssim e_3}{\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\; E_0\; e_1 \lesssim \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\; E_2\; e_3} \qquad \frac{v_0 \lesssim v_2 \qquad E_1 \lesssim E_3}{\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\; v_0\; E_1 \lesssim \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\; v_2\; E_3}$$

$$\frac{E_0 \lesssim E_1}{unop\{{}^{\tau}/_{\mathcal{U}}\}\; E_0 \lesssim unop\{{}^{\tau}/_{\mathcal{U}}\}\; E_1} \qquad \frac{E_0 \lesssim E_2 \qquad e_1 \lesssim e_3}{binop\{{}^{\tau}/_{\mathcal{U}}\}\; E_0\; e_1 \lesssim binop\{{}^{\tau}/_{\mathcal{U}}\}\; E_2\; e_3}$$

$$\frac{v_0 \lesssim v_2 \qquad E_1 \lesssim E_3}{binop\{{}^{\tau}/_{\mathcal{U}}\}\; v_0\; E_1 \lesssim binop\{{}^{\tau}/_{\mathcal{U}}\}\; v_2\; E_3} \qquad \frac{b_0 \leqslant: b_1 \qquad E_0 \lesssim E_1}{\mathsf{dyn}\; b_0\; E_0 \lesssim \mathsf{dyn}\; b_1\; E_1} \qquad \frac{b_0 \leqslant: b_1 \qquad E_0 \lesssim E_1}{\mathsf{stat}\; b_0\; E_0 \lesssim \mathsf{stat}\; b_1\; E_1}$$

$$\frac{b_0 \leqslant: b_1 \qquad E_0 \lesssim E_1}{\mathsf{trace}\; b_0\; E_0 \lesssim \mathsf{trace}\; b_1\; E_1} \qquad \frac{b_0 \leqslant: b_1 \qquad \mathsf{trace}\; \overline{b}_0\; E_0 \lesssim \mathsf{trace}\; \overline{b}_1\; E_1}{\mathsf{trace}\; b_0\overline{b}_0\; E_0 \lesssim \mathsf{trace}\; b_1\overline{b}_1\; E_1}$$

Theorem 6.61 (Forgetful Amnesic error preorder). $F \lesssim A$

Proof Sketch. By showing that $e \lesssim e$ is a lock-step bisimulation. More details in appendix: lemma A.36. □

Theorem 6.62. $A \not\lesssim F$

Proof. Forgetful checks the types that come from boundaries, but Amnesic checks local annotations. The annotations may be supertypes of the boundary types.

$e_0 = \mathsf{fst}\{\mathsf{Int}\}\,(\mathsf{dyn}\,(\ell_0 \blacktriangleleft (\mathsf{Nat}\times\mathsf{Nat}) \blacktriangleleft \ell_1)\ \langle -4, 4\rangle)$

Since −4 is an integer, Amnesic reduces to a value. Forgetful detects an error. □

6.10 Erasure and its Properties

6.10.1 Semantics, Type Soundness.

$\boxed{e \rhd_{\mathsf{E}} e}$

$$
\begin{array}{lll}
\mathit{unop}\{\tau_0\}\ v_0 & \rhd_{\mathsf{E}} & \mathsf{BoundaryErr}\,(\emptyset, v_0) \\
\quad \text{if } \delta(\mathit{unop}, v_0) \text{ is undefined} & & \\
\mathit{unop}\{\mathcal{U}\}\ v_0 & \rhd_{\mathsf{E}} & \mathsf{TagErr} \\
\quad \text{if } \delta(\mathit{unop}, v_0) \text{ is undefined} & & \\
\mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\ v_0 & \rhd_{\mathsf{E}} & \delta(\mathit{unop}, v_0) \\
\quad \text{if } \delta(\mathit{unop}, v_0) \text{ is defined} & & \\
\mathit{binop}\{\tau_0\}\ v_0\ v_1 & \rhd_{\mathsf{E}} & \mathsf{BoundaryErr}\,(\emptyset, v_0) \\
\quad \text{if } \delta(\mathit{binop}, v_0, v_1) \text{ is undefined and } v_0 \notin i & & \\
\mathit{binop}\{\tau_0\}\ v_0\ v_1 & \rhd_{\mathsf{E}} & \mathsf{BoundaryErr}\,(\emptyset, v_1) \\
\quad \text{if } \delta(\mathit{binop}, v_0, v_1) \text{ is undefined and } v_0 \in i \text{ and } v_1 \notin i & & \\
\mathit{binop}\{\mathcal{U}\}\ v_0\ v_1 & \rhd_{\mathsf{E}} & \mathsf{TagErr} \\
\quad \text{if } \delta(\mathit{binop}, v_0, v_1) \text{ is undefined} & & \\
\mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\ v_0\ v_1 & \rhd_{\mathsf{E}} & \delta(\mathit{binop}, v_0, v_1) \\
\quad \text{if } \delta(\mathit{binop}, v_0, v_1) \text{ is defined} & & \\
\mathsf{app}\{\tau_0\}\ v_0\ v_1 & \rhd_{\mathsf{E}} & \mathsf{BoundaryErr}\,(\emptyset, v_0) \\
\quad \text{if } v_0 \notin (\lambda x.\, e) \cup (\lambda(x : \tau).\, e) & & \\
\mathsf{app}\{\mathcal{U}\}\ v_0\ v_1 & \rhd_{\mathsf{E}} & \mathsf{TagErr} \\
\quad \text{if } v_0 \notin (\lambda x.\, e) \cup (\lambda(x : \tau).\, e) & & \\
\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\ (\lambda(x_0 : \tau_0).\, e_0)\ v_0 & \rhd_{\mathsf{E}} & e_0[x_0 \leftarrow v_0] \\
\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\ (\lambda x_0.\, e_0)\ v_0 & \rhd_{\mathsf{E}} & e_0[x_0 \leftarrow v_0] \\
\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 & \rhd_{\mathsf{E}} & v_0 \\
\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 & \rhd_{\mathsf{E}} & v_0
\end{array}
$$

$\boxed{e \rightarrow^*_{\mathsf{E}} e}$ is the transitive, reflexive, compatible (with respect to evaluation contexts E, section 6.2) closure of the relation $\rhd_{\mathsf{E}}$

Theorem 6.63 (Erasure unsoundness). *Erasure satisfies neither* $\mathbf{TS}\,(\mathbf{1})$ *nor* $\mathbf{TS}\,(\mathbf{s})$

Proof. Dynamic-to-static boundaries are unsound. A function, for example, can enter a typed context that expects an integer:

$$\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathsf{Int} \blacktriangleleft \ell_1)\,(\lambda x_0.\,42) \;\rhd_{\mathsf{E}}\; (\lambda x_0.\,42)$$

□

Theorem 6.64 (Erasure dyn soundness). *Erasure satisfies* $\mathbf{TS}\,(\mathbf{0})$

Proof. By progress (lemma 6.65) and preservation (lemma 6.66). □

Lemma 6.65 (Erasure type progress). *If* $\cdot \vdash_{\mathbf{0}} E_0[e_0] : \mathcal{U}$ *then one of the following holds:*

- $e_0 \in v \cup \mathsf{Err}$
- $\exists\, e_1.\, e_0 \rhd_{\mathsf{E}} e_1$

Proof Sketch. By unique decomposition (lemma 6.1) and case analysis. More details in appendix: lemma A.43. □

Lemma 6.66 (Erasure type preservation).
If $\cdot \vdash_{\mathbf{0}} e_0 : \mathcal{U}$ *and* $e_0 \rhd_{\mathsf{E}} e_1$ *then* $\cdot \vdash_{\mathbf{0}} e_1 : \mathcal{U}$.

Proof Sketch. By case analysis of the reduction relation. More details in appendix: lemma A.44. □

6.10.2 *Lifted Semantics, Complete Monitoring, Blame.*

$\boxed{(e)^{\ell} \rhd_{\overline{\mathsf{E}}} (e)^{\ell}}$ lifted version of $\rhd_{\mathsf{E}}$

$$
\begin{array}{ll}
(unop\{\tau_0\}\ (\!(v_0)\!)^{\overline{\ell_0}})^{\ell_0} & \rhd_{\overline{\mathsf{E}}}\ (\mathsf{BoundaryErr}\,(\emptyset, (\!(v_0)\!)^{\overline{\ell_0}}))^{\ell_0} \\
\quad \text{if } v_0 \notin (v)^{\ell} \text{ and } \delta(unop, v_0) \text{ is undefined} & \\
(unop\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}})^{\ell_0} & \rhd_{\overline{\mathsf{E}}}\ (\mathsf{TagErr})^{\ell_0} \\
\quad \text{if } v_0 \notin (v)^{\ell} \text{ and } \delta(unop, v_0) \text{ is undefined} & \\
(unop\{{}^{\tau}/_{\mathcal{U}}\}\ (\!(v_0)\!)^{\overline{\ell_0}})^{\ell_0} & \rhd_{\overline{\mathsf{E}}}\ (\delta(unop, v_0))^{\overline{\ell_0}\ell_0} \\
\quad \text{if } \delta(unop, v_0) \text{ is defined} & \\
(binop\{\tau_0\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ (\!(v_1)\!)^{\overline{\ell_1}})^{\ell_0} & \rhd_{\mathsf{E}}\ (\mathsf{BoundaryErr}\,(\emptyset, v_0))^{\ell_0} \\
\quad \text{if } v_0 \notin (v)^{\ell} \text{ and } v_1 \notin (v)^{\ell} \text{ and } \delta(binop, v_0, v_1) \text{ is undefined and } v_0 \notin i & \\
(binop\{\tau_0\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ (\!(v_1)\!)^{\overline{\ell_1}})^{\ell_0} & \rhd_{\mathsf{E}}\ (\mathsf{BoundaryErr}\,(\emptyset, v_1))^{\ell_0} \\
\quad \text{if } v_0 \notin (v)^{\ell} \text{ and } v_1 \notin (v)^{\ell} \text{ and } \delta(binop, v_0, v_1) \text{ is undefined and } v_0 \in i \text{ and } v_1 \notin i & \\
(binop\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ (\!(v_1)\!)^{\overline{\ell_1}})^{\ell_0} & \rhd_{\overline{\mathsf{E}}}\ (\mathsf{TagErr})^{\ell_0} \\
\quad \text{if } v_0 \notin (v)^{\ell} \text{ and } v_1 \notin (v)^{\ell} \text{ and } \delta(binop, v_0, v_1) \text{ is undefined} & \\
(binop\{{}^{\tau}/_{\mathcal{U}}\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ (\!(v_1)\!)^{\overline{\ell_1}})^{\ell_0} & \rhd_{\overline{\mathsf{E}}}\ (\delta(binop, v_0, v_1))^{\ell_0} \\
\quad \text{if } \delta(binop, v_0, v_1) \text{ is defined} & \\
(\mathsf{app}\{\tau_0\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ v_1)^{\ell_0} & \rhd_{\overline{\mathsf{E}}}\ (\mathsf{BoundaryErr}\,(\emptyset, (\!(v_0)\!)^{\overline{\ell_0}}))^{\ell_0} \\
\quad \text{if } v_0 \notin (v)^{\ell} \cup (\lambda x.\, e) \cup (\lambda (x : \tau).\, e) & \\
(\mathsf{app}\{\mathcal{U}\}\ (\!(v_0)\!)^{\overline{\ell_0}}\ v_1)^{\ell_0} & \rhd_{\overline{\mathsf{E}}}\ (\mathsf{TagErr})^{\ell_0} \\
\quad \text{if } v_0 \notin (v)^{\ell} \cup (\lambda x.\, e) \cup (\lambda (x : \tau).\, e) & \\
(\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\ (\!(\lambda (x_0 : \tau_0).\, e_0)\!)^{\overline{\ell_0}}\ v_0)^{\ell_0} & \rhd_{\overline{\mathsf{E}}}\ (\!(e_0[x_0 \leftarrow (\!(v_0)\!)^{\ell_0 rev(\overline{\ell_0})}])\!)^{\overline{\ell_0}\ell_0} \\
(\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\ (\!(\lambda x_0.\, e_0)\!)^{\overline{\ell_0}}\ v_0)^{\ell_0} & \rhd_{\overline{\mathsf{E}}}\ (\!(e_0[x_0 \leftarrow (\!(v_0)\!)^{\ell_0 rev(\overline{\ell_0})}])\!)^{\overline{\ell_0}\ell_0} \\
(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)^{\ell_0} & \rhd_{\overline{\mathsf{E}}}\ (v_0)^{\ell_0} \\
(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)^{\ell_0} & \rhd_{\overline{\mathsf{E}}}\ (v_0)^{\ell_0}
\end{array}
$$

THEOREM 6.67 (ERASURE INCOMPLETE MONITORING). *Erasure does not satisfy* **CM**

PROOF. The evaluation of a boundary term adds a new owner, breaking single-owner consistency. For example, $(\mathsf{dyn}\ (\ell_0 \blacktriangleleft (\mathsf{Int} \Rightarrow \mathsf{Nat}) \blacktriangleleft \ell_1)\ (\lambda x_0.\, x_0)^{\ell_1})^{\ell_0} \rhd_{\overline{\mathsf{E}}} ((\lambda x_0.\, x_0))^{\ell_0 \ell_1}$. □

THEOREM 6.68 (ERASURE BLAME SOUNDNESS). *Erasure satisfies* **BS**

PROOF. By inspection, the only Erasure rules that raise a boundary error blame the empty set. An empty set is trivially blame sound. □

THEOREM 6.69 (ERASURE BLAME INCOMPLETENESS). *Erasure does not satisfy* **BC**

PROOF. The empty set is trivially incomplete, because every value has at least one label for its context. □

6.10.3 Relation to Amnesic.

$\boxed{v \lesssim v}$

$$\frac{}{i_0 \lesssim i_0} \qquad \frac{v_0 \lesssim v_2}{\langle v_0, v_1\rangle \lesssim \langle v_2, v_3\rangle} \qquad \frac{e_0 \lesssim e_1}{\lambda x_0.\, e_0 \lesssim \lambda x_0.\, e_1} \qquad \frac{e_0 \lesssim e_1}{\lambda(x_0 : \tau_0).\, e_0 \lesssim \lambda(x_0 : \tau_0).\, e_1}$$

$$\frac{v_0 \lesssim v_1}{\mathbb{G}\, b_0\, v_0 \lesssim v_1} \qquad \frac{v_0 \lesssim v_1}{\mathbb{T}\, \overline{b}_0\, v_0 \lesssim v_1}$$

$\boxed{e \lesssim e}$

$$\frac{}{x_0 \lesssim x_0} \qquad \frac{e_0 \lesssim e_2 \qquad e_1 \lesssim e_3}{\langle e_0, e_1\rangle \lesssim \langle e_2, e_3\rangle} \qquad \frac{e_0 \lesssim e_2 \qquad e_1 \lesssim e_3}{\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, e_0\, e_1 \lesssim \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, e_2\, e_3}$$

$$\frac{e_0 \lesssim e_1}{\mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\, e_0 \lesssim \mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\, e_1} \qquad \frac{e_0 \lesssim e_2 \qquad e_1 \lesssim e_3}{\mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, e_0\, e_1 \lesssim \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, e_2\, e_3} \qquad \frac{e_0 \lesssim e_1}{\mathsf{dyn}\, b_0\, e_0 \lesssim \mathsf{dyn}\, b_0\, e_1}$$

$$\frac{e_0 \lesssim e_1}{\mathsf{stat}\, b_0\, e_0 \lesssim \mathsf{stat}\, b_0\, e_1} \qquad \frac{e_0 \lesssim e_1}{\mathsf{dyn}\, b_0\, e_0 \lesssim e_1} \qquad \frac{e_0 \lesssim e_1}{\mathsf{stat}\, b_0\, e_0 \lesssim e_1} \qquad \frac{e_0 \lesssim e_1}{\mathsf{trace}\, \overline{b}_0\, e_0 \lesssim e_1}$$

$$\frac{}{\mathsf{TagErr} \lesssim \mathsf{TagErr}} \qquad \frac{}{\mathsf{DivErr} \lesssim \mathsf{DivErr}} \qquad \frac{}{\mathsf{BoundaryErr}\,(b_0, v_0) \lesssim e_1}$$

$$\frac{}{\mathsf{TagErr} \lesssim \mathsf{BoundaryErr}\,(b_0, v_0)}$$

$\boxed{E \lesssim E}$

$$\frac{}{[\,] \lesssim [\,]} \qquad \frac{E_0 \lesssim E_2 \qquad e_1 \lesssim e_3}{\langle E_0, e_1\rangle \lesssim \langle E_2, e_3\rangle} \qquad \frac{v_0 \lesssim v_2 \qquad E_1 \lesssim E_3}{\langle v_0, E_1\rangle \lesssim \langle v_2, E_3\rangle} \qquad \frac{E_0 \lesssim E_2 \qquad e_1 \lesssim e_3}{\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, E_0\, e_1 \lesssim \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, E_2\, e_3}$$

$$\frac{v_0 \lesssim v_2 \qquad E_1 \lesssim E_3}{\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, v_0\, E_1 \lesssim \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, v_2\, E_3} \qquad \frac{E_0 \lesssim E_1}{\mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\, E_0 \lesssim \mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\, E_1}$$

$$\frac{E_0 \lesssim E_2 \qquad e_1 \lesssim e_3}{\mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, E_0\, e_1 \lesssim \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, E_2\, e_3} \qquad \frac{v_0 \lesssim v_2 \qquad E_1 \lesssim E_3}{\mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, v_0\, E_1 \lesssim \mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, v_2\, E_3}$$

$$\frac{E_0 \lesssim E_1}{\mathsf{dyn}\, b_0\, E_0 \lesssim \mathsf{dyn}\, b_0\, E_1} \qquad \frac{E_0 \lesssim E_1}{\mathsf{stat}\, b_0\, E_0 \lesssim \mathsf{stat}\, b_0\, E_1} \qquad \frac{E_0 \lesssim E_1}{\mathsf{trace}\, \overline{b}_0\, E_0 \lesssim E_1}$$

Theorem 6.70 (Amnesic Erasure error preorder). $A \lesssim E$

Proof. By lemma 6.72 and that $e_0 \lesssim \mathsf{BoundaryErr}\,(\overline{b}_1, v_1)$ implies $e_0 \in \mathsf{BoundaryErr}\,(b, v)$. □

Theorem 6.71. $E \not\lesssim A$

Proof. Because Amnesic enforces types at boundaries. For example, $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathsf{Nat} \blacktriangleleft \ell_1)\ {-1}$ raises a boundary error in Amnesic and computes a negative number in Erasure. □

Lemma 6.72.
There is a stuttering simulation between Amnesic and Erasure. More precisely, the following two results hold:

- *If* $e_0 \lesssim e_2$ *and* $e_0 \rightarrow_{\mathsf{A}} e_1$ *then* $\exists\, e_3, e_4$ *such that* $e_1 \rightarrow^*_{\mathsf{A}} e_3$ *and* $e_2 \rightarrow_{\mathsf{E}} e_4$ *and* $e_3 \lesssim e_4$*.*
- *If* $e_0 \lesssim e_2$ *and* $e_2 \rightarrow_{\mathsf{E}} e_3$ *then* $\exists\, e_1$ *and* $e_0 \rightarrow^*_{\mathsf{A}} e_1$ *and* $e_1 \lesssim e_4$

Proof Sketch. Amnesic takes extra steps to unwrap at elimination forms and to combine traces into a single wrapper. More details in appendix: lemma A.45. □

A PROOFS

A.1 Natural

Lemma A.1 (Natural type progress). *If* $\cdot \vdash_1 E_0[e_0] : {}^{\tau}/_{\mathcal{U}}$ *and* $N(E_0[e_0])$ *then one of the following holds:*

- $e_0 \in v \cup \mathsf{Err}$
- ${}^{\tau}/_{\mathcal{U}} \in \tau$ *and* $\exists\, e_1.\ e_0 \triangleright_{\mathsf{N}} e_1$
- ${}^{\tau}/_{\mathcal{U}} \in \mathcal{U}$ *and* $\exists\, e_1.\ e_0 \blacktriangleright_{\mathsf{N}} e_1$

Proof. By unique decomposition (lemma 6.1) and case analysis:

Case: $\cdot \vdash_1 n_0 : \mathsf{Nat}$
Immediate.
Case: $\cdot \vdash_1 i_0 : \mathsf{Int}$
Immediate.
Case: $\cdot \vdash_1 \lambda(x_0 : \tau_0).\, e_1 : \tau_0 \Rightarrow \tau_1$
Immediate.
Case: $\cdot \vdash_1 \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$
Immediate.
Case: $\cdot \vdash_1 \mathit{unop}\{\tau_0\}\, v_0 : \tau_0$
- $\triangleright_{\mathsf{N}}\ \delta(\mathit{unop}, v_0)$ if defined
- $\triangleright_{\mathsf{N}}\ \mathsf{Err}$ otherwise

Case: $\cdot \vdash_1 \mathit{binop}\{\tau_0\}\, v_0\, v_1 : \tau_0$
- $\triangleright_{\mathsf{N}}\ \delta(\mathit{binop}, v_0, v_1)$ if defined
- $\triangleright_{\mathsf{N}}\ \mathsf{Err}$ otherwise

Case: $\cdot \vdash_1 \mathsf{app}\{\tau_0\}\, v_0\, v_1 : \tau_0$
- $\triangleright_{\mathsf{N}}\ e_1[x_0 \leftarrow v_1]$
  if $v_0 = \lambda(\tau_1 : x_0).\, e_1$
- $\triangleright_{\mathsf{N}}\ \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ (\mathsf{app}\{\mathcal{U}\}\ v_2\ (\mathsf{stat}\ (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\ v_1))$
  if $v_0 = \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1)\ v_2$
- $\triangleright_{\mathsf{N}}\ \mathsf{Err}$ otherwise

Case: $\cdot \vdash_1 \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 : \tau_0$
- $\triangleright_{\mathsf{N}}\ \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0$
  if $\tau_0 \in \tau \Rightarrow \tau$ and $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
- $\triangleright_{\mathsf{N}}\ \langle (\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_1), (\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\ v_2) \rangle$
  if $\tau_0 = \tau_1 \times \tau_2$ and $v_0 = \langle v_1, v_2 \rangle$
- $\triangleright_{\mathsf{N}}\ v_0$
  if $v_0 \in i$ and $\tau_0 \in \mathsf{Int}$
- $\triangleright_{\mathsf{N}}\ v_0$
  if $v_0 \in n$ and $\tau_0 \in \mathsf{Nat}$
- $\triangleright_{\mathsf{N}}\ \mathsf{Err}$ otherwise

Case: $\cdot \vdash_1 \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1)\ v_0 : \tau_0$
Immediate.
Case: $\cdot \vdash_1 \mathsf{Err} : \tau_0$
Immediate.
Case: $\cdot \vdash_1 i : \mathcal{U}$
Immediate.
Case: $\cdot \vdash_1 \lambda x_0.\, e_0 : \mathcal{U}$
Immediate.

Case: $\cdot \vdash_1 \langle v_0, v_1 \rangle : \mathcal{U}$

Immediate.

Case: $\cdot \vdash_1 \mathit{unop}\{\mathcal{U}\}\, v_0 : \mathcal{U}$

- $\blacktriangleright_{\mathsf{N}}\ \delta(\mathit{unop}, v_0)$ if defined
- $\blacktriangleright_{\mathsf{N}}\ \mathsf{Err}$ otherwise

Case: $\cdot \vdash_1 \mathit{binop}\{\mathcal{U}\}\, v_0\, v_1 : \mathcal{U}$

- $\blacktriangleright_{\mathsf{N}}\ \delta(\mathit{binop}, v_0, v_1)$ if defined
- $\blacktriangleright_{\mathsf{N}}\ \mathsf{Err}$ otherwise

Case: $\cdot \vdash_1 \mathsf{app}\{\mathcal{U}\}\, v_0\, v_1 : \mathcal{U}$

- $\blacktriangleright_{\mathsf{N}}\ e_1[x_0 \leftarrow v_1]$
  if $v_0 = \lambda x_0.\, e_1$
- $\blacktriangleright_{\mathsf{N}}\ \mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{app}\{\tau_0\}\, v_2\, (\mathsf{dyn}\, (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1))$
  if $v_0 = \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1)\, v_2$
- $\blacktriangleright_{\mathsf{N}}\ \mathsf{Err}$ otherwise

Case: $\cdot \vdash_1 \mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 : \mathcal{U}$

- $\blacktriangleright_{\mathsf{N}}\ \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0$
  if $\tau_0 \in \tau \Rightarrow \tau$ and $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
- $\blacktriangleright_{\mathsf{N}}\ \langle (\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_1), (\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\, v_2) \rangle$
  if $\tau_0 = \tau_1 \times \tau_2$ and $v_0 = \langle v_1, v_2 \rangle$
- $\blacktriangleright_{\mathsf{N}}\ v_0$
  if $v_0 \in i$ and $\tau_0 \in \mathsf{Int}$
- $\blacktriangleright_{\mathsf{N}}\ v_0$
  if $v_0 \in n$ and $\tau_0 \in \mathsf{Nat}$
- $\blacktriangleright_{\mathsf{N}}\ \mathsf{Err}$ otherwise

Case: $\cdot \vdash_1 \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1)\, v_0 : \mathcal{U}$

Immediate.

Case: $\cdot \vdash_1 \mathsf{Err} : \mathcal{U}$

Immediate.

$\square$

Lemma A.2 (Natural type preservation).
If $\cdot \vdash_1 E_0[e_0] : {}^{\tau}/_{\mathcal{U}}$ *and* $N(E_0[e_0])$ *and* $e_0(\rhd_N \cup \blacktriangleright_N)e_1$ *then* $\cdot \vdash_1 E_0[e_1] : {}^{\tau}/_{\mathcal{U}}$ *and* $N(E_0[e_1])$*.*

Proof. By case analysis of each reduction relation:

Case: $unop\{\tau_0\}\, v_0 \rhd_N \mathsf{InvariantErr}$
Immediate.
Case: $unop\{\tau_0\}\, v_0 \rhd_N \delta(unop, v_0)$
By lemma 6.2.
Case: $binop\{\tau_0\}\, v_0\, v_1 \rhd_N \mathsf{InvariantErr}$
Immediate.
Case: $binop\{\tau_0\}\, v_0\, v_1 \rhd_N \delta(binop, v_0, v_1)$
By lemma 6.2.
Case: $\mathsf{app}\{\tau_0\}\, v_0\, v_1 \rhd_N \mathsf{InvariantErr}$
Immediate.
Case: $\mathsf{app}\{\tau_0\}\, (\lambda(x_0 : \tau_1).\, e_0)\, v_0 \rhd_N e_0[x_0 \leftarrow v_0]$
By substitution lemmas for typed functions and for $N(\cdot)$.
Case: $\mathsf{app}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_2) \blacktriangleleft \ell_1)\, v_0)\, v_1 \rhd_N \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_0\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1))$
(1) $\cdot \vdash_1 v_0 : \mathcal{U}$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 v_1 : \tau_1$
By $\vdash_1$ on the redex
(3) $\cdot \vdash_1 \mathsf{stat}\, (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1 : \mathcal{U}$
By (2)
(4) $\cdot \vdash_1 \mathsf{app}\{\mathcal{U}\}\, v_0\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1) : \mathcal{U}$
By (1) and (3)
(5) $\tau_2 \leqslant: \tau_0$
By $\vdash_1$ on the redex
(6) $\cdot \vdash_1 \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_0\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1)) : \tau_0$
By (4) and (5)
(7) $N(\mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_0\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1)))$
By similar reasoning
Case: $\mathsf{dyn}\, (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\, v_0 \rhd_N \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\, v_0$
(1) $\cdot \vdash_1 v_0 : \mathcal{U}$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\, v_0 : \tau_0 \Rightarrow \tau_1$
By (1)
Case: $\mathsf{dyn}\, (\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1)\, \langle v_0, v_1 \rangle \rhd_N \langle \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0, \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_1 \rangle$
(1) $\cdot \vdash_1 v_0 : \mathcal{U}$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 v_1 : \mathcal{U}$
By $\vdash_1$ on the redex
(3) $\cdot \vdash_1 \langle \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0, \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_1 \rangle : \tau_0 \times \tau_1$
By (1) and (2)
Case: $\mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathsf{Int} \blacktriangleleft \ell_1)\, i_0 \rhd_N i_0$
Immediate.
Case: $\mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathsf{Nat} \blacktriangleleft \ell_1)\, n_0 \rhd_N n_0$
Immediate.

Case: $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \vartriangleright_{\mathsf{N}} \mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), v_0)$
Immediate.
Case: $unop\{\mathcal{U}\}\ v_0 \blacktriangleright_{\mathsf{N}} \mathsf{TagErr}$
Immediate.
Case: $unop\{\mathcal{U}\}\ v_0 \blacktriangleright_{\mathsf{N}} \delta(unop, v_0)$
Immediate.
Case: $binop\{\mathcal{U}\}\ v_0\ v_1 \blacktriangleright_{\mathsf{N}} \mathsf{TagErr}$
Immediate.
Case: $binop\{\mathcal{U}\}\ v_0\ v_1 \blacktriangleright_{\mathsf{N}} \delta(binop, v_0, v_1)$
Immediate.
Case: $\mathsf{app}\{\mathcal{U}\}\ v_0\ v_1 \blacktriangleright_{\mathsf{N}} \mathsf{TagErr}$
Immediate.
Case: $\mathsf{app}\{\mathcal{U}\}\ (\lambda x_0.\, e_0)\ v_0 \blacktriangleright_{\mathsf{N}} e_0[x_0 \leftarrow v_0]$
By substitution lemmas for untyped functions and for $N(\cdot)$.
Case: $\mathsf{app}\{\mathcal{U}\}\ (\mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_2) \blacktriangleleft \ell_1)\ v_0)\ v_1 \blacktriangleright_{\mathsf{N}} \mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\ (\mathsf{app}\{\tau_2\}\ v_0\ (\mathsf{dyn}\ (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\ v_1))$
(1) $\cdot \vdash_1 v_0 : \tau_1 \Rightarrow \tau_2$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 v_1 : \mathcal{U}$
By $\vdash_1$ on the redex
(3) $\cdot \vdash_1 \mathsf{dyn}\ (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\ v_1 : \tau_1$
By (2)
(4) $\cdot \vdash_1 \mathsf{app}\{\tau_2\}\ v_0\ (\mathsf{dyn}\ (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\ v_1) : \tau_2$
By (1) and (3)
(5) $\cdot \vdash_1 \mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\ (\mathsf{app}\{\tau_2\}\ v_0\ (\mathsf{dyn}\ (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\ v_1)) : \mathcal{U}$
By (4)
Case: $\mathsf{stat}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ v_0 \blacktriangleright_{\mathsf{N}} \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ v_0$
(1) $\cdot \vdash_1 v_0 : \tau_0 \Rightarrow \tau_1$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ v_0 : \mathcal{U}$
By (1)
Case: $\mathsf{stat}\ (\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1)\ \langle v_0, v_1 \rangle \blacktriangleright_{\mathsf{N}} \langle \mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0, \mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_1 \rangle$
(1) $\cdot \vdash_1 v_0 : \tau_0$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 v_1 : \tau_1$
By $\vdash_1$ on the redex
(3) $\cdot \vdash_1 \langle \mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0, \mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_1 \rangle : \mathcal{U}$
By (1) and (2)
Case: $\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathsf{Int} \blacktriangleleft \ell_1)\ i_0 \blacktriangleright_{\mathsf{N}} i_0$
Immediate.
Case: $\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathsf{Nat} \blacktriangleleft \ell_1)\ n_0 \blacktriangleright_{\mathsf{N}} n_0$
Immediate.
Case: $\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \blacktriangleright_{\mathsf{N}} \mathsf{InvariantErr}$
Immediate.

□

Theorem A.3 (Natural complete monitoring). *Natural satisfies* **CM**

Proof. By preservation of single-owner consistency ($\Vdash$) for $\rhd_{\overline{\mathsf{N}}}$ and $\blacktriangleright_{\overline{\mathsf{N}}}$.

Case: $(unop\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell_0}})^{\ell_0} \rhd_{\overline{\mathsf{N}}} (\mathsf{InvariantErr})^{\ell_0}$

Immediate: $\ell_0; \cdot \Vdash (\mathsf{TagErr})^{\ell_0}$

Case: $(unop\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell_0}})^{\ell_0} \rhd_{\overline{\mathsf{N}}} (\delta(unop, v_0))^{\overline{\ell_0}\ell_0}$

(1) $v_0 = \langle v_1, v_2\rangle$ and $\delta(unop, v_0) \in \{v_1, v_2\}$
By definition

(2) $\ell_0; \cdot \Vdash v_0$
By $\Vdash$ on the redex

(3) $\ell_0; \cdot \Vdash v_1$ and $\ell_0; \cdot \Vdash v_2$
By (2)

(4) $\ell_0; \cdot \Vdash \delta(unop, v_0)$
By (1) and (3)

Case: $(binop\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell_0}}\,(\!(v_1)\!)^{\overline{\ell_1}})^{\ell_0} \rhd_{\overline{\mathsf{N}}} (\mathsf{InvariantErr})^{\ell_0}$

Immediate.

Case: $(binop\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell_0}}\,(\!(v_1)\!)^{\overline{\ell_1}})^{\ell_0} \rhd_{\overline{\mathsf{N}}} (\delta(binop, v_0, v_1))^{\ell_0}$

(1) $\delta(binop, v_0, v_1) \in i$
By definition of δ

(2) $\ell_0; \cdot \Vdash \delta(binop, v_0, v_1)$
By (1)

Case: $(\mathsf{app}\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell_0}}\,v_1)^{\ell_0} \rhd_{\overline{\mathsf{N}}} (\mathsf{InvariantErr})^{\ell_0}$

Immediate.

Case: $(\mathsf{app}\{\tau_0\}\,(\!(\lambda(x_0 : \tau_1).\,e_0)\!)^{\overline{\ell_0}}\,v_1)^{\ell_0} \rhd_{\overline{\mathsf{N}}} (\!(e_0[x_0 \leftarrow (\!(v_1)\!)^{\ell_0 rev(\overline{\ell_0})}])\!)^{\overline{\ell_0}\ell_0}$

(1) $\ell_0; \cdot \Vdash \lambda(x_0 : \tau_1).\,e_0$
By $\Vdash$ on the redex

(2) $\ell_0; \cdot \Vdash v_0$
By $\Vdash$ on the redex

(3) $\ell_0; \cdot \Vdash (\!(v_0)\!)^{\ell_0 rev(\overline{\ell_0})}$
By (1) and (2)

(4) $\ell_0; \cdot \Vdash x_0$ for each occurrence of x_0 in e_0
By $\Vdash$ on the redex

(5) $\ell_0; \cdot \Vdash (\!(e_0[x_0 \leftarrow (\!(v_1)\!)^{\ell_0 rev(\overline{\ell_0})}])\!)^{\overline{\ell_0}\ell_0}$
By (3) and (4)

Case: $(\mathsf{app}\{\tau_0\}\,(\!(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(v_0)^{\ell_2})\!)^{\overline{\ell_0}}\,v_1)^{\ell_3} \rhd_{\overline{\mathsf{N}}}$

$(\!(\mathsf{dyn}\,(\ell_0 \blacktriangleleft cod(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\,v_0\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\,(\!(v_1)\!)^{\ell_3 rev(\overline{\ell_0})}))^{\ell_2})\!)^{\overline{\ell_0}\ell_3}$

(1) $\ell_2; \cdot \Vdash v_0$
By $\Vdash$ on the redex

(2) $\ell_3; \cdot \Vdash v_1$
By $\Vdash$ on the redex

(3) $\ell_3; \cdot \Vdash (\!(v_1)\!)^{\ell_3 rev(\overline{\ell_0})}$
By (2) and $\Vdash$ on the redex

(4) $\ell_2; \cdot \Vdash \mathsf{stat}\,(\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\,(\!(v_1)\!)^{\ell_3 rev(\overline{\ell_0})}$
By (3) and $\Vdash$ on the redex

(5) $\ell_3; \cdot \Vdash (\!(\mathsf{dyn}\,(\ell_0 \blacktriangleleft cod(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\,v_0\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\,(\!(v_1)\!)^{\ell_3 rev(\overline{\ell_0})}))^{\ell_2}\,)\!)^{\overline{\ell_0}\ell_3}$
By (1) and (4)

Case: $(\mathsf{dyn}\,(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\,(\!(v_0)\!)^{\overline{\ell_0}})^{\ell_2} \rhd_{\overline{\mathsf{N}}} (\mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\,(\!(v_0)\!)^{\overline{\ell_0}})^{\ell_2}$
Immediate.

Case: $(\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\!(\langle v_0, v_1\rangle)\!)^{\overline{\ell_0}})^{\ell_2} \rhd_{\overline{\mathsf{N}}}$
$(\langle \mathsf{dyn}\,(\ell_0 \blacktriangleleft fst(\tau_0) \blacktriangleleft \ell_1)\,(\!(v_0)\!)^{\overline{\ell_0}}, \mathsf{dyn}\,(\ell_0 \blacktriangleleft snd(\tau_0) \blacktriangleleft \ell_1)\,(\!(v_1)\!)^{\overline{\ell_0}}\rangle)^{\ell_2}$

(1) $\ell_1; \cdot \Vdash (\!(v_0)\!)^{\overline{\ell_0}}$ and $\ell_1; \cdot \Vdash (\!(v_1)\!)^{\overline{\ell_0}}$
By $\Vdash$ on the redex

(2) $\ell_2; \cdot \Vdash \langle \mathsf{dyn}\,(\ell_0 \blacktriangleleft fst(\tau_0) \blacktriangleleft \ell_1)\,(\!(v_0)\!)^{\overline{\ell_0}}, \mathsf{dyn}\,(\ell_0 \blacktriangleleft snd(\tau_0) \blacktriangleleft \ell_1)\,(\!(v_1)\!)^{\overline{\ell_0}}\rangle$
By (1) and $\Vdash$ on the redex

Case: $(\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\!(i_0)\!)^{\overline{\ell_0}})^{\ell_2} \rhd_{\overline{\mathsf{N}}} (i_0)^{\ell_2}$
Immediate.

Case: $(\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\!(v_0)\!)^{\overline{\ell_0}})^{\ell_2} \rhd_{\overline{\mathsf{N}}} (\mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), (\!(v_0)\!)^{\overline{\ell_0}}))^{\ell_2}$
Immediate.

Case: $(unop\{\mathcal{U}\}\,(\!(v_0)\!)^{\overline{\ell_0}})^{\ell_0} \blacktriangleright_{\overline{\mathsf{N}}} (\mathsf{TagErr})^{\ell_0}$
Immediate.

Case: $(unop\{\mathcal{U}\}\,(\!(v_0)\!)^{\overline{\ell_0}})^{\ell_0} \blacktriangleright_{\overline{\mathsf{N}}} (\delta(unop, v_0))^{\overline{\ell_0}\ell_0}$

(1) $v_0 = \langle v_1, v_2\rangle$ and $\delta(unop, v_0) \in \{v_1, v_2\}$
By definition

(2) $\ell_0; \cdot \Vdash v_0$
By $\Vdash$ on the redex

(3) $\ell_0; \cdot \Vdash v_1$ and $\ell_0; \cdot \Vdash v_2$
By (2)

(4) $\ell_0; \cdot \Vdash \delta(unop, v_0)$
By (1) and (3)

Case: $(binop\{\mathcal{U}\}\,(\!(v_0)\!)^{\overline{\ell_0}}\,(\!(v_1)\!)^{\overline{\ell_1}})^{\ell_0} \blacktriangleright_{\overline{\mathsf{N}}} (\mathsf{TagErr})^{\ell_0}$
Immediate.

