

# 1 Typed–Untyped Interactions: A Comparative Analysis 2 (Supplementary Material) 3

4 BEN GREENMAN\*, PLT @ Brown University, USA

5 CHRISTOS DIMOULAS, PLT @ Northwestern University, USA

6 MATTHIAS FELLEISEN, PLT @ Northeastern University, USA  
7

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

## 10 ACM Reference Format:

11 Ben Greenman, Christos Dimoulas, and Matthias Felleisen. 2022. Typed–Untyped Interactions: A Comparative  
12 Analysis (Supplementary Material). *ACM Trans. Program. Lang. Syst.* 1, 1 (November 2022), 143 pages. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>  
13  
14

## 15 CONTENTS

|    |                                              |     |
|----|----------------------------------------------|-----|
| 16 | Abstract                                     | 1   |
| 17 | Contents                                     | 1   |
| 18 | 6 Technical Development                      | 2   |
| 19 | 6.1 Surface Language, Types, and Ownership   | 2   |
| 20 | 6.2 Three Evaluation Languages               | 5   |
| 21 | 6.3 Properties of Interest                   | 15  |
| 22 | 6.4 Common Higher-Order Notions of Reduction | 16  |
| 23 | 6.5 Natural and its Properties               | 17  |
| 24 | 6.6 Co-Natural and its Properties            | 23  |
| 25 | 6.7 Forgetful and its Properties             | 31  |
| 26 | 6.8 Transient and its Properties             | 40  |
| 27 | 6.9 Amnesic and its Properties               | 46  |
| 28 | 6.10 Erasure and its Properties              | 58  |
| 29 | A Proofs                                     | 64  |
| 30 | A.1 Natural                                  | 64  |
| 31 | A.2 Co-Natural                               | 71  |
| 32 | A.3 Forgetful                                | 87  |
| 33 | A.4 Transient                                | 105 |
| 34 | A.5 Amnesic                                  | 109 |
| 35 | A.6 Erasure                                  | 136 |
| 36 |                                              |     |

37 \*Research completed at Northeastern University prior to joining Brown

38  
39 Authors' addresses: Ben Greenman, PLT @ Brown University, Providence, Rhode Island, USA, [benjaminlgreenman@gmail.com](mailto:benjaminlgreenman@gmail.com);  
40 Christos Dimoulas, PLT @ Northwestern University, Evanston, Illinois, USA, [chrdimo@northwestern.edu](mailto:chrdimo@northwestern.edu); Matthias  
41 Felleisen, PLT @ Northeastern University, Boston, Massachusetts, USA, [matthias@ccs.neu.edu](mailto:matthias@ccs.neu.edu).

42 Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee  
43 provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and  
44 the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored.  
45 Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires  
46 prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

47 © 2022 Association for Computing Machinery.

48 0164-0925/2022/11-ART \$15.00

49 <https://doi.org/10.1145/nnnnnnn.nnnnnnn>

## 6 TECHNICAL DEVELOPMENT

### 6.1 Surface Language, Types, and Ownership

#### Surface Syntax

$e = x \mid i \mid n \mid \langle e, e \rangle \mid \lambda x. e \mid \lambda(x : \tau). e \mid \text{app}\{\tau/\mathcal{U}\} e e \mid \text{unop}\{\tau/\mathcal{U}\} e \mid \text{binop}\{\tau/\mathcal{U}\} e e \mid \text{dyn } b e \mid \text{stat } b e$

$\tau = \text{Int} \mid \text{Nat} \mid \tau \Rightarrow \tau \mid \tau \times \tau$

$\tau/\mathcal{U} = \tau \mid \mathcal{U}$

$\Gamma = \cdot \mid (x : \tau/\mathcal{U}), \Gamma$

$b = (\ell \blacktriangleleft \tau \blacktriangleright \ell)$

$\ell = \text{countable set of names}$

$\text{unop} = \text{fst} \mid \text{snd}$

$\text{binop} = \text{sum} \mid \text{quotient}$

$i = \mathbb{Z}$

$n = \mathbb{N}$

$\Delta : \text{unop} \times \tau \longrightarrow \tau$

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

$\Delta : \text{binop} \times \tau \times \tau \longrightarrow \tau$

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

99  $\Gamma \vdash e : \tau$

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

$$\frac{\Gamma_0 \vdash e_0 : \tau_0 \quad \Gamma_0 \vdash e_1 : \tau_1}{\Gamma_0 \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma_0 \vdash e_0 : \tau_1 \quad \Delta(\text{unop}, \tau_1) \leq \tau_0}{\Gamma_0 \vdash \text{unop}\{\tau_0\} e_0 : \tau_0}$$

$$\frac{\Gamma_0 \vdash e_0 : \tau_1 \quad \Gamma_0 \vdash e_1 : \tau_2 \quad \Delta(\text{binop}, \tau_1, \tau_2) \leq \tau_0}{\Gamma_0 \vdash \text{binop}\{\tau_0\} e_0 e_1 : \tau_0}$$

$$\frac{\Gamma_0 \vdash e_0 : \tau_1 \Rightarrow \tau_2 \quad \Gamma_0 \vdash e_1 : \tau_1 \quad \tau_2 \leq \tau_0}{\Gamma_0 \vdash \text{app}\{\tau_0\} e_0 e_1 : \tau_0} \quad \frac{\Gamma_0 \vdash e_0 : \mathcal{U}}{\Gamma_0 \vdash \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) e_0 : \tau_0}$$

$$\frac{\Gamma_0 \vdash e_0 : \tau_1 \quad \tau_1 \leq \tau_0}{\Gamma_0 \vdash e_0 : \tau_0}$$

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

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

$$\frac{\Gamma_0 \vdash e_0 : \mathcal{U}}{\Gamma_0 \vdash \text{unop}\{\mathcal{U}\} e_0 : \mathcal{U}} \quad \frac{\Gamma_0 \vdash e_0 : \mathcal{U} \quad \Gamma_0 \vdash e_1 : \mathcal{U}}{\Gamma_0 \vdash \text{binop}\{\mathcal{U}\} e_0 e_1 : \mathcal{U}} \quad \frac{\Gamma_0 \vdash e_0 : \mathcal{U} \quad \Gamma_0 \vdash e_1 : \mathcal{U}}{\Gamma_0 \vdash \text{app}\{\mathcal{U}\} e_0 e_1 : \mathcal{U}}$$

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

127  $\tau \leq \tau$

$$\frac{}{\text{Nat} \leq \text{Int}} \quad \frac{\tau_0 \leq \tau_2 \quad \tau_1 \leq \tau_3}{\tau_0 \times \tau_1 \leq \tau_2 \times \tau_3} \quad \frac{\tau_2 \leq \tau_0 \quad \tau_1 \leq \tau_3}{\tau_0 \Rightarrow \tau_1 \leq \tau_2 \Rightarrow \tau_3} \quad \frac{}{\tau_0 \leq \tau_0}$$

132  $b \leq b$

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

148 **Ownership Syntax**

149  $e = x \mid i \mid n \mid \langle e, e \rangle \mid \lambda x. e \mid \lambda(x : \tau). e \mid \text{app}\{\tau/\mathcal{U}\} e e \mid \text{unop}\{\tau/\mathcal{U}\} e \mid \text{binop}\{\tau/\mathcal{U}\} e e \mid$   
 150  $\text{dyn } b(e)^\ell \mid \text{stat } b(e)^\ell \mid (e)^\ell$

151  $\ell = \text{countable set}$

152  $\mathcal{L} = \cdot \mid (x : \ell), \mathcal{L}$

153  **$e : \tau/\mathcal{U}$  wf**

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

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

156  **$\Gamma \vdash e : \tau$**  additional rules for the ownership syntax

157

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

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

159

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

160  **$\mathcal{L}; \ell \Vdash e$**

161

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

162

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

163

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

164

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

## 6.2 Three Evaluation Languages

### Common Evaluation Syntax

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

$\lfloor \cdot \rfloor : \tau \rightarrow s$

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

$\text{shape-match} : s \times v \rightarrow \mathcal{B}$

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

$\delta : \text{unop} \times v \rightarrow v$

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

$\delta : \text{binop} \times v \times v \rightarrow v$

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

$\text{fst} : \tau \times \tau \rightarrow \tau$

$\text{fst}(\tau_0 \times \tau_1) = \tau_0$

$\text{snd} : \tau \times \tau \rightarrow \tau$

$\text{snd}(\tau_0 \times \tau_1) = \tau_1$

$\text{dom} : \tau \Rightarrow \tau \rightarrow \tau$

$\text{dom}(\tau_0 \Rightarrow \tau_1) = \tau_0$

$\text{cod} : \tau \Rightarrow \tau \rightarrow \tau$

$\text{cod}(\tau_0 \Rightarrow \tau_1) = \tau_1$

LEMMA 6.1 (UNIQUE DECOMPOSITION). *For all  $e_0$  one of the following holds:*

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

PROOF SKETCH. By induction on the structure of  $e_0$ . □

LEMMA 6.2 ( $\delta$  COMPATIBILITY).

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

PROOF SKETCH. By case analysis of  $\delta$ . □

### Ownership Evaluation Syntax

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

$$\text{rev} : B \longrightarrow B$$

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

$$\text{rev} : \bar{\ell} \longrightarrow \bar{\ell}$$

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

$$\text{senders} : B \longrightarrow L$$

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

$$\text{owners} : v \longrightarrow \bar{\ell}$$

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

$$((e_0))^{\ell_n \cdots \ell_1} = e_1 \iff e_1 = (\cdots (e_0)^{\ell_n} \cdots)^{\ell_1}$$

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

## Higher-Order Evaluation Syntax

$e = x \mid i \mid n \mid \langle e, e \rangle \mid \lambda x. e \mid \lambda(x : \tau). e \mid \text{app}\{\tau/\mathcal{U}\} e e \mid \text{unop}\{\tau/\mathcal{U}\} e \mid \text{binop}\{\tau/\mathcal{U}\} e e \mid$   
 $\text{dyn } b e \mid \text{stat } b e \mid \text{trace } \bar{b} e \mid \text{Err}$   
 $v = i \mid n \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x : \tau). e \mid \mathbb{G}(\ell \blacktriangleleft \tau \Rightarrow \tau \blacktriangleleft \ell) v \mid \mathbb{G}(\ell \blacktriangleleft \tau \times \tau \blacktriangleleft \ell) v \mid \mathbb{T} \bar{b} v$   
 $\text{Err} = \text{InvariantErr} \mid \text{TagErr} \mid \text{BoundaryErr}(\bar{b}, v) \mid \text{DivErr}$