Case: $(binop\{\mathcal{U}\}\,(\!(v_0)\!)^{\overline{\ell_0}}\,(\!(v_1)\!)^{\overline{\ell_1}})^{\ell_0} \blacktriangleright_{\overline{\mathsf{N}}} (\delta(binop, v_0, v_1))^{\ell_0}$

(1) $\delta(binop, v_0, v_1) \in i$
By definition of δ

(2) $\ell_0; \cdot \Vdash \delta(binop, v_0, v_1)$
By (1)

Case: $(\mathsf{app}\{\mathcal{U}\}\,(\!(v_0)\!)^{\overline{\ell_0}}\,v_1)^{\ell_0} \blacktriangleright_{\overline{\mathsf{N}}} (\mathsf{TagErr})^{\ell_0}$
Immediate.

Case: $(\mathsf{app}\{\mathcal{U}\}\,(\!(\lambda x_0.\,e_0)\!)^{\overline{\ell_0}}\,v_1)^{\ell_0} \blacktriangleright_{\overline{\mathsf{N}}} (\!(e_0[x_0 \leftarrow (\!(v_1)\!)^{\ell_0 rev(\overline{\ell_0})}])\!)^{\overline{\ell_0}\ell_0}$

(1) $\ell_0; \cdot \Vdash \lambda x_0.\,e_0$
By $\Vdash$ on the redex

(2) $\ell_0; \cdot \Vdash v_0$
By $\Vdash$ on the redex

(3) $\ell_0; \cdot \Vdash (\!(v_0)\!)^{\ell_0 rev(\overline{\ell}_0)}$
By (1) and (2)
(4) $\ell_0; \cdot \Vdash x_0$ for each occurrence of x_0 in e_0
By $\Vdash$ on the redex
(5) $\ell_0; \cdot \Vdash (\!(e_0[x_0 \leftarrow (\!(v_1)\!)^{\ell_0 rev(\overline{\ell}_0)}])\!)^{\overline{\ell}_0 \ell_0}$
By (3) and (4)

Case: $(\mathsf{app}\{\mathcal{U}\}\ (\!(\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2})\!)^{\overline{\ell}_0}\ v_1)^{\ell_3} \blacktriangleright_{\overline{\mathsf{N}}}$

$(\!(\mathsf{stat}\ (\ell_0 \blacktriangleleft cod(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{app}\{cod(\tau_0)\}\ v_0\ (\mathsf{dyn}\ (\ell_1 \blacktriangleleft dom(\tau_0) \blacktriangleleft \ell_0)\ (\!(v_1)\!)^{\ell_3 rev(\overline{\ell}_0)}))^{\ell_2})\!)^{\overline{\ell}_0 \ell_3}$
(1) $\ell_2; \cdot \Vdash v_0$
By $\Vdash$ on the redex
(2) $\ell_3; \cdot \Vdash v_1$
By $\Vdash$ on the redex
(3) $\ell_3; \cdot \Vdash (\!(v_1)\!)^{\ell_3 rev(\overline{\ell}_0)}$
By (2) and $\Vdash$ on the redex
(4) $\ell_2; \cdot \Vdash \mathsf{dyn}\ (\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\ (\!(v_1)\!)^{\ell_3 rev(\overline{\ell}_0)}$
By (3) and $\Vdash$ on the redex
(5) $\ell_3; \cdot \Vdash (\!(\mathsf{stat}\ (\ell_0 \blacktriangleleft cod(\tau_1) \blacktriangleleft \ell_1)\ (\mathsf{app}\{cod(\tau_0)\}\ v_0\ (\mathsf{dyn}\ (\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\ (\!(v_1)\!)^{\ell_3 rev(\overline{\ell}_0)}))^{\ell_2})\!)^{\overline{\ell}_0 \ell_3}$
By (1) and (4)

Case: $(\mathsf{stat}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell}_0})^{\ell_2} \blacktriangleright_{\overline{\mathsf{N}}} (\mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell}_0})^{\ell_2}$
Immediate.

Case: $(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(\langle v_0, v_1\rangle)\!)^{\overline{\ell}_0})^{\ell_2} \blacktriangleright_{\overline{\mathsf{N}}}$

$(\langle \mathsf{stat}\ (\ell_0 \blacktriangleleft fst(\tau_0) \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell}_0}, \mathsf{stat}\ (\ell_0 \blacktriangleleft snd(\tau_0) \blacktriangleleft \ell_1)\ (\!(v_1)\!)^{\overline{\ell}_0}\rangle)^{\ell_2}$
(1) $\ell_1; \cdot \Vdash (\!(v_0)\!)^{\overline{\ell}_0}$ and $\ell_1; \cdot \Vdash (\!(v_1)\!)^{\overline{\ell}_0}$
By $\Vdash$ on the redex
(2) $\ell_2; \cdot \Vdash \langle \mathsf{stat}\ (\ell_0 \blacktriangleleft fst(\tau_0) \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell}_0}, \mathsf{stat}\ (\ell_0 \blacktriangleleft snd(\tau_0) \blacktriangleleft \ell_1)\ (\!(v_1)\!)^{\overline{\ell}_0}\rangle$
By (1) and $\Vdash$ on the redex

Case: $(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(i_0)\!)^{\overline{\ell}_2})^{\ell_3} \blacktriangleright_{\overline{\mathsf{N}}} (i_0)^{\ell_3}$
Immediate.

Case: $(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\!(v_0)\!)^{\overline{\ell}_2})^{\ell_2} \blacktriangleright_{\overline{\mathsf{N}}} (\mathsf{InvariantErr})^{\ell_2}$
Immediate.

□

A.2 Co-Natural

Lemma A.4 (Co-Natural type progress).
If $\cdot \vdash_1 E_0[e_0] : {}^{\tau}/_{\mathcal{U}}$ *and* $C(E_0[e_0])$ *then one of the following holds:*

- $e_0 \in v \cup \mathsf{Err}$
- ${}^{\tau}/_{\mathcal{U}} \in \tau$ *and* $\exists\, e_1.\ e_0 \rhd_{\mathsf{C}} e_1$
- ${}^{\tau}/_{\mathcal{U}} \in \mathcal{U}$ *and* $\exists\, e_1.\ e_0 \blacktriangleright_{\mathsf{C}} e_1$

Proof. By unique decomposition (lemma 6.1) and case analysis:

Case: $\cdot \vdash_1 n_0 : \mathsf{Nat}$
Immediate.
Case: $\cdot \vdash_1 i_0 : \mathsf{Int}$
Immediate.
Case: $\cdot \vdash_1 \lambda(x_0 : \tau_0).\, e_1 : \tau_0 \Rightarrow \tau_1$
Immediate.
Case: $\cdot \vdash_1 \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$
Immediate.
Case: $\cdot \vdash_1 \mathit{unop}\{\tau_0\}\, v_0 : \tau_0$
- $\rhd_{\mathsf{C}}$ $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathcal{U}\}\, v_1)$
 if $\mathit{unop} = \mathsf{fst}$ and $v_0 = \mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\, v_1$
- $\rhd_{\mathsf{C}}$ $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathcal{U}\}\, v_1)$
 if $\mathit{unop} = \mathsf{snd}$ and $v_0 = \mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\, v_1$
- $\rhd_{\mathsf{C}}$ $\delta(\mathit{unop}, v_0)$ if defined
- $\rhd_{\mathsf{C}}$ Err otherwise

Case: $\cdot \vdash_1 \mathit{binop}\{\tau_0\}\, v_0\, v_1 : \tau_0$
- $\rhd_{\mathsf{C}}$ $\delta(\mathit{binop}, v_0, v_1)$ if defined
- $\rhd_{\mathsf{C}}$ Err otherwise

Case: $\cdot \vdash_1 \mathsf{app}\{\tau_0\}\, v_0\, v_1 : \tau_0$
- $\rhd_{\mathsf{C}}$ $e_1[x_0 \leftarrow v_1]$
 if $v_0 = \lambda(\tau_1 : x_0).\, e_1$
- $\rhd_{\mathsf{C}}$ $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_2\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1))$
 if $v_0 = \mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1)\, v_2$
- $\rhd_{\mathsf{C}}$ Err otherwise

Case: $\cdot \vdash_1 \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 : \tau_0$
- $\rhd_{\mathsf{C}}$ $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0$
 if $\tau_0 \in \tau \Rightarrow \tau \cup \tau \times \tau$ and $\mathit{shape\text{-}match}\,(\lfloor \tau_0 \rfloor, v_0)$
- $\rhd_{\mathsf{C}}$ v_0
 if $v_0 \in i$ and $\tau_0 \in \mathsf{Int}$
- $\rhd_{\mathsf{C}}$ v_0
 if $v_0 \in n$ and $\tau_0 \in \mathsf{Nat}$
- $\rhd_{\mathsf{C}}$ Err otherwise

Case: $\cdot \vdash_1 \mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\, v_0 : \tau_0$
Immediate.
Case: $\cdot \vdash_1 \mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1)\, v_0 : \tau_0$
Immediate.
Case: $\cdot \vdash_1 \mathsf{Err} : \tau_0$
Immediate.
Case: $\cdot \vdash_1 i : \mathcal{U}$
Immediate.

Case: $\cdot \vdash_1 \lambda x_0.\, e_0 : \mathcal{U}$
Immediate.
Case: $\cdot \vdash_1 \langle v_0, v_1 \rangle : \mathcal{U}$
Immediate.
Case: $\cdot \vdash_1 unop\{\mathcal{U}\}\, v_0 : \mathcal{U}$

- $\blacktriangleright_C$ stat $(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$ $(\mathsf{fst}\{\tau_1\}\, v_1)$
  if $unop = \mathsf{fst}$ and $v_0 = \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\, v_1$
- $\blacktriangleright_C$ stat $(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$ $(\mathsf{snd}\{\tau_2\}\, v_1)$
  if $unop = \mathsf{snd}$ and $v_0 = \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\, v_1$
- $\blacktriangleright_C$ $\delta(unop, v_0)$ if defined
- $\blacktriangleright_C$ Err otherwise

Case: $\cdot \vdash_1 binop\{\mathcal{U}\}\, v_0\, v_1 : \mathcal{U}$

- $\blacktriangleright_C$ $\delta(binop, v_0, v_1)$ if defined
- $\blacktriangleright_C$ Err otherwise

Case: $\cdot \vdash_1 \mathsf{app}\{\mathcal{U}\}\, v_0\, v_1 : \mathcal{U}$

- $\blacktriangleright_C$ $e_1[x_0 \leftarrow v_1]$
  if $v_0 = \lambda x_0.\, e_1$
- $\blacktriangleright_C$ stat $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$ $(\mathsf{app}\{\tau_0\}\, v_2\, (\mathsf{dyn}\, (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1))$
  if $v_0 = \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1)\, v_2$
- $\blacktriangleright_C$ Err otherwise

Case: $\cdot \vdash_1$ stat $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 : \mathcal{U}$

- $\blacktriangleright_C$ $\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0$
  if $\tau_0 \in \tau \Rightarrow \tau \cup \tau \times \tau$ and $\textit{shape-match}(\lfloor \tau_0 \rfloor, v_0)$
- $\blacktriangleright_C$ v_0
  if $v_0 \in i$ and $\tau_0 \in \mathsf{Int}$
- $\blacktriangleright_C$ v_0
  if $v_0 \in n$ and $\tau_0 \in \mathsf{Nat}$
- $\blacktriangleright_C$ Err otherwise

Case: $\cdot \vdash_1 \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1)\, v_0 : \mathcal{U}$
Immediate.
Case: $\cdot \vdash_1 \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \times \tau_0) \blacktriangleleft \ell_1)\, v_0 : \mathcal{U}$
Immediate.
Case: $\cdot \vdash_1 \mathsf{Err} : \mathcal{U}$
Immediate.

□

Lemma A.5 (Co-Natural type preservation).
If $\cdot \vdash_1 E_0[e_0] : {}^{\tau}/_{\mathcal{U}}$ *and* $C(E_0[e_0])$ *and* $e_0(\rhd_C \cup \blacktriangleright_C)e_1$ *then* $\cdot \vdash_1 E_0[e_1] : {}^{\tau}/_{\mathcal{U}}$ *and* $C(E_0[e_1])$.

Proof. By case analysis of each reduction relation.

Case: $unop\{\tau_0\}\, v_0 \rhd_C \mathsf{InvariantErr}$
Immediate.
Case: $unop\{\tau_0\}\, v_0 \rhd_C \delta(unop, v_0)$
By lemma 6.2.
Case: $\mathsf{fst}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\, v_0) \rhd_C \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathcal{U}\}\, v_0)$
(1) $\cdot \vdash_1 v_0 : \mathcal{U}$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 \mathsf{fst}\{\mathcal{U}\}\, v_0 : \mathcal{U}$
By (1)
(3) $\tau_1 \leqslant: \tau_0$
By $\vdash_1$ on the redex
(4) $\cdot \vdash_1 \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathcal{U}\}\, v_0) : \tau_0$
By (2) and (3)
(5) $C(\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathcal{U}\}\, v_0))$
By similar reasoning
Case: $\mathsf{snd}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\, v_0 \rhd_C \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathcal{U}\}\, v_0)$
(1) $\cdot \vdash_1 v_0 : \mathcal{U}$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 \mathsf{snd}\{\mathcal{U}\}\, v_0 : \mathcal{U}$
By (1)
(3) $\tau_2 \leqslant: \tau_0$
By $\vdash_1$ on the redex
(4) $\cdot \vdash_1 \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathcal{U}\}\, v_0) : \tau_0$
By (2) and (3)
Case: $binop\{\tau_0\}\, v_0\, v_1 \rhd_C \mathsf{InvariantErr}$
Immediate.
Case: $binop\{\tau_0\}\, v_0\, v_1 \rhd_C \delta(binop, v_0, v_1)$
By lemma 6.2.
Case: $\mathsf{app}\{\tau_0\}\, v_0\, v_1 \rhd_C \mathsf{InvariantErr}$
Immediate.
Case: $\mathsf{app}\{\tau_0\}\,(\lambda(x_0 : \tau_1).\, e_0)\, v_0 \rhd_C e_0[x_0 \leftarrow v_0]$
By substitution lemmas for typed functions and for $C(\cdot)$.
Case: $\mathsf{app}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0)\, v_1 \rhd_C \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_0\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1))$
(1) $\cdot \vdash_1 v_0 : \mathcal{U}$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 v_1 : \tau_1$
By $\vdash_1$ on the redex
(3) $\cdot \vdash_1 \mathsf{stat}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1 : \mathcal{U}$
By (2)
(4) $\cdot \vdash_1 \mathsf{app}\{\mathcal{U}\}\, v_0\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1) : \mathcal{U}$
By (1) and (3)
(5) $\tau_2 \leqslant: \tau_0$
By $\vdash_1$ on the redex

(6) $\cdot \vdash_1 \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\,v_0\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\,v_1)) : \tau_0$
 By (4) and (5)
(7) $C(\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\,v_0\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\,v_1)))$
 By similar reasoning

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0 \triangleright_{\mathsf{C}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0$
 Immediate.

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,i_0 \triangleright_{\mathsf{C}} i_0$
 Immediate.

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0 \triangleright_{\mathsf{C}} \mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), v_0)$
 Immediate.

Case: $\mathit{unop}\{\mathcal{U}\}\,v_0 \blacktriangleright_{\mathsf{C}} \mathsf{TagErr}$
 Immediate.

Case: $\mathit{unop}\{\mathcal{U}\}\,v_0 \blacktriangleright_{\mathsf{C}} \delta(\mathit{unop}, v_0)$
 Immediate.

Case: $\mathsf{fst}\{\mathcal{U}\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\,v_0) \blacktriangleright_{\mathsf{C}} \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\tau_1\}\,v_0)$
(1) $\cdot \vdash_1 v_0 : \tau_1 \times \tau_2$
 By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 \mathsf{fst}\{\tau_1\}\,v_0 : \tau_1$
 By (1)
(3) $\cdot \vdash_1 \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\tau_1\}\,v_0) : \mathcal{U}$
 By (2)

Case: $\mathsf{snd}\{\mathcal{U}\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\,v_0 \blacktriangleright_{\mathsf{C}} \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\tau_2\}\,v_0)$
(1) $\cdot \vdash_1 v_0 : \tau_1 \times \tau_2$
 By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 \mathsf{snd}\{\tau_2\}\,v_0 : \tau_2$
 By (1)
(3) $\cdot \vdash_1 \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\tau_2\}\,v_0) : \mathcal{U}$
 By (2)

Case: $\mathit{binop}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{C}} \mathsf{TagErr}$
 Immediate.

Case: $\mathit{binop}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{C}} \delta(\mathit{binop}, v_0, v_1)$
 Immediate.

Case: $\mathsf{app}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{C}} \mathsf{TagErr}$
 Immediate.

Case: $\mathsf{app}\{\mathcal{U}\}\,(\lambda x_0.\,e_0)\,v_0 \blacktriangleright_{\mathsf{C}} e_0[x_0 \leftarrow v_0]$
 By substitution lemmas for untyped functions and for $C(\cdot)$.

Case: $\mathsf{app}\{\mathcal{U}\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_2) \blacktriangleleft \ell_1)\,v_0)\,v_1 \blacktriangleright_{\mathsf{C}} \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\tau_2\}\,v_0\,(\mathsf{dyn}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\,v_1))$
(1) $\cdot \vdash_1 v_0 : \tau_1 \Rightarrow \tau_2$
 By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 v_1 : \mathcal{U}$
 By $\vdash_1$ on the redex
(3) $\cdot \vdash_1 \mathsf{dyn}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\,v_1 : \tau_1 \Rightarrow \tau_2$
 By (2)
(4) $\cdot \vdash_1 \mathsf{app}\{\tau_2\}\,v_0\,(\mathsf{dyn}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\,v_1) : \tau_2$
 By (1) and (3)
(5) $\cdot \vdash_1 \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\tau_2\}\,v_0\,(\mathsf{dyn}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\,v_1)) : \mathcal{U}$
 By (4)

Case: $\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \blacktriangleright_{\mathsf{C}} \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0$
Immediate.

Case: $\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ i_0 \blacktriangleright_{\mathsf{C}} i_0$
Immediate.

Case: $\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \blacktriangleright_{\mathsf{C}} \mathsf{InvariantErr}$
Immediate.

□

Theorem A.6 (Co-Natural complete monitoring). *Co-Natural satisfies* **CM**

Proof. By preservation of single-owner consistency ($\Vdash$) for $\rhd_{\overline{\mathsf{C}}}$ and $\blacktriangleright_{\overline{\mathsf{C}}}$.

Case: $(\mathit{unop}\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell}_0})^{\ell_0} \rhd_{\overline{\mathsf{C}}} (\mathsf{InvariantErr})^{\ell_0}$

Immediate: $\ell_0; \cdot \Vdash (\mathsf{InvariantErr})^{\ell_0}$

Case: $(\mathit{unop}\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell}_0})^{\ell_0} \rhd_{\overline{\mathsf{C}}} (\delta(\mathit{unop}, v_0))^{\overline{\ell}_0 \ell_0}$

(1) $v_0 = \langle v_1, v_2 \rangle$ and $\delta(\mathit{unop}, v_0) \in \{v_1, v_2\}$
By definition

(2) $\ell_0; \cdot \Vdash v_0$
By $\Vdash$ on the redex

(3) $\ell_0; \cdot \Vdash v_1$ and $\ell_0; \cdot \Vdash v_2$
By (2)

(4) $\ell_0; \cdot \Vdash \delta(\mathit{unop}, v_0)$
By (1) and (3)

Case: $(\mathsf{fst}\{\tau_0\}\,(\!(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(v_0)^{\ell_2})\!)^{\overline{\ell}_0})^{\ell_3} \rhd_{\overline{\mathsf{C}}} (\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathcal{U}\}\,(v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$

(1) $\ell_1; \cdot \Vdash (v_0)^{\ell_2}$
By $\Vdash$ on the redex

(2) $\ell_1; \cdot \Vdash \mathsf{fst}\{\mathcal{U}\}\,(v_0)^{\ell_2}$
By (1)

(3) $\ell_3; \cdot \Vdash (\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathcal{U}\}\,(v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$
By (1) and $\Vdash$ on the redex

Case: $(\mathsf{snd}\{\tau_0\}\,(\!(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(v_0)^{\ell_2})\!)^{\overline{\ell}_0})^{\ell_3} \rhd_{\overline{\mathsf{C}}} (\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathcal{U}\}\,(v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$

(1) $\ell_1; \cdot \Vdash (v_0)^{\ell_2}$
By $\Vdash$ on the redex

(2) $\ell_1; \cdot \Vdash \mathsf{snd}\{\mathcal{U}\}\,(v_0)^{\ell_2}$
By (1)

(3) $\ell_3; \cdot \Vdash (\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathcal{U}\}\,(v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$
By (1) and $\Vdash$ on the redex

Case: $(\mathit{binop}\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell}_0}\,(\!(v_1)\!)^{\overline{\ell}_1})^{\ell_0} \rhd_{\overline{\mathsf{C}}} (\mathsf{InvariantErr})^{\ell_0}$

Immediate.

Case: $(\mathit{binop}\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell}_0}\,(\!(v_1)\!)^{\overline{\ell}_1})^{\ell_0} \rhd_{\overline{\mathsf{C}}} (\delta(\mathit{binop}, v_0, v_1))^{\ell_0}$

(1) $\delta(\mathit{binop}, v_0, v_1) \in i$
By definition of δ

(2) $\ell_0; \cdot \Vdash \delta(\mathit{binop}, v_0, v_1)$
By (1)

Case: $(\mathsf{app}\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell}_0}\,v_1)^{\ell_0} \rhd_{\overline{\mathsf{C}}} (\mathsf{InvariantErr})^{\ell_0}$

Immediate.

Case: $(\mathsf{app}\{\tau_0\}\,(\!(\lambda(x_0 : \tau_1).\,e_0)\!)^{\overline{\ell}_0}\,v_0)^{\ell_0} \rhd_{\overline{\mathsf{C}}} (\!(e_0[x_0 \leftarrow (\!(v_0)\!)^{\ell_0 \mathit{rev}(\overline{\ell}_0)}])\!)^{\overline{\ell}_0 \ell_0}$

(1) $\ell_0; \cdot \Vdash \lambda(x_0 : \tau_1).\,e_0$
By $\Vdash$ on the redex

(2) $\ell_0; \cdot \Vdash v_0$
By $\Vdash$ on the redex

(3) $\ell_0; \cdot \Vdash \llparenthesis v_0 \rrparenthesis^{\ell_0 rev(\overline{\ell}_0)}$
By (1) and (2)
(4) $\ell_0; \cdot \Vdash x_0$ for each occurrence of x_0 in e_0
By $\Vdash$ on the redex
(5) $\ell_0; \cdot \Vdash \llparenthesis e_0[x_0 \leftarrow \llparenthesis v_1 \rrparenthesis^{\ell_0 rev(\overline{\ell}_0)}] \rrparenthesis^{\overline{\ell}_0 \ell_0}$
By (3) and (4)

Case: $(\mathsf{app}\{\tau_0\}\, \llparenthesis \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_0}\; v_1)^{\ell_3} \;\rhd_{\overline{\mathsf{C}}}$

$\llparenthesis \mathsf{dyn}\,(\ell_0 \blacktriangleleft cod(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_0\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\, \llparenthesis v_1 \rrparenthesis^{\ell_3 rev(\overline{\ell}_0)}))^{\ell_2} \rrparenthesis^{\overline{\ell}_0 \ell_3}$

(1) $\ell_2; \cdot \Vdash v_0$
By $\Vdash$ on the redex
(2) $\ell_3; \cdot \Vdash v_1$
By $\Vdash$ on the redex
(3) $\ell_3; \cdot \Vdash \llparenthesis v_1 \rrparenthesis^{\ell_3 rev(\overline{\ell}_0)}$
By (2) and $\Vdash$ on the redex
(4) $\ell_2; \cdot \Vdash \mathsf{stat}\,(\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\, \llparenthesis v_1 \rrparenthesis^{\ell_3 rev(\overline{\ell}_0)}$
By (3) and $\Vdash$ on the redex
(5) $\ell_3; \cdot \Vdash \llparenthesis \mathsf{dyn}\,(\ell_0 \blacktriangleleft cod(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_0\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\, \llparenthesis v_1 \rrparenthesis^{\ell_3 rev(\overline{\ell}_0)}))^{\ell_2} \rrparenthesis^{\overline{\ell}_0 \ell_3}$
By (1) and (4)

Case: $(\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_2} \;\rhd_{\overline{\mathsf{C}}}\; (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_2}$
Immediate.

Case: $(\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, \llparenthesis i_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_2} \;\rhd_{\overline{\mathsf{C}}}\; (i_0)^{\ell_2}$
Immediate.

Case: $(\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_2} \;\rhd_{\overline{\mathsf{C}}}\; (\mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}))^{\ell_2}$
Immediate.

Case: $(unop\{\mathcal{U}\}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_0} \;\blacktriangleright_{\overline{\mathsf{C}}}\; (\mathsf{TagErr})^{\ell_0}$
Immediate.

Case: $(unop\{\mathcal{U}\}\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_0} \;\blacktriangleright_{\overline{\mathsf{C}}}\; (\delta(unop, v_0))^{\overline{\ell}_0 \ell_0}$
(1) $v_0 = \langle v_1, v_2 \rangle$ and $\delta(unop, v_0) \in \{v_1, v_2\}$
By definition
(2) $\ell_0; \cdot \Vdash v_0$
By $\Vdash$ on the redex
(3) $\ell_0; \cdot \Vdash v_1$ and $\ell_0; \cdot \Vdash v_2$
By (2)
(4) $\ell_0; \cdot \Vdash \delta(unop, v_0)$
By (1) and (3)

Case: $(\mathsf{fst}\{\mathcal{U}\}\, \llparenthesis \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_0})^{\ell_3} \;\blacktriangleright_{\overline{\mathsf{C}}}\; (\mathsf{stat}\,(\ell_0 \blacktriangleleft fst(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{fst(\tau_0)\}\,(v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$
(1) $\ell_1; \cdot \Vdash (v_0)^{\ell_2}$
By $\Vdash$ on the redex
(2) $\ell_1; \cdot \Vdash \mathsf{fst}\{\mathcal{U}\}\,(v_0)^{\ell_2}$
By (1)
(3) $\ell_3; \cdot \Vdash (\mathsf{dyn}\,(\ell_0 \blacktriangleleft fst(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathcal{U}\}\,(v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$
By (1) and $\Vdash$ on the redex

Case: $(\mathsf{snd}\{\mathcal{U}\}\,\llparenthesis\mathbb{G}\,(\ell_0\blacktriangleleft\tau_0\blacktriangleleft\ell_1)\,(v_0)^{\ell_2}\rrparenthesis^{\overline{\ell_0}})^{\ell_3} \blacktriangleright_{\overline{\mathsf{C}}} (\mathsf{stat}\,(\ell_0\blacktriangleleft snd(\tau_0)\blacktriangleleft\ell_1)\,(\mathsf{snd}\{\tau_1\}\,(v_0)^{\ell_2}))^{\overline{\ell_0}\ell_3}$

(1) $\ell_1;\cdot\Vdash(v_0)^{\ell_2}$
 By $\Vdash$ on the redex

(2) $\ell_1;\cdot\Vdash\mathsf{snd}\{\mathcal{U}\}\,(v_0)^{\ell_2}$
 By (1)

(3) $\ell_3;\cdot\Vdash(\mathsf{dyn}\,(\ell_0\blacktriangleleft snd(\tau_1)\blacktriangleleft\ell_1)\,(\mathsf{snd}\{\mathcal{U}\}\,(v_0)^{\ell_2}))^{\overline{\ell_0}\ell_3}$
 By (1) and $\Vdash$ on the redex

Case: $(binop\{\mathcal{U}\}\,\llparenthesis v_0\rrparenthesis^{\overline{\ell_0}}\,\llparenthesis v_1\rrparenthesis^{\overline{\ell_1}})^{\ell_0} \blacktriangleright_{\overline{\mathsf{C}}} (\mathsf{TagErr})^{\ell_0}$
 Immediate.

Case: $(binop\{\mathcal{U}\}\,\llparenthesis v_0\rrparenthesis^{\overline{\ell_0}}\,\llparenthesis v_1\rrparenthesis^{\overline{\ell_1}})^{\ell_0} \blacktriangleright_{\overline{\mathsf{C}}} (\delta(binop, v_0, v_1))^{\ell_0}$

(1) $\delta(binop, v_0, v_1)\in i$
 By definition of δ

(2) $\ell_0;\cdot\Vdash\delta(binop, v_0, v_1)$
 By (1)

Case: $(\mathsf{app}\{\mathcal{U}\}\,\llparenthesis v_0\rrparenthesis^{\overline{\ell_0}}\,v_1)^{\ell_0} \blacktriangleright_{\overline{\mathsf{C}}} (\mathsf{TagErr})^{\ell_0}$
 Immediate.

Case: $(\mathsf{app}\{\mathcal{U}\}\,\llparenthesis\lambda x_0.\,e_0\rrparenthesis^{\overline{\ell_0}}\,v_1)^{\ell_0} \blacktriangleright_{\overline{\mathsf{C}}} \llparenthesis e_0[x_0\leftarrow\llparenthesis v_1\rrparenthesis^{\ell_0 rev(\overline{\ell_0})}]\rrparenthesis^{\overline{\ell_0}\ell_0}$

(1) $\ell_0;\cdot\Vdash\lambda x_0.\,e_0$
 By $\Vdash$ on the redex

(2) $\ell_0;\cdot\Vdash v_0$
 By $\Vdash$ on the redex

(3) $\ell_0;\cdot\Vdash\llparenthesis v_0\rrparenthesis^{\ell_0 rev(\overline{\ell_0})}$
 By (1) and (2)

(4) $\ell_0;\cdot\Vdash x_0$ for each occurrence of x_0 in e_0
 By $\Vdash$ on the redex

(5) $\ell_0;\cdot\Vdash\llparenthesis e_0[x_0\leftarrow\llparenthesis v_1\rrparenthesis^{\ell_0 rev(\overline{\ell_0})}]\rrparenthesis^{\overline{\ell_0}\ell_0}$
 By (3) and (4)

Case: $(\mathsf{app}\{\mathcal{U}\}\,\llparenthesis\mathbb{G}\,(\ell_0\blacktriangleleft\tau_0\blacktriangleleft\ell_1)\,(v_0)^{\ell_2}\rrparenthesis^{\overline{\ell_0}}\,v_1)^{\ell_3} \blacktriangleright_{\overline{\mathsf{C}}}$

$\llparenthesis\mathsf{stat}\,(\ell_0\blacktriangleleft cod(\tau_0)\blacktriangleleft\ell_1)\,(\mathsf{app}\{cod(\tau_0)\}\,v_0\,(\mathsf{dyn}\,(\ell_1\blacktriangleleft dom(\tau_0)\blacktriangleleft\ell_0)\,\llparenthesis v_1\rrparenthesis^{\ell_3 rev(\overline{\ell_0})}))^{\ell_2}\rrparenthesis^{\overline{\ell_0}\ell_3}$

(1) $\ell_2;\cdot\Vdash v_0$
 By $\Vdash$ on the redex

(2) $\ell_3;\cdot\Vdash v_1$
 By $\Vdash$ on the redex

(3) $\ell_3;\cdot\Vdash\llparenthesis v_1\rrparenthesis^{\ell_3 rev(\overline{\ell_0})}$
 By (2) and $\Vdash$ on the redex

(4) $\ell_2;\cdot\Vdash\mathsf{dyn}\,(\ell_1\blacktriangleleft dom(\tau_1)\blacktriangleleft\ell_0)\,\llparenthesis v_1\rrparenthesis^{\ell_3 rev(\overline{\ell_0})}$
 By (3) and $\Vdash$ on the redex

(5) $\ell_3;\cdot\Vdash\llparenthesis\mathsf{stat}\,(\ell_0\blacktriangleleft cod(\tau_1)\blacktriangleleft\ell_1)\,(\mathsf{app}\{cod(\tau_0)\}\,v_0\,(\mathsf{dyn}\,(\ell_1\blacktriangleleft dom(\tau_1)\blacktriangleleft\ell_0)\,\llparenthesis v_1\rrparenthesis^{\ell_3 rev(\overline{\ell_0})}))^{\ell_2}\rrparenthesis^{\overline{\ell_0}\ell_3}$
 By (1) and (4)

Case: $(\mathsf{stat}\,(\ell_0\blacktriangleleft\tau_0\blacktriangleleft\ell_1)\,\llparenthesis v_0\rrparenthesis^{\overline{\ell_0}})^{\ell_2} \blacktriangleright_{\overline{\mathsf{C}}} (\mathbb{G}\,(\ell_0\blacktriangleleft\tau_0\blacktriangleleft\ell_1)\,\llparenthesis v_0\rrparenthesis^{\overline{\ell_0}})^{\ell_2}$
 Immediate.

Case: $(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\!(i_0)\!)^{\overline{\ell}_2})^{\ell_3} \blacktriangleright_{\overline{\mathsf{C}}} (i_0)^{\ell_3}$

Immediate.

Case: $(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\!(v_0)\!)^{\overline{\ell}_2})^{\ell_2} \blacktriangleright_{\overline{\mathsf{C}}} (\mathsf{InvariantErr})^{\ell_2}$

Immediate.

□

Lemma A.7 ($N \lesssim C$).

- *If* $e_0 \lesssim e_2$ *and* $e_0 \rightarrow_{\mathsf{N}} e_1$ *then* $\exists\, e_3, e_4$ *such that* $e_1 \rightarrow^*_{\mathsf{N}} e_3$ *and* $e_2 \rightarrow^*_{\mathsf{C}} e_4$ *and* $e_3 \lesssim e_4$.
- *If* $e_0 \lesssim e_2$ *and* $e_2 \rightarrow_{\mathsf{C}} e_3$ *then* $\exists\, e_1, e_4$ *such that* $e_3 \rightarrow^*_{\mathsf{C}} e_4$ *and* $e_0 \rightarrow^*_{\mathsf{N}} e_1$ *and* $e_1 \lesssim e_4$

Proof. By lemma A.8 and lemma A.9. □

$\boxed{\mathrm{wfr}_{NC}(e_0, e_1)}$ holds for well-formed residuals of a common term; that is, pairs such that there exists an e_2 where $e_2 : {}^{\tau}/_{\mathcal{U}}$ **wf** and $e_2 \rightarrow^*_{\mathsf{N}} e_0$ and $e_2 \rightarrow^*_{\mathsf{C}} e_1$

Lemma A.8.
If $\mathrm{wfr}_{NC}(e_0, e_2)$ *and* $e_0 \lesssim e_2$ *and* $e_0 \rightarrow_{\mathsf{N}} e_1$ *then* $\exists\, e_3, e_4$ *such that* $e_1 \rightarrow^*_{\mathsf{N}} e_3$ *and* $e_2 \rightarrow^*_{\mathsf{C}} e_4$ *and* $e_3 \lesssim e_4$.

Proof. By lemma A.10, lemma A.13, and case analysis of $\vartriangleright_{\mathsf{N}} \cup \blacktriangleright_{\mathsf{N}}$.