 $\Gamma \vdash_1 e : \tau$ 

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

$$\frac{\Gamma_0 \vdash_1 e_0 : \tau_0 \quad \Gamma_0 \vdash_1 e_1 : \tau_1}{\Gamma_0 \vdash_1 \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma_0 \vdash_1 e_0 : \tau_1 \quad \Delta(\text{unop}, \tau_1) \leq \tau_0}{\Gamma_0 \vdash_1 \text{unop}\{\tau_0\} e_0 : \tau_0}$$

$$\frac{\Gamma_0 \vdash_1 e_0 : \tau_1 \quad \Gamma_0 \vdash_1 e_1 : \tau_2 \quad \Delta(\text{binop}, \tau_1, \tau_2) \leq \tau_0}{\Gamma_0 \vdash_1 \text{binop}\{\tau_0\} e_0 e_1 : \tau_0}$$

$$\frac{\Gamma_0 \vdash_1 e_0 : \tau_1 \Rightarrow \tau_2 \quad \Gamma_0 \vdash_1 e_1 : \tau_1 \quad \tau_2 \leq \tau_0}{\Gamma_0 \vdash_1 \text{app}\{\tau_0\} e_0 e_1 : \tau_0} \quad \frac{\Gamma_0 \vdash_1 e_0 : \mathcal{U}}{\Gamma_0 \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) e_0 : \tau_0}$$

$$\frac{\Gamma_0 \vdash_1 e_0 : \tau_1 \quad \tau_1 \leq \tau_0}{\Gamma_0 \vdash_1 e_0 : \tau_0} \quad \frac{\Gamma_0 \vdash_1 v_0 : \mathcal{U}}{\Gamma_0 \vdash_1 \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 : \tau_0} \quad \frac{}{\Gamma_0 \vdash_1 \text{Err} : \tau_0}$$
 $\Gamma \vdash_1 e : \mathcal{U}$ 

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

$$\frac{\Gamma_0 \vdash_1 e_0 : \mathcal{U}}{\Gamma_0 \vdash_1 \text{unop}\{\mathcal{U}\} e_0 : \mathcal{U}} \quad \frac{\Gamma_0 \vdash_1 e_0 : \mathcal{U} \quad \Gamma_0 \vdash_1 e_1 : \mathcal{U}}{\Gamma_0 \vdash_1 \text{binop}\{\mathcal{U}\} e_0 e_1 : \mathcal{U}} \quad \frac{\Gamma_0 \vdash_1 e_0 : \mathcal{U} \quad \Gamma_0 \vdash_1 e_1 : \mathcal{U}}{\Gamma_0 \vdash_1 \text{app}\{\mathcal{U}\} e_0 e_1 : \mathcal{U}}$$

$$\frac{\Gamma_0 \vdash_1 e_0 : \tau_0}{\Gamma_0 \vdash_1 \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) e_0 : \mathcal{U}} \quad \frac{\Gamma_0 \vdash_1 v_0 : \tau_0}{\Gamma_0 \vdash_1 \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 : \mathcal{U}} \quad \frac{\Gamma_0 \vdash_1 v_0 : \mathcal{U}}{\Gamma_0 \vdash_1 \mathbb{T} \bar{b}_0 v_0 : \mathcal{U}}$$

$$\frac{\Gamma_0 \vdash_1 e_0 : \mathcal{U}}{\Gamma_0 \vdash_1 \text{trace } \bar{b}_0 e_0 : \mathcal{U}} \quad \frac{}{\Gamma_0 \vdash_1 \text{Err} : \mathcal{U}}$$

## Higher-Order Evaluation Syntax, with Ownership

$e = x \mid i \mid n \mid \langle e, e \rangle \mid \lambda x. e \mid \lambda(x : \tau). e \mid \text{app}\{\tau/\mathcal{U}\} e e \mid \text{unop}\{\tau/\mathcal{U}\} e \mid \text{binop}\{\tau/\mathcal{U}\} e e \mid$   
 $\text{dyn } b (e)^\ell \mid \text{stat } b (e)^\ell \mid \text{trace } \bar{b} e \mid (e)^\ell \mid \text{Err}$   
 $v = i \mid n \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x : \tau). e \mid \mathbb{G} b (v)^\ell \mid \mathbb{T} \bar{b} v \mid (v)^\ell$

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

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

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

$$\frac{\mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \text{unop}\{\tau/\mathcal{U}\} e_0} \quad \frac{\mathcal{L}_0; \ell_0 \Vdash e_0 \quad \mathcal{L}_0; \ell_0 \Vdash e_1}{\mathcal{L}_0; \ell_0 \Vdash \text{binop}\{\tau/\mathcal{U}\} e_0 e_1} \quad \frac{\mathcal{L}_0; \ell_0 \Vdash e_0 \quad \mathcal{L}_0; \ell_0 \Vdash e_1}{\mathcal{L}_0; \ell_0 \Vdash \text{app}\{\tau/\mathcal{U}\} e_0 e_1}$$

$$\frac{\mathcal{L}_0; \ell_1 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) e_0} \quad \frac{\mathcal{L}_0; \ell_1 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) e_0} \quad \frac{\mathcal{L}_0; \ell_0 \Vdash v_0}{\mathcal{L}_0; \ell_0 \Vdash \mathbb{T} \bar{b}_0 v_0}$$

$$\frac{\mathcal{L}_0; \ell_0 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \text{trace } \bar{b}_0 e_0} \quad \frac{}{\mathcal{L}_0; \ell_0 \Vdash \text{Err}}$$

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

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

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

$$\frac{\mathcal{L}_0; \ell_0 \Vdash_p e_0}{\mathcal{L}_0; \ell_0 \Vdash_p \text{unop}\{\tau/\mathcal{U}\} e_0} \quad \frac{\mathcal{L}_0; \ell_0 \Vdash_p e_0 \quad \mathcal{L}_0; \ell_0 \Vdash_p e_1}{\mathcal{L}_0; \ell_0 \Vdash_p \text{binop}\{\tau/\mathcal{U}\} e_0 e_1} \quad \frac{\mathcal{L}_0; \ell_0 \Vdash_p e_0 \quad \mathcal{L}_0; \ell_0 \Vdash_p e_1}{\mathcal{L}_0; \ell_0 \Vdash_p \text{app}\{\tau/\mathcal{U}\} e_0 e_1}$$

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

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

$$\frac{\bar{b}_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \cdots (\ell_{n-1} \blacktriangleleft \tau_{n-1} \blacktriangleleft \ell_n) \quad \mathcal{L}_0; \ell_n \Vdash_p e_0}{\mathcal{L}_0; \ell_0 \Vdash_p (\text{trace } \bar{b}_0 ((e_0))^{\ell_n \cdots \ell_1})^{\ell_0}} \quad \frac{}{\mathcal{L}_0; \ell_0 \Vdash_p \text{Err}}$$



393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441

LEMMA 6.3 (HIGHER-ORDER INITIALIZATION).

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

## First-Order Evaluation Syntax

$$e = x \mid i \mid n \mid \lambda x. e \mid \lambda(x : \tau). e \mid \langle e, e \rangle \mid \text{app}\{\tau/\mathcal{U}\} e e \mid \text{unop}\{\tau/\mathcal{U}\} e \mid \text{binop}\{\tau/\mathcal{U}\} e e \mid \text{dyn } b e \mid \text{stat } b e \mid p \mid \text{check}\{\tau/\mathcal{U}\} e p \mid \text{Err}$$

$$v = i \mid n \mid p$$

$$w = \lambda x. e \mid \lambda(x : \tau). e \mid \langle v, v \rangle$$

$$p = \text{countable set of heap locations}$$

$$\text{Err} = \text{InvariantErr} \mid \text{TagErr} \mid \text{BoundaryErr}(b^*, v) \mid \text{DivErr}$$

$$\mathcal{H} = \mathcal{P}((p \mapsto w))$$

$$\mathcal{B} = \mathcal{P}((p \mapsto b^*))$$

$$\mathcal{T} = \cdot \mid (p : s), \mathcal{T}$$

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

$$\mathcal{H}_0(v_0) = \begin{cases} w_0 & \text{if } v_0 \in p \text{ and } (v_0 \mapsto w_0) \in \mathcal{H}_0 \\ v_0 & \text{if } v_0 \notin p \end{cases}$$

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

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

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

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

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

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

$$\mathcal{T}; \Gamma \vdash_s e; \mathcal{H}; \mathcal{B} : s$$

$$\frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : s_0 \quad \mathcal{T}_0 \vdash_s \mathcal{H}_0}{\mathcal{T}_0; \Gamma_0 \vdash_s e_0; \mathcal{H}_0; \mathcal{B}_0 : s_0}$$

$$\mathcal{T}; \Gamma \vdash_s e; \mathcal{H}; \mathcal{B} : \mathcal{U}$$

$$\frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : \mathcal{U} \quad \mathcal{T}_0 \vdash_s \mathcal{H}_0}{\mathcal{T}_0; \Gamma_0 \vdash_s e_0; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}}$$

$$\mathcal{T} \vdash_s \mathcal{H}$$

$$\frac{\forall (p_0 \mapsto v_0) \in \mathcal{H}_0. \forall (p_0 \mapsto s_0) \in \mathcal{T}_0. \mathcal{T}_0; \cdot \vdash_s v_0 : s_0}{\mathcal{T}_0 \vdash_s \mathcal{H}_0}$$

491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539

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

$$\frac{(p_0 : s_0) \in \mathcal{T}_0}{\mathcal{T}_0; \Gamma_0 \vdash_s p_0 : s_0} \quad \frac{(x_0 : \tau_0) \in \Gamma_0}{\mathcal{T}_0; \Gamma_0 \vdash_s x_0 : \lfloor \tau_0 \rfloor} \quad \frac{}{\mathcal{T}_0; \Gamma_0 \vdash_s i_0 : \text{Int}} \quad \frac{}{\mathcal{T}_0; \Gamma_0 \vdash_s n_0 : \text{Nat}}$$

$$\frac{\mathcal{T}_0; (x_0 : \mathcal{U}), \Gamma_0 \vdash_s e_0 : \mathcal{U}}{\mathcal{T}_0; \Gamma_0 \vdash_s \lambda x_0. e_0 : \text{Fun}} \quad \frac{\mathcal{T}_0; (x_0 : \tau_0), \Gamma_0 \vdash_s e_0 : s_0}{\mathcal{T}_0; \Gamma_0 \vdash_s \lambda(x_0 : \tau_0). e_0 : \text{Fun}} \quad \frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : s_0 \quad \mathcal{T}_0; \Gamma_0 \vdash_s e_1 : s_1}{\mathcal{T}_0; \Gamma_0 \vdash_s \langle e_0, e_1 \rangle : \text{Pair}}$$

$$\frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : \text{Fun} \quad \mathcal{T}_0; \Gamma_0 \vdash_s e_1 : s_0}{\mathcal{T}_0; \Gamma_0 \vdash_s \text{app}\{\tau_0\} e_0 e_1 : \lfloor \tau_0 \rfloor} \quad \frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : \text{Pair}}{\mathcal{T}_0; \Gamma_0 \vdash_s \text{unop}\{\tau_0\} e_0 : \lfloor \tau_0 \rfloor}$$

$$\frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : s_0 \quad \mathcal{T}_0; \Gamma_0 \vdash_s e_0 : s_1 \quad \Delta(\text{binop}, s_0, s_1) = \tau_1 \quad \tau_1 \leq s_0}{\mathcal{T}_0; \Gamma_0 \vdash_s \text{binop}\{\tau_0\} e_0 e_1 : \lfloor \tau_0 \rfloor}$$

$$\frac{\mathcal{T}_0; \Gamma_0 \vdash e_0 : \mathcal{U}}{\mathcal{T}_0; \Gamma_0 \vdash \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) e_0 : \lfloor \tau_0 \rfloor} \quad \frac{\mathcal{T}_0; \Gamma_0 \vdash e_0 : \mathcal{U}}{\mathcal{T}_0; \Gamma_0 \vdash_s \text{check}\{\tau_0\} e_0 p_0 : \lfloor \tau_0 \rfloor}$$

$$\frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : s_0}{\mathcal{T}_0; \Gamma_0 \vdash_s \text{check}\{\tau_0\} e_0 p_0 : \lfloor \tau_0 \rfloor} \quad \frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : s_1 \quad s_1 \leq s_0}{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : s_0} \quad \frac{}{\mathcal{T}_0; \Gamma_0 \vdash_s \text{Err} : s_0}$$

$$\boxed{\mathcal{T}; \Gamma \vdash_s e : \mathcal{U}}$$

$$\frac{(p_0 : s_0) \in \mathcal{T}_0}{\mathcal{T}_0; \Gamma_0 \vdash_s p_0 : \mathcal{U}} \quad \frac{(x_0 : \mathcal{U}) \in \Gamma_0}{\mathcal{T}_0; \Gamma_0 \vdash_s x_0 : \mathcal{U}} \quad \frac{}{\mathcal{T}_0; \Gamma_0 \vdash_s i_0 : \mathcal{U}} \quad \frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : \mathcal{U} \quad \mathcal{T}_0; \Gamma_0 \vdash_s e_1 : \mathcal{U}}{\mathcal{T}_0; \Gamma_0 \vdash_s \langle e_0, e_1 \rangle : \mathcal{U}}$$

$$\frac{\mathcal{T}_0; (x_0 : \mathcal{U}), \Gamma_0 \vdash_s e_0 : \mathcal{U}}{\mathcal{T}_0; \Gamma_0 \vdash_s \lambda x_0. e_0 : \mathcal{U}} \quad \frac{\mathcal{T}_0; (x_0 : \tau_0), \Gamma_0 \vdash_s e_0 : s_0}{\mathcal{T}_0; \Gamma_0 \vdash_s \lambda(x_0 : \tau_0). e_0 : \mathcal{U}} \quad \frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : \mathcal{U} \quad \mathcal{T}_0; \Gamma_0 \vdash_s e_1 : \mathcal{U}}{\mathcal{T}_0; \Gamma_0 \vdash_s \text{app}\{\mathcal{U}\} e_0 e_1 : \mathcal{U}}$$

$$\frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : \mathcal{U}}{\mathcal{T}_0; \Gamma_0 \vdash_s \text{unop}\{\mathcal{U}\} e_0 : \mathcal{U}} \quad \frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : \mathcal{U} \quad \mathcal{T}_0; \Gamma_0 \vdash_s e_1 : \mathcal{U}}{\mathcal{T}_0; \Gamma_0 \vdash_s \text{binop}\{\mathcal{U}\} e_0 e_1 : \mathcal{U}}$$

$$\frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : \lfloor \tau_0 \rfloor}{\mathcal{T}_0; \Gamma_0 \vdash_s \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) e_0 : \mathcal{U}} \quad \frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : \mathcal{U}}{\mathcal{T}_0; \Gamma_0 \vdash_s \text{check}\{\mathcal{U}\} e_0 p_0 : \mathcal{U}}$$

$$\frac{\mathcal{T}_0; \Gamma_0 \vdash_s e_0 : s_0}{\mathcal{T}_0; \Gamma_0 \vdash_s \text{check}\{\mathcal{U}\} e_0 p_0 : \mathcal{U}} \quad \frac{}{\mathcal{T}_0; \Gamma_0 \vdash_s \text{Err} : \mathcal{U}}$$

$$\boxed{s \leq s}$$

$$\frac{}{\text{Nat} \leq \text{Int}}$$

$$\frac{}{s_0 \leq s_0}$$

540 LEMMA 6.5 (FIRST-ORDER INITIALIZATION).

- 541 • If  $(e_0)^{\ell_0} : \tau_0$  **wf** then  $\cdot \vdash_s (e_0)^{\ell_0} : \lfloor \tau_0 \rfloor$  and  $\cdot ; \ell_0 \Vdash (e_0)^{\ell_0}; \emptyset; \emptyset$ .  
 542 • If  $(e_0)^{\ell_0} : \mathcal{U}$  **wf** then  $\cdot \vdash_s (e_0)^{\ell_0} : \mathcal{U}$  and  $\cdot ; \ell_0 \Vdash (e_0)^{\ell_0}; \emptyset; \emptyset$ .

543

544

PROOF SKETCH. By lemma 6.6. □

545

LEMMA 6.6.

- 546 • If  $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}$  and  $\Gamma_0 \vdash (e_0)^{\ell_0} : \tau_0$  then  $\Gamma_0 \vdash_s (e_0)^{\ell_0} : \tau_0$  and  $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}$ .  
 547 • If  $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}$  and  $\Gamma_0 \vdash (e_0)^{\ell_0} : \mathcal{U}$  then  $\Gamma_0 \vdash_s (e_0)^{\ell_0} : \mathcal{U}$  and  $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}; \emptyset; \emptyset$ .

549

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

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

## 6.2.3 Erased Language.

## Erased Evaluation Syntax

$e = x \mid i \mid n \mid \langle e, e \rangle \mid \lambda x. e \mid \lambda(x : \tau). e \mid \text{app}\{\tau/\mathcal{U}\} e e \mid \text{unop}\{\tau/\mathcal{U}\} e \mid \text{binop}\{\tau/\mathcal{U}\} e e \mid$   
 $\text{dyn } b e \mid \text{stat } b e \mid \text{Err}$   
 $v = i \mid n \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x : \tau). e$   
 $\text{Err} = \text{InvariantErr} \mid \text{TagErr} \mid \text{BoundaryErr}(b^*, v) \mid \text{DivErr}$

 $\Gamma \vdash_0 e : \mathcal{U}$ 

$$\frac{(x_0 : \tau/\mathcal{U}) \in \Gamma_0}{\Gamma_0 \vdash_0 x_0 : \mathcal{U}} \quad \frac{}{\Gamma_0 \vdash_0 i_0 : \mathcal{U}} \quad \frac{(x_0 : \tau_0), \Gamma_0 \vdash_0 e_0 : \mathcal{U}}{\Gamma_0 \vdash_0 \lambda(x_0 : \tau_0). e_0 : \mathcal{U}} \quad \frac{(x_0 : \mathcal{U}), \Gamma_0 \vdash_0 e_0 : \mathcal{U}}{\Gamma_0 \vdash_0 \lambda x_0. e_0 : \mathcal{U}}$$

$$\frac{\Gamma_0 \vdash_0 e_0 : \mathcal{U} \quad \Gamma_0 \vdash_0 e_1 : \mathcal{U}}{\Gamma_0 \vdash_0 \langle e_0, e_1 \rangle : \mathcal{U}} \quad \frac{\Gamma_0 \vdash_0 e_0 : \mathcal{U}}{\Gamma_0 \vdash_0 \text{unop}\{\mathcal{U}\} e_0 : \mathcal{U}} \quad \frac{\Gamma_0 \vdash_0 e_0 : \mathcal{U} \quad \Gamma_0 \vdash_0 e_1 : \mathcal{U}}{\Gamma_0 \vdash_0 \text{binop}\{\mathcal{U}\} e_0 e_1 : \mathcal{U}}$$

$$\frac{\Gamma_0 \vdash_0 e_0 : \mathcal{U} \quad \Gamma_0 \vdash_0 e_1 : \mathcal{U}}{\Gamma_0 \vdash_0 \text{app}\{\mathcal{U}\} e_0 e_1 : \mathcal{U}} \quad \frac{\Gamma_0 \vdash_0 e_0 : \mathcal{U}}{\Gamma_0 \vdash_0 \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) e_0 : \mathcal{U}} \quad \frac{\Gamma_0 \vdash_0 e_0 : \mathcal{U}}{\Gamma_0 \vdash_0 \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) e_0 : \mathcal{U}}$$

$$\frac{}{\Gamma_0 \vdash_0 \text{Err} : \mathcal{U}}$$

## Erased Evaluation Syntax, with Ownership

$e = x \mid i \mid n \mid \langle e, e \rangle \mid \lambda x. e \mid \lambda(x : \tau). e \mid \text{app}\{\tau/\mathcal{U}\} e e \mid \text{unop}\{\tau/\mathcal{U}\} e \mid \text{binop}\{\tau/\mathcal{U}\} e e \mid$   
 $\text{dyn } b (e)^\ell \mid \text{stat } b (e)^\ell \mid (e)^\ell \mid \text{Err}$   
 $v = i \mid n \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x : \tau). e \mid (v)^\ell$

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

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

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

$$\frac{\mathcal{L}_0; \ell_0 \Vdash e_0 \quad \mathcal{L}_0; \ell_0 \Vdash e_1}{\mathcal{L}_0; \ell_0 \Vdash \text{binop}\{\tau/\mathcal{U}\} e_0 e_1} \quad \frac{\mathcal{L}_0; \ell_0 \Vdash e_0 \quad \mathcal{L}_0; \ell_0 \Vdash e_1}{\mathcal{L}_0; \ell_0 \Vdash \text{app}\{\tau/\mathcal{U}\} e_0 e_1} \quad \frac{\mathcal{L}_0; \ell_1 \Vdash e_0}{\mathcal{L}_0; \ell_0 \Vdash \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) e_0}$$

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

638 LEMMA 6.7 (ERASED INITIALIZATION). *If  $(e_0)^{\ell_0} : \tau/\mathcal{U}$  wf then  $\cdot \vdash_0 (e_0)^{\ell_0} : \mathcal{U}$  and  $;\ell_0 \Vdash (e_0)^{\ell_0}$ .*

639 PROOF SKETCH. By lemma 6.8. □

641 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  $\Gamma_0 \vdash_0 (e_0)^{\ell_0} : \mathcal{U}$  and  $\mathcal{L}_0; \ell_0 \Vdash (e_0)^{\ell_0}$ .*

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

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

### 6.3 Properties of Interest

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

- $e_0 \rightarrow_X^* v_0$  and  $\vdash_F v_0 : F(\tau/\mathcal{U})$
- $e_0 \rightarrow_X^* \{\text{TagErr}, \text{DivErr}\} \cup \text{BoundaryErr}(b^*, v)$
- $e_0$  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 **CM** if for all  $(e_0)^{\ell_0} : \tau/\mathcal{U}$  **wf** and all  $e_1$  such that  $e_0 \rightarrow_X^* e_1$ , 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  $e_0 \rightarrow_X^* \text{BoundaryErr}(b_0^*, v_0)$ :

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

DEFINITION 6.12 (ERROR PREORDER).  $X \lesssim Y$  iff  $e_0 \rightarrow_Y^* \text{Err}$  implies  $e_0 \rightarrow_X^* \text{Err}$  for all well-formed expressions  $e_0$ .