Case: $\mathit{unop}\{\tau_0\}\, v_0 \vartriangleright_{\mathsf{N}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathit{unop}\{\tau_0\}\, v_0 \vartriangleright_{\mathsf{N}} \delta(\mathit{unop}, v_0)$
(1) $e_1 = \mathit{unop}\{\tau_0\}\, v_1$ and $v_0 \lesssim v_1$
By $\lesssim$ on the redex
(2) If $v_1 \in \langle v, v\rangle$ then $\delta(\mathit{unop}, v_1)$ is defined and $\delta(\mathit{unop}, v_0) \lesssim \delta(\mathit{unop}, v_1)$
(3) Otherwise $v_1 \in \mathbb{G}\, b\, v$ and $e_1 \rightarrow^*_{\mathsf{C}} v_2$ where $\delta(\mathit{unop}, v_0) \lesssim v_2$

Case: $\mathit{binop}\{\tau_0\}\, v_0\, v_1 \vartriangleright_{\mathsf{N}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathit{binop}\{\tau_0\}\, v_0\, v_1 \vartriangleright_{\mathsf{N}} \delta(\mathit{binop}, v_0, v_1)$
(1) $e_1 = \mathit{binop}\{\tau_0\}\, v_2\, v_3$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex
(2) $\delta(\mathit{binop}, v_2, v_3)$ is defined
By (1)
(3) $\delta(\mathit{binop}, v_0, v_1) \lesssim \delta(\mathit{binop}, v_2, v_3)$
By δ

Case: $\mathsf{app}\{\tau_0\}\, v_0\, v_1 \vartriangleright_{\mathsf{N}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathsf{app}\{\tau_0\}\, (\lambda(x_0 : \tau_1).\, e_0)\, v_0 \vartriangleright_{\mathsf{N}} e_0[x_0 \leftarrow v_0]$
(1) $e_1 = \mathsf{app}\{\tau_0\}\, v_1\, v_2$ and $(\lambda(x_0 : \tau_1).\, e_4) \lesssim v_1$ and $v_0 \lesssim v_2$
By $\lesssim$ on the redex
(2) $v_1 = \lambda(x_0 : \tau_1).\, e_5$
By (1)
(3) $e_4[x_0 \leftarrow v_0] \lesssim e_5[x_0 \leftarrow v_2]$

Case: $\mathsf{app}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0)\, v_1 \vartriangleright_{\mathsf{N}}$
$\mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_0\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_1))$
(1) $e_1 = \mathsf{app}\{\tau_0\}\, v_2\, v_3$ and $(\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0) \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex
(2) $v_2 = \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_4$
By (1)
(3) $e_1 \vartriangleright_{\mathsf{C}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_4\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_3))$
By (2)
(4) $\mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_0\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_1)) \lesssim$
$\mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_4\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_3))$

Case: $\mathsf{dyn}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ v_0 \rhd_{\mathsf{N}} \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ v_0$

(1) $e_1 = \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\ v_1$ and $v_0 \lesssim v_1$ and $\tau_0 \Rightarrow \tau_1 = \tau_2$
By $\lesssim$

(2) $e_1 \rhd_{\mathsf{C}} \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\ v_1$
By $\rhd_{\mathsf{C}}$

(3) $\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \Rightarrow \tau_1 \blacktriangleleft \ell_1)\ v_0 \lesssim \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\ v_1$
By (1)

Case: $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \langle v_0, v_1 \rangle \rhd_{\mathsf{N}} \langle \mathsf{dyn}\ (\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\ v_0, \mathsf{dyn}\ (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\ v_1 \rangle$

(1) $e_1 = \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_1 \times \tau_2 \blacktriangleleft \ell_1)\ v_1$ and $v_0 \lesssim v_1$ and $\tau_0 = \tau_1 \times \tau_2$
By $\lesssim$

(2) $e_1 \rhd_{\mathsf{C}} \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \times \tau_2 \blacktriangleleft \ell_1)\ v_1$
By $\rhd_{\mathsf{C}}$

(3) Either $e_0 \rightarrow^*_{\mathsf{N}} \mathsf{BoundaryErr}\ (\overline{b}, v)$
or $e_0 \rightarrow^*_{\mathsf{N}} \langle v_2, v_3 \rangle$ and $\langle v_2, v_3 \rangle \lesssim \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \times \tau_2 \blacktriangleleft \ell_1)\ v_1$

Case: $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ i_0 \rhd_{\mathsf{N}} i_0$

(1) $e_1 = \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ i_0$
By $\lesssim$

(2) $i_0 \lesssim i_0$

Case: $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \rhd_{\mathsf{N}} \mathsf{BoundaryErr}\ ((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), v_0)$
Immediate

Case: $\mathit{unop}\{\mathcal{U}\}\ v_0 \blacktriangleright_{\mathsf{N}} \mathsf{TagErr}$

(1) $e_1 = \mathit{unop}\{\mathcal{U}\}\ v_1$ and $v_0 \lesssim v_1$
By $\lesssim$ on the redex

(2) $\delta(\mathit{unop}, v_1)$ is undefined
By (1)

(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathit{unop}\{\mathcal{U}\}\ v_0 \blacktriangleright_{\mathsf{N}} \delta(\mathit{unop}, v_0)$

(1) $e_1 = \mathit{unop}\{\mathcal{U}\}\ v_1$ and $v_0 \lesssim v_1$
By $\lesssim$ on the redex

(2) If $v_1 \in \langle v, v \rangle$ then $\delta(\mathit{unop}, v_1)$ is defined
By (1)

(3) Otherwise $v_1 \in \mathbb{G}\ b\ v$ and $e_1 \rightarrow^*_{\mathsf{C}} 2$ where $\delta(\mathit{unop}, v_0) \lesssim v_2$

Case: $\mathit{binop}\{\mathcal{U}\}\ v_0\ v_1 \blacktriangleright_{\mathsf{N}} \mathsf{TagErr}$

(1) $e_1 = \mathit{binop}\{\mathcal{U}\}\ v_2\ v_3$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex

(2) $\delta(\mathit{binop}, v_2, v_3)$ is undefined
By (1)

(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathit{binop}\{\mathcal{U}\}\ v_0\ v_1 \blacktriangleright_{\mathsf{N}} \delta(\mathit{binop}, v_0, v_1)$

(1) $e_1 = \mathit{binop}\{\mathcal{U}\}\ v_2\ v_3$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex

(2) $\delta(\mathit{binop}, v_2, v_3)$ is defined
By (1)

(3) $\delta(\mathit{binop}, v_0, v_1) \lesssim \delta(\mathit{binop}, v_2, v_3)$
By δ

Case: $\mathsf{app}\{\mathcal{U}\}\ v_0\ v_1 \blacktriangleright_{\mathsf{N}} \mathsf{TagErr}$

(1) $e_1 = \mathsf{app}\{\mathcal{U}\}\, v_2\, v_3$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex
(2) $v_2 \notin \lambda x.\, e \cup \mathbb{G}\, b\, v$
By (1)
(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathsf{app}\{\mathcal{U}\}\, (\lambda x_0.\, e_0)\, v_0 \blacktriangleright_{\mathsf{N}} e_0[x_0 \leftarrow v_0]$
(1) $e_1 = \mathsf{app}\{\mathcal{U}\}\, v_1\, v_2$ and $(\lambda x_0.\, e_4) \lesssim v_1$ and $v_0 \lesssim v_2$
By $\lesssim$ on the redex
(2) $v_1 = (\lambda x_0.\, e_5)$
By (1)
(3) $(e_4[x_0 \leftarrow v_1]) \lesssim (e_5[x_0 \leftarrow v_2])$

Case: $\mathsf{app}\{\mathcal{U}\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0)\, v_1 \blacktriangleright_{\mathsf{N}}$
$\mathsf{stat}\, (\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathit{cod}(\tau_0)\}\, v_0\, (\mathsf{dyn}\, (\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\, v_1))$
(1) $e_1 = \mathsf{app}\{\mathcal{U}\}\, v_2\, v_3$ and $(\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0) \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex
(2) $v_2 = (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_4)$ and $\tau_0 = \tau_1$
By (1)
(3) $e_1 \blacktriangleright_{\mathsf{C}} \mathsf{stat}\, (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_4\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_3))$
By (2)
(4) $\mathsf{stat}\, (\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathit{cod}(\tau_0)\}\, v_0\, (\mathsf{dyn}\, (\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\, v_1)) \lesssim$
$\mathsf{stat}\, (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_4\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_3))$

Case: $\mathsf{stat}\, (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\, v_0 \blacktriangleright_{\mathsf{N}} \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\, v_0$
(1) $e_1 = \mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \Rightarrow \tau_1 \blacktriangleleft \ell_1)\, v_1$ and $v_0 \lesssim v_1$
By $\lesssim$
(2) $e_1 \blacktriangleright_{\mathsf{C}} \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \Rightarrow \tau_1 \blacktriangleleft \ell_1)\, v_1$
By $\blacktriangleright_{\mathsf{C}}$
(3) $\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \Rightarrow \tau_1 \blacktriangleleft \ell_1)\, v_0 \lesssim \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \Rightarrow \tau_1 \blacktriangleleft \ell_1)\, v_1$
By (1)

Case: $\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, \langle v_0, v_1 \rangle \blacktriangleright_{\mathsf{N}} \langle \mathsf{stat}\, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\, v_0, \mathsf{stat}\, (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\, v_1 \rangle$
(1) $e_1 = \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_1 \times \tau_2 \blacktriangleleft \ell_1)\, v_1$ and $v_0 \lesssim v_1$ and $\tau_0 = \tau_1 \times \tau_2$
By $\lesssim$
(2) $e_1 \blacktriangleright_{\mathsf{C}} \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \times \tau_2 \blacktriangleleft \ell_1)\, v_1$
By $\blacktriangleright_{\mathsf{C}}$
(3) Either $e_0 \rightarrow^*_{\mathsf{N}} \mathsf{BoundaryErr}\, (\overline{b}, v)$
or $e_0 \rightarrow^*_{\mathsf{N}} \langle v_2, v_3 \rangle$ and $\langle v_2, v_3 \rangle \lesssim \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \times \tau_2 \blacktriangleleft \ell_1)\, v_1$

Case: $\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, i_0 \blacktriangleright_{\mathsf{N}} i_0$
(1) $e_1 = \mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, i_0$
By $\lesssim$
(2) $i_0 \lesssim i_0$

Case: $\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \blacktriangleright_{\mathsf{N}} \mathsf{InvariantErr}$
Impossible, by type soundness

□

Lemma A.9.
If $\mathrm{wfr}_{NC}(e_0, e_2)$ *and* $e_0 \lesssim e_2$ *and* $e_2 \rightarrow_{\mathsf{C}} e_3$ *then* $\exists\, e_1, e_4$ *such that* $e_3 \rightarrow^*_{\mathsf{C}} e_4$ *and* $e_0 \rightarrow^*_{\mathsf{N}} e_1$ *and* $e_1 \lesssim e_4$

Proof. By lemma A.10, lemma A.13, and case analysis of $\rhd_{\mathsf{C}} \cup \blacktriangleright_{\mathsf{C}}$.

Case: $\mathit{unop}\{\tau_0\}\, v_0 \rhd_{\mathsf{C}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathit{unop}\{\tau_0\}\, v_0 \rhd_{\mathsf{C}} \delta(\mathit{unop}, v_0)$
(1) $e_0 = \mathit{unop}\{\tau_0\}\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex
(2) $v_1 \in \langle v, v\rangle$ and $\delta(\mathit{unop}, v_1)$ is defined
By (1)
(3) $\delta(\mathit{unop}, v_1) \lesssim \delta(\mathit{unop}, v_0)$

Case: $\mathsf{fst}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0) \rhd_{\mathsf{C}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_0)$
(1) $e_0 = \mathsf{fst}\{\tau_0\}\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex
(2) $v_1 \in \langle v, v\rangle$ and $\delta(\mathit{unop}, v_1)$ is defined
By (1)
(3) $\mathsf{dyn}\, b_0\, (\mathsf{fst}\{\mathcal{U}\}\, v_0) \rightarrow^*_{\mathsf{C}} v_2$
By (2)
(4) $\delta(\mathsf{fst}, v_1) \lesssim v_2$

Case: $\mathsf{snd}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0 \rhd_{\mathsf{C}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_0)$
(1) $e_0 = \mathsf{snd}\{\tau_0\}\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex
(2) $v_1 \in \langle v, v\rangle$ and $\delta(\mathit{unop}, v_1)$ is defined
By (1)
(3) $\mathsf{dyn}\, b_0\, (\mathsf{snd}\{\mathcal{U}\}\, v_0) \rightarrow^*_{\mathsf{C}} v_2$
By (2)
(4) $\delta(\mathsf{snd}, v_1) \lesssim v_2$

Case: $\mathit{binop}\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{C}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathit{binop}\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{C}} \delta(\mathit{binop}, v_0, v_1)$
(1) $e_0 = \mathit{binop}\{\tau_0\}\, v_2\, v_3$ and $v_2 \lesssim v_0$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex
(2) $\delta(\mathit{binop}, v_2, v_3)$ is defined
By (1)
(3) $\delta(\mathit{binop}, v_2, v_3) \lesssim \delta(\mathit{binop}, v_0, v_1)$
By δ

Case: $\mathsf{app}\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{C}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathsf{app}\{\tau_0\}\, (\lambda(x_0 : \tau_1).\, e_0)\, v_0 \rhd_{\mathsf{C}} e_0[x_0 \leftarrow v_0]$
(1) $e_0 = \mathsf{app}\{\tau_0\}\, v_1\, v_2$ and $v_1 \lesssim (\lambda(x_0 : \tau_1).\, e_4)$ and $v_2 \lesssim v_0$
By $\lesssim$ on the redex
(2) $v_1 = \lambda(x_0 : \tau_1).\, e_5$
By (1)
(3) $e_5[x_0 \leftarrow v_2] \lesssim e_4[x_0 \leftarrow v_0]$

Case: $\mathsf{app}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0)\, v_1 \rhd_{\mathsf{C}}$
$\mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_0\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_1))$

(1) $e_0 = \mathsf{app}\{\tau_0\}\, v_2\, v_3$ and $v_2 \lesssim (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0)$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex
(2) $v_2 = \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_4$
By (1)
(3) $e_0 \rhd_{\mathsf{N}} \mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_4\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_3))$
By (2)
(4) $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_4\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_3)) \lesssim$
$\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_0\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_1))$

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \rhd_{\mathsf{C}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0$
(1) $e_0 = \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$
(2) If $\tau_0 \in \tau \Rightarrow \tau$ then $e_0 \rhd_{\mathsf{N}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1$
(3) If $\tau_0 \in \tau \times \tau$ then either $e_0 \rhd_{\mathsf{N}} \mathsf{BoundaryErr}\,(\overline{b}, v)$ or $e_0 \rightarrow^*_{\mathsf{N}} \langle v_2, v_3\rangle$ where $\langle v_2, v_3\rangle \lesssim$ $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0$

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, i_0 \rhd_{\mathsf{C}} i_0$
(1) $e_0 = \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, i_0$
By $\lesssim$
(2) $i_0 \lesssim i_0$

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \rhd_{\mathsf{C}} \mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), v_0)$
(1) $e_0 = \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$
(2) $e_0 \rhd_{\mathsf{N}} \mathsf{BoundaryErr}\,(\overline{b}, v_1)$

Case: $\mathit{unop}\{\mathcal{U}\}\, v_0 \blacktriangleright_{\mathsf{C}} \mathsf{TagErr}$
(1) $e_0 = \mathit{unop}\{\mathcal{U}\}\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex
(2) $\delta(\mathit{unop}, v_1)$ is undefined
By (1)
(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathit{unop}\{\mathcal{U}\}\, v_0 \blacktriangleright_{\mathsf{C}} \delta(\mathit{unop}, v_0)$
(1) $e_0 = \mathit{unop}\{\mathcal{U}\}\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex
(2) $\delta(\mathit{unop}, v_1)$ is defined
By (1)
(3) $\delta(\mathit{unop}, v_1) \lesssim \delta(\mathit{unop}, v_0)$

Case: $\mathsf{fst}\{\mathcal{U}\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0) \blacktriangleright_{\mathsf{C}} \mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\tau_1\}\, v_0)$
(1) $e_0 = \mathsf{fst}\{\tau_0\}\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex
(2) $v_1 \in \langle v, v\rangle$ and $\delta(\mathit{unop}, v_1)$ is defined
By (1)
(3) $\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathcal{U}\}\, v_0) \rightarrow^*_{\mathsf{C}} v_2$
By (2)
(4) $\delta(\mathsf{fst}, v_1) \lesssim v_2$

Case: $\mathsf{snd}\{\mathcal{U}\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \blacktriangleright_{\mathsf{C}} \mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\tau_1\}\, v_0)$
(1) $e_0 = \mathsf{snd}\{\tau_0\}\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex
(2) $v_1 \in \langle v, v\rangle$ and $\delta(\mathit{unop}, v_1)$ is defined
By (1)

(3) $\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathcal{U}\}\,v_0) \rightarrow^*_{\mathsf{C}} v_2$
By (2)
(4) $\delta(\mathsf{snd}, v_1) \lesssim v_2$

Case: $\mathit{binop}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{C}} \mathsf{TagErr}$
(1) $e_0 = \mathit{binop}\{\mathcal{U}\}\,v_2\,v_3$ and $v_2 \lesssim v_0$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex
(2) $\delta(\mathit{binop}, v_2, v_3)$ is undefined
By (1)
(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathit{binop}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{C}} \delta(\mathit{binop}, v_0, v_1)$
(1) $e_0 = \mathit{binop}\{\mathcal{U}\}\,v_2\,v_3$ and $v_2 \lesssim v_0$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex
(2) $\delta(\mathit{binop}, v_2, v_3)$ is defined
By (1)
(3) $\delta(\mathit{binop}, v_2, v_3) \lesssim \delta(\mathit{binop}, v_0, v_1)$
By δ

Case: $\mathsf{app}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{C}} \mathsf{TagErr}$
(1) $e_0 = \mathsf{app}\{\mathcal{U}\}\,v_2\,v_3$ and $v_2 \lesssim v_0$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex
(2) $v_2 \notin \lambda x.\,e \cup \mathbb{G}\,b\,v$
By (1)
(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathsf{app}\{\mathcal{U}\}\,(\lambda x_0.\,e_0)\,v_0 \blacktriangleright_{\mathsf{C}} e_0[x_0 \leftarrow v_0]$
(1) $e_0 = \mathsf{app}\{\mathcal{U}\}\,v_1\,v_2$ and $v_1 \lesssim (\lambda x_0.\,e_4)$ and $v_2 \lesssim v_0$
By $\lesssim$ on the redex
(2) $v_1 = (\lambda x_0.\,e_5)$
By (1)
(3) $(e_5[x_0 \leftarrow v_2]) \lesssim (e_4[x_0 \leftarrow v_1])$

Case: $\mathsf{app}\{\mathcal{U}\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0)\,v_1 \blacktriangleright_{\mathsf{C}}$
$\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathit{cod}(\tau_0)\}\,v_0\,(\mathsf{dyn}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\,v_1))$
(1) $e_0 = \mathsf{app}\{\mathcal{U}\}\,v_2\,v_3$ and $v_2 \lesssim (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0)$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex
(2) $v_2 = (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,v_4)$ and $\tau_0 = \tau_1$
By (1)
(3) $e_0 \blacktriangleright_{\mathsf{N}} \mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\,v_4\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\,v_3))$
By (2)
(4) $\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\,v_4\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\,v_3)) \lesssim$
$\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathit{cod}(\tau_0)\}\,v_0\,(\mathsf{dyn}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\,v_1))$

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0 \blacktriangleright_{\mathsf{C}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0$
(1) $e_0 = \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_1$ and $v_1 \lesssim v_0$ and $\tau_1 = \tau_0$
By $\lesssim$
(2) If $\tau_0 \in \tau \Rightarrow \tau$ then $e_1 \blacktriangleright_{\mathsf{N}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_1$
(3) Otherwise $\tau_0 \in \tau \times \tau$ and either $e_0 \rightarrow^*_{\mathsf{N}} \mathsf{BoundaryErr}\,(\overline{b}, v)$ or $e_0 \rightarrow^*_{\mathsf{N}} \langle v_2, v_3 \rangle$ where $\langle v_2, v_3 \rangle \lesssim \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0$
By $\rightarrow^*_{\mathsf{N}}$

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,i_0 \blacktriangleright_{\mathsf{C}} i_0$

(1) $e_0 = \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ i_0$
By $\lesssim$
(2) $i_0 \lesssim i_0$

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \blacktriangleright_{\mathsf{C}} \mathsf{InvariantErr}$
Impossible, by type soundness

□

Lemma A.10.
If $\mathrm{wfr}_{NC}(e_0, e_1)$ *and* $e_0 \lesssim e_1$ *and either* $e_0 \rightarrow_{\mathsf{N}} e_2$ *or* $e_1 \rightarrow_{\mathsf{C}} e_3$ *then the following results hold:*

- $e_0 = E_0[e_4]$
- $e_1 = E_1[e_5]$
- $E_0 \lesssim E_1$
- $e_4 \lesssim e_5$.

Proof. By lemma A.11 and lemma A.12. □

Lemma A.11.
If $\mathrm{wfr}_{NC}(E_0[e_0], e_1)$ *and* $E_0[e_0] \lesssim e_1$ *and* $e_0(\triangleright_{\mathsf{N}} \cup \blacktriangleright_{\mathsf{N}})e_2$ *then the following results hold:*

- $e_1 = E_1[e_3]$
- $E_0 \lesssim E_1$
- $e_0 \lesssim e_3$.

Proof. By induction on $E_0[e_0] \lesssim e_1$, proceeding by case analysis of $E_0[e_0]$. □

Lemma A.12.
If $\mathrm{wfr}_{NC}(e_0, E_1[e_1])$ *and* $e_0 \lesssim E_1[e_1]$ *and* $e_1(\triangleright_{\mathsf{C}} \cup \blacktriangleright_{\mathsf{C}})e_3$ *then the following results hold:*

- $e_0 = E_0[e_2]$
- $E_0 \lesssim E_1$
- $e_2 \lesssim e_1$.

Proof. By induction on $e_0 \lesssim E_1[e_1]$, proceeding by case analysis of $E_1[e_1]$. □

Lemma A.13.
If $E_0 \lesssim E_1$ *and* $e_2 \lesssim e_3$ *then* $E_0[e_2] \lesssim E_1[e_3]$.

Proof. By induction on $E_0 \lesssim E_1$. □

A.3 Forgetful

Lemma A.14 (Forgetful type progress). *If* $\cdot \vdash_1 E_0[e_0] : {}^{\tau}/_{\mathcal{U}}$ *and* $F(E_0[e_0])$ *then one of the following holds:*

- $e_0 \in v \cup \mathsf{Err}$
- ${}^{\tau}/_{\mathcal{U}} \in \tau$ *and* $\exists\, e_1.\ e_0 \rhd_{\mathsf{F}} e_1$
- ${}^{\tau}/_{\mathcal{U}} \in \mathcal{U}$ *and* $\exists\, e_1.\ e_0 \blacktriangleright_{\mathsf{F}} e_1$

Proof. By unique decomposition (lemma 6.1) and case analysis:

Case: $\cdot \vdash_1 n_0 : \mathsf{Nat}$
Immediate.
Case: $\cdot \vdash_1 i_0 : \mathsf{Int}$
Immediate.
Case: $\cdot \vdash_1 \lambda(x_0 : \tau_0).\ e_1 : \tau_0 \Rightarrow \tau_1$
Immediate.
Case: $\cdot \vdash_1 \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$
Immediate.
Case: $\cdot \vdash_1 \mathit{unop}\{\tau_0\}\ v_0 : \tau_0$
- $\rhd_{\mathsf{F}}$ $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ (\mathsf{fst}\{\mathcal{U}\}\ v_1)$
  if $\mathit{unop} = \mathsf{fst}$ and $v_0 = \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\ v_1$
- $\rhd_{\mathsf{F}}$ $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\ (\mathsf{snd}\{\mathcal{U}\}\ v_1)$
  if $\mathit{unop} = \mathsf{snd}$ and $v_0 = \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\ v_1$
- $\rhd_{\mathsf{F}}$ $\delta(\mathit{unop}, v_0)$ if defined
- $\rhd_{\mathsf{F}}$ Err otherwise

Case: $\cdot \vdash_1 \mathit{binop}\{\tau_0\}\ v_0\ v_1 : \tau_0$
- $\rhd_{\mathsf{F}}$ $\delta(\mathit{binop}, v_0, v_1)$ if defined
- $\rhd_{\mathsf{F}}$ Err otherwise

Case: $\cdot \vdash_1 \mathsf{app}\{\tau_0\}\ v_0\ v_1 : \tau_0$
- $\rhd_{\mathsf{F}}$ $e_1[x_0 \leftarrow v_1]$
  if $v_0 = \lambda(\tau_1 : x_0).\ e_1$
- $\rhd_{\mathsf{F}}$ $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ (\mathsf{app}\{\mathcal{U}\}\ v_2\ (\mathsf{stat}\ (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\ v_1))$
  if $v_0 = \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1)\ v_2$
- $\rhd_{\mathsf{F}}$ Err otherwise

Case: $\cdot \vdash_1 \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 : \tau_0$
- $\rhd_{\mathsf{F}}$ $\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0$
  if $\tau_0 \in \tau \Rightarrow \tau \cup \tau \times \tau$ and $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
- $\rhd_{\mathsf{F}}$ v_0
  if $v_0 \in \mathbb{T}_?\ \overline{b}_0\ i$ and $\tau_0 \in \mathsf{Int}$
- $\rhd_{\mathsf{F}}$ v_0
  if $v_0 \in \mathbb{T}_?\ \overline{b}_0\ n$ and $\tau_0 \in \mathsf{Nat}$
- $\rhd_{\mathsf{F}}$ Err otherwise

Case: $\cdot \vdash_1 \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ v_0 : \tau_0$
Immediate.
Case: $\cdot \vdash_1 \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1)\ v_0 : \tau_0$
Immediate.
Case: $\cdot \vdash_1 \mathsf{Err} : \tau_0$
Immediate.

Case: $\cdot \vdash_1 i : \mathcal{U}$
Immediate.
Case: $\cdot \vdash_1 \lambda x_0.\, e_0 : \mathcal{U}$
Immediate.
Case: $\cdot \vdash_1 \langle v_0, v_1 \rangle : \mathcal{U}$
Immediate.
Case: $\cdot \vdash_1 \mathit{unop}\{\mathcal{U}\}\, v_0 : \mathcal{U}$
- $\blacktriangleright_{\mathsf{F}}$ $\mathsf{trace}\, \overline{b}_0\, (\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\tau_1\}\, v_1))$
  if $\mathit{unop} = \mathsf{fst}$ and $v_0 = \mathbb{T}_?\, \overline{b}_0\, (\mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\, v_1)$
- $\blacktriangleright_{\mathsf{F}}$ $\mathsf{trace}\, \overline{b}_0\, (\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\tau_2\}\, v_1))$
  if $\mathit{unop} = \mathsf{snd}$ and $v_0 = \mathbb{T}_?\, \overline{b}_0\, (\mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\, v_1)$
- $\blacktriangleright_{\mathsf{F}}$ $\mathit{add\text{-}trace}(\mathit{get\text{-}trace}(v_0), \delta(\mathit{unop}, \mathit{rem\text{-}trace}(v_0)))$ if defined
- $\blacktriangleright_{\mathsf{F}}$ Err otherwise

Case: $\cdot \vdash_1 \mathit{binop}\{\mathcal{U}\}\, v_0\, v_1 : \mathcal{U}$
- $\blacktriangleright_{\mathsf{F}}$ $\delta(\mathit{binop}, \mathit{rem\text{-}trace}(v_0), \mathit{rem\text{-}trace}(v_1))$ if defined
- $\blacktriangleright_{\mathsf{F}}$ Err otherwise

Case: $\cdot \vdash_1 \mathsf{app}\{\mathcal{U}\}\, v_0\, v_1 : \mathcal{U}$
- $\blacktriangleright_{\mathsf{F}}$ $\mathsf{trace}\, \overline{b}_0\, (e_1[x_0 \leftarrow (\mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), v_1)])$
  if $v_0 = \mathbb{T}_?\, \overline{b}_0\, (\lambda x_0.\, e_1)$
- $\blacktriangleright_{\mathsf{F}}$ $\mathsf{trace}\, \overline{b}_0\, \mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{app}\{\tau_0\}\, v_2\, (\mathsf{dyn}\, (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), v_1)))$
  if $v_0 = \mathbb{T}_?\, \overline{b}_0\, (\mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1)\, v_2)$
- $\blacktriangleright_{\mathsf{F}}$ Err otherwise

Case: $\cdot \vdash_1 \mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 : \mathcal{U}$
- $\blacktriangleright_{\mathsf{F}}$ $\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0$
  if $\tau_0 \in \tau \Rightarrow \tau \cup \tau \times \tau$ and $v_0 \in (\lambda(x : \tau).\, e) \cup \langle v, v \rangle$ and $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
- $\blacktriangleright_{\mathsf{F}}$ $\mathsf{trace}\, (b_0 b_1 \overline{b}_0)\, v_1$
  if $\tau_0 \in \tau \Rightarrow \tau \cup \tau \times \tau$ and $v_0 = \mathbb{G}\, b_1\, (\mathbb{T}_?\, \overline{b}_0\, v_1)$ and $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
- $\blacktriangleright_{\mathsf{F}}$ v_0
  if $v_0 \in i$ and $\tau_0 \in \mathsf{Int}$
- $\blacktriangleright_{\mathsf{F}}$ v_0
  if $v_0 \in n$ and $\tau_0 \in \mathsf{Nat}$
- $\blacktriangleright_{\mathsf{F}}$ Err otherwise

Case: $\cdot \vdash_1 \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1)\, v_0 : \mathcal{U}$
Immediate.
Case: $\cdot \vdash_1 \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \times \tau_0) \blacktriangleleft \ell_1)\, v_0 : \mathcal{U}$
Immediate.
Case: $\cdot \vdash_1 \mathbb{T}\, \overline{b}_0\, v_0 : \mathcal{U}$
Immediate.
Case: $\cdot \vdash_1 \mathsf{trace}\, \overline{b}_0\, v_0 : \mathcal{U}$
- $\blacktriangleright_{\mathsf{F}}$ $\mathit{add\text{-}trace}(\overline{b}_0, v_0)$

Case: $\cdot \vdash_1 \mathsf{Err} : \mathcal{U}$
Immediate.

$\square$

Lemma A.15 (Forgetful type preservation).
If $\cdot \vdash_1 E_0[e_0] : {}^{\tau}\!/_{\mathcal{U}}$ *and* $F(E_0[e_0])$ *and* $e_0(\rhd_{\mathsf{F}} \cup \blacktriangleright_{\mathsf{F}})e_1$ *then* $\cdot \vdash_1 E_0[e_1] : {}^{\tau}\!/_{\mathcal{U}}$ *and* $F(E_0[e_1])$.

Proof. By case analysis of each reduction relation. An interesting case is the $\blacktriangleright_{\mathsf{F}}$ rule that removes a guard wrapper; the rule preserves soundness because it unwraps an untyped value in an untyped context.

Case: $\mathit{unop}\{\tau_0\}\, v_0 \rhd_{\mathsf{F}} \mathsf{InvariantErr}$
Immediate.
Case: $\mathit{unop}\{\tau_0\}\, v_0 \rhd_{\mathsf{F}} \delta(\mathit{unop}, v_0)$
By lemma 6.2.
Case: $\mathsf{fst}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\, v_0) \rhd_{\mathsf{F}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_0)$
(1) $\cdot \vdash_1 v_0 : \mathcal{U}$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 \mathsf{fst}\{\mathcal{U}\}\, v_0 : \mathcal{U}$
By (1)
(3) $\tau_1 \leqslant: \tau_0$
By $\vdash_1$ on the redex
(4) $\cdot \vdash_1 \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_0) : \tau_0$
By (2) and (3)
(5) $F(\mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_0))$
By similar reasoning
Case: $\mathsf{snd}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\, v_0 \rhd_{\mathsf{F}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_0)$
(1) $\cdot \vdash_1 v_0 : \mathcal{U}$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 \mathsf{snd}\{\mathcal{U}\}\, v_0 : \mathcal{U}$
By (1)
(3) $\tau_2 \leqslant: \tau_0$
By $\vdash_1$ on the redex
(4) $\cdot \vdash_1 \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_0) : \tau_0$
By (2) and (3)
Case: $\mathit{binop}\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{F}} \mathsf{InvariantErr}$
Immediate.
Case: $\mathit{binop}\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{F}} \delta(\mathit{binop}, v_0, v_1)$
Immediate.
Case: $\mathsf{app}\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{F}} \mathsf{InvariantErr}$
Immediate.
Case: $\mathsf{app}\{\tau_0\}\, (\lambda(x_0 : \tau_1).\, e_0)\, v_0 \rhd_{\mathsf{F}} e_0[x_0 \leftarrow v_0]$
By substitution lemmas for typed functions and for $F(\cdot)$.
Case: $\mathsf{app}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0)\, v_1 \rhd_{\mathsf{F}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_0\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1))$
(1) $\cdot \vdash_1 v_0 : \mathcal{U}$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 v_1 : \tau_1$
By $\vdash_1$ on the redex
(3) $\cdot \vdash_1 \mathsf{stat}\, (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1 : \mathcal{U}$
By (2)
(4) $\cdot \vdash_1 \mathsf{app}\{\mathcal{U}\}\, v_0\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1) : \mathcal{U}$
By (1) and (3)

(5) $\tau_2 \leqslant: \tau_0$
By $\vdash_1$ on the redex
(6) $\cdot \vdash_1 \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\,v_0\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\,v_1)) : \tau_0$
By (4) and (5)
(7) $F(\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\,v_0\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\,v_1)))$
By similar reasoning

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0 \rhd_{\mathsf{F}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0$
Immediate.

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathbb{T}_?\,\overline{b}_0\,i_0) \rhd_{\mathsf{F}} i_0$
Immediate.

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0 \rhd_{\mathsf{F}} \mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b}_0, v_0)$
Immediate.

Case: $\mathit{unop}\{\mathcal{U}\}\,v_0 \blacktriangleright_{\mathsf{F}} \mathsf{TagErr}$
Immediate.

Case: $\mathit{unop}\{\mathcal{U}\}\,v_0 \blacktriangleright_{\mathsf{F}} \mathit{add\text{-}trace}(\mathit{get\text{-}trace}(v_0), \delta(\mathit{unop}, v_1))$
Immediate.

Case: $\mathsf{fst}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\,v_0)) \blacktriangleright_{\mathsf{F}} \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\tau_1\}\,v_0))$
(1) $\cdot \vdash_1 v_0 : \tau_1 \times \tau_2$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 \mathsf{fst}\{\tau_1\}\,v_0 : \tau_1$
By (1)
(3) $\cdot \vdash_1 \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\tau_1\}\,v_0)) : \mathcal{U}$
By (2)

Case: $\mathsf{snd}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\,v_0)) \blacktriangleright_{\mathsf{F}} \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\tau_2\}\,v_0))$
(1) $\cdot \vdash_1 v_0 : \tau_1 \times \tau_2$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 \mathsf{snd}\{\tau_2\}\,v_0 : \tau_2$
By (1)
(3) $\cdot \vdash_1 \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\tau_2\}\,v_0) : \mathcal{U}$
By (2)

Case: $\mathit{binop}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{F}} \mathsf{TagErr}$
Immediate.

Case: $\mathit{binop}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{F}} \delta(\mathit{binop}, v_2, v_3)$
Immediate.

Case: $\mathsf{app}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{F}} \mathsf{TagErr}$
Immediate.

Case: $\mathsf{app}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\lambda x_0.\,e_0))\,v_0 \blacktriangleright_{\mathsf{F}} \mathsf{trace}\,\overline{b}_0\,(e_0[x_0 \leftarrow v_1])$
By substitution lemmas for untyped functions and for $F(\cdot)$.

Case: $\mathsf{app}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_2) \blacktriangleleft \ell_1)\,v_0))\,v_1 \blacktriangleright_{\mathsf{F}}$
$\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\tau_2\}\,v_0\,(\mathsf{dyn}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\,v_2)))$
(1) $\cdot \vdash_1 v_0 : \tau_1 \Rightarrow \tau_2$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 v_1 : \mathcal{U}$
By $\vdash_1$ on the redex
(3) $\cdot \vdash_1 \mathsf{dyn}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\,v_1 : \tau_1 \Rightarrow \tau_2$
By (2)

(4) $\cdot \vdash_1 \mathsf{app}\{\tau_2\}\, v_0\, (\mathsf{dyn}\, (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_1) : \tau_2$
By (1) and (3)

(5) $\cdot \vdash_1 \mathsf{trace}\, \overline{b}_0\, (\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\, (\mathsf{app}\{\tau_2\}\, v_0\, (\mathsf{dyn}\, (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, v_2))) : \mathcal{U}$
By (4)

Case: $\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \blacktriangleright_{\mathsf{F}} \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0$
Immediate.

Case: $\mathsf{stat}\, b_0\, (\mathbb{G}\, b_1\, (\mathbb{T}_?\, \overline{b}_0\, v_0)) \blacktriangleright_{\mathsf{F}} \mathsf{trace}\, (b_0 b_1 \overline{b}_0)\, v_0$

(1) $\cdot \vdash_1 v_0 : \mathcal{U}$
By $\vdash_1$ on the redex

(2) $\cdot \vdash_1 \mathsf{trace}\, (b_0 b_1 \overline{b}_0)\, v_0 : \mathcal{U}$
By (1)

Case: $\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, i_0 \blacktriangleright_{\mathsf{F}} i_0$
Immediate.

Case: $\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \blacktriangleright_{\mathsf{F}} \mathsf{InvariantErr}$
Immediate.

Case: $\mathsf{trace}\, \overline{b}_0\, v_0 \blacktriangleright_{\mathsf{F}} \mathit{add\text{-}trace}(\overline{b}_0, v_0)$
Immediate.

□

Theorem A.16 (Forgetful blame soundness and completeness). *Forgetful satisfies* **BS** *and* **BC**.

Proof. By preservation of path-owner consistency ($\Vdash_p$) for $\rhd_{\overline{\mathsf{F}}}$ and $\blacktriangleright_{\overline{\mathsf{F}}}$.

Case: $(\mathit{unop}\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell}_0})^{\ell_0} \rhd_{\overline{\mathsf{F}}} (\mathsf{InvariantErr})^{\ell_0}$
Immediate.

Case: $(\mathit{unop}\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell}_0})^{\ell_0} \rhd_{\overline{\mathsf{F}}} (\delta(\mathit{unop}, v_0))^{\overline{\ell}_0\ell_0}$

(1) $v_0 = \langle v_1, v_2\rangle$ and $\delta(\mathit{unop}, v_0) \in \{v_1, v_2\}$
By definition

(2) $\ell_0; \cdot \Vdash_p v_0$
By $\Vdash_p$ on the redex

(3) $\ell_0; \cdot \Vdash_p v_1$ and $\ell_0; \cdot \Vdash_p v_2$
By (2) and (3)

(4) $\ell_0; \cdot \Vdash_p \delta(\mathit{unop}, v_0)$
By (1) and (3)

Case: $(\mathsf{fst}\{\tau_0\}\,(\!(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(v_0)^{\ell_2})\!)^{\overline{\ell}_0})^{\ell_3} \rhd_{\overline{\mathsf{F}}} (\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathcal{U}\}\,(v_0)^{\ell_2}))^{\overline{\ell}_0\ell_3}$

(1) $\ell_1; \cdot \Vdash_p (v_0)^{\ell_2}$
By $\Vdash_p$ on the redex

(2) $\ell_1; \cdot \Vdash_p \mathsf{fst}\{\mathcal{U}\}\,(v_0)^{\ell_2}$
By (1)

(3) $\ell_3; \cdot \Vdash_p (\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathcal{U}\}\,(v_0)^{\ell_2}))^{\overline{\ell}_0\ell_3}$
By (1) and $\Vdash_p$ on the redex

Case: $(\mathsf{snd}\{\tau_0\}\,(\!(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(v_0)^{\ell_2})\!)^{\overline{\ell}_0})^{\ell_3} \rhd_{\overline{\mathsf{F}}} (\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathcal{U}\}\,(v_0)^{\ell_2}))^{\overline{\ell}_0\ell_3}$

(1) $\ell_1; \cdot \Vdash_p (v_0)^{\ell_2}$
By $\Vdash_p$ on the redex

(2) $\ell_1; \cdot \Vdash_p \mathsf{snd}\{\mathcal{U}\}\,(v_0)^{\ell_2}$
By (1)

(3) $\ell_3; \cdot \Vdash_p (\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathcal{U}\}\,(v_0)^{\ell_2}))^{\overline{\ell}_0\ell_3}$
By (1) and $\Vdash_p$ on the redex

Case: $(\mathit{binop}\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell}_0}\,(\!(v_1)\!)^{\overline{\ell}_1})^{\ell_0} \rhd_{\overline{\mathsf{F}}} (\mathsf{InvariantErr})^{\ell_0}$
Immediate.

Case: $(\mathit{binop}\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell}_0}\,(\!(v_1)\!)^{\overline{\ell}_1})^{\ell_0} \rhd_{\overline{\mathsf{F}}} (\delta(\mathit{binop}, v_0, v_1))^{\ell_0}$

(1) $\delta(\mathit{binop}, v_0, v_1) \in i$
By definition of δ

(2) $\ell_0; \cdot \Vdash_p \delta(\mathit{binop}, v_0, v_1)$
By (1)

Case: $(\mathsf{app}\{\tau_0\}\,(\!(v_0)\!)^{\overline{\ell}_0}\,v_1)^{\ell_0} \rhd_{\overline{\mathsf{F}}} (\mathsf{InvariantErr})^{\ell_0}$
Immediate.

Case: $(\mathsf{app}\{\tau_0\}\,(\!(\lambda(x_0 : \tau_1).\,e_0)\!)^{\overline{\ell}_0}\,v_0)^{\ell_0} \rhd_{\overline{\mathsf{F}}} (\!(e_0[x_0 \leftarrow (\!(v_0)\!)^{\ell_0 \mathit{rev}(\overline{\ell}_0)}])\!)^{\overline{\ell}_0\ell_0}$

(1) $\ell_0; \cdot \Vdash_p \lambda(x_0 : \tau_1).\,e_0$
By $\Vdash_p$ on the redex

(2) $\ell_0; \cdot \Vdash_p v_0$
By $\Vdash_p$ on the redex

(3) $\ell_0; \cdot \Vdash_p \llparenthesis v_0 \rrparenthesis^{\ell_0 \, rev(\overline{\ell}_0)}$
By (1) and (2)

(4) $\ell_0; \cdot \Vdash_p x_0$ for each occurrence of x_0 in e_0
By $\Vdash_p$ on the redex

(5) $\ell_0; \cdot \Vdash_p \llparenthesis e_0[x_0 \leftarrow \llparenthesis v_1 \rrparenthesis^{\ell_0 \, rev(\overline{\ell}_0)}] \rrparenthesis^{\overline{\ell}_0 \ell_0}$
By (3) and (4)

Case: $(\mathsf{app}\{\tau_0\} \, \llparenthesis \mathbb{G} \, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) \, (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_0} \; v_1)^{\ell_3} \rhd_{\overline{\mathsf{F}}}$

$\llparenthesis \mathsf{dyn} \, (\ell_0 \blacktriangleleft cod(\tau_1) \blacktriangleleft \ell_1) \, (\mathsf{app}\{\mathcal{U}\} \, v_0 \, (\mathsf{stat} \, (\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0) \, \llparenthesis v_1 \rrparenthesis^{\ell_3 \, rev(\overline{\ell}_0)}))^{\ell_2} \rrparenthesis^{\overline{\ell}_0 \ell_3}$

(1) $\ell_2; \cdot \Vdash_p v_0$
By $\Vdash_p$ on the redex

(2) $\ell_3; \cdot \Vdash_p v_1$
By $\Vdash_p$ on the redex

(3) $\ell_3; \cdot \Vdash_p \llparenthesis v_1 \rrparenthesis^{\ell_3 \, rev(\overline{\ell}_0)}$
By (2) and $\Vdash_p$ on the redex

(4) $\ell_2; \cdot \Vdash_p \mathsf{stat} \, (\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0) \, \llparenthesis v_1 \rrparenthesis^{\ell_3 \, rev(\overline{\ell}_0)}$
By (3) and $\Vdash_p$ on the redex

(5) $\ell_3; \cdot \Vdash_p \llparenthesis \mathsf{dyn} \, (\ell_0 \blacktriangleleft cod(\tau_1) \blacktriangleleft \ell_1) \, (\mathsf{app}\{\mathcal{U}\} \, v_0 \, (\mathsf{stat} \, (\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0) \, \llparenthesis v_1 \rrparenthesis^{\ell_3 \, rev(\overline{\ell}_0)}))^{\ell_2} \rrparenthesis^{\overline{\ell}_0 \ell_3}$
By (1) and (4)

Case: $(\mathsf{dyn} \, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_2} \rhd_{\overline{\mathsf{F}}} (\mathbb{G} \, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_2}$
Immediate.

Case: $(\mathsf{dyn} \, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \, \llparenthesis \mathbb{T}_? \, \overline{b}_0 \, \llparenthesis i_0 \rrparenthesis^{\overline{\ell}_0} \rrparenthesis^{\overline{\ell}_1})^{\ell_2} \rhd_{\overline{\mathsf{F}}} (i_0)^{\ell_2}$
Immediate.

Case: $(\mathsf{dyn} \, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_2})^{\ell_3} \rhd_{\overline{\mathsf{F}}} (\mathsf{BoundaryErr} \, ((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b}_0, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_2}))^{\ell_3}$
Immediate.

Case: $(unop\{\mathcal{U}\} \, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0})^{\ell_0} \blacktriangleright_{\overline{\mathsf{F}}} (\mathsf{TagErr})^{\ell_0}$
Immediate.

Case: $(unop\{\mathcal{U}\} \, v_0)^{\ell_0} \blacktriangleright_{\overline{\mathsf{F}}}$

$(add\text{-}trace(get\text{-}trace(v_0), \delta(unop, rem\text{-}trace(v_0))))^{\ell_0}$

(1) $v_0 = \mathbb{T}_? \, \overline{b}_0 \, \langle v_1, v_2 \rangle$ and $\delta(unop, rem\text{-}trace(v_0)) \in \{v_1, v_2\}$
By definition

(2) $\ell_0; \cdot \Vdash_p v_0$ and $\ell_n; \cdot \Vdash_p rem\text{-}trace(v_0)$
By $\Vdash_p$ on the redex

(3) $\ell_n; \cdot \Vdash_p v_1$ and $\ell_n; \cdot \Vdash_p v_2$
By (2)

(4) $\ell_0; \cdot \Vdash_p add\text{-}trace(get\text{-}trace(v_0), \delta(unop, rem\text{-}trace(v_0)))$
By (1) and (3)

Case: $(\mathsf{fst}\{\mathcal{U}\} \, \llparenthesis \mathbb{T}_? \, \overline{b}_0 \, \llparenthesis \mathbb{G} \, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \, (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3} \rrparenthesis^{\overline{\ell}_4})^{\ell_5} \blacktriangleright_{\overline{\mathsf{F}}}$

$(\mathsf{trace} \, \overline{b}_0 \, \llparenthesis \mathsf{stat} \, (\ell_0 \blacktriangleleft fst(\tau_0) \blacktriangleleft \ell_1) \, (\mathsf{fst}\{fst(\tau_0)\} \, v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3})^{\overline{\ell}_4 \ell_5}$

(1) $\ell_5; \cdot \Vdash_p \mathbb{T}_? \, \overline{b}_0 \, \llparenthesis \mathbb{G} \, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \, (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3}$
By $\Vdash_p$ on the redex
(2) $\ell_0; \cdot \Vdash_p \mathbb{G} \, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \, (v_0)^{\ell_2}$
By (1)
(3) $\ell_1; \cdot \Vdash_p v_0$
By (2)
(4) $\ell_1; \cdot \Vdash_p \mathsf{fst}\{\mathit{fst}(\tau_0)\} \, v_0$
By (3)
(5) $\ell_0; \cdot \Vdash_p \mathsf{stat} \, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1) \, (\mathsf{fst}\{\mathit{fst}(\tau_0)\} \, v_0)^{\ell_2}$
By (4)
(6) $\ell_5; \cdot \Vdash_p \mathsf{trace} \, \overline{b}_0 \, \llparenthesis \mathsf{stat} \, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1) \, (\mathsf{fst}\{\mathit{fst}(\tau_0)\} \, v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3}$
By (1) and (5)

Case: $(\mathsf{snd}\{\mathcal{U}\} \, \llparenthesis \mathbb{T}_? \, \overline{b}_0 \, \llparenthesis \mathbb{G} \, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \, (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3} \rrparenthesis^{\overline{\ell}_4})^{\ell_5} \; \blacktriangleright_{\overline{\mathsf{F}}}$
$(\mathsf{trace} \, \overline{b}_0 \, \llparenthesis \mathsf{stat} \, b_0 \, (\mathsf{snd}\{\mathit{snd}(\tau_0)\} \, v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3})^{\overline{\ell}_4 \ell_5}$
(1) $\ell_5; \cdot \Vdash_p \mathbb{T}_? \, \overline{b}_0 \, \llparenthesis \mathbb{G} \, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \, (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3}$
By $\Vdash_p$ on the redex
(2) $\ell_0; \cdot \Vdash_p \mathbb{G} \, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \, (v_0)^{\ell_2}$
By (1)
(3) $\ell_1; \cdot \Vdash_p v_0$
By (2)
(4) $\ell_1; \cdot \Vdash_p \mathsf{snd}\{\mathit{snd}(\tau_0)\} \, v_0$
By (3)
(5) $\ell_0; \cdot \Vdash_p \mathsf{stat} \, (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1) \, (\mathsf{snd}\{\mathit{snd}(\tau_0)\} \, v_0)^{\ell_2}$
By (4)
(6) $\ell_5; \cdot \Vdash_p \mathsf{trace} \, \overline{b}_0 \, \llparenthesis \mathsf{stat} \, (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1) \, (\mathsf{snd}\{\mathit{snd}(\tau_0)\} \, v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3}$
By (1) and (5)

Case: $(\mathit{binop}\{\mathcal{U}\} \, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0} \, \llparenthesis v_1 \rrparenthesis^{\overline{\ell}_1})^{\ell_0} \; \blacktriangleright_{\overline{\mathsf{F}}} \; (\mathsf{TagErr})^{\ell_0}$
Immediate.

Case: $(\mathit{binop}\{\mathcal{U}\} \, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0} \, \llparenthesis v_1 \rrparenthesis^{\overline{\ell}_1})^{\ell_0} \; \blacktriangleright_{\overline{\mathsf{F}}} \; \delta(\mathit{binop}, v_2, v_3)$
Immediate.

Case: $(\mathsf{app}\{\mathcal{U}\} \, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0} \, v_1)^{\ell_0} \; \blacktriangleright_{\overline{\mathsf{F}}} \; (\mathsf{TagErr})^{\ell_0}$
Immediate.

Case: $(\mathsf{app}\{\mathcal{U}\} \, \llparenthesis \mathbb{T}_? \, \overline{b}_0 \, \llparenthesis \lambda x_0.\, e_0 \rrparenthesis^{\overline{\ell}_0} \rrparenthesis^{\overline{\ell}_1} \, v_0)^{\ell_2} \; \blacktriangleright_{\overline{\mathsf{F}}}$
$(\mathsf{trace} \, \overline{b}_0 \, \llparenthesis e_0[x_0 \leftarrow \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), \llparenthesis v_0 \rrparenthesis^{\ell_2 \mathit{rev}(\overline{\ell}_1) \mathit{rev}(\overline{\ell}_0)})] \rrparenthesis^{\overline{\ell}_0})^{\overline{\ell}_1 \ell_2}$
(1) $\ell_2; \cdot \Vdash_p \mathbb{T}_? \, \overline{b}_0 \, \llparenthesis \lambda x_0.\, e_0 \rrparenthesis^{\overline{\ell}_0}$
By $\Vdash_p$ on the redex
(2) $\ell_n; \cdot \Vdash_p \lambda x_0.\, e_0$
By (1)
(3) $\ell_2; \cdot \Vdash_p v_0$
By $\Vdash_p$ on the redex

(4) $\ell_2; \cdot \Vdash_p v_0$
By $\Vdash_p$ on the redex

(5) $\ell_n; \cdot \Vdash_p \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), (\!(v_0)\!)^{\ell_2 \mathit{rev}(\overline{\ell}_1) \mathit{rev}(\overline{\ell}_0)})$
By (2) and (4)

(6) $\ell_n; \cdot \Vdash_p x_0$ for each occurrence of x_0 in e_0
By $\Vdash_p$ on the redex

(7) $\ell_2; \cdot \Vdash_p \mathsf{trace}\,\overline{b}_0\,(\!(e_0[x_0 \leftarrow \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), (\!(v_0)\!)^{\ell_2 \mathit{rev}(\overline{\ell}_1) \mathit{rev}(\overline{\ell}_0)})])\!)^{\overline{\ell}_0}$
By (5) and (6)

Case: $(\mathsf{app}\{\mathcal{U}\}\,(\!(\mathbb{T}_?\,\overline{b}_0\,(\!(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(v_0)^{\ell_2})\!)^{\overline{\ell}_3})\!)^{\overline{\ell}_4}\ v_1)^{\ell_5} \blacktriangleright_{\overline{\mathsf{F}}}$

$(\!(\mathsf{trace}\,\overline{b}_0\,(\!(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathit{cod}(\tau_0)\}\,v_0\ v_2)^{\ell_2})\!)^{\overline{\ell}_3})\!)^{\overline{\ell}_4 \ell_5}$
where $v_2 = \mathsf{dyn}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\ \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), (\!(v_1)\!)^{\ell_5 \mathit{rev}(\overline{\ell}_3 \overline{\ell}_4)})$

(1) $\ell_5; \cdot \Vdash_p \mathbb{T}_?\,\overline{b}_0\,(\!(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(v_0)^{\ell_2})\!)^{\overline{\ell}_3}$
By $\Vdash_p$ on the redex

(2) $\ell_0; \cdot \Vdash_p \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(v_0)^{\ell_2}$ and $\ell_1; \cdot \Vdash_p v_0$
By (1)

(3) $\ell_5; \cdot \Vdash_p v_1$
By $\Vdash_p$ on the redex

(4) $\ell_0; \cdot \Vdash_p \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), (\!(v_1)\!)^{\ell_5 \mathit{rev}(\overline{\ell}_3 \overline{\ell}_4)})$
By (1) and (3)

(5) $\ell_1; \cdot \Vdash_p \mathsf{dyn}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\ \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), (\!(v_1)\!)^{\ell_5 \mathit{rev}(\overline{\ell}_3 \overline{\ell}_4)})$
By (4)

(6) $\ell_5; \cdot \Vdash_p \mathsf{trace}\,\overline{b}_0\,(\!(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathit{cod}(\tau_0)\}\,v_0\ v_2)^{\ell_2})\!)^{\overline{\ell}_3}$
where $v_2 = \mathsf{dyn}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\ \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), (\!(v_1)\!)^{\ell_5 \mathit{rev}(\overline{\ell}_3 \overline{\ell}_4)})$
By (1) and (5)

Case: $(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)^{\ell_2} \blacktriangleright_{\overline{\mathsf{F}}} (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)^{\ell_2}$
Immediate.

Case: $(\mathsf{stat}\,b_0\,(\!(\mathbb{G}\,b_1\,(\!(\mathbb{T}_?\,\overline{b}_2\,v_0)\!)^{\overline{\ell}_0})\!)^{\overline{\ell}_1})^{\ell_2} \blacktriangleright_{\overline{\mathsf{F}}} (\mathsf{trace}\,(b_0 b_1 \overline{b}_2)\,(\!(v_0)\!)^{\overline{\ell}_0 \overline{\ell}_1 \ell_2})^{\ell_2}$

(1) $b_0 = (\ell_2 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)$
By $\Vdash_p$ on the redex

(2) $\ell_1; \cdot \Vdash_p (\!(\mathbb{G}\,b_1\,(\!(\mathbb{T}_?\,\overline{b}_2\,v_0)\!)^{\overline{\ell}_0})\!)^{\overline{\ell}_1}$
By $\Vdash_p$ on the redex and (1)

(3) $\ell_0; \cdot \Vdash_p (\!(\mathbb{T}_?\,\overline{b}_2\,v_0)\!)^{\overline{\ell}_0}$
By $\Vdash_p$ on the redex and (1)

(4) $\ell_2; \cdot \Vdash_p \mathsf{trace}\,(b_0 b_1 \overline{b}_2)\,(\!(v_0)\!)^{\overline{\ell}_0 \overline{\ell}_1 \ell_2}$
By (2) and (3)

Case: $(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\!(i_0)\!)^{\overline{\ell}_2})^{\ell_3} \blacktriangleright_{\overline{\mathsf{F}}} (i_0)^{\ell_3}$
Immediate.

Case: $(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\!(v_0)\!)^{\overline{\ell}_2})^{\ell_3} \blacktriangleright_{\overline{\mathsf{F}}} (\mathsf{InvariantErr})^{\ell_3}$
Immediate.

Case: $(\mathsf{trace}\,\overline{b}_0\;v_0)^{\ell_0} \blacktriangleright_{\overline{\mathsf{F}}} (\mathit{add\text{-}trace}(\overline{b}_0, v_0))^{\ell_0}$
Immediate.

□

Lemma A.17 ($C \lesssim F$).

- *If* $e_0 \lesssim e_2$ *and* $e_0 \rightarrow_{\mathsf{C}} e_1$ *then* $\exists\, e_3, e_4$ *such that* $e_1 \rightarrow^*_{\mathsf{C}} e_3$ *and* $e_2 \rightarrow^*_{\mathsf{F}} e_4$ *and* $e_3 \lesssim e_4$.
- *If* $e_0 \lesssim e_2$ *and* $e_2 \rightarrow_{\mathsf{F}} e_3$ *then* $\exists\, e_1, e_4$ *such that* $e_3 \rightarrow^*_{\mathsf{F}} e_4$ *and* $e_0 \rightarrow^*_{\mathsf{C}} e_1$ *and* $e_1 \lesssim e_4$

Proof. By lemma A.18 and lemma A.19. □

$\boxed{\mathrm{wfr}_{CF}(e_0, e_1)}$ holds for well-formed residuals of a common term; that is, pairs such that there exists an e_2 where $e_2 : {}^{\tau}/_{\mathcal{U}}$ **wf** and $e_2 \rightarrow^*_{\mathsf{C}} e_0$ and $e_2 \rightarrow^*_{\mathsf{F}} e_1$

Lemma A.18.
If $\mathrm{wfr}_{CF}(e_0, e_2)$ *and* $e_0 \lesssim e_2$ *and* $e_0 \rightarrow_{\mathsf{C}} e_1$ *then* $\exists\, e_3, e_4$ *such that* $e_1 \rightarrow^*_{\mathsf{C}} e_3$ *and* $e_2 \rightarrow^*_{\mathsf{F}} e_4$ *and* $e_3 \lesssim e_4$.

Proof. By lemma A.20, lemma A.23, and case analysis of $\rhd_{\mathsf{C}} \cup \blacktriangleright_{\mathsf{C}}$.

Case: $unop\{\tau_0\}\, v_0 \rhd_{\mathsf{C}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $unop\{\tau_0\}\, v_0 \rhd_{\mathsf{C}} \delta(unop, v_0)$
(1) $e_1 = unop\{\tau_0\}\, v_1$ and $v_0 \lesssim v_1$
By $\lesssim$ on the redex
(2) $\delta(unop, v_1)$ is defined
By (1)
(3) $\delta(unop, v_0) \lesssim \delta(unop, v_1)$

Case: $\mathsf{fst}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0) \rhd_{\mathsf{C}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_0)$
(1) $e_1 = \mathsf{fst}\{\tau_0\}\, v_1$ and $v_0 \lesssim v_1$
By $\lesssim$ on the redex
(2) $v_1 \in \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_5$
(3) $e_1 \rhd_{\mathsf{F}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_1)$
and $\mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_5) \lesssim \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_1)$

Case: $\mathsf{snd}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0 \rhd_{\mathsf{C}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_0)$
(1) $e_1 = \mathsf{snd}\{\tau_0\}\, v_1$ and $v_0 \lesssim v_1$
By $\lesssim$ on the redex
(2) $v_1 \in \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_5$
(3) $e_1 \rhd_{\mathsf{F}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_1)$
and $\mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_5) \lesssim \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_1)$

Case: $binop\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{C}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $binop\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{C}} \delta(binop, v_0, v_1)$
(1) $e_1 = binop\{\tau_0\}\, v_2\, v_3$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex
(2) $\delta(binop, v_2, v_3)$ is defined
By (1)
(3) $\delta(binop, v_0, v_1) \lesssim \delta(binop, v_2, v_3)$
By δ

Case: $\mathsf{app}\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{C}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathsf{app}\{\tau_0\}\, (\lambda(x_0 : \tau_1).\, e_0)\, v_0 \rhd_{\mathsf{C}} e_0[x_0 \leftarrow v_0]$
(1) $e_1 = \mathsf{app}\{\tau_0\}\, v_1\, v_2$ and $(\lambda(x_0 : \tau_1).\, e_4) \lesssim v_1$ and $v_0 \lesssim v_2$
By $\lesssim$ on the redex

(2) $v_1 = \lambda(x_0 : \tau_1).\, e_5$
By (1)
(3) $e_4[x_0 \leftarrow v_0] \lesssim e_5[x_0 \leftarrow v_2]$
Case: $\mathsf{app}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0)\, v_1 \rhd_{\mathsf{C}}$
$\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_0\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_1))$
(1) $e_1 = \mathsf{app}\{\tau_0\}\, v_2\, v_3$ and $(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0) \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex
(2) $v_2 = \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_4$
(3) $e_1 \rhd_{\mathsf{F}} \mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_4\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_3))$
(4) $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_0\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_1)) \lesssim$
$\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_4\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_3))$
Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \rhd_{\mathsf{C}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0$
(1) $e_1 = \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1$ and $v_0 \lesssim v_1$
By $\lesssim$
(2) $e_1 \rhd_{\mathsf{F}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1$
By $\rhd_{\mathsf{F}}$
(3) $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \lesssim \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1$
Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, i_0 \rhd_{\mathsf{C}} i_0$
(1) $e_1 = \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1$ and $i_0 \lesssim v_1$
By $\lesssim$
(2) $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1 \rhd_{\mathsf{F}} v_1$ and $i_0 \lesssim v_1$
Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \rhd_{\mathsf{C}} \mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), v_0)$
Immediate
Case: $\mathit{unop}\{\mathcal{U}\}\, v_0 \blacktriangleright_{\mathsf{C}} \mathsf{TagErr}$
(1) $e_1 = \mathit{unop}\{\mathcal{U}\}\, v_1$ and $v_0 \lesssim v_1$
By $\lesssim$ on the redex
(2) $\delta(\mathit{unop}, v_1)$ is undefined
By (1)
(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$
Case: $\mathit{unop}\{\mathcal{U}\}\, v_0 \blacktriangleright_{\mathsf{C}} \delta(\mathit{unop}, v_0)$
(1) $e_1 = \mathit{unop}\{\tau_0\}\, v_1$ and $v_0 \lesssim v_1$
By $\lesssim$ on the redex
(2) $\delta(\mathit{unop}, v_1)$ is defined
By (1)
(3) $\delta(\mathit{unop}, v_0) \lesssim \delta(\mathit{unop}, v_1)$
Case: $\mathsf{fst}\{\mathcal{U}\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0) \blacktriangleright_{\mathsf{C}} \mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathit{fst}(\tau_0)\}\, v_0)$
(1) $e_1 = \mathsf{fst}\{\tau_0\}\, v_1$ and $v_0 \lesssim v_1$
By $\lesssim$ on the redex
(2) If $v_1 \in \mathbb{T}\, \overline{b}_0\, v_2$ then either $\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathit{fst}(\tau_0)\}\, v_0) \rightarrow^*_{\mathsf{C}} \mathsf{BoundaryErr}\,(\overline{b}, v)$ or
$\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathit{fst}(\tau_0)\}\, v_0) \rightarrow^*_{\mathsf{C}} v_3$ and $e_1 \rightarrow^*_{\mathsf{F}} v_4$ and $v_3 \lesssim v_4$
(3) Otherwise $v_1 \in \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_5$ and $e_1 \blacktriangleright_{\mathsf{F}} \mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathit{fst}(\tau_0)\}\, v_1)$
and $\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathit{fst}(\tau_0)\}\, v_5) \lesssim \mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathit{fst}(\tau_0)\}\, v_1)$
Case: $\mathsf{snd}\{\mathcal{U}\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \blacktriangleright_{\mathsf{C}} \mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathit{snd}(\tau_0)\}\, v_0)$
(1) $e_1 = \mathsf{snd}\{\tau_0\}\, v_1$ and $v_0 \lesssim v_1$
By $\lesssim$ on the redex
(2) If $v_1 \in \mathbb{T}\, \overline{b}_0\, v_2$ then either $\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathit{snd}(\tau_0)\}\, v_0) \rightarrow^*_{\mathsf{C}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
or $\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathit{snd}(\tau_0)\}\, v_0) \rightarrow^*_{\mathsf{C}} v_3$ and $e_1 \rightarrow^*_{\mathsf{F}} v_4$ and $v_3 \lesssim v_4$

(3) Otherwise $v_1 \in \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_5$ and $e_1 \blacktriangleright_{\mathsf{F}}$ $\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{snd}\{\mathit{snd}(\tau_0)\}\ v_1)$ and $\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{snd}\{\mathit{snd}(\tau_0)\}\ v_5) \lesssim \mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\ (\mathsf{snd}\{\mathit{snd}(\tau_0)\}\ v_1)$

Case: $\mathit{binop}\{\mathcal{U}\}\ v_0\ v_1 \blacktriangleright_{\mathsf{C}} \mathsf{TagErr}$

(1) $e_1 = \mathit{binop}\{\mathcal{U}\}\ v_2\ v_3$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex

(2) $\delta(\mathit{binop}, \mathit{rem\text{-}trace}(v_2), \mathit{rem\text{-}trace}(v_3))$ is undefined
By (1)

(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathit{binop}\{\mathcal{U}\}\ v_0\ v_1 \blacktriangleright_{\mathsf{C}} \delta(\mathit{binop}, v_0, v_1)$

(1) $e_1 = \mathit{binop}\{\mathcal{U}\}\ v_2\ v_3$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex

(2) $\delta(\mathit{binop}, \mathit{rem\text{-}trace}(v_2), \mathit{rem\text{-}trace}(v_3))$ is defined
By (1)

(3) $\delta(\mathit{binop}, v_0, v_1) \lesssim \delta(\mathit{binop}, \mathit{rem\text{-}trace}(v_2), \mathit{rem\text{-}trace}(v_3))$
By δ

Case: $\mathsf{app}\{\mathcal{U}\}\ v_0\ v_1 \blacktriangleright_{\mathsf{C}} \mathsf{TagErr}$

(1) $e_1 = \mathsf{app}\{\mathcal{U}\}\ v_2\ v_3$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex

(2) $v_2 \notin \lambda x.\, e \cup \mathbb{G}\ b\ v$
By (1)

(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathsf{app}\{\mathcal{U}\}\ (\lambda x_0.\, e_0)\ v_0 \blacktriangleright_{\mathsf{C}} e_0[x_0 \leftarrow v_0]$

(1) $e_1 = \mathsf{app}\{\mathcal{U}\}\ v_1\ v_2$ and $(\lambda x_0.\, e_4) \lesssim v_1$ and $v_0 \lesssim v_2$
By $\lesssim$ on the redex

(2) $v_1 = (\lambda x_0.\, e_5)$
By (1)

(3) $(e_4[x_0 \leftarrow v_1]) \lesssim (e_5[x_0 \leftarrow v_2])$

Case: $\mathsf{app}\{\mathcal{U}\}\ (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)\ v_1 \blacktriangleright_{\mathsf{C}}$
$\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{app}\{\mathit{cod}(\tau_0)\}\ v_0\ (\mathsf{dyn}\ (\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\ v_1))$

(1) $e_1 = \mathsf{app}\{\mathcal{U}\}\ v_2\ v_3$ and $(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_0) \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex

(2) If $v_2 = \mathbb{T}\,\overline{b}_0\ v_4$ then either
$\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{app}\{\mathit{cod}(\tau_0)\}\ v_0\ (\mathsf{dyn}\ (\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\ v_1)) \rightarrow^*_{\mathsf{C}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
or $\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{app}\{\mathit{cod}(\tau_0)\}\ v_0\ (\mathsf{dyn}\ (\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\ v_1)) \rightarrow^*_{\mathsf{C}} v_5$
and $e_1 \rightarrow^*_{\mathsf{F}} v_6$ and $v_5 \lesssim v_6$

(3) Otherwise $v_2 \in \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_7$
and $e_1 \blacktriangleright_{\mathsf{F}} \mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{app}\{\mathcal{U}\}\ v_7\ (\mathsf{stat}\ (\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\ v_3))$
and $\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{app}\{\mathit{cod}(\tau_0)\}\ v_0\ (\mathsf{dyn}\ (\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\ v_1)) \lesssim$
$\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{app}\{\mathcal{U}\}\ v_7\ (\mathsf{stat}\ (\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\ v_3))$

Case: $\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \blacktriangleright_{\mathsf{C}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0$

(1) $e_1 = \mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$ and $v_0 \lesssim v_1$
By $\lesssim$

(2) If $e_1 \notin \mathbb{G}\ b\ v$ then $e_1 \blacktriangleright_{\mathsf{F}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$ and $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \lesssim \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$
By $\blacktriangleright_{\mathsf{F}}$

(3) Otherwise $e_1 = \mathbb{G}\ b_1\ (\mathbb{T}_?\ \overline{b}_0\ v_2)$ and $e_1 \rightarrow^*_{\mathsf{F}} \mathbb{T}\ b_0 b_1 \overline{b}_0\ v_2$ and $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \lesssim \mathbb{T}\ b_0 b_1 \overline{b}_0\ v_2$

Case: $\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ i_0 \blacktriangleright_{\mathsf{C}} i_0$

(1) $e_1 = \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$ and $i_0 \lesssim v_1$

By $\lesssim$

(2) $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1 \blacktriangleright_{\mathsf{F}} v_1$ and $i_0 \lesssim v_1$

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \blacktriangleright_{\mathsf{C}} \mathsf{InvariantErr}$

Impossible, by type soundness

□

Lemma A.19.
If $\mathrm{wfr}_{CF}(e_0, e_2)$ *and* $e_0 \lesssim e_2$ *and* $e_2 \rightarrow_{\mathsf{F}} e_3$ *then* $\exists\, e_1, e_4$ *such that* $e_3 \rightarrow^*_{\mathsf{F}} e_4$ *and* $e_0 \rightarrow^*_{\mathsf{C}} e_1$ *and* $e_1 \lesssim e_4$

Proof. By lemma A.20, lemma A.23, and case analysis of $\triangleright_{\mathsf{F}} \cup \blacktriangleright_{\mathsf{F}}$.

Case: $\mathit{unop}\{\tau_0\}\, v_0 \triangleright_{\mathsf{F}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathit{unop}\{\tau_0\}\, v_0 \triangleright_{\mathsf{F}} \delta(\mathit{unop}, v_0)$

(1) $e_0 = \mathit{unop}\{\tau_0\}\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex

(2) $\delta(\mathit{unop}, v_1)$ is defined
By (1)

(3) $\delta(\mathit{unop}, v_1) \lesssim \delta(\mathit{unop}, v_0)$

Case: $\mathsf{fst}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0) \triangleright_{\mathsf{F}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_0)$

(1) $e_0 = \mathsf{fst}\{\tau_0\}\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex

(2) $v_1 \in \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_5$

(3) $e_1 \triangleright_{\mathsf{C}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_1)$
and $\mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_5) \lesssim \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_1)$

Case: $\mathsf{snd}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0 \triangleright_{\mathsf{F}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_0)$

(1) $e_0 = \mathsf{snd}\{\tau_0\}\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex

(2) $v_1 \in \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_5$

(3) $e_1 \triangleright_{\mathsf{C}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_1)$
and $\mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_5) \lesssim \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_1)$

Case: $\mathit{binop}\{\tau_0\}\, v_0\, v_1 \triangleright_{\mathsf{F}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathit{binop}\{\tau_0\}\, v_0\, v_1 \triangleright_{\mathsf{F}} \delta(\mathit{binop}, v_0, v_1)$

(1) $e_0 = \mathit{binop}\{\tau_0\}\, v_2\, v_3$ and $v_2 \lesssim v_0$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex

(2) $\delta(\mathit{binop}, v_2, v_3)$ is defined
By (1)

(3) $\delta(\mathit{binop}, v_2, v_3) \lesssim \delta(\mathit{binop}, v_0, v_1)$
By δ

Case: $\mathsf{app}\{\tau_0\}\, v_0\, v_1 \triangleright_{\mathsf{F}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathsf{app}\{\tau_0\}\, (\lambda(x_0 : \tau_1).\, e_0)\, v_0 \triangleright_{\mathsf{F}} e_0[x_0 \leftarrow v_0]$

(1) $e_0 = \mathsf{app}\{\tau_0\}\, v_1\, v_2$ and $v_1 \lesssim (\lambda(x_0 : \tau_1).\, e_4)$ and $v_2 \lesssim v_0$
By $\lesssim$ on the redex

(2) $v_1 = \lambda(x_0 : \tau_1).\, e_5$
By (1)

(3) $e_5[x_0 \leftarrow v_2] \lesssim e_4[x_0 \leftarrow v_0]$

Case: $\mathsf{app}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0)\, v_1 \triangleright_{\mathsf{F}}$
$\mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_0\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_1))$

(1) $e_0 = \mathsf{app}\{\tau_0\}\, v_2\, v_3$ and $v_2 \lesssim (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0)$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex

(2) $v_2 \in \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_4$

(3) $e_0 \triangleright_{\mathsf{C}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_4\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_3))$

(4) $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\ (\mathsf{app}\{\mathcal{U}\}\ v_4\ (\mathsf{stat}\ (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\ v_3)) \lesssim$
$\mathsf{dyn}\ (\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\ (\mathsf{app}\{\mathcal{U}\}\ v_0\ (\mathsf{stat}\ (\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\ v_1))$

Case: $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \rhd_{\mathsf{F}} \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0$
(1) $e_0 = \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$ and $v_1 \lesssim v_0$
By $\lesssim$
(2) $e_0 \rhd_{\mathsf{C}} \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$
By $\rhd_{\mathsf{C}}$
(3) $\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1 \lesssim \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0$

Case: $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\mathbb{T}_?\ \overline{b}_0\ i_0) \rhd_{\mathsf{F}} i_0$
(1) $e_0 = \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ i_1$ and $i_1 \lesssim i_0$
By $\lesssim$
(2) $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ i_1 \rhd_{\mathsf{C}} i_1$ and $i_1 \lesssim i_0$

Case: $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \rhd_{\mathsf{F}} \mathsf{BoundaryErr}\ ((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b}_0, v_0)$
(1) $e_0 = \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$ and $v_1 \lesssim v_0$
By $\lesssim$
(2) $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1 \rhd_{\mathsf{C}} \mathsf{BoundaryErr}\ (\overline{b}, v)$

Case: $\mathit{unop}\{\mathcal{U}\}\ v_0 \blacktriangleright_{\mathsf{F}} \mathsf{TagErr}$
(1) $e_0 = \mathit{unop}\{\mathcal{U}\}\ v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex
(2) $\delta(\mathit{unop}, v_1)$ is undefined
By (1)
(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathit{unop}\{\mathcal{U}\}\ v_0 \blacktriangleright_{\mathsf{F}} \mathit{add\text{-}trace}(\mathit{get\text{-}trace}(v_0), \delta(\mathit{unop}, v_1))$
(1) $e_0 = \mathit{unop}\{\tau_0\}\ v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex
(2) $\delta(\mathit{unop}, v_1)$ is defined
By (1)
(3) $\delta(\mathit{unop}, v_1) \lesssim \delta(\mathit{unop}, v_0)$

Case: $\mathsf{fst}\{\mathcal{U}\}\ (\mathbb{T}_?\ \overline{b}_0\ (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)) \blacktriangleright_{\mathsf{F}} \mathsf{trace}\ \overline{b}_0\ (\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{fst}\{\mathit{fst}(\tau_0)\}\ v_0))$
(1) $e_0 = \mathsf{fst}\{\tau_0\}\ v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex
(2) If $\overline{b}_0$ is not empty then either $\mathsf{fst}\{\tau_0\}\ v_1 \rightarrow^*_{\mathsf{C}} \mathsf{BoundaryErr}\ (\overline{b}, v)$ or $\mathsf{fst}\{\tau_0\}\ v_1 \rightarrow^*_{\mathsf{C}} v_3$ and $e_1 \rightarrow^*_{\mathsf{F}} v_4$ (unfolding guards and collecting traces) and $v_3 \lesssim v_4$
(3) Otherwise $\overline{b}_0$ is empty and $\mathsf{fst}\{\tau_0\}\ v_1 \blacktriangleright_{\mathsf{C}} \mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{fst}\{\mathit{fst}(\tau_0)\}\ v_1)$
and $e_0 \blacktriangleright_{\mathsf{F}} \mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{fst}\{\mathit{fst}(\tau_0)\}\ v_0)$
and $\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{fst}\{\mathit{fst}(\tau_0)\}\ v_1) \lesssim \mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{fst}\{\mathit{fst}(\tau_0)\}\ v_0)$

Case: $\mathsf{snd}\{\mathcal{U}\}\ (\mathbb{T}_?\ \overline{b}_0\ (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)) \blacktriangleright_{\mathsf{F}} \mathsf{trace}\ \overline{b}_0\ (\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{snd}\{\tau_1\}\ v_0))$
(1) $e_0 = \mathsf{snd}\{\tau_0\}\ v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex
(2) If $\overline{b}_0$ is not empty then either $\mathsf{snd}\{\tau_0\}\ v_1 \rightarrow^*_{\mathsf{C}} \mathsf{BoundaryErr}\ (\overline{b}, v)$ or $\mathsf{snd}\{\tau_0\}\ v_1 \rightarrow^*_{\mathsf{C}} v_3$ and $e_1 \rightarrow^*_{\mathsf{F}} v_4$ (unfolding guards and collecting traces) and $v_3 \lesssim v_4$
(3) Otherwise $\overline{b}_0$ is empty and $\mathsf{snd}\{\tau_0\}\ v_1 \blacktriangleright_{\mathsf{C}} \mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{snd}\{\mathit{snd}(\tau_0)\}\ v_1)$
and $e_0 \blacktriangleright_{\mathsf{F}} \mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{snd}\{\mathit{snd}(\tau_0)\}\ v_0)$
and $\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{snd}\{\mathit{snd}(\tau_0)\}\ v_1) \lesssim \mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{snd}\{\mathit{snd}(\tau_0)\}\ v_0)$

Case: $\mathit{binop}\{\mathcal{U}\}\ v_0\ v_1 \blacktriangleright_{\mathsf{F}} \mathsf{TagErr}$
(1) $e_0 = \mathit{binop}\{\mathcal{U}\}\ v_2\ v_3$ and $v_2 \lesssim v_0$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex

(2) $\delta(binop, rem\text{-}trace(v_2), rem\text{-}trace(v_3))$ is undefined
By (1)
(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $binop\{\mathcal{U}\}\, v_0\, v_1 \blacktriangleright_{\mathsf{F}} \delta(binop, v_2, v_3)$
(1) $e_0 = binop\{\mathcal{U}\}\, v_2\, v_3$ and $v_2 \lesssim v_0$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex
(2) $\delta(binop, rem\text{-}trace(v_2), rem\text{-}trace(v_3))$ is defined
By (1)
(3) $\delta(binop, rem\text{-}trace(v_2), rem\text{-}trace(v_3)) \lesssim \delta(binop, v_0, v_1)$
By δ

Case: $\mathsf{app}\{\mathcal{U}\}\, v_0\, v_1 \blacktriangleright_{\mathsf{F}} \mathsf{TagErr}$
(1) $e_0 = \mathsf{app}\{\mathcal{U}\}\, v_2\, v_3$ and $v_2 \lesssim v_0$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex
(2) $v_2 \notin \lambda x.\, e \cup \mathbb{G}\, b\, v$
By (1)
(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathsf{app}\{\mathcal{U}\}\, (\mathbb{T}_?\, \overline{b}_0\, (\lambda x_0.\, e_0))\, v_0 \blacktriangleright_{\mathsf{F}} \mathsf{trace}\, \overline{b}_0\, (e_0[x_0 \leftarrow v_1])$
(1) $e_1 = \mathsf{app}\{\mathcal{U}\}\, v_1\, v_2$ and $v_1 \lesssim (\lambda x_0.\, e_4)$ and $v_2 \lesssim v_0$ and $\overline{b}_0$ is empty
By $\lesssim$ on the redex
(2) $v_1 = (\lambda x_0.\, e_5)$
By (1)
(3) $(e_5[x_0 \leftarrow v_2]) \lesssim (e_4[x_0 \leftarrow v_1])$

Case: $\mathsf{app}\{\mathcal{U}\}\, (\mathbb{T}_?\, \overline{b}_0\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0))\, v_1 \blacktriangleright_{\mathsf{F}} \mathsf{trace}\, \overline{b}_0\, (\mathsf{stat}\, b_0\, (\mathsf{app}\{\tau_1\}\, v_0\, (\mathsf{dyn}\, b_1\, v_1)))$
(1) $e_0 = \mathsf{app}\{\mathcal{U}\}\, v_2\, v_3$ and $v_2 \lesssim (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0)$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex
(2) If $\overline{b}_0$ is not empty then either $\mathsf{app}\{\mathcal{U}\}\, v_2\, v_3 \rightarrow^*_{\mathsf{C}} \mathsf{BoundaryErr}\, (\overline{b}, v)$
or $\mathsf{app}\{\mathcal{U}\}\, v_2\, v_3 \rightarrow^*_{\mathsf{C}} v_5$
and $e_1 \rightarrow^*_{\mathsf{F}} v_6$ (unfolding guards and collecting traces) and $v_5 \lesssim v_6$
(3) Otherwise $\overline{b}_0$ is empty
and $e_1 \blacktriangleright_{\mathsf{F}} \mathsf{stat}\, (\ell_0 \blacktriangleleft cod(\tau_0) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_7\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft dom(\tau_0) \blacktriangleleft \ell_0)\, v_1))$
and $e_0 \blacktriangleright_{\mathsf{C}} \mathsf{stat}\, (\ell_0 \blacktriangleleft cod(\tau_0) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_8\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft dom(\tau_0) \blacktriangleleft \ell_0)\, v_3))$
and $\mathsf{stat}\, (\ell_0 \blacktriangleleft cod(\tau_0) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_8\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft dom(\tau_0) \blacktriangleleft \ell_0)\, v_3)) \lesssim$
$\mathsf{stat}\, (\ell_0 \blacktriangleleft cod(\tau_0) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathcal{U}\}\, v_7\, (\mathsf{stat}\, (\ell_1 \blacktriangleleft dom(\tau_0) \blacktriangleleft \ell_0)\, v_1))$

Case: $\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \blacktriangleright_{\mathsf{F}} \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0$
(1) $e_0 = \mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$
(2) $e_1 \blacktriangleright_{\mathsf{C}} \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0$
(3) $\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \lesssim \mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0$

Case: $\mathsf{stat}\, b_0\, (\mathbb{G}\, b_1\, (\mathbb{T}_?\, \overline{b}_0\, v_0)) \blacktriangleright_{\mathsf{F}} \mathsf{trace}\, (b_0 b_1 \overline{b}_0)\, v_0$
(1) $e_0 = \mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1$ and $v_1 \lesssim \mathbb{G}\, b_1\, (\mathbb{T}_?\, \overline{b}_0\, v_0)$
By $\lesssim$
(2) $v_1 = \mathbb{G}\, b_1\, v_2$ and $v_2 \lesssim \mathbb{T}_?\, \overline{b}_0\, v_0$
By (1)
(3) $e_0 \blacktriangleright_{\mathsf{C}} \mathbb{G}\, b_0\, (\mathbb{G}\, b_1\, v_2)$
By (2)
(4) $e_1 \blacktriangleright_{\mathsf{F}} \mathbb{T}\, (b_0 b_1 \overline{b}_0)\, v_0$
By $\blacktriangleright_{\mathsf{F}}$

(5) $\mathbb{G}\, b_0\, (\mathbb{G}\, b_1\, v_2) \lesssim \mathbb{T}\, (b_0 b_1 \overline{b}_0)\, v_0$

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, i_0 \blacktriangleright_{\mathsf{F}} i_0$

(1) $e_0 = \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, i_1$ and $i_1 \lesssim i_0$

By $\lesssim$

(2) $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, i_1 \blacktriangleright_{\mathsf{F}} i_1$ and $i_1 \lesssim i_0$

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \blacktriangleright_{\mathsf{F}} \mathsf{InvariantErr}$

Impossible, by type soundness

Case: $\mathsf{trace}\, \overline{b}_0\, v_0 \blacktriangleright_{\mathsf{F}} \mathit{add\text{-}trace}(\overline{b}_0, v_0)$

(1) $e_0 = \mathsf{stat}\, b_0\, (\mathsf{dyn}\, b_1\, v_1)$ and $\overline{b}_0 = b_0 b_1 \overline{b}_0$

By $\lesssim$

(2) $\mathit{add\text{-}trace}(\overline{b}_0, v_0) = \mathbb{T}\, \overline{b}_0\, v_0$

By (1)

(3) Either $e_0 \rightarrow_{\mathsf{C}}^{*} \mathsf{BoundaryErr}\,(\overline{b}, v)$ or $e_0 \rightarrow_{\mathsf{C}}^{*} v_2$ and $v_2 \lesssim \mathbb{T}\, \overline{b}_0\, v_0$

□

Lemma A.20.
If $\mathrm{wfr}_{CF}(e_0, e_1)$ *and* $e_0 \lesssim e_1$ *and either* $e_0 \rightarrow_{\mathsf{C}} e_2$ *or* $e_1 \rightarrow_{\mathsf{F}} e_3$ *then the following results hold:*

- $e_0 = E_0[e_4]$
- $e_1 = E_1[e_5]$
- $E_0 \lesssim E_1$
- $e_4 \lesssim e_5$.