DEFINITION 6.13 (ERROR EQUIVALENCE).  $X \approx Y$  iff  $X \lesssim Y$  and  $Y \lesssim X$ .

**736 6.4 Common Higher-Order Notions of Reduction**

737 This section is intentionally left blank. The common notions of reduction are inlined into the  
738 definitions that require them.  
739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784



## 6.5 Natural and its Properties

### 6.5.1 Semantics, Type Soundness.

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

|     |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| 834 | $e \xrightarrow{N} e$                                                                                                                                                                                                                                                                                          |                                                                                                                    |
| 835 | $unop\{\mathcal{U}\} v_0$                                                                                                                                                                                                                                                                                      | $\xrightarrow{N} \text{TagErr}$                                                                                    |
| 836 | if $\delta(unop, v_0)$ is undefined                                                                                                                                                                                                                                                                            |                                                                                                                    |
| 837 | $unop\{\mathcal{U}\} v_0$                                                                                                                                                                                                                                                                                      | $\xrightarrow{N} \delta(unop, v_0)$                                                                                |
| 838 | if $\delta(unop, v_0)$ is defined                                                                                                                                                                                                                                                                              |                                                                                                                    |
| 839 | $binop\{\mathcal{U}\} v_0 v_1$                                                                                                                                                                                                                                                                                 | $\xrightarrow{N} \text{TagErr}$                                                                                    |
| 840 | if $\delta(binop, v_0, v_1)$ is undefined                                                                                                                                                                                                                                                                      |                                                                                                                    |
| 841 | $binop\{\mathcal{U}\} v_0 v_1$                                                                                                                                                                                                                                                                                 | $\xrightarrow{N} \delta(binop, v_0, v_1)$                                                                          |
| 842 | if $\delta(binop, v_0, v_1)$ is defined                                                                                                                                                                                                                                                                        |                                                                                                                    |
| 843 | $app\{\mathcal{U}\} v_0 v_1$                                                                                                                                                                                                                                                                                   | $\xrightarrow{N} \text{TagErr}$                                                                                    |
| 844 | if $v_0 \notin (\lambda x. e) \cup (\mathbb{G} b v)$                                                                                                                                                                                                                                                           |                                                                                                                    |
| 845 | $app\{\mathcal{U}\} (\lambda x_0. e_0) v_0$                                                                                                                                                                                                                                                                    | $\xrightarrow{N} e_0[x_0 \leftarrow v_0]$                                                                          |
| 846 | $app\{\mathcal{U}\} (\mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0) v_1$                                                                                                                                                                                                         | $\xrightarrow{N} \text{stat } b_0 (app\{cod(\tau_0)\} v_0 (\text{dyn } b_1 v_1))$                                  |
| 847 | where $b_0 = (\ell_0 \blacktriangleleft \tau_0) \blacktriangleleft \ell_1$ and $b_1 = (\ell_1 \blacktriangleleft dom(\tau_0) \blacktriangleleft \ell_0)$                                                                                                                                                       |                                                                                                                    |
| 848 | $stat (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) v_0$                                                                                                                                                                                                                   | $\xrightarrow{N} \mathbb{G} (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) v_0$ |
| 849 | if $shape\text{-}match(\lfloor \tau_0 \Rightarrow \tau_1 \rfloor, v_0)$ and $v_0 \in (\lambda(x : \tau). e) \cup (\mathbb{G} b v)$                                                                                                                                                                             |                                                                                                                    |
| 850 | $stat (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \langle v_0, v_1 \rangle$                                                                                                                                                                                                                   | $\xrightarrow{N} \langle \text{stat } b_0 v_0, \text{stat } b_1 v_1 \rangle$                                       |
| 851 | if $shape\text{-}match(\lfloor \tau_0 \rfloor, \langle v_0, v_1 \rangle)$ and $b_0 = (\ell_0 \blacktriangleleft fst(\tau_0) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_0 \blacktriangleleft snd(\tau_0) \blacktriangleleft \ell_1)$                                                                          |                                                                                                                    |
| 852 | $stat (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0$                                                                                                                                                                                                                                        | $\xrightarrow{N} i_0$                                                                                              |
| 853 | if $shape\text{-}match(\lfloor \tau_0 \rfloor, i_0)$                                                                                                                                                                                                                                                           |                                                                                                                    |
| 854 | $stat (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$                                                                                                                                                                                                                                        | $\xrightarrow{N} \text{InvariantErr}$                                                                              |
| 855 | if $\neg shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$                                                                                                                                                                                                                                                      |                                                                                                                    |
| 856 | $e \xrightarrow{N^*} e$                                                                                                                                                                                                                                                                                        | is the transitive, reflexive, compatible (with respect to evaluation contexts $E$ , section 6.2)                   |
| 857 |                                                                                                                                                                                                                                                                                                                | closure of the relation $\cup \{\xrightarrow{N}, \xrightarrow{N^*}\}$                                              |
| 858 | $N(e)$                                                                                                                                                                                                                                                                                                         | holds for expressions that contain no subterms of the form $(\mathbb{T} \bar{b} v)$ , (trace $\bar{b} e$ ), or     |
| 859 |                                                                                                                                                                                                                                                                                                                | $(\mathbb{G} \tau v)$ where $\tau$ is not a function type.                                                         |
| 860 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 861 | $\frac{}{\overline{N(x_0)}} \quad \frac{}{\overline{N(i_0)}} \quad \frac{}{\overline{N(\text{Err})}} \quad \frac{N(e_0)}{\overline{N(\lambda x_0. e_0)}} \quad \frac{N(e_0)}{\overline{N(\lambda(x_0 : \tau_0). e_0)}}$                                                                                        |                                                                                                                    |
| 862 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 863 | $\frac{N(e_0)}{\overline{N(\mathbb{G} (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) e_0)}} \quad \frac{N(e_0)}{\overline{N(unop\{\tau/\mathcal{U}\} e_0)}} \quad \frac{N(e_0)}{\overline{N(\text{dyn } b_0 e_0)}} \quad \frac{N(e_0)}{\overline{N(\text{stat } b_0 e_0)}}$ |                                                                                                                    |
| 864 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 865 | $\frac{N(e_0) \quad N(e_1)}{\overline{N(app\{\tau/\mathcal{U}\} e_0 e_1)}} \quad \frac{N(e_0) \quad N(e_1)}{\overline{N(binop\{\tau/\mathcal{U}\} e_0 e_1)}}$                                                                                                                                                  |                                                                                                                    |
| 866 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 867 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 868 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 869 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 870 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 871 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 872 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 873 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 874 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 875 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 876 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 877 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 878 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 879 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 880 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 881 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |
| 882 |                                                                                                                                                                                                                                                                                                                |                                                                                                                    |

883 THEOREM 6.14 (NATURAL TYPE SOUNDNESS). *Natural satisfies TS(1)*

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

885 LEMMA 6.15. *If  $e_0 : \tau/\mathcal{U}$  wf then  $N(e_0)$ .*

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

888 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*  
889 *holds:*

- 891 •  $e_0 \in v \cup \text{Err}$
- 892 •  $\tau/\mathcal{U} \in \tau$  and  $\exists e_1. e_0 \triangleright_N e_1$
- 893 •  $\tau/\mathcal{U} \in \mathcal{U}$  and  $\exists e_1. e_0 \blacktriangleright_N e_1$

894 PROOF SKETCH. By unique decomposition (lemma 6.1) and case analysis. More details in appen-  
895 dix: lemma A.1. □

897 LEMMA 6.17 (NATURAL TYPE PRESERVATION).

898 *If  $\cdot \vdash_1 E_0[e_0] : \tau/\mathcal{U}$  and  $N(E_0[e_0])$  and  $e_0 (\triangleright_N \cup \blacktriangleright_N) e_1$  then  $\cdot \vdash_1 E_0[e_1] : \tau/\mathcal{U}$  and  $N(E_0[e_1])$ .*

899 PROOF SKETCH. By case analysis of each reduction relation. More details in appendix: lemma A.2.  
900 □

902 LEMMA 6.18.

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

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

6.5.2 *Lifted Semantics, Complete Monitoring, Blame.*

$(e)^\ell \triangleright_{\mathbb{N}} (e)^\ell$  lifted version of  $\triangleright_{\mathbb{N}}$

$(unop\{\tau_0\}((v_0))^{\bar{\ell}_0})^{\ell_0} \triangleright_{\mathbb{N}} (InvariantErr)^{\ell_0}$   
 if  $v_0 \notin (v)^\ell$  and  $\delta(unop, v_0)$  is undefined

$(unop\{\tau_0\}((v_0))^{\bar{\ell}_0})^{\ell_0} \triangleright_{\mathbb{N}} (\delta(unop, v_0))^{\bar{\ell}_0 \ell_0}$   
 if  $\delta(unop, v_0)$  is defined

$(binop\{\tau_0\}((v_0))^{\bar{\ell}_0}((v_1))^{\bar{\ell}_1})^{\ell_0} \triangleright_{\mathbb{N}} (InvariantErr)^{\ell_0}$   
 if  $v_0 \notin (v)^\ell$  and  $v_1 \notin (v)^\ell$  and  $\delta(binop, v_0, v_1)$  is undefined

$(binop\{\tau_0\}((v_0))^{\bar{\ell}_0}((v_1))^{\bar{\ell}_1})^{\ell_0} \triangleright_{\mathbb{N}} (\delta(binop, v_0, v_1))^{\ell_0}$   
 if  $\delta(binop, v_0, v_1)$  is defined

$(app\{\tau_0\}((v_0))^{\bar{\ell}_0} v_1)^{\ell_0} \triangleright_{\mathbb{N}} (InvariantErr)^{\ell_0}$   
 if  $v_0 \notin (v)^\ell \cup (\lambda x. e) \cup (\mathbb{G} b v)$

$(app\{\tau_0\}((\lambda(x_0 : \tau_1). e_0))^{\bar{\ell}_0} v_1)^{\ell_0} \triangleright_{\mathbb{N}} ((e_0[x_0 \leftarrow ((v_1))^{\ell_0 rev(\bar{\ell}_0)}]))^{\bar{\ell}_0 \ell_0}$

$(app\{\tau_0\}((\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)(v_0))^{\bar{\ell}_0})^{\ell_3} v_1)^{\ell_3} \triangleright_{\mathbb{N}}$   
 $((\text{dyn } b_0 (\text{app}\{\mathcal{U}\} v_0 (\text{stat } b_1 ((v_1))^{\ell_3 rev(\bar{\ell}_0)}))^{\ell_2})^{\bar{\ell}_0 \ell_3})$   
 where  $b_0 = (\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1)$  and  $b_1 = (\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0)$