Proof. By lemma A.21 and lemma A.22. □

Lemma A.21.
If $\mathrm{wfr}_{CF}(E_0[e_0], e_1)$ *and* $E_0[e_0] \lesssim e_1$ *and* $e_0(\rhd_{\mathsf{C}} \cup \blacktriangleright_{\mathsf{C}})e_2$ *then the following results hold:*

- $e_1 = E_1[e_3]$
- $E_0 \lesssim E_1$
- $e_0 \lesssim e_3$.

Proof. By induction on $E_0[e_0] \lesssim e_1$, proceeding by case analysis of $E_0[e_0]$. □

Lemma A.22.
If $\mathrm{wfr}_{CF}(e_0, E_1[e_1])$ *and* $e_0 \lesssim E_1[e_1]$ *and* $e_1(\rhd_{\mathsf{F}} \cup \blacktriangleright_{\mathsf{F}})e_3$ *then the following results hold:*

- $e_0 = E_0[e_2]$
- $E_0 \lesssim E_1$
- $e_2 \lesssim e_1$.

Proof. By induction on $e_0 \lesssim E_1[e_1]$, proceeding by case analysis of $E_1[e_1]$. □

Lemma A.23.
If $E_0 \lesssim E_1$ *and* $e_2 \lesssim e_3$ *then* $E_0[e_2] \lesssim E_1[e_3]$.

Proof. By induction on $E_0 \lesssim E_1$. □

A.4 Transient

Lemma A.24 (Transient type progress).
If $\mathcal{T}_0; \cdot \vdash_s E_0[e_0]; \mathcal{H}_0; \mathcal{B}_0 : s \cup \mathcal{U}$ *then one of the following holds:*

- $e_0 \in v \cup \mathsf{Err}$
- $\exists\, e_1, \mathcal{H}_1, \mathcal{B}_1.\ e_0; \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} e_1; \mathcal{H}_1; \mathcal{B}_1$

Proof. By unique decomposition (lemma 6.1) and case analysis:

Case: $\mathcal{T}_0; \cdot \vdash_s i_0; \mathcal{H}_0; \mathcal{B}_0 : \mathsf{Int}$
Immediate.
Case: $\mathcal{T}_0; \cdot \vdash_s n_0; \mathcal{H}_0; \mathcal{B}_0 : \mathsf{Nat}$
Immediate.
Case: $\mathcal{T}_0; \cdot \vdash_s (\lambda x_0.\, e_0); \mathcal{H}_0; \mathcal{B}_0 : \mathsf{Fun}$
$\rhd_{\mathsf{T}}\ \mathsf{p}_0; (\{\mathsf{p}_0 \mapsto (\lambda x_0.\, e_0)\} \cup \mathcal{H}_0); (\{\mathsf{p}_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$
Case: $\mathcal{T}_0; \cdot \vdash_s (\lambda(x_0 : \tau_0).\, e_0); \mathcal{H}_0; \mathcal{B}_0 : \mathsf{Fun}$
$\rhd_{\mathsf{T}}\ \mathsf{p}_0; (\{\mathsf{p}_0 \mapsto (\lambda(x_0 : \tau_0).\, e_0)\} \cup \mathcal{H}_0); (\{\mathsf{p}_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$
Case: $\mathcal{T}_0; \cdot \vdash_s \langle v_0, v_1\rangle; \mathcal{H}_0; \mathcal{B}_0 : \mathsf{Pair}$
$\rhd_{\mathsf{T}}\ \mathsf{p}_0; (\{\mathsf{p}_0 \mapsto \langle v_0, v_1\rangle\} \cup \mathcal{H}_0); (\{\mathsf{p}_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$
Case: $\mathcal{T}_0; \cdot \vdash_s (\mathsf{app}\{\tau_0\}\, v_0\, v_1); \mathcal{H}_0; \mathcal{B}_0 : \lfloor \tau_0 \rfloor$
- $\rhd_{\mathsf{T}}\ (\mathsf{check}\{\tau_0\}\, (e_0[x_0 \leftarrow v_1])\, v_0; \mathcal{H}_0; \mathcal{B}_0[v_1 \cup \mathit{rev}(\mathcal{B}_0(v_0))]$
  if $\mathcal{H}_0(v_0) = \lambda(x_0 : \tau_1).\, e_0$ and $\mathit{shape\text{-}match}(\lfloor \tau_1 \rfloor, v_1)$
- $\rhd_{\mathsf{T}}\ (\mathsf{check}\{\tau_0\}\, (e_0[x_0 \leftarrow v_1])\, v_0); \mathcal{H}_0; \mathcal{B}_0[v_1 \cup \mathit{rev}(\mathcal{B}_0(v_0))]$
  if $\mathcal{H}_0(v_0) = \lambda x_0.\, e_0$
- $\rhd_{\mathsf{T}}$ Err otherwise

Case: $\mathcal{T}_0; \cdot \vdash_s (\mathit{unop}\{\tau_0\}\, v_0); \mathcal{H}_0; \mathcal{B}_0 : \lfloor \tau_0 \rfloor$
- $\rhd_{\mathsf{T}}\ \mathsf{check}\{\tau_0\}\, \delta(\mathit{unop}, \mathcal{H}_0(v_0))\, v_0; \mathcal{H}_0; \mathcal{B}_0$ if defined
- $\rhd_{\mathsf{T}}$ Err otherwise

Case: $\mathcal{T}_0; \cdot \vdash_s (\mathit{binop}\{\tau_0\}\, v_0\, v_1); \mathcal{H}_0; \mathcal{B}_0 : \lfloor \tau_0 \rfloor$
- $\rhd_{\mathsf{T}}\ \delta(\mathit{binop}, v_0, v_1); \mathcal{H}_0; \mathcal{B}_0$ if defined
- $\rhd_{\mathsf{T}}$ Err otherwise

Case: $\mathcal{T}_0; \cdot \vdash_s (\mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0); \mathcal{H}_0; \mathcal{B}_0 : \lfloor \tau_0 \rfloor$
- $\rhd_{\mathsf{T}}\ v_0; \mathcal{H}_0; \mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}]$
  if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$
- $\rhd_{\mathsf{T}}$ Err otherwise

Case: $\mathcal{T}_0; \cdot \vdash_s (\mathsf{check}\{\tau_0\}\, v_0\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0 : \lfloor \tau_0 \rfloor$
- $\rhd_{\mathsf{T}}\ v_0; \mathcal{H}_0; \mathcal{B}_0[v_0 \cup \mathcal{B}_0(\mathsf{p}_0)]$
  if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
- $\rhd_{\mathsf{T}}$ Err otherwise

Case: $\mathcal{T}_0; \cdot \vdash_s \mathsf{p}_0; \mathcal{H}_0; \mathcal{B}_0 : s_0$
Immediate.
Case: $\mathcal{T}_0; \cdot \vdash_s \mathsf{Err}; \mathcal{H}_0; \mathcal{B}_0 : s_0$
Immediate.
Case: $\mathcal{T}_0; \cdot \vdash_s i_0; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$
Immediate.
Case: $\mathcal{T}_0; \cdot \vdash_s n_0; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$
Immediate.
Case: $\mathcal{T}_0; \cdot \vdash_s (\lambda x_0.\, e_0); \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$
$\rhd_{\mathsf{T}}\ \mathsf{p}_0; (\{\mathsf{p}_0 \mapsto (\lambda x_0.\, e_0)\} \cup \mathcal{H}_0); (\{\mathsf{p}_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$

Case: $\mathcal{T}_0; \cdot \vdash_s (\lambda(x_0 : \tau_0).\, e_0); \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$
$\rhd_{\mathsf{T}}$ $\mathsf{p}_0; (\{\mathsf{p}_0 \mapsto (\lambda(x_0 : \tau_0).\, e_0)\} \cup \mathcal{H}_0); (\{\mathsf{p}_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$

Case: $\mathcal{T}_0; \cdot \vdash_s \langle v_0, v_1 \rangle; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$
$\rhd_{\mathsf{T}}$ $\mathsf{p}_0; (\{\mathsf{p}_0 \mapsto \langle v_0, v_1 \rangle\} \cup \mathcal{H}_0); (\{\mathsf{p}_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$

Case: $\mathcal{T}_0; \cdot \vdash_s (\mathsf{app}\{\mathcal{U}\}\, v_0\, v_1); \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$
- $\rhd_{\mathsf{T}}$ $(\mathsf{check}\{\mathcal{U}\}\, (e_0[x_0 \leftarrow v_1])\, v_0; \mathcal{H}_0; \mathcal{B}_0[v_1 \cup \mathit{rev}(\mathcal{B}_0(v_0))]$
  if $\mathcal{H}_0(v_0) = \lambda(x_0 : \tau_1).\, e_0$ and $\mathit{shape\text{-}match}(\lfloor \tau_1 \rfloor, v_1)$
- $\rhd_{\mathsf{T}}$ $(e_0[x_0 \leftarrow v_1]); \mathcal{H}_0; \mathcal{B}_0$
  if $\mathcal{H}_0(v_0) = \lambda x_0.\, e_0$
- $\rhd_{\mathsf{T}}$ Err otherwise

Case: $\mathcal{T}_0; \cdot \vdash_s (\mathit{unop}\{\mathcal{U}\}\, v_0); \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$
- $\rhd_{\mathsf{T}}$ $\mathsf{check}\{\mathcal{U}\}\, \delta(\mathit{unop}, \mathcal{H}_0(v_0))\, v_0; \mathcal{H}_0; \mathcal{B}_0$ if defined
- $\rhd_{\mathsf{T}}$ Err otherwise

Case: $\mathcal{T}_0; \cdot \vdash_s (\mathit{binop}\{\mathcal{U}\}\, v_0\, v_1); \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$
- $\rhd_{\mathsf{T}}$ $\delta(\mathit{binop}, v_0, v_1); \mathcal{H}_0; \mathcal{B}_0$ if defined
- $\rhd_{\mathsf{T}}$ Err otherwise

Case: $\mathcal{T}_0; \cdot \vdash_s (\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0); \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$
- $\rhd_{\mathsf{T}}$ $v_0; \mathcal{H}_0; \mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}]$
  if $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$
- $\rhd_{\mathsf{T}}$ Err otherwise

Case: $\mathcal{T}_0; \cdot \vdash_s (\mathsf{check}\{\mathcal{U}\}\, v_0\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$
$\rhd_{\mathsf{T}}$ $v_0; \mathcal{H}_0; \mathcal{B}_0$

Case: $\mathcal{T}_0; \cdot \vdash_s \mathsf{p}_0; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$
Immediate.

Case: $\mathcal{T}_0; \cdot \vdash_s \mathsf{Err}; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$
Immediate.

□

Lemma A.25 (Transient type preservation).
If $\mathcal{T}_0; \cdot \vdash_{\mathsf{s}} e_0; \mathcal{H}_0; \mathcal{B}_0 : {}^{\tau}/_{\mathcal{U}}$ *and* $e_0; \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} e_1; \mathcal{H}_1; \mathcal{B}_1$ *then* $\exists\, \mathcal{T}_1.\ \mathcal{T}_0 \subseteq \mathcal{T}_1$ *and* $\mathcal{T}_1; \cdot \vdash_{\mathsf{s}} e_1; \mathcal{H}_1; \mathcal{B}_1 : {}^{\tau}/_{\mathcal{U}}$.

Proof. By case analysis of the reduction relation. The new heap typing $\mathcal{T}_1$ gains an entry only when the value heap does; if $\mathcal{H}_1 = \{\mathsf{p}_0 \mapsto \mathsf{w}_0\} \cup \mathcal{H}_0$ then $\mathcal{T}_1 = \{(\mathsf{p}_0 : s_0)\} \cup \mathcal{T}_0$, where s_0 is the shape of the pre-value (lemma 6.47).

Case: $\mathsf{w}_0; \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{p}_0; (\{\mathsf{p}_0 \mapsto \mathsf{w}_0\} \cup \mathcal{H}_0); (\{\mathsf{p}_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$
(1) $\mathcal{T}_0; \cdot \vdash_{\mathsf{s}} \mathsf{w}_0; \mathcal{H}_0; \mathcal{B}_0 : s_0$
By $\vdash_{\mathsf{s}}$ on the redex
(2) $\mathcal{T}_1 = (\mathsf{p}_0 : s_0), \mathcal{T}_0$
(3) $\mathcal{T}_1; \cdot \vdash_{\mathsf{s}} \mathsf{p}_0; (\{\mathsf{p}_0 \mapsto \mathsf{w}_0\} \cup \mathcal{H}_0); (\{\mathsf{p}_0 \mapsto \emptyset\} \cup \mathcal{B}_0) : s_0$
By (1) and (2)
Case: $(\mathit{unop}\{\tau_0\}\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$
Impossible for a well-typed redex
Case: $(\mathit{unop}\{\mathcal{U}\}\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{TagErr}; \mathcal{H}_0; \mathcal{B}_0$
$\mathcal{T}_1 = \mathcal{T}_0$
Case: $(\mathit{unop}\{{}^{\tau}/_{\mathcal{U}}\}\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} (\mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\, \delta(\mathit{unop}, \mathcal{H}_0(\mathsf{p}_0))\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0$
(1) $\mathcal{T}_1 = \mathcal{T}_0$
(2) $\mathcal{T}_1; \cdot \vdash_{\mathsf{s}} \delta(\mathit{unop}, \mathcal{H}_0(\mathsf{p}_0)); \mathcal{H}_0; \mathcal{B}_0 : s_1$
By a variant of lemma 6.2 for $\vdash_{\mathsf{s}}$.
(3) $\mathcal{T}_1; \cdot \vdash_{\mathsf{s}} (\mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\, \delta(\mathit{unop}, \mathcal{H}_0(\mathsf{p}_0))\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0 : {}^{\tau}/_{\mathcal{U}}$
By (2)
Case: $(\mathit{binop}\{\tau_0\}\, v_0\, v_1); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$
Impossible for a well-typed redex
Case: $(\mathit{binop}\{\mathcal{U}\}\, v_0\, v_1); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{TagErr}; \mathcal{H}_0; \mathcal{B}_0$
$\mathcal{T}_1 = \mathcal{T}_0$
Case: $(\mathit{binop}\{{}^{\tau}/_{\mathcal{U}}\}\, i_0\, i_1); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \delta(\mathit{binop}, i_0, i_1); \mathcal{H}_0; \mathcal{B}_0$
(1) $\mathcal{T}_1 = \mathcal{T}_0$
(2) $\mathcal{T}_1; \cdot \vdash_{\mathsf{s}} \delta(\mathit{binop}, i_0, i_1); \mathcal{H}_0; \mathcal{B}_0 : {}^{\tau}/_{\mathcal{U}}$
By lemma 6.2 (restated for tags rather than types)
Case: $(\mathsf{app}\{\tau_0\}\, v_0\, v_1); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$
Impossible for a well-typed redex
Case: $(\mathsf{app}\{\mathcal{U}\}\, v_0\, v_1); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{TagErr}; \mathcal{H}_0; \mathcal{B}_0$
$\mathcal{T}_1 = \mathcal{T}_0$
Case: $(\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, \mathsf{p}_0\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} (\mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\, e_0[x_0 \leftarrow v_0]\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_1$
(1) $\mathcal{T}_1 = \mathcal{T}_0$
(2) $\mathcal{T}_0; \cdot \vdash_{\mathsf{s}} e_0[x_0 \leftarrow v_0]; \mathcal{H}_0; \mathcal{B}_0 : s_1$
By a substitution lemma for $\vdash_{\mathsf{s}}$
(3) $\mathcal{T}_1; \cdot \vdash_{\mathsf{s}} e_0[x_0 \leftarrow v_0]; \mathcal{H}_0; \mathcal{B}_1 : s_1$
By a store extension lemma and (2)
(4) $\mathcal{T}_1; \cdot \vdash_{\mathsf{s}} (\mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\, e_0[x_0 \leftarrow v_0]\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_1 : \lfloor {}^{\tau}/_{\mathcal{U}} \rfloor$
By (3)
Case: $(\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, \mathsf{p}_0\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{BoundaryErr}\,(\mathit{rev}(\mathcal{B}_0(\mathsf{p}_0)), v_0); \mathcal{H}_0; \mathcal{B}_1$
$\mathcal{T}_1 = \mathcal{T}_0$
Case: $(\mathsf{app}\{\tau_0\}\, \mathsf{p}_0\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} (\mathsf{check}\{\tau_0\}\, e_0[x_0 \leftarrow v_0]\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_1$
(1) $\mathcal{T}_1 = \mathcal{T}_0$
(2) $\mathcal{T}_0; \cdot \vdash_{\mathsf{s}} e_0[x_0 \leftarrow v_0]; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$
By a substitution lemma for $\vdash_{\mathsf{s}}$

(3) $\mathcal{T}_1; \cdot \vdash_{\mathsf{s}} e_0[x_0 \leftarrow v_0]; \mathcal{H}_0; \mathcal{B}_1 : \mathcal{U}$
By a store extension lemma and (2)
(4) $\mathcal{T}_1; \cdot \vdash_{\mathsf{s}} (\mathsf{check}\{\tau_0\}\, e_0[x_0 \leftarrow v_0]\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_1 : \lfloor {}^{\tau}/_{\mathcal{U}} \rfloor$
By (3)
Case: $(\mathsf{app}\{\mathcal{U}\}\, \mathsf{p}_0\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} (e_0[x_0 \leftarrow v_0]); \mathcal{H}_0; \mathcal{B}_0$
(1) $\mathcal{T}_1 = \mathcal{T}_0$
(2) $\mathcal{T}_1; \cdot \vdash_{\mathsf{s}} e_0[x_0 \leftarrow v_0]; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$
By a substitution lemma for $\vdash_{\mathsf{s}}$
Case: $(\mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}])$
(1) $\mathcal{T}_1 = \mathcal{T}_0$
(2) $\mathcal{T}_1; \cdot \vdash_{\mathsf{s}} v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}]) : \lfloor \tau_0 \rfloor$
By a lemma for *shape-match* $(\lfloor \tau_0 \rfloor, \cdot)$ and $\vdash_{\mathsf{s}}$
Case: $(\mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{BoundaryErr}\, (\{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}, v_0); \mathcal{H}_0; \mathcal{B}_0$
$\mathcal{T}_1 = \mathcal{T}_0$
Case: $(\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}])$
(1) $\mathcal{T}_1 = \mathcal{T}_0$
(2) $\mathcal{T}_1; \cdot \vdash_{\mathsf{s}} v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}]) : \lfloor \tau_0 \rfloor$
By a lemma for *shape-match* $(\lfloor \tau_0 \rfloor, \cdot)$ and $\vdash_{\mathsf{s}}$
Case: $(\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$
Impossible for a well-typed redex
Case: $(\mathsf{check}\{\mathcal{U}\}\, v_0\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} v_0; \mathcal{H}_0; \mathcal{B}_0$
$\mathcal{T}_1 = \mathcal{T}_0$
Case: $(\mathsf{check}\{\tau_0\}\, v_0\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \mathcal{B}_0(\mathsf{p}_0)])$
(1) $\mathcal{T}_1 = \mathcal{T}_0$
(2) $\mathcal{T}_1; \cdot \vdash_{\mathsf{s}} v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}]) : \lfloor \tau_0 \rfloor$
By a lemma for *shape-match* $(\lfloor \tau_0 \rfloor, \cdot)$ and $\vdash_{\mathsf{s}}$
Case: $(\mathsf{check}\{\tau_0\}\, v_0\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{BoundaryErr}\, (\mathcal{B}_0(v_0) \cup \mathcal{B}_0(\mathsf{p}_0), v_0); \mathcal{H}_0; \mathcal{B}_0$
$\mathcal{T}_1 = \mathcal{T}_0$

□

A.5 Amnesic

Lemma A.26 (Amnesic type progress). *If* $\cdot \vdash_1 E_0[e_0] : {}^{\tau}\!/_{\mathcal{U}}$ *and* $A(E_0[e_0])$ *then one of the following holds:*

- $e_0 \in v \cup \mathsf{Err}$
- ${}^{\tau}\!/_{\mathcal{U}} \in \tau$ *and* $\exists\, e_1.\ e_0 \rhd_{\mathsf{A}} e_1$
- ${}^{\tau}\!/_{\mathcal{U}} \in \mathcal{U}$ *and* $\exists\, e_1.\ e_0 \blacktriangleright_{\mathsf{A}} e_1$

Proof. By unique decomposition (lemma 6.1) and case analysis:

Case: $\cdot \vdash_1 n_0 : \mathsf{Nat}$
Immediate.
Case: $\cdot \vdash_1 i_0 : \mathsf{Int}$
Immediate.
Case: $\cdot \vdash_1 \lambda(x_0 : \tau_0).\, e_1 : \tau_0 \Rightarrow \tau_1$
Immediate.
Case: $\cdot \vdash_1 \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$
Immediate.
Case: $\cdot \vdash_1 \mathit{unop}\{\tau_0\}\, v_0 : \tau_0$
- $\rhd_{\mathsf{A}}$ $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\mathsf{fst}\{\mathcal{U}\}\ v_1)$
  if $\mathit{unop} = \mathsf{fst}$ and $v_0 = \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\ v_1$
- $\rhd_{\mathsf{A}}$ $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\mathsf{snd}\{\mathcal{U}\}\ v_1)$
  if $\mathit{unop} = \mathsf{snd}$ and $v_0 = \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\ v_1$
- $\rhd_{\mathsf{A}}$ $\delta(\mathit{unop}, v_0)$ if defined
- $\rhd_{\mathsf{A}}$ Err otherwise

Case: $\cdot \vdash_1 \mathit{binop}\{\tau_0\}\, v_0\, v_1 : \tau_0$
- $\rhd_{\mathsf{A}}$ $\delta(\mathit{binop}, v_0, v_1)$ if defined
- $\rhd_{\mathsf{A}}$ Err otherwise

Case: $\cdot \vdash_1 \mathsf{app}\{\tau_0\}\ v_0\ v_1 : \tau_0$
- $\rhd_{\mathsf{A}}$ $e_1[x_0 \leftarrow v_1]$
  if $v_0 = \lambda(\tau_1 : x_0).\, e_1$
- $\rhd_{\mathsf{A}}$ $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\mathsf{app}\{\mathcal{U}\}\ v_2\ (\mathsf{stat}\ (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\ v_1))$
  if $v_0 = \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_2) \blacktriangleleft \ell_1)\ v_2$
- $\rhd_{\mathsf{A}}$ Err otherwise

Case: $\cdot \vdash_1 \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 : \tau_0$
- $\rhd_{\mathsf{A}}$ $\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0$
  if $\tau_0 \in \tau \Rightarrow \tau \cup \tau \times \tau$ and $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
- $\rhd_{\mathsf{A}}$ v_0
  if $v_0 \in \mathbb{T}_?\, \overline{b}_0\, i$ and $\tau_0 \in \mathsf{Int}$
- $\rhd_{\mathsf{A}}$ v_0
  if $v_0 \in \mathbb{T}_?\, \overline{b}_0\, n$ and $\tau_0 \in \mathsf{Nat}$
- $\rhd_{\mathsf{A}}$ Err otherwise

Case: $\cdot \vdash_1 \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)\ v_0 : \tau_0$
Immediate.
Case: $\cdot \vdash_1 \mathbb{G}\ (\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1)\ v_0 : \tau_0$
Immediate.
Case: $\cdot \vdash_1 \mathsf{Err} : \tau_0$
Immediate.

Case: $\cdot \vdash_1 i : \mathcal{U}$

Immediate.

Case: $\cdot \vdash_1 \lambda x_0.\, e_0 : \mathcal{U}$

Immediate.

Case: $\cdot \vdash_1 \langle v_0, v_1 \rangle : \mathcal{U}$

Immediate.

Case: $\cdot \vdash_1 \mathit{unop}\{\mathcal{U}\}\, v_0 : \mathcal{U}$

- $\blacktriangleright_{\mathsf{A}}$ $\mathsf{trace}\, \overline{b}_0\, (\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\tau_1\}\, v_1))$
  if $\mathit{unop} = \mathsf{fst}$ and $v_0 = \mathbb{T}_?\, \overline{b}_0\, (\mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\, v_1)$
- $\blacktriangleright_{\mathsf{A}}$ $\mathsf{trace}\, \overline{b}_0\, (\mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\tau_2\}\, v_1))$
  if $\mathit{unop} = \mathsf{snd}$ and $v_0 = \mathbb{T}_?\, \overline{b}_0\, (\mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\, v_1)$
- $\blacktriangleright_{\mathsf{A}}$ $\mathit{add\text{-}trace}(\mathit{get\text{-}trace}(v_0), \delta(\mathit{unop}, \mathit{rem\text{-}trace}(v_0)))$ if defined
- $\blacktriangleright_{\mathsf{A}}$ Err otherwise

Case: $\cdot \vdash_1 \mathit{binop}\{\mathcal{U}\}\, v_0\, v_1 : \mathcal{U}$

- $\blacktriangleright_{\mathsf{A}}$ $\delta(\mathit{binop}, \mathit{rem\text{-}trace}(v_0), \mathit{rem\text{-}trace}(v_1))$ if defined
- $\blacktriangleright_{\mathsf{A}}$ Err otherwise

Case: $\cdot \vdash_1 \mathsf{app}\{\mathcal{U}\}\, v_0\, v_1 : \mathcal{U}$

- $\blacktriangleright_{\mathsf{A}}$ $\mathsf{trace}\, \overline{b}_0\, (e_1[x_0 \leftarrow (\mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), v_1)])$
  if $v_0 = \mathbb{T}_?\, \overline{b}_0\, (\lambda x_0.\, e_1)$
- $\blacktriangleright_{\mathsf{A}}$ $\mathsf{trace}\, \overline{b}_0\, \mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{app}\{\tau_0\}\, v_2\, (\mathsf{dyn}\, (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\, \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), v_1)))$
  if $v_0 = \mathbb{T}_?\, \overline{b}_0\, (\mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1)\, v_2)$
- $\blacktriangleright_{\mathsf{A}}$ Err otherwise

Case: $\cdot \vdash_1 \mathsf{stat}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 : \mathcal{U}$

- $\blacktriangleright_{\mathsf{A}}$ $\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0$
  if $\tau_0 \in \tau \Rightarrow \tau \cup \tau \times \tau$ and $v_0 \in (\lambda(x : \tau).\, e) \cup \langle v, v \rangle$ and $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
- $\blacktriangleright_{\mathsf{A}}$ $\mathsf{trace}\, (b_0 b_1 \overline{b}_0)\, v_1$
  if $\tau_0 \in \tau \Rightarrow \tau \cup \tau \times \tau$ and $v_0 = \mathbb{G}\, b_1\, (\mathbb{T}_?\, \overline{b}_0\, v_1)$ and $\mathit{shape\text{-}match}(\lfloor \tau_0 \rfloor, v_0)$
- $\blacktriangleright_{\mathsf{A}}$ v_0
  if $v_0 \in i$ and $\tau_0 \in \mathsf{Int}$
- $\blacktriangleright_{\mathsf{A}}$ v_0
  if $v_0 \in n$ and $\tau_0 \in \mathsf{Nat}$
- $\blacktriangleright_{\mathsf{A}}$ Err otherwise

Case: $\cdot \vdash_1 \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1)\, v_0 : \mathcal{U}$

Immediate.

Case: $\cdot \vdash_1 \mathbb{G}\, (\ell_0 \blacktriangleleft (\tau_1 \times \tau_0) \blacktriangleleft \ell_1)\, v_0 : \mathcal{U}$

Immediate.

Case: $\cdot \vdash_1 \mathbb{T}\, \overline{b}_0\, v_0 : \mathcal{U}$

Immediate.

Case: $\cdot \vdash_1 \mathsf{trace}\, \overline{b}_0\, v_0 : \mathcal{U}$

- $\blacktriangleright_{\mathsf{A}}$ $\mathit{add\text{-}trace}(\overline{b}_0, v_0)$

Case: $\cdot \vdash_1 \mathsf{Err} : \mathcal{U}$

Immediate.

□

Lemma A.27 (Amnesic type preservation).
If $\cdot \vdash_1 E_0[e_0] : {}^{\tau}/_{\mathcal{U}}$ *and* $A(E_0[e_0])$ *and* $e_0(\rhd_{\mathsf{A}} \cup \blacktriangleright_{\mathsf{A}})e_1$ *then* $\cdot \vdash_1 E_0[e_1] : {}^{\tau}/_{\mathcal{U}}$ *and* $A(E_0[e_1])$.

Proof. By case analysis of each reduction relation.

Case: $\mathit{unop}\{\tau_0\}\; v_0 \rhd_{\mathsf{A}}$ InvariantErr
Immediate.
Case: $\mathit{unop}\{\tau_0\}\; v_0 \rhd_{\mathsf{A}} \delta(\mathit{unop}, v_0)$
By lemma 6.2.
Case: $\mathsf{fst}\{\tau_0\}\; (\mathbb{G}\; (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\; v_0) \rhd_{\mathsf{A}} \mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; (\mathsf{fst}\{\mathcal{U}\}\; v_0)$
(1) $\cdot \vdash_1 v_0 : \mathcal{U}$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 \mathsf{fst}\{\mathcal{U}\}\; v_0 : \mathcal{U}$
By (1)
(3) $\cdot \vdash_1 \mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; (\mathsf{fst}\{\mathcal{U}\}\; v_0) : \tau_0$
By (2)
(4) $A(\mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; (\mathsf{fst}\{\mathcal{U}\}\; v_0))$
By similar reasoning
Case: $\mathsf{snd}\{\tau_0\}\; (\mathbb{G}\; (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\; v_0 \rhd_{\mathsf{A}} \mathsf{dyn}\; (\ell_0 \blacktriangleleft (\tau_0 \times \tau_2) \blacktriangleleft \ell_1)\; (\mathsf{snd}\{\mathcal{U}\}\; v_0)$
(1) $\cdot \vdash_1 v_0 : \mathcal{U}$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 \mathsf{snd}\{\mathcal{U}\}\; v_0 : \mathcal{U}$
By (1)
(3) $\cdot \vdash_1 \mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; (\mathsf{snd}\{\mathcal{U}\}\; v_0) : \tau_0$
By (2)
Case: $\mathit{binop}\{\tau_0\}\; v_0\; v_1 \rhd_{\mathsf{A}}$ InvariantErr
Immediate.
Case: $\mathit{binop}\{\tau_0\}\; v_0\; v_1 \rhd_{\mathsf{A}} \delta(\mathit{binop}, v_0, v_1)$
Immediate.
Case: $\mathsf{app}\{\tau_0\}\; v_0\; v_1 \rhd_{\mathsf{A}}$ InvariantErr
Immediate.
Case: $\mathsf{app}\{\tau_0\}\; (\lambda(x_0 : \tau_1).\, e_0)\; v_0 \rhd_{\mathsf{A}} e_0[x_0 \leftarrow v_0]$
By substitution lemmas for typed functions and for $A(\cdot)$.
Case: $\mathsf{app}\{\tau_0\}\; (\mathbb{G}\; (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_2) \blacktriangleleft \ell_1)\; v_0)\; v_1 \rhd_{\mathsf{A}} \mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; (\mathsf{app}\{\mathcal{U}\}\; v_0\; (\mathsf{stat}\; (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_1))$
(1) $\cdot \vdash_1 v_0 : \mathcal{U}$
By $\vdash_1$ on the redex
(2) $\cdot \vdash_1 v_1 : \tau_1$
By $\vdash_1$ on the redex
(3) $\cdot \vdash_1 \mathsf{stat}\; (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\; v_1 : \mathcal{U}$
By (2)
(4) $\cdot \vdash_1 \mathsf{app}\{\mathcal{U}\}\; v_0\; (\mathsf{stat}\; (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\; v_1) : \mathcal{U}$
By (1) and (3)
(5) $\cdot \vdash_1 \mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; (\mathsf{app}\{\mathcal{U}\}\; v_0\; (\mathsf{stat}\; (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\; v_1)) : \tau_0$
By (4)
(6) $A(\mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; (\mathsf{app}\{\mathcal{U}\}\; v_0\; (\mathsf{stat}\; (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\; v_1)))$
By similar reasoning
Case: $\mathsf{dyn}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \rhd_{\mathsf{A}} \mathbb{G}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0$
Immediate.

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathbb{T}_{?}\,\overline{b}_0\,i_0) \triangleright_{\mathsf{A}} i_0$
Immediate.

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0 \triangleright_{\mathsf{A}} \mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b}_0, v_0)$
Immediate.

Case: $\mathit{unop}\{\mathcal{U}\}\,v_0 \blacktriangleright_{\mathsf{A}} \mathsf{TagErr}$
Immediate.

Case: $\mathit{unop}\{\mathcal{U}\}\,v_0 \blacktriangleright_{\mathsf{A}} \mathit{add\text{-}trace}(\mathit{get\text{-}trace}(v_0), \delta(\mathit{unop}, v_1))$
Immediate.

Case: $\mathsf{fst}\{\mathcal{U}\}\,(\mathbb{T}_{?}\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\,v_0)) \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\tau_1\}\,v_0))$

(1) $\cdot \vdash_1 v_0 : \tau_1 \times \tau_2$
By $\vdash_1$ on the redex

(2) $\cdot \vdash_1 \mathsf{fst}\{\tau_1\}\,v_0 : \tau_1$
By (1)

(3) $\cdot \vdash_1 \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\tau_1\}\,v_0)) : \mathcal{U}$
By (2)

Case: $\mathsf{snd}\{\mathcal{U}\}\,(\mathbb{T}_{?}\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1)\,v_0)) \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\tau_2\}\,v_0))$

(1) $\cdot \vdash_1 v_0 : \tau_1 \times \tau_2$
By $\vdash_1$ on the redex

(2) $\cdot \vdash_1 \mathsf{snd}\{\tau_2\}\,v_0 : \tau_2$
By (1)

(3) $\cdot \vdash_1 \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\tau_2\}\,v_0) : \mathcal{U}$
By (2)

Case: $\mathit{binop}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{A}} \mathsf{TagErr}$
Immediate.

Case: $\mathit{binop}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{A}} \delta(\mathit{binop}, v_2, v_3)$
Immediate.

Case: $\mathsf{app}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{A}} \mathsf{TagErr}$
Immediate.

Case: $\mathsf{app}\{\mathcal{U}\}\,(\mathbb{T}_{?}\,\overline{b}_0\,(\lambda x_0.\,e_0))\,v_0 \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,\overline{b}_0\,(e_0[x_0 \leftarrow v_1])$
By substitution lemmas for untyped functions and for $A(\cdot)$.

Case: $\mathsf{app}\{\mathcal{U}\}\,(\mathbb{T}_{?}\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_2) \blacktriangleleft \ell_1)\,v_0))\,v_1 \blacktriangleright_{\mathsf{A}}$
$\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\tau_2\}\,v_0\,(\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,v_2)))$

(1) $\cdot \vdash_1 v_0 : \tau_1 \Rightarrow \tau_2$
By $\vdash_1$ on the redex

(2) $\cdot \vdash_1 v_1 : \mathcal{U}$
By $\vdash_1$ on the redex

(3) $\cdot \vdash_1 \mathsf{dyn}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\,v_1 : \tau_1 \Rightarrow \tau_2$
By (2)

(4) $\cdot \vdash_1 \mathsf{app}\{\tau_2\}\,v_0\,(\mathsf{dyn}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\,v_1) : \tau_2$
By (1) and (3)

(5) $\cdot \vdash_1 \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\tau_2\}\,v_0\,(\mathsf{dyn}\,(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)\,v_2))) : \mathcal{U}$
By (4)

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0 \blacktriangleright_{\mathsf{A}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0$
Immediate.

Case: $\mathsf{stat}\,b_0\,(\mathbb{G}\,b_1\,(\mathbb{T}_{?}\,\overline{b}_0\,v_0)) \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,(b_0 b_1 \overline{b}_0)\,v_0$

(1) $\cdot \vdash_1 v_0 : \mathcal{U}$
By $\vdash_1$ on the redex

(2) $\cdot \vdash_1 \mathsf{trace}\,(b_0 b_1 \overline{b}_0)\, v_0 : \mathcal{U}$

By (1)

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; i_0 \blacktriangleright_{\mathsf{A}} i_0$

Immediate.

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \blacktriangleright_{\mathsf{A}} \mathsf{InvariantErr}$

Immediate.

Case: $\mathsf{trace}\,\overline{b}_0\, v_0 \blacktriangleright_{\mathsf{A}} v_1$

Immediate.

□

Theorem A.28 (Amnesic blame soundness and completeness). *Amnesic satisfies* **BS** *and* **BC**

Proof. By preservation of path-owner consistency ($\Vdash_p$) for $\rhd_{\overline{\mathsf{A}}}$ and $\blacktriangleright_{\overline{\mathsf{A}}}$.