$(\text{dyn } (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2} \triangleright_{\mathbb{N}} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2}$   
 if  $\text{shape-match}(\lfloor \tau_0 \Rightarrow \tau_1 \rfloor, v_0)$  and  $v_0 \in (\lambda x. e) \cup (\mathbb{G} b v)$

$(\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\langle v_0, v_1 \rangle))^{\bar{\ell}_0 \ell_2} \triangleright_{\mathbb{N}} (\langle \text{dyn } b_0 ((v_0))^{\bar{\ell}_0}, \text{dyn } b_1 ((v_1))^{\bar{\ell}_0} \rangle)^{\ell_2}$   
 if  $\text{shape-match}(\lfloor \tau_0 \rfloor, \langle v_0, v_1 \rangle)$  and  $b_0 = (\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1)$  and  $b_1 = (\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1)$

$(\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((i_0))^{\bar{\ell}_0})^{\ell_2} \triangleright_{\mathbb{N}} (i_0)^{\ell_2}$   
 if  $\text{shape-match}(\lfloor \tau_0 \rfloor, i_0)$

$(\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2} \triangleright_{\mathbb{N}} (BoundaryErr((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), ((v_0))^{\bar{\ell}_0}))^{\ell_2}$   
 if  $\neg \text{shape-match}(\lfloor \tau_0 \rfloor, v_0)$

|      |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 981  | $(e)^\ell \blacktriangleright_{\mathbb{N}} (e)^\ell$                                                                                                                                                                      | lifted version of $\blacktriangleright_{\mathbb{N}}$                                                                                                                            |
| 982  |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 983  | $(unop\{\mathcal{U}\} \langle v_0 \rangle^{\bar{\ell}_0})^{\ell_0}$                                                                                                                                                       | $\blacktriangleright_{\mathbb{N}} (\text{TagErr})^{\ell_0}$                                                                                                                     |
| 984  | if $v_0 \notin (v)^\ell$ and $\delta(unop, v_0)$ is undefined                                                                                                                                                             |                                                                                                                                                                                 |
| 985  |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 986  | $(unop\{\mathcal{U}\} \langle v_0 \rangle^{\bar{\ell}_0})^{\ell_0}$                                                                                                                                                       | $\blacktriangleright_{\mathbb{N}} (\delta(unop, v_0))^{\bar{\ell}_0 \ell_0}$                                                                                                    |
| 987  | if $\delta(unop, v_0)$ is defined                                                                                                                                                                                         |                                                                                                                                                                                 |
| 988  |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 989  | $(binop\{\mathcal{U}\} \langle v_0 \rangle^{\bar{\ell}_0} \langle v_1 \rangle^{\bar{\ell}_1})^{\ell_0}$                                                                                                                   | $\blacktriangleright_{\mathbb{N}} (\text{TagErr})^{\ell_0}$                                                                                                                     |
| 990  | if $v_0 \notin (v)^\ell$ and $v_1 \notin (v)^\ell$ and $\delta(binop, v_0, v_1)$ is undefined                                                                                                                             |                                                                                                                                                                                 |
| 991  |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 992  | $(binop\{\mathcal{U}\} \langle v_0 \rangle^{\bar{\ell}_0} \langle v_1 \rangle^{\bar{\ell}_1})^{\ell_0}$                                                                                                                   | $\blacktriangleright_{\mathbb{N}} (\delta(binop, v_0, v_1))^{\ell_0}$                                                                                                           |
| 993  | if $\delta(binop, v_0, v_1)$ is defined                                                                                                                                                                                   |                                                                                                                                                                                 |
| 994  |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 995  | $(app\{\mathcal{U}\} \langle v_0 \rangle^{\bar{\ell}_0} v_1)^{\ell_0}$                                                                                                                                                    | $\blacktriangleright_{\mathbb{N}} (\text{TagErr})^{\ell_0}$                                                                                                                     |
| 996  | if $v_0 \notin (v)^\ell \cup (\lambda x. e) \cup (\mathbb{G} b v)$                                                                                                                                                        |                                                                                                                                                                                 |
| 997  | $(app\{\mathcal{U}\} \langle (\lambda x_0. e_0) \rangle^{\bar{\ell}_0} v_1)^{\ell_0}$                                                                                                                                     | $\blacktriangleright_{\mathbb{N}} (\langle e_0[x_0 \leftarrow \langle v_1 \rangle^{\ell_0 rev(\bar{\ell}_0)}] \rangle)^{\bar{\ell}_0 \ell_0}$                                   |
| 998  |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 999  | $(app\{\mathcal{U}\} \langle (\mathbb{G} (\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) (v_0)^{\ell_2}) \rangle^{\bar{\ell}_0} v_1)^{\ell_3}$                                                             | $\blacktriangleright_{\mathbb{N}}$                                                                                                                                              |
| 1000 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1001 | $(\langle \text{stat } b_0 (app\{\tau_1\} v_0 (dyn b_1 \langle v_1 \rangle^{\ell_3 rev(\bar{\ell}_0)})^{\ell_2}) \rangle^{\bar{\ell}_0 \ell_3})^{\ell_2}$                                                                 |                                                                                                                                                                                 |
| 1002 | where $b_0 = (\ell_0 \blacktriangleright cod(\tau_0) \blacktriangleright \ell_1)$ and $b_1 = (\ell_1 \blacktriangleright dom(\tau_0) \blacktriangleright \ell_0)$ and $\tau_1 = cod(\tau_0)$                              |                                                                                                                                                                                 |
| 1003 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1004 | $(\text{stat } (\ell_0 \blacktriangleright (\tau_0 \Rightarrow \tau_1) \blacktriangleright \ell_1) \langle v_0 \rangle^{\bar{\ell}_0})^{\ell_2}$                                                                          | $\blacktriangleright_{\mathbb{N}} (\mathbb{G} (\ell_0 \blacktriangleright (\tau_0 \Rightarrow \tau_1) \blacktriangleright \ell_1) \langle v_0 \rangle^{\bar{\ell}_0})^{\ell_2}$ |
| 1005 | if $shape\text{-}match(\lfloor \tau_0 \Rightarrow \tau_1 \rfloor, v_0)$ and $v_0 \in (\lambda x. e) \cup (\mathbb{G} b v)$                                                                                                |                                                                                                                                                                                 |
| 1006 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1007 | $(\text{stat } (\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) \langle \langle v_0, v_1 \rangle \rangle^{\bar{\ell}_0})^{\ell_2}$                                                                          | $\blacktriangleright_{\mathbb{N}} (\langle \langle dyn b_0 \langle v_0 \rangle^{\bar{\ell}_0}, dyn b_1 \langle v_1 \rangle^{\bar{\ell}_0} \rangle \rangle)^{\ell_2}$            |
| 1008 | if $shape\text{-}match(\langle v_0, v_1 \rangle, \tau_0)$ and $b_0 = (\ell_0 \blacktriangleright fst(\tau_0) \blacktriangleright \ell_1)$ and $b_1 = (\ell_0 \blacktriangleright snd(\tau_0) \blacktriangleright \ell_1)$ |                                                                                                                                                                                 |
| 1009 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1010 | $(\text{stat } (\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) \langle i_0 \rangle^{\bar{\ell}_2})^{\ell_3}$                                                                                               | $\blacktriangleright_{\mathbb{N}} (i_0)^{\ell_3}$                                                                                                                               |
| 1011 | if $shape\text{-}match(i_0, \tau_0)$                                                                                                                                                                                      |                                                                                                                                                                                 |
| 1012 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1013 | $(\text{stat } (\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) \langle v_0 \rangle^{\bar{\ell}_2})^{\ell_2}$                                                                                               | $\blacktriangleright_{\mathbb{N}} (\text{InvariantErr})^{\ell_2}$                                                                                                               |
| 1014 | if $\neg shape\text{-}match(v_0, \tau_0)$                                                                                                                                                                                 |                                                                                                                                                                                 |
| 1015 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1016 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1017 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1018 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1019 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1020 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1021 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1022 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1023 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1024 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1025 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1026 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1027 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1028 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |
| 1029 |                                                                                                                                                                                                                           |                                                                                                                                                                                 |

1030 THEOREM 6.19 (NATURAL COMPLETE MONITORING). *Natural satisfies CM*

1031 PROOF SKETCH. By preservation of single-owner consistency ( $\Vdash$ ) for  $\triangleright_{\mathbb{N}}$  and  $\blacktriangleright_{\mathbb{N}}$ . More details in  
 1032 appendix: theorem A.3. □

1034 LEMMA 6.20 (NATURAL BLAME SOUNDNESS AND COMPLETENESS). *If  $e_0$  is well-formed and  $e_0 \rightarrow_{\mathbb{N}}^*$   
 1035  $\text{BoundaryErr}(\bar{b}_0, v_0)$ , then  $\text{senders}(\bar{b}_0) = \text{owners}(v_0)$  and furthermore  $\bar{b}_0$  contains exactly one bound-  
 1036 ary specification.*

1037 PROOF. By complete monitoring (theorem 6.19) and the definition of  $\rightarrow_{\mathbb{N}}^*$ . There is only one rule  
 1038 that produces a boundary error. It blames a single boundary, and complete monitoring guarantees  
 1039 that the component names (*senders*) and labels (*owners*) match. □

1041 COROLLARY 6.21. *Natural satisfies BS and BC*

1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078

## 6.6 Co-Natural and its Properties

### 6.6.1 Semantics, Type Soundness.

|                                                                                                                                                               |                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| $e \triangleright_C e$                                                                                                                                        |                                                                                                      |
| $unop\{\tau_0\} v_0$                                                                                                                                          | $\triangleright_C$ InvariantErr                                                                      |
| if $v_0 \notin (\mathbb{G}(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell) v)$ and $\delta(unop, v_0)$ is undefined                       |                                                                                                      |
| $unop\{\tau_0\} v_0$                                                                                                                                          | $\triangleright_C$ $\delta(unop, v_0)$                                                               |
| if $\delta(unop, v_0)$ is defined                                                                                                                             |                                                                                                      |
| $fst\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0)$                                                                  | $\triangleright_C$ $dyn\ b_0 (fst\{\mathcal{U}\} v_0)$                                               |
| where $\tau_2 = fst(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$                                                         |                                                                                                      |
| $snd\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0)$                                                                  | $\triangleright_C$ $dyn\ b_0 (snd\{\mathcal{U}\} v_0)$                                               |
| where $\tau_2 = snd(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$                                                         |                                                                                                      |
| $binop\{\tau_0\} v_0 v_1$                                                                                                                                     | $\triangleright_C$ InvariantErr                                                                      |
| if $\delta(binop, v_0, v_1)$ is undefined                                                                                                                     |                                                                                                      |
| $binop\{\tau_0\} v_0 v_1$                                                                                                                                     | $\triangleright_C$ $\delta(binop, v_0, v_1)$                                                         |
| if $\delta(binop, v_0, v_1)$ is defined                                                                                                                       |                                                                                                      |
| $app\{\tau_0\} v_0 v_1$                                                                                                                                       | $\triangleright_C$ InvariantErr                                                                      |
| if $v_0 \notin (\lambda(x : \tau). e) \cup (\mathbb{G} b v)$                                                                                                  |                                                                                                      |
| $app\{\tau_0\} (\lambda(x_0 : \tau_1). e_0) v_0$                                                                                                              | $\triangleright_C$ $e_0[x_0 \leftarrow v_0]$                                                         |
| $app\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) v_1$                                                              | $\triangleright_C$ $dyn\ b_0 (app\{\mathcal{U}\} v_0 (stat\ b_1 v_1))$                               |
| where $b_0 = (\ell_0 \blacktriangleleft cod(\tau_1) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)$ |                                                                                                      |
| $dyn(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$                                                                                         | $\triangleright_C$ $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$      |
| if $shape-match(\lfloor \tau_0 \rfloor, v_0)$ and $v_0 \in \langle v, v \rangle \cup (\lambda x. e) \cup (\mathbb{G} b v)$                                    |                                                                                                      |
| $dyn(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0$                                                                                         | $\triangleright_C$ $i_0$                                                                             |
| if $shape-match(\lfloor \tau_0 \rfloor, i_0)$                                                                                                                 |                                                                                                      |
| $dyn(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$                                                                                         | $\triangleright_C$ BoundaryErr $((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), v_0)$ |
| if $\neg shape-match(\lfloor \tau_0 \rfloor, v_0)$                                                                                                            |                                                                                                      |

|      |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------|--------------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| 1128 | $e \triangleright_C e$                                                                                                                                        |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1129 | $unop\{\mathcal{U}\} v_0$                                                                                                                                     | $\triangleright_C \text{TagErr}$                                                              |                                                                    |                                      |                                                |                                                                                                                     |
| 1130 | if $v_0 \notin (\mathbb{G}(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell) v)$ and $\delta(unop, v_0)$ is undefined                       |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1131 | $unop\{\mathcal{U}\} v_0$                                                                                                                                     | $\triangleright_C \delta(unop, v_0)$                                                          |                                                                    |                                      |                                                |                                                                                                                     |
| 1132 | if $\delta(unop, v_0)$ is defined                                                                                                                             |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1133 | $fst\{\mathcal{U}\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)$                                                             | $\triangleright_C \text{stat } b_0 (fst\{\tau_1\} v_0)$                                       |                                                                    |                                      |                                                |                                                                                                                     |
| 1134 | where $\tau_1 = fst(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$                                                         |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1135 | $snd\{\mathcal{U}\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)$                                                             | $\triangleright_C \text{stat } b_0 (snd\{\tau_1\} v_0)$                                       |                                                                    |                                      |                                                |                                                                                                                     |
| 1136 | where $\tau_1 = snd(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$                                                         |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1137 | $binop\{\mathcal{U}\} v_0 v_1$                                                                                                                                | $\triangleright_C \text{TagErr}$                                                              |                                                                    |                                      |                                                |                                                                                                                     |
| 1138 | if $\delta(binop, v_0, v_1)$ is undefined                                                                                                                     |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1139 | $binop\{\mathcal{U}\} v_0 v_1$                                                                                                                                | $\triangleright_C \delta(binop, v_0, v_1)$                                                    |                                                                    |                                      |                                                |                                                                                                                     |
| 1140 | if $\delta(binop, v_0, v_1)$ is defined                                                                                                                       |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1141 | $app\{\mathcal{U}\} v_0 v_1$                                                                                                                                  | $\triangleright_C \text{TagErr}$                                                              |                                                                    |                                      |                                                |                                                                                                                     |
| 1142 | if $v_0 \notin (\lambda x. e) \cup (\mathbb{G} b v)$                                                                                                          |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1143 | $app\{\mathcal{U}\} (\lambda x_0. e_0) v_0$                                                                                                                   | $\triangleright_C e_0[x_0 \leftarrow v_0]$                                                    |                                                                    |                                      |                                                |                                                                                                                     |
| 1144 | $app\{\mathcal{U}\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0) v_1$                                                         | $\triangleright_C \text{stat } b_0 (app\{cod(\tau_0)\} v_0 (dyn b_1 v_1))$                    |                                                                    |                                      |                                                |                                                                                                                     |
| 1145 | where $b_0 = (\ell_0 \blacktriangleleft cod(\tau_0) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft dom(\tau_0) \blacktriangleleft \ell_0)$ |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1146 | $stat(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$                                                                                        | $\triangleright_C \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$ |                                                                    |                                      |                                                |                                                                                                                     |
| 1147 | if $shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$ and $v_0 \in \langle v, v \rangle \cup (\lambda(x : \tau). e) \cup (\mathbb{G} b v)$                     |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1148 | $stat(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0$                                                                                        | $\triangleright_C i_0$                                                                        |                                                                    |                                      |                                                |                                                                                                                     |
| 1149 | if $shape\text{-}match(\lfloor \tau_0 \rfloor, i_0)$                                                                                                          |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1150 | $stat(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$                                                                                        | $\triangleright_C \text{InvariantErr}$                                                        |                                                                    |                                      |                                                |                                                                                                                     |
| 1151 | if $\neg shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$                                                                                                     |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1152 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1153 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1154 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1155 | $e \rightarrow_C^* e$ is the transitive, reflexive, compatible (with respect to evaluation contexts $E$ , section 6.2)                                        |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1156 | closure of the relation $\cup\{\triangleright_C, \blacktriangleright_C\}$                                                                                     |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1157 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1158 | $C(e)$ holds for expressions that contain no subterms of the form $(\mathbb{T} \bar{b} v)$ , $(\text{trace } \bar{b} e)$ , or                                 |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1159 | $(\mathbb{G} \tau v)$ where $\tau$ is not a pair or function type.                                                                                            |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1160 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1161 | $\frac{}{C(x_0)}$                                                                                                                                             | $\frac{}{C(i_0)}$                                                                             | $\frac{}{C(\text{Err})}$                                           | $\frac{C(e_0)}{C(\lambda x_0. e_0)}$ | $\frac{C(e_0)}{C(\lambda(x_0 : \tau_0). e_0)}$ | $\frac{C(e_0)}{C(\mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) e_0)}$ |
| 1162 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1163 | $\frac{C(e_0)}{C(\mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1) e_0)}$                                                | $\frac{C(e_0)}{C(unop\{\tau/\mathcal{U}\} e_0)}$                                              | $\frac{C(e_0)}{C(dyn b_0 e_0)}$                                    | $\frac{C(e_0)}{C(stat b_0 e_0)}$     |                                                |                                                                                                                     |
| 1164 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1165 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1166 | $\frac{C(e_0) \quad C(e_1)}{C(app\{\tau/\mathcal{U}\} e_0 e_1)}$                                                                                              |                                                                                               | $\frac{C(e_0) \quad C(e_1)}{C(binop\{\tau/\mathcal{U}\} e_0 e_1)}$ |                                      |                                                |                                                                                                                     |
| 1167 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1168 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1169 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1170 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1171 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1172 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1173 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1174 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1175 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |
| 1176 |                                                                                                                                                               |                                                                                               |                                                                    |                                      |                                                |                                                                                                                     |



1177 THEOREM 6.22 (CO-NATURAL TYPE SOUNDNESS). *Co-Natural satisfies TS(1)*

1178 PROOF. By lemma 6.23, progress (lemma 6.24), and preservation (lemma 6.25). □

1179 LEMMA 6.23. *If  $e_0 : \tau/\mathcal{U}$  wf then  $C(e_0)$ .*

1181 PROOF. Wrappers and trace expressions are not part of the surface language. □

1182 LEMMA 6.24 (CO-NATURAL TYPE PROGRESS).

1184 *If  $\cdot \vdash_1 E_0[e_0] : \tau/\mathcal{U}$  and  $C(E_0[e_0])$  then one of the following holds:*

- 1185 •  $e_0 \in \nu \cup \text{Err}$
- 1186 •  $\tau/\mathcal{U} \in \tau$  and  $\exists e_1. e_0 \triangleright_C e_1$
- 1187 •  $\tau/\mathcal{U} \in \mathcal{U}$  and  $\exists e_1. e_0 \blacktriangleright_C e_1$

1188 PROOF SKETCH. By unique decomposition (lemma 6.1) and case analysis. More details in appen-  
1189 dix: lemma A.4. □

1191 LEMMA 6.25. [*Co-Natural type preservation*]

1192 *If  $\cdot \vdash_1 E_0[e_0] : \tau/\mathcal{U}$  and  $C(E_0[e_0])$  and  $e_0(\triangleright_C \cup \blacktriangleright_C)e_1$  then  $\cdot \vdash_1 E_0[e_1] : \tau/\mathcal{U}$  and  $C(E_0[e_1])$ .*

1193 PROOF SKETCH. By case analysis of each reduction relation. More details in appendix: lemma A.5.

1194 □

1195 LEMMA 6.26.

- 1196 • *If  $C(E_0[e_0])$  then  $C(e_0)$*
- 1197 • *If  $C(E_0[e_0])$  and  $C(e_1)$  then  $C(E_0[e_1])$*