Case: $(\mathit{unop}\{\tau_0\}\, (\!(v_0)\!)^{\overline{\ell}_0})^{\ell_0} \rhd_{\overline{\mathsf{A}}} (\mathsf{InvariantErr})^{\ell_0}$
Immediate.

Case: $(\mathit{unop}\{\tau_0\}\, (\!(v_0)\!)^{\overline{\ell}_0})^{\ell_0} \rhd_{\overline{\mathsf{A}}} (\delta(\mathit{unop}, v_0))^{\overline{\ell}_0 \ell_0}$

(1) $v_0 = \langle v_1, v_2 \rangle$ and $\delta(\mathit{unop}, v_0) \in \{v_1, v_2\}$
By definition

(2) $\ell_0; \cdot \Vdash_p v_0$
By $\Vdash_p$ on the redex

(3) $\ell_0; \cdot \Vdash_p v_1$ and $\ell_0; \cdot \Vdash_p v_2$
By (2) and (3)

(4) $\ell_0; \cdot \Vdash_p \delta(\mathit{unop}, v_0)$
By (1) and (3)

Case: $(\mathsf{fst}\{\tau_0\}\, (\!(\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, (v_0)^{\ell_2})\!)^{\overline{\ell}_0})^{\ell_3} \rhd_{\overline{\mathsf{A}}} (\mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, (v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$

(1) $\ell_1; \cdot \Vdash_p (v_0)^{\ell_2}$
By $\Vdash_p$ on the redex

(2) $\ell_1; \cdot \Vdash_p \mathsf{fst}\{\mathcal{U}\}\, (v_0)^{\ell_2}$
By (1)

(3) $\ell_3; \cdot \Vdash_p (\mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, (v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$
By (1) and $\Vdash_p$ on the redex

Case: $(\mathsf{snd}\{\tau_0\}\, (\!(\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, (v_0)^{\ell_2})\!)^{\overline{\ell}_0})^{\ell_3} \rhd_{\overline{\mathsf{A}}} (\mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, (v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$

(1) $\ell_1; \cdot \Vdash_p (v_0)^{\ell_2}$
By $\Vdash_p$ on the redex

(2) $\ell_1; \cdot \Vdash_p \mathsf{snd}\{\mathcal{U}\}\, (v_0)^{\ell_2}$
By (1)

(3) $\ell_3; \cdot \Vdash_p (\mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, (v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$
By (1) and $\Vdash_p$ on the redex

Case: $(\mathit{binop}\{\tau_0\}\, (\!(v_0)\!)^{\overline{\ell}_0}\, (\!(v_1)\!)^{\overline{\ell}_1})^{\ell_0} \rhd_{\overline{\mathsf{A}}} (\mathsf{InvariantErr})^{\ell_0}$
Immediate.

Case: $(\mathit{binop}\{\tau_0\}\, (\!(v_0)\!)^{\overline{\ell}_0}\, (\!(v_1)\!)^{\overline{\ell}_1})^{\ell_0} \rhd_{\overline{\mathsf{A}}} (\delta(\mathit{binop}, v_0, v_1))^{\ell_0}$

(1) $\delta(\mathit{binop}, v_0, v_1) \in i$
By definition of δ

(2) $\ell_0; \cdot \Vdash_p \delta(\mathit{binop}, v_0, v_1)$
By (1)

Case: $(\mathsf{app}\{\tau_0\}\, (\!(v_0)\!)^{\overline{\ell}_0}\, v_1)^{\ell_0} \rhd_{\overline{\mathsf{A}}} (\mathsf{InvariantErr})^{\ell_0}$
Immediate.

Case: $(\mathsf{app}\{\tau_0\}\, (\!(\lambda(x_0 : \tau_1).\, e_0)\!)^{\overline{\ell}_0}\, v_0)^{\ell_0} \rhd_{\overline{\mathsf{A}}} (\!(e_0[x_0 \leftarrow (\!(v_0)\!)^{\ell_0 \mathit{rev}(\overline{\ell}_0)}])\!)^{\overline{\ell}_0 \ell_0}$

(1) $\ell_0; \cdot \Vdash_p \lambda(x_0 : \tau_1).\, e_0$
By $\Vdash_p$ on the redex

(2) $\ell_0; \cdot \Vdash_p v_0$
By $\Vdash_p$ on the redex

(3) $\ell_0; \cdot \Vdash_p \llparenthesis v_0 \rrparenthesis^{\ell_0 rev(\overline{\ell_0})}$
By (1) and (2)

(4) $\ell_0; \cdot \Vdash_p x_0$ for each occurrence of x_0 in e_0
By $\Vdash_p$ on the redex

(5) $\ell_0; \cdot \Vdash_p \llparenthesis e_0[x_0 \leftarrow \llparenthesis v_1 \rrparenthesis^{\ell_0 rev(\overline{\ell_0})}] \rrparenthesis^{\overline{\ell_0}\ell_0}$
By (3) and (4)

Case: $(\mathsf{app}\{\tau_0\}\ \llparenthesis \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell_0}}\ v_1)^{\ell_3} \rhd_{\overline{\mathsf{A}}}$

$\llparenthesis \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\mathsf{app}\{\mathcal{U}\}\ v_0\ (\mathsf{stat}\ (\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\ \llparenthesis v_1 \rrparenthesis^{\ell_3 rev(\overline{\ell_0})}))^{\ell_2} \rrparenthesis^{\overline{\ell_0}\ell_3}$

(1) $\ell_2; \cdot \Vdash_p v_0$
By $\Vdash_p$ on the redex

(2) $\ell_3; \cdot \Vdash_p v_1$
By $\Vdash_p$ on the redex

(3) $\ell_3; \cdot \Vdash_p \llparenthesis v_1 \rrparenthesis^{\ell_3 rev(\overline{\ell_0})}$
By (2) and $\Vdash_p$ on the redex

(4) $\ell_2; \cdot \Vdash_p \mathsf{stat}\ (\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\ \llparenthesis v_1 \rrparenthesis^{\ell_3 rev(\overline{\ell_0})}$
By (3) and $\Vdash_p$ on the redex

(5) $\ell_3; \cdot \Vdash_p \llparenthesis \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\mathsf{app}\{\mathcal{U}\}\ v_0\ (\mathsf{stat}\ (\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\ \llparenthesis v_1 \rrparenthesis^{\ell_3 rev(\overline{\ell_0})}))^{\ell_2} \rrparenthesis^{\overline{\ell_0}\ell_3}$
By (1) and (4)

Case: $(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}})^{\ell_2} \rhd_{\overline{\mathsf{A}}} (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}})^{\ell_2}$
Immediate.

Case: $(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis \mathbb{T}_?\ \overline{b_0}\ \llparenthesis i_0 \rrparenthesis^{\overline{\ell_0}} \rrparenthesis^{\overline{\ell_1}})^{\ell_2} \rhd_{\overline{\mathsf{A}}} (i_0)^{\ell_2}$
Immediate.

Case: $(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell_2}})^{\ell_3} \rhd_{\overline{\mathsf{A}}} (\mathsf{BoundaryErr}\ ((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b_0}, \llparenthesis v_0 \rrparenthesis^{\overline{\ell_2}}))^{\ell_3}$
Immediate.

Case: $(unop\{\mathcal{U}\}\ \llparenthesis v_0 \rrparenthesis^{\overline{\ell_0}})^{\ell_0} \blacktriangleright_{\overline{\mathsf{A}}} (\mathsf{TagErr})^{\ell_0}$
Immediate.

Case: $(unop\{\mathcal{U}\}\ v_0)^{\ell_0} \blacktriangleright_{\overline{\mathsf{A}}} (add\text{-}trace(get\text{-}trace(v_0), \delta(unop, v_1)))^{\ell_0}$

(1) $v_0 = \mathbb{T}_?\ \overline{b_0}\ \langle v_1, v_2 \rangle$ and $\delta(unop, rem\text{-}trace(v_0)) \in \{v_1, v_2\}$
By definition

(2) $\ell_0; \cdot \Vdash_p v_0$ and $\ell_n; \cdot \Vdash_p rem\text{-}trace(v_0)$
By $\Vdash_p$ on the redex

(3) $\ell_n; \cdot \Vdash_p v_1$ and $\ell_n; \cdot \Vdash_p v_2$
By (2)

(4) $\ell_0; \cdot \Vdash_p add\text{-}trace(get\text{-}trace(v_0), \delta(unop, rem\text{-}trace(v_0)))$
By (1) and (3)

Case: $(\mathsf{fst}\{\mathcal{U}\}\ \llparenthesis \mathbb{T}_?\ \overline{b_0}\ \llparenthesis \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell_3}} \rrparenthesis^{\overline{\ell_4}})^{\ell_5} \blacktriangleright_{\overline{\mathsf{A}}}$

$(\mathsf{trace}\ \overline{b_0}\ \llparenthesis \mathsf{stat}\ (\ell_0 \blacktriangleleft fst(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{fst}\{fst(\tau_0)\}\ v_0)^{\ell_2} \rrparenthesis^{\overline{\ell_3}})^{\overline{\ell_4}\ell_5}$

(1) $\ell_5; \cdot \Vdash_p \mathbb{T}_?\ \overline{b_0}\ \llparenthesis \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell_3}}$
By $\Vdash_p$ on the redex

(2) $\ell_0; \cdot \Vdash_p \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(v_0)^{\ell_2}$
By (1)

(3) $\ell_1; \cdot \Vdash_p v_0$
By (2)

(4) $\ell_1; \cdot \Vdash_p \mathsf{fst}\{\mathit{fst}(\tau_0)\}\,v_0$
By (3)

(5) $\ell_0; \cdot \Vdash_p \mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathit{fst}(\tau_0)\}\,v_0)^{\ell_2}$
By (4)

(6) $\ell_5; \cdot \Vdash_p \mathsf{trace}\,\overline{b}_0\,\llparenthesis \mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathit{fst}(\tau_0)\}\,v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3}$
By (1) and (5)

Case: $(\mathsf{snd}\{\mathcal{U}\}\,\llparenthesis \mathbb{T}_?\,\overline{b}_0\,\llparenthesis \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3} \rrparenthesis^{\overline{\ell}_4})^{\ell_5} \blacktriangleright_{\overline{\mathsf{A}}}$

$(\mathsf{trace}\,\overline{b}_0\,\llparenthesis \mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathit{snd}(\tau_0)\}\,v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3})^{\overline{\ell}_4 \ell_5}$

(1) $\ell_5; \cdot \Vdash_p \mathbb{T}_?\,\overline{b}_0\,\llparenthesis \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3}$
By $\Vdash_p$ on the redex

(2) $\ell_0; \cdot \Vdash_p \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(v_0)^{\ell_2}$
By (1)

(3) $\ell_1; \cdot \Vdash_p v_0$
By (2)

(4) $\ell_1; \cdot \Vdash_p \mathsf{snd}\{\mathit{snd}(\tau_0)\}\,v_0$
By (3)

(5) $\ell_0; \cdot \Vdash_p \mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathit{snd}(\tau_0)\}\,v_0)^{\ell_2}$
By (4)

(6) $\ell_5; \cdot \Vdash_p \mathsf{trace}\,\overline{b}_0\,\llparenthesis \mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathit{snd}(\tau_0)\}\,v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3}$
By (1) and (5)

Case: $(\mathit{binop}\{\mathcal{U}\}\,\llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}\,\llparenthesis v_1 \rrparenthesis^{\overline{\ell}_1})^{\ell_0} \blacktriangleright_{\overline{\mathsf{A}}} (\mathsf{TagErr})^{\ell_0}$
Immediate.

Case: $(\mathit{binop}\{\mathcal{U}\}\,\llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}\,\llparenthesis v_1 \rrparenthesis^{\overline{\ell}_1})^{\ell_0} \blacktriangleright_{\overline{\mathsf{A}}} \delta(\mathit{binop}, v_2, v_3)$
Immediate.

Case: $(\mathsf{app}\{\mathcal{U}\}\,\llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0}\,v_1)^{\ell_0} \blacktriangleright_{\overline{\mathsf{A}}} (\mathsf{TagErr})^{\ell_0}$
Immediate.

Case: $(\mathsf{app}\{\mathcal{U}\}\,\llparenthesis \mathbb{T}_?\,\overline{b}_0\,\llparenthesis \lambda x_0.\,e_0 \rrparenthesis^{\overline{\ell}_0} \rrparenthesis^{\overline{\ell}_1}\,v_0)^{\ell_2} \blacktriangleright_{\overline{\mathsf{A}}}$

$(\mathsf{trace}\,\overline{b}_0\,\llparenthesis e_0[x_0 \leftarrow \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), \llparenthesis v_0 \rrparenthesis^{\ell_2 \mathit{rev}(\overline{\ell}_1) \mathit{rev}(\overline{\ell}_0)})] \rrparenthesis^{\overline{\ell}_0})^{\overline{\ell}_1 \ell_2}$

(1) $\ell_2; \cdot \Vdash_p \mathbb{T}_?\,\overline{b}_0\,\llparenthesis \lambda x_0.\,e_0 \rrparenthesis^{\overline{\ell}_0}$
By $\Vdash_p$ on the redex

(2) $\ell_n; \cdot \Vdash_p \lambda x_0.\,e_0$
By (1)

(3) $\ell_2; \cdot \Vdash_p v_0$
By $\Vdash_p$ on the redex

(4) $\ell_2; \cdot \Vdash_p v_0$
By $\Vdash_p$ on the redex

(5) $\ell_n; \cdot \Vdash_p \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), \llparenthesis v_0 \rrparenthesis^{\ell_2 \mathit{rev}(\overline{\ell}_1) \mathit{rev}(\overline{\ell}_0)})$
By (2) and (4)

(6) $\ell_n; \cdot \Vdash_p x_0$ for each occurrence of x_0 in e_0
By $\Vdash_p$ on the redex

(7) $\ell_2; \cdot \Vdash_p \mathsf{trace}\,\overline{b}_0\, \llparenthesis e_0[x_0 \leftarrow \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), \llparenthesis v_0 \rrparenthesis^{\ell_2 \mathit{rev}(\overline{\ell}_1)\mathit{rev}(\overline{\ell}_0)})] \rrparenthesis^{\overline{\ell}_0}$
By (5) and (6)

Case: $(\mathsf{app}\{\mathcal{U}\}\, \llparenthesis \mathbb{T}_?\, \overline{b}_0\, \llparenthesis \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3} \rrparenthesis^{\overline{\ell}_4}\, v_1)^{\ell_5} \blacktriangleright_{\overline{\mathsf{A}}}$

$\llparenthesis \mathsf{trace}\,\overline{b}_0\, \llparenthesis \mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathit{cod}(\tau_0)\}\, v_0\, (\mathsf{dyn}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\, v_2))^{\ell_2} \rrparenthesis^{\overline{\ell}_3} \rrparenthesis^{\overline{\ell}_4 \ell_5}$
where $v_2 = \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), \llparenthesis v_1 \rrparenthesis^{\ell_5 \mathit{rev}(\overline{\ell}_3 \overline{\ell}_4)})$

(1) $\ell_5; \cdot \Vdash_p \mathbb{T}_?\, \overline{b}_0\, \llparenthesis \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (v_0)^{\ell_2} \rrparenthesis^{\overline{\ell}_3}$
By $\Vdash_p$ on the redex

(2) $\ell_0; \cdot \Vdash_p \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (v_0)^{\ell_2}$ and $\ell_1; \cdot \Vdash_p v_0$
By (1)

(3) $\ell_5; \cdot \Vdash_p v_1$
By $\Vdash_p$ on the redex

(4) $\ell_0; \cdot \Vdash_p \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), \llparenthesis v_1 \rrparenthesis^{\ell_5 \mathit{rev}(\overline{\ell}_3 \overline{\ell}_4)})$
By (1) and (3)

(5) $\ell_1; \cdot \Vdash_p \mathsf{dyn}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\, \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), \llparenthesis v_1 \rrparenthesis^{\ell_5 \mathit{rev}(\overline{\ell}_3 \overline{\ell}_4)})$
By (4)

(6) $\ell_5; \cdot \Vdash_p \mathsf{trace}\,\overline{b}_0\, \llparenthesis \mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\, (\mathsf{app}\{\mathit{cod}(\tau_0)\}\, v_0\, v_2)^{\ell_2} \rrparenthesis^{\overline{\ell}_3}$
where $v_2 = \mathsf{dyn}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\, \mathit{add\text{-}trace}(\mathit{rev}(\overline{b}_0), \llparenthesis v_1 \rrparenthesis^{\ell_5 \mathit{rev}(\overline{\ell}_3 \overline{\ell}_4)})$
By (1) and (5)

Case: $(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0)^{\ell_2} \blacktriangleright_{\overline{\mathsf{A}}} (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0)^{\ell_2}$
Immediate.

Case: $(\mathsf{stat}\, b_0\, \llparenthesis \mathbb{G}\, b_1\, \llparenthesis \mathbb{T}_?\, \overline{b}_2\, v_0 \rrparenthesis^{\overline{\ell}_0} \rrparenthesis^{\overline{\ell}_1})^{\ell_2} \blacktriangleright_{\overline{\mathsf{A}}} (\mathsf{trace}\,(b_0 b_1 \overline{b}_2)\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0 \overline{\ell}_1 \ell_2})^{\ell_2}$

(1) $b_0 = (\ell_2 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)$
By $\Vdash_p$ on the redex

(2) $\ell_1; \cdot \Vdash_p \llparenthesis \mathbb{G}\, b_1\, \llparenthesis \mathbb{T}_?\, \overline{b}_2\, v_0 \rrparenthesis^{\overline{\ell}_0} \rrparenthesis^{\overline{\ell}_1}$
By $\Vdash_p$ on the redex and (1)

(3) $\ell_0; \cdot \Vdash_p \llparenthesis \mathbb{T}_?\, \overline{b}_2\, v_0 \rrparenthesis^{\overline{\ell}_0}$
By $\Vdash_p$ on the redex and (1)

(4) $\ell_2; \cdot \Vdash_p \mathsf{trace}\,(b_0 b_1 \overline{b}_2)\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_0 \overline{\ell}_1 \ell_2}$
By (2) and (3)

Case: $(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, \llparenthesis i_0 \rrparenthesis^{\overline{\ell}_2})^{\ell_3} \blacktriangleright_{\overline{\mathsf{A}}} (i_0)^{\ell_3}$
Immediate.

Case: $(\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, \llparenthesis v_0 \rrparenthesis^{\overline{\ell}_2})^{\ell_3} \blacktriangleright_{\overline{\mathsf{A}}} (\mathsf{InvariantErr})^{\ell_3}$
Immediate.

Case: $(\mathsf{trace}\,\overline{b}_0\, v_0)^{\ell_0} \blacktriangleright_{\overline{\mathsf{A}}} (\mathit{add\text{-}trace}(\overline{b}_0, v_0))^{\ell_0}$
Immediate.

□

Lemma A.29 ($A \approx T$). *If* $e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0$ *then:*

- *if* $e_0 \rightarrow_{\mathsf{A}} e_2$ *then* $e_2 \rightarrow^*_{\mathsf{A}} e_3$ *and* $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} e_4; \mathcal{H}_1; \mathcal{B}_1$ *and* $e_3 \approx e_4; \mathcal{H}_1; \mathcal{B}_1$
- *if* $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\mathsf{T}} e_3; \mathcal{H}_1; \mathcal{B}_1$ *then* $e_0 \rightarrow^*_{\mathsf{A}} e_2$ *and* $e_2 \approx e_3; \mathcal{H}_1; \mathcal{B}_1$

Proof. By lemma A.30 and lemma A.31. □

$\boxed{\mathrm{wfr}_{AT}(e_0, e_1)}$ holds for well-formed residuals of a common term; that is, pairs such that there exists an e_2 where $e_2 : {}^{\tau}/_{\mathcal{U}}$ **wf** and $e_2 \rightarrow^*_{\mathsf{A}} e_0$ and $e_2; \cdot; \cdot \rightarrow^*_{\mathsf{T}} e_1; \mathcal{H}_1; \mathcal{B}_1$

Lemma A.30. *If* $\mathrm{wfr}_{AT}(e_0, e_1)$ *and* $e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0$ *and* $e_0 \rightarrow_{\mathsf{A}} e_2$ *then* $e_2 \rightarrow^*_{\mathsf{A}} e_3$ *and* $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} e_4; \mathcal{H}_1; \mathcal{B}_1$ *and* $e_3 \approx e_4; \mathcal{H}_1; \mathcal{B}_1$

Proof. By lemma A.32, lemma A.35, and case analysis of $\rhd_{\mathsf{A}} \cup \blacktriangleright_{\mathsf{A}}$.

Case: $unop\{\tau_0\}\, v_0 \rhd_{\mathsf{A}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $unop\{\tau_0\}\, v_0 \rhd_{\mathsf{A}} \delta(unop, v_0)$
1. $e_1 = unop\{\tau_0\}\, e_5$ and $v_0 \lesssim e_5$
   By $\lesssim$ on the redex
2. If e_5 is a pre-value, it gets allocated. If not, e_5 must be a value. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} unop\{\tau_0\}\, v_1; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \lesssim v_1$
3. $\delta(unop, v_1)$ is defined
   By (2)
4. $\delta(unop, v_0) \approx \delta(unop, v_1); \mathcal{H}_1; \mathcal{B}_1$
   By δ

Case: $\mathsf{fst}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0) \rhd_{\mathsf{A}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_0)$
1. $e_1 = \mathsf{fst}\{\tau_0\}\, e_5$ and $v_0 \lesssim e_5$
   By $\lesssim$ on the redex
2. If e_5 is a pre-value, it gets allocated. If not, e_5 must be a value. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} \mathsf{fst}\{\tau_0\}\, v_1; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \lesssim v_1$
3. $\mathsf{fst}\{\tau_0\}\, v_1; \mathcal{H}_1; \mathcal{B}_1 \rightarrow^*_{\mathsf{T}} \mathsf{check}\{\tau_0\}\, \delta(\mathsf{fst}, v_1)\, v_1; \mathcal{H}_1; \mathcal{B}_1$
   By $\rightarrow^*_{\mathsf{T}}$
4. If $v_0 = \langle v_2, v_3 \rangle$ then $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_2$
   and $\mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_2 \approx \mathsf{check}\{\tau_0\}\, \delta(\mathsf{fst}, v_1)\, v_1; \mathcal{H}_1; \mathcal{B}_1$
   By (3)
5. Otherwise $v_0 = \mathbb{G}\, b_1\, \langle v_2, v_3 \rangle$ and $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{stat}\, b_1\, v_2)$
   and $\mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{stat}\, b_1\, v_2) \approx \mathsf{check}\{\tau_0\}\, \delta(\mathsf{fst}, v_1)\, v_1; \mathcal{H}_1; \mathcal{B}_1$

Case: $\mathsf{snd}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0 \rhd_{\mathsf{A}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_0)$
1. $e_1 = \mathsf{snd}\{\tau_0\}\, e_5$ and $v_0 \lesssim e_5$
   By $\lesssim$ on the redex
2. If e_5 is a pre-value, it gets allocated. If not, e_5 must be a value. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} \mathsf{snd}\{\tau_0\}\, v_1; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \lesssim v_1$
3. $\mathsf{snd}\{\tau_0\}\, v_1; \mathcal{H}_1; \mathcal{B}_1 \rightarrow^*_{\mathsf{T}} \mathsf{check}\{\tau_0\}\, \delta(\mathsf{snd}, v_1)\, v_1; \mathcal{H}_1; \mathcal{B}_1$
   By $\rightarrow^*_{\mathsf{T}}$
4. If $v_0 = \langle v_2, v_3 \rangle$ then $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_2$
   and $\mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_2 \approx \mathsf{check}\{\tau_0\}\, \delta(\mathsf{snd}, v_1)\, v_1; \mathcal{H}_1; \mathcal{B}_1$
   By (3)

(5) Otherwise $v_0 = \mathbb{G}\, b_1\, \langle v_2, v_3\rangle$ and $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{stat}\, b_1\, v_2)$ and $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{stat}\, b_1\, v_2) \approx \mathsf{check}\{\tau_0\}\,\delta(\mathsf{snd}, v_1)\, v_1; \mathcal{H}_1; \mathcal{B}_1$

Case: $\mathit{binop}\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{A}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathit{binop}\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{A}} \delta(\mathit{binop}, v_0, v_1)$

(1) $e_1 = \mathit{binop}\{\tau_0\}\, e_5\, e_6$ and $v_0 \lesssim e_5$ and $v_1 \lesssim e_6$
By $\lesssim$ on the redex

(2) If e_5 a pre-value, it gets allocated. If not, e_5 must be a value. Similarly for e_6. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} \mathit{binop}\{\tau_0\}\, v_2\, v_3; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$

(3) $\delta(\mathit{binop}, v_2, v_3)$ is defined
By (2)

(4) $\delta(\mathit{binop}, v_0, v_1) \approx \delta(\mathit{binop}, v_2, v_3); \mathcal{H}_1; \mathcal{B}_1$
By δ

Case: $\mathsf{app}\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{A}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathsf{app}\{\tau_0\}\, (\lambda(x_0 : \tau_1).\, e_0)\, v_0 \rhd_{\mathsf{A}} \mathsf{check}\{\tau_0\}\, e_0[x_0 \leftarrow v_0]\, \bullet$

(1) $e_1 = \mathsf{app}\{\tau_0\}\, e_5\, e_6$ and $(\lambda(x_0 : \tau_1).\, e_4) \lesssim e_5$ and $v_0 \lesssim e_6$
By $\lesssim$ on the redex

(2) If e_5 a pre-value, it gets allocated. If not, e_5 must be a value. Similarly for e_6. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} \mathsf{app}\{\tau_0\}\, v_2\, v_3; \mathcal{H}_1; \mathcal{B}_1$ and $(\lambda(x_0 : \tau_1).\, e_4) \lesssim v_2$ and $v_0 \lesssim v_3$

(3) $e_1; \mathcal{H}_1; \mathcal{B}_1 \rightarrow^*_{\mathsf{T}} \mathsf{check}\{\tau_0\}\, e_7[x_0 \leftarrow 3]\, v_2; \mathcal{H}_2; \mathcal{B}_2$
By (2)

(4) $\mathsf{check}\{\tau_0\}\, e_0[x_0 \leftarrow v_0]\, \bullet \approx \mathsf{check}\{\tau_0\}\, e_7[x_0 \leftarrow 3]\, v_2; \mathcal{H}_2; \mathcal{B}_2$
By (3) and a substitution lemma

Case: $\mathsf{app}\{\tau_0\}\, (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0)\, v_1 \rhd_{\mathsf{A}}$
$\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_0\, (\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_1))$

(1) $e_1 = \mathsf{app}\{\tau_0\}\, e_5\, e_6$ and $(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0) \lesssim e_5$ and $v_1 \lesssim e_6$
By $\lesssim$ on the redex

(2) If e_5 a pre-value, it gets allocated. If not, e_5 must be a value. Similarly for e_6. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} \mathsf{app}\{\tau_0\}\, v_2\, v_3; \mathcal{H}_1; \mathcal{B}_1$ and $(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0) \lesssim v_2$ and $v_1 \lesssim v_3$

(3) $\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_1 \rightarrow^*_{\mathsf{A}} v_4$
By $v_1 \lesssim v_3$

(4) $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_0\, v_4) \approx \mathsf{app}\{\tau_0\}\, v_2\, v_3; \mathcal{H}_1; \mathcal{B}_1$
By (3)

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \rhd_{\mathsf{A}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0$

(1) If $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1; \mathcal{H}_1; \mathcal{B}_1$ then $v_0 \lesssim v_1$ and $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} v_1; \mathcal{H}_2; \mathcal{B}_2$ and $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \lesssim v_1; \mathcal{H}_2; \mathcal{B}_2$

(2) Otherwise $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} \mathsf{check}\{\tau_0\}\, v_1\, \mathsf{p}_0; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \approx v_1; \mathcal{H}_1; \mathcal{B}_1$

(3) $\mathsf{check}\{\tau_0\}\, v_1\, \mathsf{p}_0; \mathcal{H}_1; \mathcal{B}_1 \rightarrow^*_{\mathsf{T}} v_1; \mathcal{H}_2; \mathcal{B}_2$
By (2)

(4) $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \approx v_1; \mathcal{H}_2; \mathcal{B}_2$

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathbb{T}_?\, \overline{b}_0\, i_0) \rhd_{\mathsf{A}} i_0$

(1) If $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1; \mathcal{H}_1; \mathcal{B}_1$ then $i_0 \lesssim v_1$ and $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} v_1; \mathcal{H}_2; \mathcal{B}_2$ and $i_0 \lesssim v_1; \mathcal{H}_2; \mathcal{B}_2$

(2) Otherwise $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} \mathsf{check}\{\tau_0\}\, v_1\, \mathsf{p}_0; \mathcal{H}_1; \mathcal{B}_1$ and $i_0 \approx v_1; \mathcal{H}_1; \mathcal{B}_1$

(3) $\mathsf{check}\{\tau_0\}\ v_1\ \mathsf{p}_0; \mathcal{H}_1; \mathcal{B}_1 \rightarrow^*_{\mathsf{T}} v_1; \mathcal{H}_2; \mathcal{B}_2$
By (2)
(4) $i_0 \approx v_1; \mathcal{H}_2; \mathcal{B}_2$

Case: $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \rhd_{\mathsf{A}} \mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b}_0, v_0)$
(1) If $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1; \mathcal{H}_1; \mathcal{B}_1$ then $v_0 \lesssim v_1$
and $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} \mathsf{BoundaryErr}\,(\overline{b}, v); \mathcal{H}_2; \mathcal{B}_2$
and $\mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b}_0, v_0) \lesssim \mathsf{BoundaryErr}\,(\overline{b}, v); \mathcal{H}_2; \mathcal{B}_2$
(2) Otherwise $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} \mathsf{check}\{\tau_0\}\ v_1\ \mathsf{p}_0; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \approx v_1; \mathcal{H}_1; \mathcal{B}_1$ and $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}}$ $\mathsf{BoundaryErr}\,(\overline{b}, v); \mathcal{H}_2; \mathcal{B}_2$ and $\mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b}_0, v_0) \lesssim \mathsf{BoundaryErr}\,(\overline{b}, v); \mathcal{H}_2; \mathcal{B}_2$

Case: $\mathit{unop}\{\mathcal{U}\}\ v_0 \blacktriangleright_{\mathsf{A}} \mathsf{TagErr}$
(1) $e_1 = \mathit{unop}\{\mathcal{U}\}\ e_5$ and $v_0 \lesssim e_5$
By $\lesssim$ on the redex
(2) If e_5 is a pre-value, it gets allocated. If not, e_5 must be a value. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}}$ $\mathit{unop}\{\mathcal{U}\}\ v_1; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \lesssim v_1$
(3) $\delta(\mathit{unop}, v_1)$ is undefined
By $v_0 \lesssim v_1$
(4) $\mathsf{TagErr} \approx \mathsf{TagErr}; \mathcal{H}_1; \mathcal{B}_1$

Case: $\mathit{unop}\{\mathcal{U}\}\ v_0 \blacktriangleright_{\mathsf{A}} \mathit{add\text{-}trace}\,(\mathit{get\text{-}trace}\,(v_0), \delta(\mathit{unop}, v_1))$
(1) $e_1 = \mathit{unop}\{\mathcal{U}\}\ e_5$ and $v_0 \lesssim e_5$
By $\lesssim$ on the redex
(2) If e_5 is a pre-value, it gets allocated. If not, e_5 must be a value. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}}$ $\mathit{unop}\{\mathcal{U}\}\ v_1; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \lesssim v_1$
(3) $\delta(\mathit{unop}, v_1)$ is undefined
By $v_0 \lesssim v_1$
(4) $\mathit{add\text{-}trace}\,(\mathit{get\text{-}trace}\,(v_0), \delta(\mathit{unop}, \mathit{rem\text{-}trace}\,(v_0))) \approx \delta(\mathit{unop}, v_1); \mathcal{H}_1; \mathcal{B}_1$

Case: $\mathsf{fst}\{\mathcal{U}\}\ (\mathbb{T}_?\,\overline{b}_0\ (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)) \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,\overline{b}_0\ (\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{fst}\,(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{fst}\{\tau_1\}\ v_0))$
(1) $e_1 = \mathsf{fst}\{\tau_0\}\ e_5$ and $v_0 \lesssim e_5$
By $\lesssim$ on the redex
(2) If e_5 is a pre-value, it gets allocated. If not, e_5 must be a value. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}}$ $\mathsf{fst}\{\mathcal{U}\}\ v_1; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \lesssim v_1$
(3) $\mathsf{fst}\{\mathcal{U}\}\ v_1; \mathcal{H}_1; \mathcal{B}_1 \rightarrow^*_{\mathsf{T}} \mathsf{check}\{\tau_0\}\ \delta(\mathsf{fst}, v_1)\ v_1; \mathcal{H}_1; \mathcal{B}_1$
By $\rightarrow^*_{\mathsf{T}}$
(4) If $v_0 = \langle v_2, v_3 \rangle$ then $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_2$
and $\mathsf{trace}\,\overline{b}_0\ (\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{fst}\,(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{fst}\{\tau_1\}\ v_0)) \approx \mathsf{check}\{\tau_0\}\ \delta(\mathsf{fst}, v_1)\ v_1; \mathcal{H}_1; \mathcal{B}_1$
By (3)
(5) Otherwise $v_0 = \mathbb{G}\ b_1\ \langle v_2, v_3 \rangle$ and $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{trace}\,\overline{b}_0\ (\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\mathsf{dyn}\ b_1\ v_2))$
and $\mathsf{trace}\,\overline{b}_0\ (\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\mathsf{dyn}\ b_1\ v_2)) \approx \mathsf{check}\{\tau_0\}\ \delta(\mathsf{fst}, v_1)\ v_1; \mathcal{H}_1; \mathcal{B}_1$

Case: $\mathsf{snd}\{\mathcal{U}\}\ (\mathbb{T}_?\,\overline{b}_0\ (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0)) \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,\overline{b}_0\ (\mathsf{stat}\ (\ell_0 \blacktriangleleft \mathit{snd}\,(\tau_0) \blacktriangleleft \ell_1)\ (\mathsf{snd}\{\tau_1\}\ v_0))$
(1) $e_1 = \mathsf{snd}\{\tau_0\}\ e_5$ and $v_0 \lesssim e_5$
By $\lesssim$ on the redex
(2) If e_5 is a pre-value, it gets allocated. If not, e_5 must be a value. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}}$ $\mathsf{snd}\{\mathcal{U}\}\ v_1; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \lesssim v_1$
(3) $\mathsf{snd}\{\mathcal{U}\}\ v_1; \mathcal{H}_1; \mathcal{B}_1 \rightarrow^*_{\mathsf{T}} \mathsf{check}\{\tau_0\}\ \delta(\mathsf{snd}, v_1)\ v_1; \mathcal{H}_1; \mathcal{B}_1$
By $\rightarrow^*_{\mathsf{T}}$

(4) If $v_0 = \langle v_2, v_3\rangle$ then $e_0 \rightarrow^*_{\mathsf{A}}$ stat $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_2$
and trace $\overline{b}_0$ (stat $(\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)$ (snd$\{\tau_1\}\; v_0$)) $\approx$ check$\{\tau_0\}\; \delta(\mathsf{snd}, v_1)\; v_1; \mathcal{H}_1; \mathcal{B}_1$
By (3)

(5) Otherwise $v_0 = \mathbb{G}\; b_1\; \langle v_2, v_3\rangle$ and $e_0 \rightarrow^*_{\mathsf{A}}$ trace $\overline{b}_0$ (stat $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$ (dyn $b_1\; v_2$))
and trace $\overline{b}_0$ (stat $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$ (dyn $b_1\; v_2$)) $\approx$ check$\{\tau_0\}\; \delta(\mathsf{snd}, v_1)\; v_1; \mathcal{H}_1; \mathcal{B}_1$

Case: $\mathit{binop}\{\mathcal{U}\}\; v_0\; v_1 \blacktriangleright_{\mathsf{A}}$ TagErr

(1) $e_1 = \mathit{binop}\{\tau_0\}\; e_5\; e_6$ and $v_0 \lesssim e_5$ and $v_1 \lesssim e_6$
By $\lesssim$ on the redex

(2) If e_5 a pre-value, it gets allocated. If not, e_5 must be a value. Similarly for e_6. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} \mathit{binop}\{\tau_0\}\; v_2\; v_3; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$

(3) $\delta(\mathit{binop}, v_2, v_3)$ is undefined
By (2)

(4) TagErr $\approx$ TagErr; $\mathcal{H}_1; \mathcal{B}_1$
By δ

Case: $\mathit{binop}\{\mathcal{U}\}\; v_0\; v_1 \blacktriangleright_{\mathsf{A}} \delta(\mathit{binop}, v_2, v_3)$

(1) $e_1 = \mathit{binop}\{\tau_0\}\; e_5\; e_6$ and $v_0 \lesssim e_5$ and $v_1 \lesssim e_6$
By $\lesssim$ on the redex

(2) If e_5 a pre-value, it gets allocated. If not, e_5 must be a value. Similarly for e_6. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} \mathit{binop}\{\tau_0\}\; v_2\; v_3; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$

(3) $\delta(\mathit{binop}, v_2, v_3)$ is defined
By (2)

(4) $\delta(\mathit{binop}, \mathit{rem\text{-}trace}(v_0), \mathit{rem\text{-}trace}(v_1)) \approx \delta(\mathit{binop}, v_2, v_3); \mathcal{H}_1; \mathcal{B}_1$
By δ

Case: app$\{\mathcal{U}\}\; v_0\; v_1 \blacktriangleright_{\mathsf{A}}$ TagErr

(1) $e_1 =$ app$\{\tau_0\}\; e_5\; e_6$ and $v_0 \lesssim e_5$ and $v_1 \lesssim e_6$
By $\lesssim$ on the redex

(2) If e_5 a pre-value, it gets allocated. If not, e_5 must be a value. Similarly for e_6. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}}$ app$\{\tau_0\}\; v_2\; v_3; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$

(3) v_2 is not a function
By (2)

(4) TagErr $\approx$ TagErr; $\mathcal{H}_1; \mathcal{B}_1$

Case: app$\{\mathcal{U}\}\; (\mathbb{T}_?\; \overline{b}_0\; (\lambda x_0.\, e_0))\; v_0 \blacktriangleright_{\mathsf{A}}$ check$\{\mathcal{U}\}$ trace $\overline{b}_0\; (e_0[x_0 \leftarrow v_1]) \bullet$

(1) $e_1 =$ app$\{\mathcal{U}\}\; e_5\; e_6$ and $(\lambda(x_0 : \tau_1).\, e_4) \lesssim e_5$ and $v_0 \lesssim e_6$
By $\lesssim$ on the redex

(2) If e_5 a pre-value, it gets allocated. If not, e_5 must be a value. Similarly for e_6. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}}$ app$\{\mathcal{U}\}\; v_2\; v_3; \mathcal{H}_1; \mathcal{B}_1$ and $(\lambda(x_0 : \tau_1).\, e_4) \lesssim v_2$ and $v_0 \lesssim v_3$

(3) $e_1; \mathcal{H}_1; \mathcal{B}_1 \rightarrow^*_{\mathsf{T}}$ check$\{\tau_0\}\; e_7[x_0 \leftarrow 3]\; v_2; \mathcal{H}_2; \mathcal{B}_2$
By (2)

(4) check$\{\mathcal{U}\}$ trace $\overline{b}_0\; (e_0[x_0 \leftarrow v_1]) \bullet \approx$ check$\{\tau_0\}\; e_7[x_0 \leftarrow 3]\; v_2; \mathcal{H}_2; \mathcal{B}_2$
By (3) and a substitution lemma

Case: app$\{\mathcal{U}\}\; (\mathbb{T}_?\; \overline{b}_0\; (\mathbb{G}\; (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0))\; v_1 \blacktriangleright_{\mathsf{A}}$
trace $\overline{b}_0$ (stat $(\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)$ (app$\{\tau_2\}\; v_0$ (dyn $(\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\; v_2$)))

(1) $e_1 =$ app$\{\tau_0\}\; e_5\; e_6$ and $(\mathbb{G}\; (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_0) \lesssim e_5$ and $v_1 \lesssim e_6$
By $\lesssim$ on the redex

(2) If e_5 a pre-value, it gets allocated. If not, e_5 must be a value. Similarly for e_6. Either way $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}}$ app$\{\tau_0\}\; v_2\; v_3; \mathcal{H}_1; \mathcal{B}_1$ and $(\mathbb{G}\; (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_0) \lesssim v_2$ and $v_1 \lesssim v_3$

(3) Either dyn $(\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\ v_1 \rightarrow^*_{\mathsf{A}}$ BoundaryErr $(\overline{b}, v)$ or dyn $(\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\ v_1 \rightarrow^*_{\mathsf{A}} v_4$ and trace $\overline{b}_0$ (stat $(\ell_0 \blacktriangleleft cod(\tau_0) \blacktriangleleft \ell_1)$ (app$\{\tau_2\}\ v_0$ (dyn $(\ell_1 \blacktriangleleft dom(\tau_0) \blacktriangleleft \ell_0)\ v_2$)))
$\approx$ app$\{\tau_0\}\ v_2\ v_3; \mathcal{H}_1; \mathcal{B}_1$
By $v_1 \lesssim v_3$

Case: stat $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \blacktriangleright_{\mathsf{A}} \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0$

(1) If $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}}$ stat $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1; \mathcal{H}_1; \mathcal{B}_1$ then $v_0 \lesssim v_1$ and $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} v_1; \mathcal{H}_2; \mathcal{B}_2$ and $\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \lesssim v_1; \mathcal{H}_2; \mathcal{B}_2$
(2) Otherwise $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}}$ check$\{\tau_0\}\ v_1\ \mathsf{p}_0; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \approx v_1; \mathcal{H}_1; \mathcal{B}_1$
(3) check$\{\tau_0\}\ v_1\ \mathsf{p}_0; \mathcal{H}_1; \mathcal{B}_1 \rightarrow^*_{\mathsf{T}} v_1; \mathcal{H}_2; \mathcal{B}_2$
By (2)
(4) $\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \approx v_1; \mathcal{H}_2; \mathcal{B}_2$

Case: stat $b_0\ (\mathbb{G}\ b_1\ (\mathbb{T}_?\ \overline{b}_0\ v_0)) \blacktriangleright_{\mathsf{A}}$ trace $(b_0 b_1 \overline{b}_0)\ v_0$

(1) If $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}}$ stat $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1; \mathcal{H}_1; \mathcal{B}_1$ then $v_0 \lesssim v_1$ and $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} v_1; \mathcal{H}_2; \mathcal{B}_2$ and trace $(b_0 b_1 \overline{b}_0)\ v_0 \lesssim v_1; \mathcal{H}_2; \mathcal{B}_2$
(2) Otherwise $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}}$ check$\{\tau_0\}\ v_1\ \mathsf{p}_0; \mathcal{H}_1; \mathcal{B}_1$ and $v_0 \approx v_1; \mathcal{H}_1; \mathcal{B}_1$
(3) check$\{\tau_0\}\ v_1\ \mathsf{p}_0; \mathcal{H}_1; \mathcal{B}_1 \rightarrow^*_{\mathsf{T}} v_1; \mathcal{H}_2; \mathcal{B}_2$
By (2)
(4) trace $(b_0 b_1 \overline{b}_0)\ v_0 \approx v_1; \mathcal{H}_2; \mathcal{B}_2$

Case: stat $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ i_0 \blacktriangleright_{\mathsf{A}} i_0$

(1) If $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}}$ stat $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1; \mathcal{H}_1; \mathcal{B}_1$ then $i_0 \lesssim v_1$ and $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}} v_1; \mathcal{H}_2; \mathcal{B}_2$ and $i_0 \lesssim v_1; \mathcal{H}_2; \mathcal{B}_2$
(2) Otherwise $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow^*_{\mathsf{T}}$ check$\{\tau_0\}\ v_1\ \mathsf{p}_0; \mathcal{H}_1; \mathcal{B}_1$ and $i_0 \approx v_1; \mathcal{H}_1; \mathcal{B}_1$
(3) check$\{\tau_0\}\ v_1\ \mathsf{p}_0; \mathcal{H}_1; \mathcal{B}_1 \rightarrow^*_{\mathsf{T}} v_1; \mathcal{H}_2; \mathcal{B}_2$
By (2)
(4) $i_0 \approx v_1; \mathcal{H}_2; \mathcal{B}_2$

Case: stat $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \blacktriangleright_{\mathsf{A}}$ InvariantErr
Impossible, by type soundness

Case: trace $\overline{b}_0\ v_0 \blacktriangleright_{\mathsf{A}} v_1$
Immediate

□

Lemma A.31. *If* $\mathrm{wfr}_{AT}(e_0, e_1)$ *and* $e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0$ *then: and* $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\mathsf{T}} e_3; \mathcal{H}_1; \mathcal{B}_1$ *then* $e_0 \rightarrow^*_{\mathsf{A}} e_2$ *and* $e_2 \approx e_3; \mathcal{H}_1; \mathcal{B}_1$

Proof. By lemma A.32, lemma A.35, and case analysis of $\rhd_{\mathsf{T}}$.

Case: $\mathsf{w}_0; \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{p}_0; \mathcal{H}_1; \mathcal{B}_1$
Immediate

Case: $(unop\{\tau_0\}\ v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$
Impossible, by type soundness

Case: $(unop\{\mathcal{U}\}\ v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{TagErr}; \mathcal{H}_0; \mathcal{B}_0$

(1) $e_0 = unop\{\mathcal{U}\}\ v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex

(2) $\delta(unop, \textit{rem-trace}(v_1))$ is undefined
By (1)

(3) $\mathsf{TagErr} \approx \mathsf{TagErr}; \mathcal{H}_0; \mathcal{B}_0$
By δ

Case: $(unop\{^{\tau}/_{\mathcal{U}}\}\ \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} (\mathsf{check}\{^{\tau}/_{\mathcal{U}}\}\ \delta(unop, \mathcal{H}_0(\mathsf{p}_0))\ \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0$

(1) $e_0 = unop\{^{\tau}/_{\mathcal{U}}\}\ v_1$ and $v_1 \lesssim \mathsf{p}_0$
By $\lesssim$ on the redex

(2) If v_1 is a pair then $\delta(unop, \textit{rem-trace}(v_1))$ is defined
and $\mathsf{check}\{^{\tau}/_{\mathcal{U}}\}\ \textit{add-trace}(\textit{get-trace}(v_1), \delta(unop, v_1)) \bullet \approx$
$; (\mathsf{check}\{^{\tau}/_{\mathcal{U}}\}\ \delta(unop, \mathcal{H}_0(\mathsf{p}_0))\ \mathsf{p}_0); \mathcal{H}_0 \mathcal{B}_0$
By (1)

(3) If v_1 is a guarded pair $\mathbb{G}\ b\ v_2$, then e_0 unfolds to one boundary (dyn or stat) for example
$\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ \delta(unop, v_2) \approx \mathsf{check}\{\tau_0\}\ \delta(unop, \mathsf{p}_0)\ \mathsf{p}_0; \mathcal{H}_1; \mathcal{B}_1$
By δ

(4) Otherwise v_1 is a pair with two wrappers $\mathbb{G}\ b\ (\mathbb{G}\ b\ v_2)$ and e_0 unfolds to two boundaries,
for example $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ (\mathsf{stat}\ b_1\ v_2) \approx \mathsf{check}\{\tau_0\}\ \delta(unop, \mathsf{p}_0)\ \mathsf{p}_0; \mathcal{H}_1; \mathcal{B}_1$
By δ

Case: $(binop\{\tau_0\}\ v_0\ v_1); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$
Impossible, by type soundness

Case: $(binop\{\mathcal{U}\}\ v_0\ v_1); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{TagErr}; \mathcal{H}_0; \mathcal{B}_0$

(1) $e_0 = binop\{\mathcal{U}\}\ v_2\ v_3$ and $v_2 \lesssim v_0$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex

(2) $\delta(binop, \textit{rem-trace}(v_2), \textit{rem-trace}(v_3))$ is undefined
By (1)

(3) $\mathsf{TagErr} \approx \mathsf{TagErr}; \mathcal{H}_0; \mathcal{B}_0$
By δ

Case: $(binop\{^{\tau}/_{\mathcal{U}}\}\ i_0\ i_1); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \delta(binop, i_0, i_1); \mathcal{H}_0; \mathcal{B}_0$

(1) $e_0 = binop\{^{\tau}/_{\mathcal{U}}\}\ v_2\ v_3$ and $v_2 \lesssim i_0$ and $v_3 \lesssim i_1$
By $\lesssim$ on the redex

(2) $\delta(binop, \textit{rem-trace}(v_2), \textit{rem-trace}(v_3))$ is defined
By (1)

(3) $\delta(binop, v_2, v_3) \approx \delta(binop, \mathcal{H}_0(\mathsf{p}_0), \mathcal{H}_0(\mathsf{p}_1); \mathcal{H}_0; \mathcal{B}_0$
By δ

Case: $(\mathsf{app}\{\tau_0\}\ v_0\ v_1); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$
Impossible, by type soundness

Case: $(\mathsf{app}\{\mathcal{U}\}\ v_0\ v_1); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{TagErr}; \mathcal{H}_0; \mathcal{B}_0$

(1) $e_0 = \mathsf{app}\{\mathcal{U}\}\, v_2\, v_3$ and $v_2 \lesssim v_0$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex
(2) v_2 is not a function
By (1)
(3) $\mathsf{TagErr} \approx \mathsf{TagErr}; \mathcal{H}_0; \mathcal{B}_0$

Case: $(\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, \mathsf{p}_0\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} (\mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\, e_0[x_0 \leftarrow v_0]\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_1$
(1) $e_0 = \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, v_2\, v_3$ and $v_2 \lesssim \mathsf{p}_0$ and $v_3 \lesssim v_0$
By $\lesssim$ on the redex
(2) If v_2 is a function, then $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\, e_1[x_0 \leftarrow v_3]\, \bullet$
and $\mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\, e_1[x_0 \leftarrow v_3]\, \bullet \approx (\mathsf{check}\{{}^{\tau}/_{\mathcal{U}}\}\, e_0[x_0 \leftarrow v_0]\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_1$
By (1)
(3) Otherwise $v_2 \in \mathbb{G}\, b\, v_4$ and unfolds to a dyn/stat boundary,
for example, $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_4\, (\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_3))$
and the argument reduces to a value, for example, $\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_3 \rightarrow^*_{\mathsf{A}} v_5$

Case: $(\mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, \mathsf{p}_0\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{BoundaryErr}\,(\mathit{rev}(\mathcal{B}_0(\mathsf{p}_0)), v_0); \mathcal{H}_0; \mathcal{B}_1$
(1) $e_0 = \mathsf{app}\{{}^{\tau}/_{\mathcal{U}}\}\, v_2\, v_3$ and $v_2 \lesssim \mathsf{p}_0$ and $v_3 \lesssim v_0$
By $\lesssim$ on the redex
(2) v_2 must be a guarded, typed function
By (1)
(3) $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(b, v)$
By type soundness
(4) $\mathsf{BoundaryErr}\,(b, v) \approx \mathsf{BoundaryErr}\,(b, v); \mathcal{H}_0; \mathcal{B}_1$

Case: $(\mathsf{app}\{\tau_0\}\, \mathsf{p}_0\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} (\mathsf{check}\{\tau_0\}\, e_0[x_0 \leftarrow v_0]\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_1$
(1) $e_0 = \mathsf{app}\{\tau_0\}\, v_2\, v_3$ and $v_2 \lesssim \mathsf{p}_0$ and $v_3 \lesssim v_0$
By $\lesssim$ on the redex
(2) If v_2 is a function, then $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{check}\{\tau_0\}\, e_1[x_0 \leftarrow v_3]\, \bullet$
and $\mathsf{check}\{\tau_0\}\, e_1[x_0 \leftarrow v_3]\, \bullet \approx (\mathsf{check}\{\tau_0\}\, e_0[x_0 \leftarrow v_0]\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_1$
By (1)
(3) Otherwise $v_2 \in \mathbb{G}\, b\, v_4$ and unfolds to a dyn/stat boundary,
for example, $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_4\, (\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_3))$ and the argument reduces to a value,
for example, $\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_3 \rightarrow^*_{\mathsf{A}} v_5$

Case: $(\mathsf{app}\{\mathcal{U}\}\, \mathsf{p}_0\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} (e_0[x_0 \leftarrow v_0]); \mathcal{H}_0; \mathcal{B}_0$
(1) $e_0 = \mathsf{app}\{\mathcal{U}\}\, v_2\, v_3$ and $v_2 \lesssim \mathsf{p}_0$ and $v_3 \lesssim v_0$
By $\lesssim$ on the redex
(2) If v_2 is a function, then $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{check}\{\tau_0\}\, e_1[x_0 \leftarrow v_3]\, \bullet$
and $\mathsf{check}\{\tau_0\}\, e_1[x_0 \leftarrow v_3]\, \bullet \approx (\mathsf{check}\{\tau_0\}\, e_0[x_0 \leftarrow v_0]\, \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_1$
By (1)
(3) Otherwise $v_2 \in \mathbb{G}\, b\, v_4$ and e_0 unfolds to
a stat boundary $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\tau\}\, v_4\, (\mathsf{dyn}\,(\ell_1 \blacktriangleleft \tau \blacktriangleleft \ell_0)\, v_3))$ and the argument reduces to a value $\mathsf{stat}\,(\ell_1 \blacktriangleleft \tau \blacktriangleleft \ell_0)\, v_3 \rightarrow^*_{\mathsf{A}} v_5$
and $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\tau\}\, v_4\, v_5) \approx (e_0[x_0 \leftarrow v_0]); \mathcal{H}_0; \mathcal{B}_0$

Case: $(\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} v_0; \mathcal{H}_0; \mathcal{B}_1$
(1) $e_0 = \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex
(2) If $v_1 \in i$ then $e_0 \rightarrow^*_{\mathsf{A}} v_1$ and $v_1 \approx v_0; \mathcal{H}_0; \mathcal{B}_1$

(3) Otherwise $e_0 \rightarrow^*_{\mathsf{A}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$ and $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1 \approx v_0; \mathcal{H}_0; \mathcal{B}_1$

Case: $(\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{BoundaryErr}\,(\{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}, v_0); \mathcal{H}_0; \mathcal{B}_0$

(1) $e_0 = \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex

(2) $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
By (1)

(3) $\mathsf{BoundaryErr}\,(\overline{b}, v) \approx \mathsf{BoundaryErr}\,(\{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}, v_0); \mathcal{H}_0; \mathcal{B}_0$

Case: $(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} v_0; \mathcal{H}_0; \mathcal{B}_1$

(1) $e_0 = \mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex

(2) If $v_1 \in i$ then $e_0 \rightarrow^*_{\mathsf{A}} v_1$ and $v_1 \approx v_0; \mathcal{H}_0; \mathcal{B}_1$

(3) If v_1 has no guard wrappers, then $e_0 \rightarrow^*_{\mathsf{A}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$ and $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1 \approx v_0; \mathcal{H}_0; \mathcal{B}_1$

(4) Otherwise $v_1 = \mathbb{G}\ b\ v_2$ and $e_0 \rightarrow^*_{\mathsf{A}} \mathbb{T}\ \overline{b}\ v_2$ and $\mathbb{T}\ \overline{b}\ v_2 \approx v_0; \mathcal{H}_0; \mathcal{B}_1$

Case: $(\mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$

Impossible, by type soundness

Case: $(\mathsf{check}\{\mathcal{U}\}\ v_0\ \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} v_0; \mathcal{H}_0; \mathcal{B}_0$

(1) If $e_0 = \mathsf{stat}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$ then $e_0 \rightarrow^*_{\mathsf{A}} v_2$ and $v_2 \approx v_0; \mathcal{H}_0; \mathcal{B}_0$

(2) Otherwise $e_0 = \mathsf{check}\{\mathcal{U}\}\ v_1\ \bullet$ and $e_0 \rightarrow^*_{\mathsf{A}} v_1$ and $v_1 \approx v_0; \mathcal{H}_0; \mathcal{B}_0$

Case: $(\mathsf{check}\{\tau_0\}\ v_0\ \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} v_0; \mathcal{H}_0; \mathcal{B}_1$

(1) If $e_0 = \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$ then $v_1 \lesssim v_0$ and $e_0 \rightarrow^*_{\mathsf{A}} v_2$ and $v_2 \approx v_0; \mathcal{H}_0; \mathcal{B}_1$
Same as the dyn case

(2) Otherwise $e_0 = \mathsf{check}\{\tau_0\}\ v_1\ \bullet$ and $e_0 \rightarrow^*_{\mathsf{A}} v_1$ and $v_1 \approx v_0; \mathcal{H}_0; \mathcal{B}_1$

Case: $(\mathsf{check}\{\tau_0\}\ v_0\ \mathsf{p}_0); \mathcal{H}_0; \mathcal{B}_0 \rhd_{\mathsf{T}} \mathsf{BoundaryErr}\,(\mathcal{B}_0(v_0) \cup \mathcal{B}_0(\mathsf{p}_0), v_0); \mathcal{H}_0; \mathcal{B}_0$

(1) If $e_0 = \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$ then $v_1 \lesssim v_0$ and $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
and $\mathsf{BoundaryErr}\,(\overline{b}, v) \approx \mathsf{BoundaryErr}\,(\mathcal{B}_0(v_0) \cup \mathcal{B}_0(\mathsf{p}_0), v_0); \mathcal{H}_0; \mathcal{B}_1$
Same as the dyn case

(2) Otherwise $e_0 = \mathsf{check}\{\tau_0\}\ v_1\ \bullet$, but this is impossible by type soundness.

□

Lemma A.32.
If $\mathrm{wfr}_{AT}(e_0, e_1)$ *and* $e_0 \lesssim e_1$ *and either* $e_0 \rightarrow_{\mathsf{A}} e_2$ *or* $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\mathsf{T}} e_3; \mathcal{H}_2; \mathcal{B}_2$ *then the following results hold:*

- $e_0 = E_0[e_4]$
- $e_1 = E_1[e_5]$
- $E_0 \lesssim E_1$
- $e_4 \lesssim e_5$.

Proof. By lemma A.33 and lemma A.34. □

Lemma A.33.
If $\mathrm{wfr}_{AT}(E_0[e_0], e_1)$ *and* $E_0[e_0] \lesssim e_1$ *and* $e_0(\rhd_{\mathsf{A}} \cup \blacktriangleright_{\mathsf{A}})e_2$ *then the following results hold:*

- $e_1 = E_1[e_3]$
- $E_0 \lesssim E_1$
- $e_0 \lesssim e_1$.

Proof. By induction on $E_0[e_0] \lesssim e_1$, proceeding by case analysis of $E_0[e_0]$. □

Lemma A.34.
If $\mathrm{wfr}_{AT}(e_0, E_1[e_1])$ *and* $e_0 \lesssim E_1[e_1]$ *and* $e_1; \mathcal{H}_1; \mathcal{B}_1 \vartriangleright_{\mathsf{T}} e_3; \mathcal{H}_3; \mathcal{B}_3$ *then the following results hold:*

- $e_0 = E_0[e_2]$
- $E_0 \lesssim E_1$
- $e_1 \lesssim e_2$.

Proof. By induction on $e_0 \lesssim E_1[e_1]$, proceeding by case analysis of $E_1[e_1]$. □

Lemma A.35.
If $E_0 \lesssim E_1$ *and* $e_2 \lesssim e_3$ *then* $E_0[e_2] \lesssim E_1[e_3]$.

Proof. By induction on $E_0 \lesssim E_1$. □

LEMMA A.36 ($F \lesssim A$). $F \lesssim A$

PROOF. By lemma A.37 and lemma A.38, the relation $e \lesssim e$ is a lock-step bisimulation. □

$\boxed{\mathrm{wfr}_{FT}(e_0, e_1)}$ holds for well-formed residuals of a common term; that is, pairs such that there exists an e_2 where $e_2 : {}^{\tau}/_{\mathcal{U}}$ **wf** and $e_2 \rightarrow^*_{\mathsf{F}} e_0$ and $e_2 \rightarrow^*_{\mathsf{A}} e_1$

LEMMA A.37. *If* $\mathrm{wfr}_{FT}(e_0, e_1)$ *and* $e_0 \lesssim e_1$ *and* $e_0 \rightarrow_{\mathsf{F}} e_2$ *then* $e_1 \rightarrow_{\mathsf{A}} e_3$

PROOF. By lemma A.39, lemma A.42, and case analysis of $\rhd_{\mathsf{F}} \cup \blacktriangleright_{\mathsf{F}}$.

Case: $unop\{\tau_0\}\, v_0 \rhd_{\mathsf{F}}$ InvariantErr
Impossible, by type soundness

Case: $unop\{\tau_0\}\, v_0 \rhd_{\mathsf{F}} \delta(unop, v_0)$
(1) $e_1 = unop\{\tau_0\}\, v_1$ and $v_0 \lesssim v_1$
By $\lesssim$ on the redex
(2) $\delta(unop, v_1)$ is defined
By (1)
(3) $\delta(unop, v_0) \lesssim \delta(unop, v_1)$
By δ

Case: $\mathsf{fst}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0) \rhd_{\mathsf{F}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_0)$
(1) $e_1 = unop\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\, v_1)$ and $v_0 \lesssim v_1$ and $\tau_1 \leqslant: \tau_2$
By $\lesssim$ on the redex
(2) $e_1 \rhd_{\mathsf{A}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_1)$
By (1)
(3) $\mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_0) \lesssim \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{fst}\{\mathcal{U}\}\, v_1)$
By $\mathit{fst}(\tau_1) \leqslant: \tau_0$

Case: $\mathsf{snd}\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0 \rhd_{\mathsf{F}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_0)$
(1) $e_1 = unop\{\tau_0\}\, (\mathbb{G}\, (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\, v_1)$ and $v_0 \lesssim v_1$ and $\tau_1 \leqslant: \tau_2$
By $\lesssim$ on the redex
(2) $e_1 \rhd_{\mathsf{A}} \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_1)$
By (1)
(3) $\mathsf{dyn}\, (\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_0) \lesssim \mathsf{dyn}\, (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, (\mathsf{snd}\{\mathcal{U}\}\, v_1)$
By $\mathit{snd}(\tau_1) \leqslant: \tau_0$

Case: $binop\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{F}}$ InvariantErr
Impossible, by type soundness

Case: $binop\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{F}} \delta(binop, v_0, v_1)$
(1) $e_1 = binop\{\tau_0\}\, v_2\, v_3$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex
(2) $\delta(binop, v_2, v_3)$ is defined
By (1)
(3) $\delta(binop, v_0, v_1) \lesssim \delta(binop, v_2, v_3)$
By δ

Case: $\mathsf{app}\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{F}}$ InvariantErr
Impossible, by type soundness

Case: $\mathsf{app}\{\tau_0\}\, (\lambda(x_0 : \tau_1).\, e_4)\, v_0 \rhd_{\mathsf{F}} e_4[x_0 \leftarrow v_0]$
(1) $e_1 = \mathsf{app}\{\tau_0\}\, v_1\, v_2$ and $(\lambda(x_0 : \tau_1).\, e_4) \lesssim v_1$ and $v_0 \lesssim v_2$
By $\lesssim$ on the redex
(2) $v_1 = \lambda(x_0 : \tau_1).\, e_5$
By (1)

(3) $e_4[x_0 \leftarrow v_0] \lesssim e_5[x_0 \leftarrow v_2]$

Case: $\mathsf{app}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_0)\; v_1 \rhd_{\mathsf{F}}$
$\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\; v_0\; (\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\; v_1))$

(1) $e_1 = \mathsf{app}\{\tau_0\}\; v_2\; v_3$ and $(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_0) \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex

(2) $v_2 = \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\; v_4$ and $\tau_1 \leqslant: \tau_2$
By (1)

(3) $e_1 \rhd_{\mathsf{A}} \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\; v_4\; (\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\; v_3))$
By (2)

(4) $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\; v_4\; (\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\; v_1)) \lesssim$
$\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\; v_0\; (\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\; v_3))$
By $\mathit{cod}(\tau_1) \leqslant: \tau_0$

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \rhd_{\mathsf{F}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0$

(1) $e_1 = \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_1$ and $v_0 \lesssim v_1$ and $\tau_0 \leqslant: \tau_1$
By $\lesssim$

(2) $e_1 \rhd_{\mathsf{A}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_1$
By $\rhd_{\mathsf{A}}$

(3) $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \lesssim \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_1$
By (1)

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathbb{T}_?\; \overline{b}_0\; i_0) \rhd_{\mathsf{F}} i_0$

(1) $e_1 = \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; i_1$ and $i_0 \lesssim i_1$ and $\tau_0 \leqslant: \tau_1$
By $\lesssim$

(2) $e_1 \rhd_{\mathsf{A}} i_1$
By $\rhd_{\mathsf{A}}$ and $\tau_0 \leqslant: \tau_1$

(3) $i_0 \lesssim i_1$
By (1)

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \rhd_{\mathsf{F}} \mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b}_0, v_0)$
Immediate, by $\mathsf{BoundaryErr}\,(\overline{b}, v) \lesssim e$

Case: $\mathit{unop}\{\mathcal{U}\}\; v_0 \blacktriangleright_{\mathsf{F}} \mathsf{TagErr}$

(1) $e_1 = \mathit{unop}\{\mathcal{U}\}\; v_1$ and $v_0 \lesssim v_1$
By $\lesssim$ on the redex

(2) $\delta(\mathit{unop}, v_1)$ is undefined
By (1)

(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathit{unop}\{\mathcal{U}\}\; v_0 \blacktriangleright_{\mathsf{F}} \mathit{add\text{-}trace}(\mathit{get\text{-}trace}(v_0), \delta(\mathit{unop}, \mathit{rem\text{-}trace}(v_0)))$

(1) $e_1 = \mathit{unop}\{\mathcal{U}\}\; v_1$ and $v_0 \lesssim v_1$
By $\lesssim$ on the redex

(2) $\delta(\mathit{unop}, \mathit{rem\text{-}trace}(v_1))$ is defined
By (1)

(3) $\delta(\mathit{unop}, \mathit{rem\text{-}trace}(v_0)) \lesssim \delta(\mathit{unop}, \mathit{rem\text{-}trace}(v_1))$
By δ

Case: $\mathsf{fst}\{\mathcal{U}\}\,(\mathbb{T}_?\; \overline{b}_0\; (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0)) \blacktriangleright_{\mathsf{F}} \mathsf{trace}\; \overline{b}_0\; (\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\; (\mathsf{fst}\{\mathit{fst}(\tau_0)\}\; v_0))$

(1) $e_1 = \mathit{unop}\{\mathcal{U}\}\,(\mathbb{T}_?\; \overline{b}_0\; (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_1))$ and $v_0 \lesssim v_1$ and $\tau_0 \leqslant: \tau_1$
By $\lesssim$ on the redex

(2) $e_1 \blacktriangleright_{\mathsf{A}} \mathsf{trace}\; \overline{b}_0\; (\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\; (\mathsf{fst}\{\mathit{fst}(\tau_1)\}\; v_1))$
By (1)

(3) $\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathit{fst}(\tau_0)\}\,v_0)) \lesssim$
$\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathit{fst}(\tau_1)\}\,v_1))$
By $\mathit{fst}(\tau_0) \leqslant: \mathit{fst}(\tau_1)$

Case: $\mathsf{snd}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0)) \blacktriangleright_{\mathsf{F}} \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathit{snd}(\tau_0)\}\,v_0))$

(1) $e_1 = \mathit{unop}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,v_1))$ and $v_0 \lesssim v_1$ and $\tau_0 \leqslant: \tau_1$
By $\lesssim$ on the redex

(2) $e_1 \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathit{snd}(\tau_1)\}\,v_1))$
By (1)

(3) $\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathit{snd}(\tau_0)\}\,v_0)) \lesssim$
$\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathit{snd}(\tau_1)\}\,v_1))$
By $\mathit{snd}(\tau_0) \leqslant: \mathit{snd}(\tau_1)$

Case: $\mathit{binop}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{F}} \mathsf{TagErr}$

(1) $e_1 = \mathit{binop}\{\mathcal{U}\}\,v_2\,v_3$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex

(2) $\delta(\mathit{binop}, v_2, v_3)$ is undefined
By (1)

(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathit{binop}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{F}} \delta(\mathit{binop}, \mathit{rem\text{-}trace}(v_0), \mathit{rem\text{-}trace}(v_1))$

(1) $e_1 = \mathit{binop}\{\mathcal{U}\}\,v_2\,v_3$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex

(2) $\delta(\mathit{binop}, \mathit{rem\text{-}trace}(v_2), \mathit{rem\text{-}trace}(v_3))$ is defined
By (1)

(3) $\delta(\mathit{binop}, \mathit{rem\text{-}trace}(v_0), \mathit{rem\text{-}trace}(v_1)) \lesssim \delta(\mathit{binop}, \mathit{rem\text{-}trace}(v_2), \mathit{rem\text{-}trace}(v_3))$
By δ

Case: $\mathsf{app}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{F}} \mathsf{TagErr}$

(1) $e_1 = \mathsf{app}\{\mathcal{U}\}\,v_2\,v_3$ and $v_0 \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex

(2) $\mathit{rem\text{-}trace}(v_2) \notin \lambda x.\,e \cup \mathbb{G}\,b\,v$
By (1)

(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathsf{app}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\lambda x_0.\,e_4))\,v_0 \blacktriangleright_{\mathsf{F}} \mathsf{trace}\,\overline{b}_0\,(e_4[x_0 \leftarrow v_1])$

(1) $e_1 = \mathsf{app}\{\mathcal{U}\}\,v_1\,v_2$ and $(\mathbb{T}_?\,\overline{b}_0\,(\lambda x_0.\,e_4)) \lesssim v_1$ and $v_0 \lesssim v_2$
By $\lesssim$ on the redex

(2) $v_1 = (\mathbb{T}_?\,\overline{b}_0\,(\lambda x_0.\,e_5))$
By (1)

(3) $\mathsf{trace}\,\overline{b}_0\,(e_4[x_0 \leftarrow v_1]) \lesssim \mathsf{trace}\,\overline{b}_0\,(e_5[x_0 \leftarrow v_2])$

Case: $\mathsf{app}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0))\,v_1 \blacktriangleright_{\mathsf{F}}$
$\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\tau_1\}\,v_0\,(\mathsf{dyn}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\,v_2)))$

(1) $e_1 = \mathsf{app}\{\mathcal{U}\}\,v_2\,v_3$ and $(\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0)) \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex

(2) $v_2 = \mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,v_4)$ and $\tau_0 \leqslant: \tau_1$
By (1)

(3) $e_1 \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\,v_4\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\,v_3)))$
By (2)

(4) $\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\tau_1\}\,v_0\,(\mathsf{dyn}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\,v_2))) \lesssim$
$\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\,v_4\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\,v_3)))$
By $\tau_0 \leqslant: \tau_1$

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \blacktriangleright_{\mathsf{F}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0$

(1) $e_1 = \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_1$ and $v_0 \lesssim v_1$ and $\tau_0 \leqslant: \tau_1$
By $\lesssim$

(2) $e_1 \blacktriangleright_{\mathsf{A}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_1$
By $\blacktriangleright_{\mathsf{A}}$

(3) $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \lesssim \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_1$
By (1)

Case: $\mathsf{stat}\ b_0\ (\mathbb{G}\ b_1\ (\mathbb{T}_?\ \overline{b_0}\ v_0)) \blacktriangleright_{\mathsf{F}} \mathsf{trace}\,(b_0 b_1 \overline{b_0})\ v_0$

(1) $e_1 = \mathsf{stat}\ b_2\ (\mathbb{G}\ b_3\ (\mathbb{T}_?\ \overline{b_1}\ v_1))$ and $v_0 \lesssim v_1$ and $\tau_0 \leqslant: \tau_1$ and $b_0 \lesssim b_2$ and $b_1 \lesssim b_3$
By $\lesssim$

(2) $e_1 \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,(b_2 b_3 \overline{b_1})\ v_1$
By $\blacktriangleright_{\mathsf{A}}$

(3) $\mathsf{trace}\,(b_0 b_1 \overline{b_0})\ v_0 \lesssim \mathsf{trace}\,(b_2 b_3 \overline{b_1})\ v_1$
By (1)

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ i_0 \blacktriangleright_{\mathsf{F}} i_0$

(1) $e_1 = \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ i_1$ and $i_0 \lesssim i_1$ and $\tau_0 \leqslant: \tau_1$
By $\lesssim$

(2) $e_1 \blacktriangleright_{\mathsf{A}} i_1$
By $\blacktriangleright_{\mathsf{A}}$ and $\tau_0 \leqslant: \tau_1$

(3) $i_0 \lesssim i_1$
By (1)

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \blacktriangleright_{\mathsf{F}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathsf{trace}\,\overline{b_0}\ v_0 \blacktriangleright_{\mathsf{F}} \mathit{add\text{-}trace}(\overline{b_0}, v_0)$

(1) $e_1 = \mathsf{trace}\,\overline{b_1}\ v_1$
By $\lesssim$

(2) $e_1 \blacktriangleright_{\mathsf{A}} \mathit{add\text{-}trace}(\overline{b_1}, v_1)$
By $\blacktriangleright_{\mathsf{A}}$

(3) $\mathit{add\text{-}trace}(\overline{b_0}, v_0) \lesssim \mathit{add\text{-}trace}(\overline{b_1}, v_1)$
By (1)

□

Lemma A.38. *If* $\mathrm{wfr}_{FT}(e_0, e_1)$ *and* $e_0 \lesssim e_1$ *and* $e_1 \rightarrow_{\mathsf{A}} e_3$ *then* $e_0 \rightarrow_{\mathsf{F}} e_2$

Proof. By lemma A.39, lemma A.42, and case analysis of $\triangleright_{\mathsf{A}} \cup \blacktriangleright_{\mathsf{A}}$.