1199 PROOF SKETCH. By induction on the structure of  $E_0$ . □

1200

1201

1202

1203

1204

1205

1206

1207

1208

1209

1210

1211

1212

1213

1214

1215

1216

1217

1218

1219

1220

1221

1222

1223

1224

1225

6.6.2 *Lifted Semantics, Complete Monitoring, Blame.*

$(e)^\ell \triangleright_{\bar{c}} (e)^\ell$  lifted version of  $\triangleright_{\bar{c}}$

|      |                                                                                                                                                               |                            |                                                                                                                |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------|
| 1226 |                                                                                                                                                               |                            |                                                                                                                |
| 1227 |                                                                                                                                                               |                            |                                                                                                                |
| 1228 |                                                                                                                                                               |                            |                                                                                                                |
| 1229 | $(unop\{\tau_0\}((v_0))^{\bar{\ell}_0})^{\ell_0}$                                                                                                             | $\triangleright_{\bar{c}}$ | $(InvariantErr)^{\ell_0}$                                                                                      |
| 1230 | if $v_0 \notin (v)^\ell \cup (\mathbb{G}(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell) v)$ and $\delta(unop, v_0)$ is undefined         |                            |                                                                                                                |
| 1231 |                                                                                                                                                               |                            |                                                                                                                |
| 1232 | $(unop\{\tau_0\}((v_0))^{\bar{\ell}_0})^{\ell_0}$                                                                                                             | $\triangleright_{\bar{c}}$ | $(\delta(unop, v_0))^{\bar{\ell}_0 \ell_0}$                                                                    |
| 1233 | if $\delta(unop, v_0)$ is defined                                                                                                                             |                            |                                                                                                                |
| 1234 |                                                                                                                                                               |                            |                                                                                                                |
| 1235 | $(fst\{\tau_0\}(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                 | $\triangleright_{\bar{c}}$ | $(dyn\ b_0(fst\{\mathcal{U}\}(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                           |
| 1236 | where $\tau_2 = fst(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$                                                         |                            |                                                                                                                |
| 1237 |                                                                                                                                                               |                            |                                                                                                                |
| 1238 | $(snd\{\tau_0\}(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                 | $\triangleright_{\bar{c}}$ | $(dyn\ b_0(snd\{\mathcal{U}\}(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                           |
| 1239 | where $\tau_2 = snd(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$                                                         |                            |                                                                                                                |
| 1240 |                                                                                                                                                               |                            |                                                                                                                |
| 1241 | $(binop\{\tau_0\}((v_0))^{\bar{\ell}_0}((v_1))^{\bar{\ell}_1})^{\ell_0}$                                                                                      | $\triangleright_{\bar{c}}$ | $(InvariantErr)^{\ell_0}$                                                                                      |
| 1242 | if $v_0 \notin (v)^\ell$ and $v_1 \notin (v)^\ell$ and $\delta(binop, v_0, v_1)$ is undefined                                                                 |                            |                                                                                                                |
| 1243 | $(binop\{\tau_0\}((v_0))^{\bar{\ell}_0}((v_1))^{\bar{\ell}_1})^{\ell_0}$                                                                                      | $\triangleright_{\bar{c}}$ | $(\delta(binop, v_0, v_1))^{\ell_0}$                                                                           |
| 1244 | if $\delta(binop, v_0, v_1)$ is defined                                                                                                                       |                            |                                                                                                                |
| 1245 |                                                                                                                                                               |                            |                                                                                                                |
| 1246 | $(app\{\tau_0\}((v_0))^{\bar{\ell}_0} v_1)^{\ell_0}$                                                                                                          | $\triangleright_{\bar{c}}$ | $(InvariantErr)^{\ell_0}$                                                                                      |
| 1247 | if $v_0 \notin (v)^\ell \cup (\lambda(x : \tau). e) \cup (\mathbb{G} b v)$                                                                                    |                            |                                                                                                                |
| 1248 |                                                                                                                                                               |                            |                                                                                                                |
| 1249 | $(app\{\tau_0\}((\lambda(x_0 : \tau_1). e_0))^{\bar{\ell}_0} v_0)^{\ell_0}$                                                                                   | $\triangleright_{\bar{c}}$ | $((e_0[x_0 \leftarrow ((v_0))^{\ell_0 rev(\bar{\ell}_0)}]))^{\bar{\ell}_0 \ell_0}$                             |
| 1250 |                                                                                                                                                               |                            |                                                                                                                |
| 1251 | $(app\{\tau_0\}(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3} v_1$                             | $\triangleright_{\bar{c}}$ |                                                                                                                |
| 1252 |                                                                                                                                                               |                            |                                                                                                                |
| 1253 | $(dyn\ b_0(app\{\mathcal{U}\} v_0 (stat\ b_1((v_1))^{\ell_3 rev(\bar{\ell}_0)})^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                             |                            |                                                                                                                |
| 1254 | where $b_0 = (\ell_0 \blacktriangleleft cod(\tau_1) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)$ |                            |                                                                                                                |
| 1255 | $(dyn(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)((v_0))^{\bar{\ell}_0})^{\ell_2}$                                                            | $\triangleright_{\bar{c}}$ | $(\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)((v_0))^{\bar{\ell}_0})^{\ell_2}$      |
| 1256 | if $shape-match(\lfloor \tau_0 \rfloor, v_0)$ and $v_0 \in \langle v, v \rangle \cup (\lambda x. e) \cup (\mathbb{G} b v)$                                    |                            |                                                                                                                |
| 1257 |                                                                                                                                                               |                            |                                                                                                                |
| 1258 | $(dyn(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)((i_0))^{\bar{\ell}_0})^{\ell_2}$                                                            | $\triangleright_{\bar{c}}$ | $(i_0)^{\ell_2}$                                                                                               |
| 1259 | if $shape-match(\lfloor \tau_0 \rfloor, i_0)$                                                                                                                 |                            |                                                                                                                |
| 1260 |                                                                                                                                                               |                            |                                                                                                                |
| 1261 | $(dyn(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)((v_0))^{\bar{\ell}_0})^{\ell_2}$                                                            | $\triangleright_{\bar{c}}$ | $(BoundaryErr((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), ((v_0))^{\bar{\ell}_0}))^{\ell_2}$ |
| 1262 | if $\neg shape-match(\lfloor \tau_0 \rfloor, v_0)$                                                                                                            |                            |                                                                                                                |
| 1263 |                                                                                                                                                               |                            |                                                                                                                |
| 1264 |                                                                                                                                                               |                            |                                                                                                                |
| 1265 |                                                                                                                                                               |                            |                                                                                                                |
| 1266 |                                                                                                                                                               |                            |                                                                                                                |
| 1267 |                                                                                                                                                               |                            |                                                                                                                |
| 1268 |                                                                                                                                                               |                            |                                                                                                                |
| 1269 |                                                                                                                                                               |                            |                                                                                                                |
| 1270 |                                                                                                                                                               |                            |                                                                                                                |
| 1271 |                                                                                                                                                               |                            |                                                                                                                |
| 1272 |                                                                                                                                                               |                            |                                                                                                                |
| 1273 |                                                                                                                                                               |                            |                                                                                                                |
| 1274 |                                                                                                                                                               |                            |                                                                                                                |

|      |                                                                                                                                                                                          |                                                                                                                                   |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| 1275 | $(e)^\ell \xrightarrow{\bar{c}} (e)^\ell$                                                                                                                                                | lifted version of $\xrightarrow{c}$                                                                                               |
| 1276 |                                                                                                                                                                                          |                                                                                                                                   |
| 1277 | $(unop\{\mathcal{U}\}((v_0))^{\bar{\ell}_0})^{\ell_0}$                                                                                                                                   | $\xrightarrow{\bar{c}}$ (TagErr) $^{\ell_0}$                                                                                      |
| 1278 | if $v_0 \notin (v)^\ell \cup (\mathbb{G}(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell) v)$ and $\delta(unop, v_0)$ is undefined                                    |                                                                                                                                   |
| 1279 |                                                                                                                                                                                          |                                                                                                                                   |
| 1280 | $(unop\{\mathcal{U}\}((v_0))^{\bar{\ell}_0})^{\ell_0}$                                                                                                                                   | $\xrightarrow{\bar{c}}$ $(\delta(unop, v_0))^{\bar{\ell}_0 \ell_0}$                                                               |
| 1281 | if $\delta(unop, v_0)$ is defined                                                                                                                                                        |                                                                                                                                   |
| 1282 |                                                                                                                                                                                          |                                                                                                                                   |
| 1283 | $(fst\{\mathcal{U}\}(\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                                       | $\xrightarrow{\bar{c}}$ $(stat\ b_0(fst\{\tau_1\}(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                          |
| 1284 | where $\tau_1 = fst(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$                                                                                    |                                                                                                                                   |
| 1285 |                                                                                                                                                                                          |                                                                                                                                   |
| 1286 | $(snd\{\mathcal{U}\}(\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                                       | $\xrightarrow{\bar{c}}$ $(stat\ b_0(snd\{\tau_1\}(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                          |
| 1287 | where $\tau_1 = snd(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$                                                                                    |                                                                                                                                   |
| 1288 |                                                                                                                                                                                          |                                                                                                                                   |
| 1289 | $(binop\{\mathcal{U}\}((v_0))^{\bar{\ell}_0}((v_1))^{\bar{\ell}_1})^{\ell_0}$                                                                                                            | $\xrightarrow{\bar{c}}$ (TagErr) $^{\ell_0}$                                                                                      |
| 1290 | if $v_0 \notin (v)^\ell$ and $v_1 \notin (v)^\ell$ and $\delta(binop, v_0, v_1)$ is undefined                                                                                            |                                                                                                                                   |
| 1291 | $(binop\{\mathcal{U}\}((v_0))^{\bar{\ell}_0}((v_1))^{\bar{\ell}_1})^{\ell_0}$                                                                                                            | $\xrightarrow{\bar{c}}$ $(\delta(binop, v_0, v_1))^{\ell_0}$                                                                      |
| 1292 | if $\delta(binop, v_0, v_1)$ is defined                                                                                                                                                  |                                                                                                                                   |
| 1293 |                                                                                                                                                                                          |                                                                                                                                   |
| 1294 | $(app\{\mathcal{U}\}((v_0))^{\bar{\ell}_0} v_1)^{\ell_0}$                                                                                                                                | $\xrightarrow{\bar{c}}$ (TagErr) $^{\ell_0}$                                                                                      |
| 1295 | if $v_0 \notin (\lambda x. e) \cup (\mathbb{G} b v)$                                                                                                                                     |                                                                                                                                   |
| 1296 |                                                                                                                                                                                          |                                                                                                                                   |
| 1297 | $(app\{\mathcal{U}\}((\lambda x_0. e_0))^{\bar{\ell}_0} v_1)^{\ell_0}$                                                                                                                   | $\xrightarrow{\bar{c}}$ $((e_0[x_0 \leftarrow (v_1)]^{\ell_0 rev(\bar{\ell}_0)}))^{\bar{\ell}_0 \ell_0}$                          |
| 1298 |                                                                                                                                                                                          |                                                                                                                                   |
| 1299 | $(app\{\mathcal{U}\}(\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3} v_1)^{\ell_3}$                                         | $\xrightarrow{\bar{c}}$                                                                                                           |
| 1300 | $((stat\ b_0(app\{\tau_1\} v_0 (dyn\ b_1((v_1))^{\ell_3 rev(\bar{\ell}_0)})^{\ell_2}))^{\bar{\ell}_0 \ell_3})^{\ell_3}$                                                                  |                                                                                                                                   |
| 1301 | 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 $\tau_1 = cod(\tau_0)$ |                                                                                                                                   |
| 1302 |                                                                                                                                                                                          |                                                                                                                                   |
| 1303 | $(stat(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)((v_0))^{\bar{\ell}_0})^{\ell_2}$                                                                                      | $\xrightarrow{\bar{c}}$ $(\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)((v_0))^{\bar{\ell}_0})^{\ell_2}$ |
| 1304 | if <i>shape-match</i> ( $\lfloor \tau_0 \rfloor, v_0$ ) and $v_0 \in \langle v, v \rangle \cup (\lambda(x : \tau). e) \cup (\mathbb{G} b v)$                                             |                                                                                                                                   |
| 1305 |                                                                                                                                                                                          |                                                                                                                                   |
| 1306 | $(stat(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)((i_0))^{\bar{\ell}_2})^{\ell_3}$                                                                                      | $\xrightarrow{\bar{c}}$ $(i_0)^{\ell_3}$                                                                                          |
| 1307 | if <i>shape-match</i> ( $\lfloor \tau_0 \rfloor, i_0$ )                                                                                                                                  |                                                                                                                                   |
| 1308 |                                                                                                                                                                                          |                                                                                                                                   |
| 1309 | $(stat(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)((v_0))^{\bar{\ell}_2})^{\ell_2}$                                                                                      | $\xrightarrow{\bar{c}}$ (InvariantErr) $^{\ell_2}$                                                                                |
| 1310 | if $\neg$ <i>shape-match</i> ( $\lfloor \tau_0 \rfloor, v_0$ )                                                                                                                           |                                                                                                                                   |
| 1311 |                                                                                                                                                                                          |                                                                                                                                   |
| 1312 |                                                                                                                                                                                          |                                                                                                                                   |
| 1313 |                                                                                                                                                                                          |                                                                                                                                   |
| 1314 |                                                                                                                                                                                          |                                                                                                                                   |
| 1315 |                                                                                                                                                                                          |                                                                                                                                   |
| 1316 |                                                                                                                                                                                          |                                                                                                                                   |
| 1317 |                                                                                                                                                                                          |                                                                                                                                   |
| 1318 |                                                                                                                                                                                          |                                                                                                                                   |
| 1319 |                                                                                                                                                                                          |                                                                                                                                   |
| 1320 |                                                                                                                                                                                          |                                                                                                                                   |
| 1321 |                                                                                                                                                                                          |                                                                                                                                   |
| 1322 |                                                                                                                                                                                          |                                                                                                                                   |
| 1323 |                                                                                                                                                                                          |                                                                                                                                   |