Case: $\mathit{unop}\{\tau_0\}\, v_0 \triangleright_{\mathsf{A}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathit{unop}\{\tau_0\}\, v_0 \triangleright_{\mathsf{A}} \delta(\mathit{unop}, v_0)$

(1) $e_0 = \mathit{unop}\{\tau_0\}\, v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex

(2) $\delta(\mathit{unop}, v_1)$ is defined
By (1)

(3) $\delta(\mathit{unop}, v_1) \lesssim \delta(\mathit{unop}, v_0)$
By δ

Case: $\mathsf{fst}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0) \triangleright_{\mathsf{A}} \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathcal{U}\}\, v_0)$

(1) $e_0 = \mathit{unop}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\, v_1)$ and $v_1 \lesssim v_0$ and $\mathit{fst}(\tau_2) \leqslant: \tau_0$
By $\lesssim$ on the redex

(2) $e_0 \triangleright_{\mathsf{F}} \mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_2) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathcal{U}\}\, v_1)$
By (1)

(3) $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_2) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathcal{U}\}\, v_1) \lesssim \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathcal{U}\}\, v_0)$
By (1)

Case: $\mathsf{snd}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0 \triangleright_{\mathsf{A}} \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathcal{U}\}\, v_0)$

(1) $e_1 = \mathit{unop}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\, v_1)$ and $v_1 \lesssim v_0$ and $\mathit{snd}(\tau_2) \leqslant: \tau_0$
By $\lesssim$ on the redex

(2) $e_0 \triangleright_{\mathsf{F}} \mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_2) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathcal{U}\}\, v_1)$
By (1)

(3) $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_2) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathcal{U}\}\, v_1) \lesssim \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathcal{U}\}\, v_0)$
By (1)

Case: $\mathit{binop}\{\tau_0\}\, v_0\, v_1 \triangleright_{\mathsf{A}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathit{binop}\{\tau_0\}\, v_0\, v_1 \triangleright_{\mathsf{A}} \delta(\mathit{binop}, v_0, v_1)$

(1) $e_0 = \mathit{binop}\{\tau_0\}\, v_2\, v_3$ and $v_2 \lesssim v_0$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex

(2) $\delta(\mathit{binop}, v_2, v_3)$ is defined
By (1)

(3) $\delta(\mathit{binop}, v_2, v_3) \lesssim \delta(\mathit{binop}, v_0, v_1)$
By δ

Case: $\mathsf{app}\{\tau_0\}\, v_0\, v_1 \triangleright_{\mathsf{A}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathsf{app}\{\tau_0\}\,(\lambda(x_0 : \tau_1).\, e_0)\, v_0 \triangleright_{\mathsf{A}} e_0[x_0 \leftarrow v_0]$

(1) $e_0 = \mathsf{app}\{\tau_0\}\, v_1\, v_2$ and $v_1 \lesssim (\lambda(x_0 : \tau_1).\, e_4)$ and $v_2 \lesssim v_0$
By $\lesssim$ on the redex

(2) $v_1 = \lambda(x_0 : \tau_1).\, e_5$
By (1)

(3) $e_5[x_0 \leftarrow v_2] \lesssim e_4[x_0 \leftarrow v_0]$

Case: $\mathsf{app}\{\tau_0\}\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0)\, v_1 \triangleright_{\mathsf{A}}$
$\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\, v_0\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\, v_1))$

(1) $e_1 = \mathsf{app}\{\tau_0\}\, v_2\, v_3$ and $v_2 \lesssim (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\, v_0)$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex

(2) $v_2 = \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)\; v_4$ and $cod(\tau_2) \leqslant: \tau_0$
By (1)
(3) $e_1 \rhd_{\mathsf{F}}$ dyn $(\ell_0 \blacktriangleleft cod(\tau_2) \blacktriangleleft \ell_1)$ (app$\{\mathcal{U}\}\; v_4$ (stat $(\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\; v_3$))
By (2)
(4) dyn $(\ell_0 \blacktriangleleft cod(\tau_2) \blacktriangleleft \ell_1)$ (app$\{\mathcal{U}\}\; v_4$ (stat $(\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\; v_3$)) $\lesssim$
dyn $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$ (app$\{\mathcal{U}\}\; v_0$ (stat $(\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)\; v_1$))
By $cod(\tau_0) \leqslant: \tau_0$

Case: dyn $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \rhd_{\mathsf{A}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0$
(1) $e_1 =$ dyn $(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_1$ and $v_1 \lesssim v_0$ and $\tau_1 \leqslant: \tau_0$
By $\lesssim$
(2) Either $e_1 \rhd_{\mathsf{F}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_1$ or $e_1 \rhd_{\mathsf{F}}$ BoundaryErr $(\overline{b}, v)$
By $\rhd_{\mathsf{F}}$
(3) $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_1 \lesssim \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0$
By (1)

Case: dyn $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; (\mathbb{T}_?\; \overline{b}_0\; i_0) \rhd_{\mathsf{A}} i_0$
(1) $e_1 =$ dyn $(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; i_1$ and $i_1 \lesssim i_0$ and $\tau_1 \leqslant: \tau_0$
By $\lesssim$
(2) Either $e_1 \rhd_{\mathsf{F}} i_1$ or $e_1 \rhd_{\mathsf{F}}$ BoundaryErr $(\overline{b}, i)$
By $\rhd_{\mathsf{F}}$ and $\tau_0 \leqslant: \tau_1$
(3) $i_1 \lesssim i_0$
By (1)

Case: dyn $(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \rhd_{\mathsf{A}}$ BoundaryErr $((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b}_0, v_0)$
(1) $e_1 =$ dyn $(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_1$ and $v_1 \lesssim v_0$ and $\tau_1 \leqslant: \tau_0$
By $\lesssim$
(2) BoundaryErr $(\overline{b}_1, v_1) \lesssim$ BoundaryErr $(\overline{b}_0, v_0)$
By (1) and $\rhd_{\mathsf{F}}$

Case: $unop\{\mathcal{U}\}\; v_0 \blacktriangleright_{\mathsf{A}}$ TagErr
(1) $e_1 = unop\{\mathcal{U}\}\; v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex
(2) $\delta(unop, rem\text{-}trace(v_1))$ is defined
By (1)
(3) $\delta(unop, rem\text{-}trace(v_1)) \lesssim \delta(unop, rem\text{-}trace(v_0))$
By δ

Case: $unop\{\mathcal{U}\}\; v_0 \blacktriangleright_{\mathsf{A}} add\text{-}trace(get\text{-}trace(v_0), \delta(unop, v_1))$
(1) $e_1 = unop\{\mathcal{U}\}\; v_1$ and $v_1 \lesssim v_0$
By $\lesssim$ on the redex
(2) $\delta(unop, rem\text{-}trace(v_1))$ is defined
By (1)
(3) $\delta(unop, rem\text{-}trace(v_1)) \lesssim \delta(unop, rem\text{-}trace(v_0))$
By δ

Case: fst$\{\mathcal{U}\}\; (\mathbb{T}_?\; \overline{b}_0\; (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0)) \blacktriangleright_{\mathsf{A}}$ trace $\overline{b}_0$ (stat $(\ell_0 \blacktriangleleft fst(\tau_0) \blacktriangleleft \ell_1)$ (fst$\{\tau_1\}\; v_0$))
(1) $e_1 = unop\{\mathcal{U}\}\; (\mathbb{T}_?\; \overline{b}_0\; (\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_1))$ and $v_1 \lesssim v_0$ and $\tau_1 \leqslant: \tau_0$
By $\lesssim$ on the redex
(2) $e_1 \blacktriangleright_{\mathsf{F}}$ trace $\overline{b}_0$ (stat $(\ell_0 \blacktriangleleft fst(\tau_1) \blacktriangleleft \ell_1)$ (fst$\{fst(\tau_1)\}\; v_1$))
By (1)

(3) $\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\mathit{fst}(\tau_1)\}\,v_1)) \lesssim$
$\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{fst}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{fst}\{\tau_1\}\,v_0))$
By $\mathit{fst}(\tau_1) \leqslant: \mathit{fst}(\tau_0)$

Case: $\mathsf{snd}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0)) \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\tau_1\}\,v_0))$

(1) $e_1 = \mathit{unop}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,v_1))$ and $v_1 \lesssim v_0$ and $\tau_1 \leqslant: \tau_0$
By $\lesssim$ on the redex

(2) $e_1 \blacktriangleright_{\mathsf{F}} \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathit{snd}(\tau_1)\}\,v_1))$
By (1)

(3) $\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\mathit{snd}(\tau_1)\}\,v_1)) \lesssim$
$\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{snd}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{snd}\{\tau_1\}\,v_0))$
By $\mathit{snd}(\tau_1) \leqslant: \mathit{snd}(\tau_0)$

Case: $\mathit{binop}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{A}} \mathsf{TagErr}$

(1) $e_1 = \mathit{binop}\{\mathcal{U}\}\,v_2\,v_3$ and $v_2 \lesssim v_0$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex

(2) $\delta(\mathit{binop}, v_2, v_3)$ is undefined
By (1)

(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathit{binop}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{A}} \delta(\mathit{binop}, v_2, v_3)$

(1) $e_1 = \mathit{binop}\{\mathcal{U}\}\,v_2\,v_3$ and $v_2 \lesssim v_0$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex

(2) $\delta(\mathit{binop}, \mathit{rem\text{-}trace}(v_2), \mathit{rem\text{-}trace}(v_3))$ is defined
By (1)

(3) $\delta(\mathit{binop}, \mathit{rem\text{-}trace}(v_2), \mathit{rem\text{-}trace}(v_3)) \lesssim \delta(\mathit{binop}, \mathit{rem\text{-}trace}(v_0), \mathit{rem\text{-}trace}(v_1))$
By δ

Case: $\mathsf{app}\{\mathcal{U}\}\,v_0\,v_1 \blacktriangleright_{\mathsf{A}} \mathsf{TagErr}$

(1) $e_1 = \mathsf{app}\{\mathcal{U}\}\,v_2\,v_3$ and $v_2 \lesssim v_0$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex

(2) $\mathit{rem\text{-}trace}(v_2) \notin \lambda x.\,e \cup \mathbb{G}\,b\,v$
By (1)

(3) $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathsf{app}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\lambda x_0.\,e_0))\,v_0 \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,\overline{b}_0\,(e_0[x_0 \leftarrow v_1])$

(1) $e_1 = \mathsf{app}\{\mathcal{U}\}\,v_1\,v_2$ and $v_1 \lesssim (\mathbb{T}_?\,\overline{b}_0\,(\lambda x_0.\,e_4))$ and $v_2 \lesssim v_0$
By $\lesssim$ on the redex

(2) $v_1 = (\mathbb{T}_?\,\overline{b}_0\,(\lambda x_0.\,e_5))$
By (1)

(3) $\mathsf{trace}\,\overline{b}_0\,(e_5[x_0 \leftarrow v_2]) \lesssim \mathsf{trace}\,\overline{b}_0\,(e_4[x_0 \leftarrow v_1])$

Case: $\mathsf{app}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0))\,v_1 \blacktriangleright_{\mathsf{A}}$
$\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\tau_2\}\,v_0\,(\mathsf{dyn}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\,v_2)))$

(1) $e_1 = \mathsf{app}\{\mathcal{U}\}\,v_2\,v_3$ and $v_2 \lesssim (\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,v_0))$ and $v_3 \lesssim v_1$
By $\lesssim$ on the redex

(2) $v_2 = \mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\,v_4)$ and $\tau_1 \leqslant: \tau_0$
By (1)

(3) $e_1 \blacktriangleright_{\mathsf{F}} \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\,v_4\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\,v_3)))$
By (2)

(4) $\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_1) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathcal{U}\}\,v_4\,(\mathsf{stat}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_1) \blacktriangleleft \ell_0)\,v_3))) \lesssim$
$\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\tau_2\}\,v_0\,(\mathsf{dyn}\,(\ell_1 \blacktriangleleft \mathit{dom}(\tau_0) \blacktriangleleft \ell_0)\,v_2)))$
By $\tau_1 \leqslant: \tau_0$

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \blacktriangleright_{\mathsf{A}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0$

(1) $e_1 = \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_1$ and $v_1 \lesssim v_0$ and $\tau_1 \leqslant: \tau_0$
By $\lesssim$

(2) Either $e_1 \blacktriangleright_{\mathsf{F}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_1$ or $e_1 \blacktriangleright_{\mathsf{F}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
By $\blacktriangleright_{\mathsf{F}}$

(3) $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; v_1 \lesssim \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0$
By (1)

Case: $\mathsf{stat}\; b_0\; (\mathbb{G}\; b_1\; (\mathbb{T}_?\, \overline{b}_0\; v_0)) \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,(b_0 b_1 \overline{b}_0)\; v_0$

(1) $e_1 = \mathsf{stat}\; b_2\; (\mathbb{G}\; b_3\; (\mathbb{T}_?\, \overline{b}_1\; v_1))$ and $v_1 \lesssim v_0$ and $\tau_1 \leqslant: \tau_0$ and $b_2 \lesssim b_0$ and $b_3 \lesssim b_1$
By $\lesssim$

(2) Either $e_1 \blacktriangleright_{\mathsf{F}} \mathsf{trace}\,(b_2 b_3 \overline{b}_1)\; v_1$ or $e_1 \blacktriangleright_{\mathsf{F}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
By $\blacktriangleright_{\mathsf{F}}$

(3) $\mathsf{trace}\,(b_2 b_3 \overline{b}_1)\; v_1 \lesssim \mathsf{trace}\,(b_0 b_1 \overline{b}_0)\; v_0$
By (1)

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; i_0 \blacktriangleright_{\mathsf{A}} i_0$

(1) $e_1 = \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\; i_1$ and $i_1 \lesssim i_0$ and $\tau_1 \leqslant: \tau_0$
By $\lesssim$

(2) Either $e_1 \blacktriangleright_{\mathsf{F}} i_1$ or $e_1 \blacktriangleright_{\mathsf{F}} \mathsf{BoundaryErr}\,(\overline{b}, i)$
By $\blacktriangleright_{\mathsf{F}}$ and $\tau_1 \leqslant: \tau_0$

(3) $i_1 \lesssim i_0$
By (1)

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \blacktriangleright_{\mathsf{A}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathsf{trace}\,\overline{b}_0\; v_0 \blacktriangleright_{\mathsf{A}} v_1$

(1) $e_1 = \mathsf{trace}\,\overline{b}_1\; v_1$
By $\lesssim$

(2) $e_1 \blacktriangleright_{\mathsf{A}} \textit{add-trace}\,(\overline{b}_1, v_1)$
By $\blacktriangleright_{\mathsf{A}}$

(3) $\textit{add-trace}\,(\overline{b}_1, v_1) \lesssim \textit{add-trace}\,(\overline{b}_0, v_0)$
By (1)

□

Lemma A.39.
If $\mathrm{wfr}_{FT}(e_0, e_1)$ *and* $e_0 \lesssim e_1$ *and either* $e_0 \rightarrow_{\mathsf{F}} e_2$ *or* $e_1 \rightarrow_{\mathsf{A}} e_3$ *then the following results hold:*

- $e_0 = E_0[e_4]$
- $e_1 = E_1[e_5]$
- $E_0 \lesssim E_1$
- $e_4 \lesssim e_5$.

Proof. By lemma A.40 and lemma A.41. □

Lemma A.40.
If $\mathrm{wfr}_{FT}(E_0[e_0], e_1)$ *and* $E_0[e_0] \lesssim e_1$ *and* $e_0(\vartriangleright_{\mathsf{F}} \cup \blacktriangleright_{\mathsf{F}})e_2$ *then the following results hold:*

- $e_1 = E_1[e_3]$
- $E_0 \lesssim E_1$
- $e_0 \lesssim e_3$.

Proof. By induction on $E_0[e_0] \lesssim e_1$, proceeding by case analysis of $E_0[e_0]$. □

Lemma A.41.
If $\mathrm{wfr}_{FT}(e_0, E_1[e_1])$ *and* $e_0 \lesssim E_1[e_1]$ *and* $e_1(\triangleright_A \cup \blacktriangleright_A)e_3$ *then the following results hold:*

- $e_0 = E_0[e_2]$
- $E_0 \lesssim E_1$
- $e_2 \lesssim e_1$.

Proof. By induction on $e_0 \lesssim E_1[e_1]$, proceeding by case analysis of $E_1[e_1]$. □

Lemma A.42.
If $E_0 \lesssim E_1$ *and* $e_2 \lesssim e_3$ *then* $E_0[e_2] \lesssim E_1[e_3]$.

Proof. By induction on $E_0 \lesssim E_1$. □

A.6 Erasure

Lemma A.43 (Erasure type progress). *If* $\cdot \vdash_0 E_0[e_0] : \mathcal{U}$ *then one of the following holds:*

- $e_0 \in v \cup \mathsf{Err}$
- $\exists\, e_1.\, e_0 \rhd_{\mathsf{E}} e_1$

Proof. By unique decomposition (lemma 6.1) and case analysis:

Case: $\cdot \vdash_1 i : \mathcal{U}$
Immediate.

Case: $\cdot \vdash_1 \lambda(x_0 : \tau_0).\, e_0 : \mathcal{U}$
Immediate.

Case: $\cdot \vdash_1 \lambda x_0.\, e_0 : \mathcal{U}$
Immediate.

Case: $\cdot \vdash_1 \langle v_0, v_1 \rangle : \mathcal{U}$
Immediate.

Case: $\cdot \vdash_1 \mathit{unop}\{\mathcal{U}\}\, v_0 : \mathcal{U}$
- $\rhd_{\mathsf{E}}\ \delta(\mathit{unop}, v_0)$ if defined
- $\rhd_{\mathsf{E}}\ \mathsf{Err}$ otherwise

Case: $\cdot \vdash_1 \mathit{binop}\{\mathcal{U}\}\, v_0\, v_1 : \mathcal{U}$
- $\rhd_{\mathsf{E}}\ \delta(\mathit{binop}, v_0, v_1)$ if defined
- $\rhd_{\mathsf{E}}\ \mathsf{Err}$ otherwise

Case: $\cdot \vdash_1 \mathsf{app}\{\mathcal{U}\}\, v_0\, v_1 : \mathcal{U}$
- $\rhd_{\mathsf{E}}\ e_1[x_0 \leftarrow v_1]$
  if $v_0 = \lambda(x_0 : \tau_0).\, e_1$
- $\rhd_{\mathsf{E}}\ e_1[x_0 \leftarrow v_1]$
  if $v_0 = \lambda x_0.\, e_1$
- $\rhd_{\mathsf{E}}\ \mathsf{Err}$ otherwise

Case: $\cdot \vdash_1 \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 : \mathcal{U}$
- $\rhd_{\mathsf{E}}\ v_0$

Case: $\cdot \vdash_1 \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 : \mathcal{U}$
- $\rhd_{\mathsf{E}}\ v_0$

Case: $\cdot \vdash_1 \mathsf{Err} : \mathcal{U}$
Immediate.

□

Lemma A.44 (Erasure type preservation).
If $\cdot \vdash_0 e_0 : \mathcal{U}$ *and* $e_0 \vartriangleright_{\mathsf{E}} e_1$ *then* $\cdot \vdash_0 e_1 : \mathcal{U}$.

Proof. By case analysis of the reduction relation.

Case: $\mathit{unop}\{\tau_0\}\, v_0 \vartriangleright_{\mathsf{E}} \mathsf{BoundaryErr}\,(\emptyset, v_0)$
Immediate.

Case: $\mathit{unop}\{\mathcal{U}\}\, v_0 \vartriangleright_{\mathsf{E}} \mathsf{TagErr}$
Immediate.

Case: $\mathit{unop}\{{}^{\tau}\!/_{\mathcal{U}}\}\, v_0 \vartriangleright_{\mathsf{E}} \delta(\mathit{unop}, v_0)$
Immediate.

Case: $\mathit{binop}\{\tau_0\}\, v_0\, v_1 \vartriangleright_{\mathsf{E}} \mathsf{BoundaryErr}\,(\emptyset, v_0)$
Immediate.

Case: $\mathit{binop}\{\tau_0\}\, v_0\, v_1 \vartriangleright_{\mathsf{E}} \mathsf{BoundaryErr}\,(\emptyset, v_1)$
Immediate.

Case: $\mathit{binop}\{\mathcal{U}\}\, v_0\, v_1 \vartriangleright_{\mathsf{E}} \mathsf{TagErr}$
Immediate.

Case: $\mathit{binop}\{{}^{\tau}\!/_{\mathcal{U}}\}\, v_0\, v_1 \vartriangleright_{\mathsf{E}} \delta(\mathit{binop}, v_0, v_1)$
Immediate.

Case: $\mathsf{app}\{\tau_0\}\, v_0\, v_1 \vartriangleright_{\mathsf{E}} \mathsf{BoundaryErr}\,(\emptyset, v_0)$
Immediate.

Case: $\mathsf{app}\{\mathcal{U}\}\, v_0\, v_1 \vartriangleright_{\mathsf{E}} \mathsf{TagErr}$
Immediate.

Case: $\mathsf{app}\{{}^{\tau}\!/_{\mathcal{U}}\}\, (\lambda(x_0 : \tau_0).\, e_0)\, v_0 \vartriangleright_{\mathsf{E}} e_0[x_0 \leftarrow v_0]$
By a substitution lemma for the erased syntax.

Case: $\mathsf{app}\{{}^{\tau}\!/_{\mathcal{U}}\}\, (\lambda x_0.\, e_0)\, v_0 \vartriangleright_{\mathsf{E}} e_0[x_0 \leftarrow v_0]$
By a substitution lemma for the erased syntax.

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \vartriangleright_{\mathsf{E}} v_0$
Immediate.

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \vartriangleright_{\mathsf{E}} v_0$
Immediate.

□

Lemma A.45 ($A \lesssim E$).
There is a stuttering simulation between Amnesic and Erasure. More precisely, the following two results hold:

- *If* $e_0 \lesssim e_2$ *and* $e_0 \rightarrow_{\mathsf{A}} e_1$ *then* $\exists\, e_3, e_4$ *such that* $e_1 \rightarrow_{\mathsf{A}}^{*} e_3$ *and* $e_2 \rightarrow_{\mathsf{E}} e_4$ *and* $e_3 \lesssim e_4$.
- *If* $e_0 \lesssim e_2$ *and* $e_2 \rightarrow_{\mathsf{E}} e_3$ *then* $\exists\, e_1$ *and* $e_0 \rightarrow_{\mathsf{A}}^{*} e_1$ *and* $e_1 \lesssim e_4$

Proof. By lemma A.46 and lemma A.47. □

$\boxed{\mathrm{wfr}_{AE}(e_0, e_1)}$ holds for well-formed residuals of a common term; that is, pairs such that there exists an e_2 where $e_2 : {}^{\tau}/_{\mathcal{U}}\ \mathbf{wf}$ and $e_2 \rightarrow_{\mathsf{A}}^{*} e_0$ and $e_2 \rightarrow_{\mathsf{E}}^{*} e_1$

Lemma A.46.
If $\mathrm{wfr}_{AE}(e_0, e_2)$ *and* $e_0 \lesssim e_2$ *and* $e_0 \rightarrow_{\mathsf{A}} e_1$ *then* $\exists\, e_3, e_4$ *such that* $e_1 \rightarrow_{\mathsf{A}}^{*} e_3$ *and* $e_2 \rightarrow_{\mathsf{E}}^{*} e_4$ *and* $e_3 \lesssim e_4$.

Proof. By lemma A.48, lemma A.51, and case analysis of $\triangleright_{\mathsf{A}} \cup \blacktriangleright_{\mathsf{A}}$.

Case: $\mathit{unop}\{\tau_0\}\ v_0 \triangleright_{\mathsf{A}} \mathsf{InvariantErr}$
  Impossible, by type soundness
Case: $\mathit{unop}\{\tau_0\}\ v_0 \triangleright_{\mathsf{A}} \delta(\mathit{unop}, v_0)$
  (1) $e_2 \rightarrow_{\mathsf{E}} \delta(\mathit{unop}, v_1)$
    By $\lesssim$ on the redex
  (2) $\delta(\mathit{unop}, v_0) \lesssim \delta(\mathit{unop}, v_1)$
    By (1)
Case: $\mathsf{fst}\{\tau_0\}\ (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_0) \triangleright_{\mathsf{A}} \mathsf{dyn}\ b_0\ (\mathsf{fst}\{\mathcal{U}\}\ v_0)$
  Immediate, $\mathsf{dyn}\ b_0\ (\mathsf{fst}\{\mathcal{U}\}\ v_0) \lesssim e_2$
Case: $\mathsf{snd}\{\tau_0\}\ (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_0 \triangleright_{\mathsf{A}} \mathsf{dyn}\ b_0\ (\mathsf{snd}\{\mathcal{U}\}\ v_0)$
  Immediate, $\mathsf{dyn}\ b_0\ (\mathsf{fst}\{\mathcal{U}\}\ v_0) \lesssim e_2$
Case: $\mathit{binop}\{\tau_0\}\ v_0\ v_1 \triangleright_{\mathsf{A}} \mathsf{InvariantErr}$
  Impossible, by type soundness
Case: $\mathit{binop}\{\tau_0\}\ v_0\ v_1 \triangleright_{\mathsf{A}} \delta(\mathit{binop}, v_0, v_1)$
  (1) $e_2 \rightarrow_{\mathsf{E}} \delta(\mathit{binop}, v_2, v_3)$
    By $\lesssim$ on the redex
  (2) $\delta(\mathit{binop}, v_0, v_1) \lesssim \delta(\mathit{binop}, v_2, v_3)$
    By (1)
Case: $\mathsf{app}\{\tau_0\}\ v_0\ v_1 \triangleright_{\mathsf{A}} \mathsf{InvariantErr}$
  Impossible, by type soundness
Case: $\mathsf{app}\{\tau_0\}\ (\lambda(x_0 : \tau_1).\ e_5)\ v_0 \triangleright_{\mathsf{A}} e_5[x_0 \leftarrow v_0]$
  (1) $e_2 = \mathsf{app}\{\tau_0\}\ (\lambda(x_0 : \tau_1).\ e_6)\ v_1$
    By $\lesssim$ on the redex
  (2) $e_5[x_0 \leftarrow v_0] \lesssim e_6[x_0 \leftarrow v_1]$
Case: $\mathsf{app}\{\tau_0\}\ (\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_0)\ v_1 \triangleright_{\mathsf{A}} \mathsf{dyn}\ b_0\ (\mathsf{app}\{\mathcal{U}\}\ v_0\ (\mathsf{stat}\ b_1\ v_1))$
  (1) $e_1 = \mathsf{app}\{\tau_0\}\ v_2\ v_3$ where $(\mathbb{G}\ (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)\ v_0) \lesssim v_2$ and $v_1 \lesssim v_3$
    By $\lesssim$ on the redex
  (2) $\mathsf{stat}\ b_1\ v_1 \blacktriangleright_{\mathsf{A}} v_4$ and $v_4 \lesssim v_3$
    By type soundness
  (3) $\mathsf{dyn}\ b_0\ (\mathsf{app}\{\mathcal{U}\}\ v_0\ v_4) \lesssim \mathsf{app}\{\tau_0\}\ v_2\ v_3$
    By (1) and (2)
Case: $\mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0 \triangleright_{\mathsf{A}} \mathbb{G}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_0$
  (1) Either $e_2 = v_1$ or $e_2 = \mathsf{dyn}\ (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\ v_1$ and $e_2 \triangleright_{\mathsf{E}} v_1$
    By $\lesssim$ on the redex

(2) $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \lesssim v_1$

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\,(\mathbb{T}_?\,\overline{b}_0\; i_0) \rhd_{\mathsf{A}} i_0$

(1) Either $e_2 = v_1$ or $e_2 = \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_1$ and $e_2 \rhd_{\mathsf{E}} v_1$
By $\lesssim$ on the redex

(2) $i_0 \lesssim v_1$

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \rhd_{\mathsf{A}} \mathsf{BoundaryErr}\,((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\overline{b}_0, v_0)$
Immediate.

Case: $\mathit{unop}\{\mathcal{U}\}\; v_0 \blacktriangleright_{\mathsf{A}} \mathsf{TagErr}$

(1) $e_2 \rightarrow_{\mathsf{E}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
By $\lesssim$ on the redex

(2) $\mathsf{TagErr} \lesssim \mathsf{BoundaryErr}\,(\overline{b}, v)$

Case: $\mathit{unop}\{\mathcal{U}\}\; v_0 \blacktriangleright_{\mathsf{A}} \mathit{add\text{-}trace}\,(\mathit{get\text{-}trace}\,(v_0), \delta(\mathit{unop}, \mathit{rem\text{-}trace}\,(v_0)))$

(1) $e_2 \rightarrow_{\mathsf{E}} \delta(\mathit{unop}, v_1)$
By $\lesssim$ on the redex

(2) $\mathit{add\text{-}trace}\,(\mathit{get\text{-}trace}\,(v_0), \delta(\mathit{unop}, \mathit{rem\text{-}trace}\,(v_0))) \lesssim \delta(\mathit{unop}, v_1)$
By (1)

Case: $\mathsf{fst}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0)) \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\; b_0\,(\mathsf{fst}\{\tau_1\}\; v_0))$
Immediate, $\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\; b_0\,(\mathsf{fst}\{\tau_1\}\; v_0)) \lesssim e_2$

Case: $\mathsf{snd}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0)) \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\; b_0\,(\mathsf{snd}\{\tau_1\}\; v_0))$
Immediate, $\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\; b_0\,(\mathsf{snd}\{\tau_1\}\; v_0)) \lesssim e_2$

Case: $\mathit{binop}\{\mathcal{U}\}\; v_0\; v_1 \blacktriangleright_{\mathsf{A}} \mathsf{TagErr}$

(1) $e_2 \rightarrow_{\mathsf{E}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
By $\lesssim$ on the redex

(2) $\mathsf{TagErr} \lesssim \mathsf{BoundaryErr}\,(\overline{b}, v)$

Case: $\mathit{binop}\{\mathcal{U}\}\; v_0\; v_1 \blacktriangleright_{\mathsf{A}} \delta(\mathit{binop}, \mathit{rem\text{-}trace}\,(v_0), \mathit{rem\text{-}trace}\,(v_1))$

(1) $e_2 \rightarrow_{\mathsf{E}} \delta(\mathit{binop}, v_2, v_3)$
By $\lesssim$ on the redex

(2) $\delta(\mathit{binop}, \mathit{rem\text{-}trace}\,(v_0), \mathit{rem\text{-}trace}\,(v_1)) \lesssim \delta(\mathit{binop}, v_2, v_3)$
By (1)

Case: $\mathsf{app}\{\mathcal{U}\}\; v_0\; v_1 \blacktriangleright_{\mathsf{A}} \mathsf{TagErr}$

(1) $e_2 \rightarrow_{\mathsf{E}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
By $\lesssim$ on the redex

(2) $\mathsf{TagErr} \lesssim \mathsf{BoundaryErr}\,(\overline{b}, v)$

Case: $\mathsf{app}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\lambda x_0.\, e_5))\; v_0 \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,\overline{b}_0\,(e_5[x_0 \leftarrow v_1])$

(1) $e_2 = \mathsf{app}\{\mathit{tdyn}\}\,(\lambda x_0.\, e_6)\; v_1$
By $\lesssim$ on the redex

(2) $e_5[x_0 \leftarrow v_0] \lesssim e_6[x_0 \leftarrow v_1]$

Case: $\mathsf{app}\{\mathcal{U}\}\,(\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0))\; v_1 \blacktriangleright_{\mathsf{A}}$
$\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}\,(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathit{cod}\,(\tau_0)\}\; v_0\,(\mathsf{dyn}\,(\ell_1 \blacktriangleleft \mathit{dom}\,(\tau_0) \blacktriangleleft \ell_0)\; \mathit{add\text{-}trace}\,(\mathit{rev}\,(\overline{b}_0), v_1))))$

(1) $e_2 = \mathsf{app}\{\mathit{tdyn}\}\; v_2\; v_3$ and $(\mathbb{T}_?\,\overline{b}_0\,(\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0)) \lesssim v_2$ and $v_1 \lesssim v_3$
By $\lesssim$ on the redex

(2) $\mathsf{dyn}\,(\ell_1 \blacktriangleleft \mathit{dom}\,(\tau_0) \blacktriangleleft \ell_0)\; \mathit{add\text{-}trace}\,(\mathit{rev}\,(\overline{b}_0), v_1)$ steps to either a boundary error or to v_4 where $v_4 \lesssim v_3$
By (1)

(3) $\mathsf{trace}\,\overline{b}_0\,(\mathsf{stat}\,(\ell_0 \blacktriangleleft \mathit{cod}\,(\tau_0) \blacktriangleleft \ell_1)\,(\mathsf{app}\{\mathit{cod}\,(\tau_0)\}\; v_0\; v_4)) \lesssim \mathsf{app}\{\mathcal{U}\}\; v_2\; v_3$

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \blacktriangleright_{\mathsf{A}} \mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0$

(1) Either $e_1 = v_1$ or $e_1 = \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_1$ and $e_1 \rhd_{\mathsf{E}} v_1$
By $\lesssim$ on the redex
(2) $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \lesssim v_1$

Case: $\mathsf{stat}\; b_0\; (\mathbb{G}\; b_1\; (\mathbb{T}_?\; \overline{b}_0\; v_0)) \blacktriangleright_{\mathsf{A}} \mathsf{trace}\,(b_0 b_1 \overline{b}_0)\; v_0$
(1) Either $e_1 = v_1$ or $e_1 = \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_1$ and $e_1 \rhd_{\mathsf{E}} v_1$
By $\lesssim$ on the redex
(2) $\mathbb{G}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \lesssim v_1$

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; i_0 \blacktriangleright_{\mathsf{A}} i_0$
(1) Either $e_1 = v_1$ or $e_1 = \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_1$ and $e_1 \rhd_{\mathsf{E}} v_1$
By $\lesssim$ on the redex
(2) $i_0 \lesssim v_1$

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\; v_0 \blacktriangleright_{\mathsf{A}} \mathsf{InvariantErr}$
Impossible, by type soundness

Case: $\mathsf{trace}\; \overline{b}_0\; v_0 \blacktriangleright_{\mathsf{A}} v_1$
Immediate, $v_1 \lesssim e_2$

□

Lemma A.47.
If $\mathrm{wfr}_{AE}(e_0, e_2)$ *and* $e_0 \lesssim e_2$ *and* $e_2 \rightarrow_{\mathsf{E}} e_3$ *then* $\exists\, e_1$ *and* $e_0 \rightarrow^*_{\mathsf{A}} e_1$ *and* $e_1 \lesssim e_4$

Proof. By lemma A.48, lemma A.51, and case analysis of $\rhd_{\mathsf{E}}$.

Case: $unop\{\tau_0\}\, v_0 \rhd_{\mathsf{E}}$ $\mathsf{BoundaryErr}\,(\emptyset, v_0)$
1. Either $e_0 \rightarrow^*_{\mathsf{A}} unop\{\tau_0\}\, v_1$ or $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
   By $\lesssim$ on the redex
2. $v_1 \notin \langle v, v\rangle \cup (\mathbb{G}\,(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell)\; v)$
   By $\lesssim$ on the redex and (1)
3. But (2) is impossible by type soundness. Amnesic must raise a boundary error earlier.

Case: $unop\{\mathcal{U}\}\, v_0 \rhd_{\mathsf{E}}$ TagErr
1. Either $e_0 \rightarrow^*_{\mathsf{A}} unop\{\tau_0\}\, v_1$ or $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
   By $\lesssim$ on the redex (e_0 is either a unop or a trace expression)
2. $v_1 \notin \langle v, v\rangle \cup (\mathbb{G}\,(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell)\; v)$
   By $\lesssim$ on the redex and (1)
3. $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $unop\{{}^{\tau}\!/_{\mathcal{U}}\}\, v_0 \rhd_{\mathsf{E}} \delta(unop, v_0)$
1. Either $e_0 \rightarrow^*_{\mathsf{A}} unop\{\tau_0\}\, v_1$ or $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
   By $\lesssim$ on the redex (e_0 is either a unop or a trace expression)
2. $unop\{\tau_0\}\, v_1 \rightarrow^*_{\mathsf{A}} E_2[unop\{\tau_0\}\, \langle v_2, v_3\rangle]$ and E_2 contains only trace expressions and boundaries
   By $\rightarrow^*_{\mathsf{A}}$
3. Either $E_2[unop\{\tau_0\}\, \langle v_2, v_3\rangle] \rightarrow^*_{\mathsf{A}} v_4$ where $v_4 \lesssim \delta(unop, v_0)$ or $E_2[unop\{\tau_0\}\, \langle v_2, v_3\rangle] \rightarrow^*_{\mathsf{A}}$ $\mathsf{BoundaryErr}\,(\overline{b}, v)$

Case: $binop\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{E}}$ $\mathsf{BoundaryErr}\,(\emptyset, v_0)$
1. $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
   By type soundness

Case: $binop\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{E}}$ $\mathsf{BoundaryErr}\,(\emptyset, v_1)$
1. $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
   By type soundness

Case: $binop\{\mathcal{U}\}\, v_0\, v_1 \rhd_{\mathsf{E}}$ TagErr
1. Either $e_0 \rightarrow^*_{\mathsf{A}} binop\{\mathcal{U}\}\, v_2\, v_3$ or $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
   By $\lesssim$ on the redex (e_0 is either a binop or a trace expression)
2. $\mathsf{TagErr} \lesssim \mathsf{BoundaryErr}\,(\overline{b}, v)$

Case: $binop\{{}^{\tau}\!/_{\mathcal{U}}\}\, v_0\, v_1 \rhd_{\mathsf{E}} \delta(binop, v_0, v_1)$
1. Either $e_0 \rightarrow^*_{\mathsf{A}} binop\{{}^{\tau}\!/_{\mathcal{U}}\}\, v_2\, v_3$ or $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
   By $\lesssim$ on the redex (e_0 is either a binop or a trace expression)
2. $\delta(binop, v_2, v_3) \lesssim \delta(binop, v_0, v_1)$

Case: $\mathsf{app}\{\tau_0\}\, v_0\, v_1 \rhd_{\mathsf{E}}$ $\mathsf{BoundaryErr}\,(\emptyset, v_0)$
1. $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
   By type soundness

Case: $\mathsf{app}\{\mathcal{U}\}\, v_0\, v_1 \rhd_{\mathsf{E}}$ TagErr
1. Either $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{TagErr}$ or $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\overline{b}, v)$
   By $\lesssim$ on the redex
2. $\mathsf{TagErr} \lesssim \mathsf{TagErr}$

Case: $\mathsf{app}\{\tau_0\}\, (\lambda(x_0 : \tau_0).\, e_0)\, v_0 \rhd_{\mathsf{E}} e_0[x_0 \leftarrow v_0]$

(1) Either $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{app}\{\tau_0\}\, v_1\, v_2$ or $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\bar{b}, v)$
By $\lesssim$ on the redex
(2) $e_0 \rightarrow^*_{\mathsf{A}} E_2[\mathsf{app}\{\tau_0\}\,(\lambda(x_0 : \tau_0).\, e_1)\, E_3[v_2]]$ and both E_2 and E_3 contain only trace expressions and boundaries
(3) Either $E_3[v_2] \rightarrow^*_{\mathsf{A}} v_4$ where $v_4 \lesssim v_0$ or $E_3[v_2] \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\bar{b}, v)$
(4) $E_2[e_1[x_0 \leftarrow v_4]] \lesssim e_0[x_0 \leftarrow v_0]$

Case: $\mathsf{app}\{\mathcal{U}\}\,(\lambda(x_0 : \tau_0).\, e_0)\, v_0 \rhd_{\mathsf{E}} e_0[x_0 \leftarrow v_0]$
(1) Either $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{app}\{\tau_0\}\, v_1\, v_2$ or $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\bar{b}, v)$
By $\lesssim$ on the redex
(2) $e_0 \rightarrow^*_{\mathsf{A}} E_2[\mathsf{app}\{\tau_0\}\,(\lambda(x_0 : \tau_0).\, e_1)\, E_3[v_2]]$ and both E_2 and E_3 contain only trace expressions and boundaries
(3) Either $E_3[v_2] \rightarrow^*_{\mathsf{A}} v_4$ where $v_4 \lesssim v_0$ or $E_3[v_2] \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\bar{b}, v)$
(4) $E_2[e_1[x_0 \leftarrow v_4]] \lesssim e_0[x_0 \leftarrow v_0]$

Case: $\mathsf{app}\{\tau_0\}\,(\lambda x_0.\, e_0)\, v_0 \rhd_{\mathsf{E}} e_0[x_0 \leftarrow v_0]$
(1) Either $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{app}\{\tau_0\}\, v_1\, v_2$ or $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\bar{b}, v)$
By $\lesssim$ on the redex
(2) $e_0 \rightarrow^*_{\mathsf{A}} E_2[\mathsf{app}\{\tau_0\}\,(\lambda x_0.\, e_1)\, E_3[v_2]]$ and both E_2 and E_3 contain only trace expressions and boundaries
(3) Either $E_3[v_2] \rightarrow^*_{\mathsf{A}} v_4$ where $v_4 \lesssim v_0$ or $E_3[v_2] \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\bar{b}, v)$
(4) $E_2[e_1[x_0 \leftarrow v_4]] \lesssim e_0[x_0 \leftarrow v_0]$

Case: $\mathsf{app}\{\mathcal{U}\}\,(\lambda x_0.\, e_0)\, v_0 \rhd_{\mathsf{E}} e_0[x_0 \leftarrow v_0]$
(1) Either $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{app}\{\tau_0\}\, v_1\, v_2$ or $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\bar{b}, v)$
By $\lesssim$ on the redex
(2) $e_0 \rightarrow^*_{\mathsf{A}} E_2[\mathsf{app}\{\tau_0\}\,(\lambda x_0.\, e_1)\, E_3[v_2]]$ and both E_2 and E_3 contain only trace expressions and boundaries
(3) Either $E_3[v_2] \rightarrow^*_{\mathsf{A}} v_4$ where $v_4 \lesssim v_0$ or $E_3[v_2] \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\bar{b}, v)$
(4) $E_2[e_1[x_0 \leftarrow v_4]] \lesssim e_0[x_0 \leftarrow v_0]$

Case: $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \rhd_{\mathsf{E}} v_0$
(1) Either $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1$ or $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\bar{b}, v)$
(2) Either $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1 \rightarrow^*_{\mathsf{A}} v_2$ or $\mathsf{dyn}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\bar{b}, v)$
(3) $v_2 \lesssim v_0$

Case: $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_0 \rhd_{\mathsf{E}} v_0$
(1) Either $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1$ or $e_0 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\bar{b}, v)$
(2) Either $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1 \rightarrow^*_{\mathsf{A}} v_2$ or $\mathsf{stat}\,(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\, v_1 \rightarrow^*_{\mathsf{A}} \mathsf{BoundaryErr}\,(\bar{b}, v)$
(3) $v_2 \lesssim v_0$

□

LEMMA A.48.
If $\mathrm{wfr}_{AE}(e_0, e_1)$ *and* $e_0 \lesssim e_1$ *and either* $e_0 \rightarrow_{\mathsf{A}} e_2$ *or* $e_1 \rightarrow_{\mathsf{E}} e_3$ *then the following results hold:*

- $e_0 = E_0[e_4]$
- $e_1 = E_1[e_5]$
- $E_0 \lesssim E_1$
- $e_4 \lesssim e_5$.

PROOF. By lemma A.49 and lemma A.50. □

Lemma A.49.
If $\mathrm{wfr}_{AE}(E_0[e_0], e_1)$ *and* $E_0[e_0] \lesssim e_1$ *and* $e_0(\rhd_{\mathsf{A}} \cup \blacktriangleright_{\mathsf{A}})e_2$ *then the following results hold:*

- $e_1 = E_1[e_3]$
- $E_0 \lesssim E_1$
- $e_0 \lesssim e_3$.

Proof. By induction on $E_0[e_0] \lesssim e_1$, proceeding by case analysis of $E_0[e_0]$. □

Lemma A.50.
If $\mathrm{wfr}_{AE}(e_0, E_1[e_1])$ *and* $e_0 \lesssim E_1[e_1]$ *and* $e_1 \rhd_{\mathsf{E}} e_3$ *then the following results hold:*

- $e_0 = E_0[e_2]$
- $E_0 \lesssim E_1$
- $e_2 \lesssim e_1$.

Proof. By induction on $e_0 \lesssim E_1[e_1]$, proceeding by case analysis of $E_1[e_1]$. □

Lemma A.51.
If $E_0 \lesssim E_1$ *and* $e_2 \lesssim e_3$ *then* $E_0[e_2] \lesssim E_1[e_3]$.

Proof. By induction on $E_0 \lesssim E_1$. □