1324 THEOREM 6.27 (CO-NATURAL COMPLETE MONITORING). *Co-Natural satisfies CM*

1325 PROOF SKETCH. By preservation of single-owner consistency ( $\Vdash$ ) for  $\triangleright_{\bar{c}}$  and  $\blacktriangleright_{\bar{c}}$ . More details in  
 1326 appendix: lemma A.6. □

1328 LEMMA 6.28 (CO-NATURAL BLAME SOUNDNESS AND COMPLETENESS). *If  $e_0$  is well-formed and*  
 1329  *$e_0 \rightarrow_{\bar{c}}^* \text{BoundaryErr}(\bar{b}_0, v_0)$ , then  $\text{senders}(\bar{b}_0) = \text{owners}(v_0)$  and furthermore  $\bar{b}_0$  contains exactly one*  
 1330 *boundary specification.*

1331 PROOF. By complete monitoring (theorem 6.27) and the definition of  $\rightarrow_{\bar{c}}^*$ . There is one rule that  
 1332 produces a boundary error; it blames a single boundary. Complete monitoring guarantees that the  
 1333 component names and labels match. □

1335 COROLLARY 6.29. *Co-Natural satisfies BS and BC*

1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372

## 6.6.3 Relation to Natural.

$$\boxed{v \lesssim v}$$

$$\frac{}{i_0 \lesssim i_0} \quad \frac{v_0 \lesssim v_2 \quad v_1 \lesssim v_3}{\langle v_0, v_1 \rangle \lesssim \langle v_2, v_3 \rangle} \quad \frac{v_0 \lesssim \mathbb{G}^{+?} \text{fst}(\bar{b}_0) v_2 \quad v_1 \lesssim \mathbb{G}^{+?} \text{snd}(\bar{b}_0) v_3}{\langle v_0, v_1 \rangle \lesssim \mathbb{G}^+ \bar{b}_0 \langle v_2, v_3 \rangle}$$

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

$$\boxed{e \lesssim e}$$

$$\frac{}{x_0 \lesssim x_0} \quad \frac{e_0 \lesssim e_2 \quad e_1 \lesssim e_3}{\langle e_0, e_1 \rangle \lesssim \langle e_2, e_3 \rangle} \quad \frac{e_0 \lesssim e_2 \quad e_1 \lesssim e_3}{\text{app}\{\tau/\mathcal{U}\} e_0 e_1 \lesssim \text{app}\{\tau/\mathcal{U}\} e_2 e_3}$$

$$\frac{e_0 \lesssim e_1}{\text{unop}\{\tau/\mathcal{U}\} e_0 \lesssim \text{unop}\{\tau/\mathcal{U}\} e_1} \quad \frac{e_0 \lesssim e_2 \quad e_1 \lesssim e_3}{\text{binop}\{\tau/\mathcal{U}\} e_0 e_1 \lesssim \text{binop}\{\tau/\mathcal{U}\} e_2 e_3} \quad \frac{e_0 \lesssim e_1}{\text{dyn } b_0 e_0 \lesssim \text{dyn } b_1 e_1}$$

$$\frac{e_0 \lesssim e_1}{\text{stat } b_0 e_0 \lesssim \text{stat } b_1 e_1} \quad \text{InvariantErr} \lesssim \text{InvariantErr} \quad \text{TagErr} \lesssim \text{TagErr}$$

$$\text{DivErr} \lesssim \text{DivErr}$$

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

$$\boxed{E \lesssim E}$$

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

$$\frac{v_0 \lesssim v_2 \quad E_1 \lesssim E_3}{\text{app}\{\tau/\mathcal{U}\} v_0 E_1 \lesssim \text{app}\{\tau/\mathcal{U}\} v_2 E_3} \quad \frac{E_0 \lesssim E_1}{\text{unop}\{\tau/\mathcal{U}\} E_0 \lesssim \text{unop}\{\tau/\mathcal{U}\} E_1}$$

$$\frac{E_0 \lesssim E_2 \quad e_1 \lesssim e_3}{\text{binop}\{\tau/\mathcal{U}\} E_0 e_1 \lesssim \text{binop}\{\tau/\mathcal{U}\} E_2 e_3} \quad \frac{v_0 \lesssim v_2 \quad E_1 \lesssim E_3}{\text{binop}\{\tau/\mathcal{U}\} v_0 E_1 \lesssim \text{binop}\{\tau/\mathcal{U}\} v_2 E_3}$$

$$\frac{b_0 \leqslant b_1 \quad E_0 \lesssim E_1}{\text{dyn } b_0 E_0 \lesssim \text{dyn } b_1 E_1} \quad \frac{b_0 \leqslant b_1 \quad E_0 \lesssim E_1}{\text{stat } b_0 E_0 \lesssim \text{stat } b_1 E_1} \quad \frac{b_0 \leqslant b_2 \quad b_1 \leqslant b_3 \quad E_0 \lesssim \text{trace } \bar{b}_4 E_1}{\text{stat } b_0 (\text{dyn } b_1 E_0) \lesssim \text{trace } b_2 b_3 \bar{b}_4 E_1}$$

$$\boxed{\text{fst} : \bar{b} \longrightarrow \bar{b}}$$

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

$$\boxed{\text{snd} : \bar{b} \longrightarrow \bar{b}}$$

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

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

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

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

1422 THEOREM 6.30 (NATURAL CO-NATURAL ERROR PREORDER).  $N \lesssim C$

1423 PROOF. By lemma 6.32 and that  $e_0 \lesssim \text{BoundaryErr}(\bar{b}_1, v_1)$  implies  $e_0 \in \text{BoundaryErr}(b, v)$ .  $\square$

1424  
1425 THEOREM 6.31.  $C \not\lesssim N$

1426 PROOF. Let  $e_0$  import an untyped pair into a typed context.

1427  $e_0 = \text{dyn}(\ell_0 \blacktriangleleft \text{Nat} \times \text{Nat} \blacktriangleleft \ell_1) \langle -2, 2 \rangle$

1428  
1429 Natural raises a boundary error and Co-Natural computes a natural number.  $\square$

1430 LEMMA 6.32.

- 1431 • If  $e_0 \lesssim e_2$  and  $e_0 \rightarrow_N e_1$  then  $\exists e_3, e_4$  such that  $e_1 \rightarrow_N^* e_3$  and  $e_2 \rightarrow_C^* e_4$  and  $e_3 \lesssim e_4$ .
- 1432 • If  $e_0 \lesssim e_2$  and  $e_2 \rightarrow_C e_3$  then  $\exists e_1, e_4$  such that  $e_3 \rightarrow_C^* e_4$  and  $e_0 \rightarrow_N^* e_1$  and  $e_1 \lesssim e_4$

1433  
1434 PROOF SKETCH. For the most part, both move in lock-step. Natural takes additional steps when  
1435 a pair reaches a boundary and Co-Natural simply creates a wrapper. Co-Natural takes additional  
1436 steps (to catch up) when eliminating a wrapped pair. The  $\lesssim$  relation shows how unwrapped pairs  
1437 match wrapped pairs in a controlled way. More details in appendix: lemma A.7.  $\square$

1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470

## 1471 6.7 Forgetful and its Properties

1472 Unlike the paper, this forgetful semantics uses trace wrappers in the same way as the Amnesic  
1473 semantics to satisfy (path-based) blame completeness.

### 1474 6.7.1 Semantics, Type Soundness.

|                                                                                                            |                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1475 $e \triangleright_F e$                                                                                |                                                                                                                                                                                                            |
| 1476                                                                                                       |                                                                                                                                                                                                            |
| 1477 $unop\{\tau_0\} v_0$                                                                                  | $\triangleright_F$ InvariantErr                                                                                                                                                                            |
| 1478                                                                                                       | if $v_0 \notin (\mathbb{G}(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell) v)$ and $\delta(unop, v_0)$ is undefined                                                                    |
| 1479 $unop\{\tau_0\} v_0$                                                                                  | $\triangleright_F$ $\delta(unop, v_0)$                                                                                                                                                                     |
| 1480                                                                                                       | if $\delta(unop, v_0)$ is defined                                                                                                                                                                          |
| 1481 $fst\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0)$          | $\triangleright_F$ $\text{dyn } b_0 (fst\{\mathcal{U}\} v_0)$                                                                                                                                              |
| 1482                                                                                                       | where $\tau_2 = fst(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$                                                                                                      |
| 1483 $snd\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0)$          | $\triangleright_F$ $\text{dyn } b_0 (snd\{\mathcal{U}\} v_0)$                                                                                                                                              |
| 1484                                                                                                       | where $\tau_2 = snd(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$                                                                                                      |
| 1485                                                                                                       |                                                                                                                                                                                                            |
| 1486 $binop\{\tau_0\} v_0 v_1$                                                                             | $\triangleright_F$ InvariantErr                                                                                                                                                                            |
| 1487                                                                                                       | if $\delta(binop, v_0, v_1)$ is undefined                                                                                                                                                                  |
| 1488 $binop\{\tau_0\} v_0 v_1$                                                                             | $\triangleright_F$ $\delta(binop, v_0, v_1)$                                                                                                                                                               |
| 1489                                                                                                       | if $\delta(binop, v_0, v_1)$ is defined                                                                                                                                                                    |
| 1490                                                                                                       |                                                                                                                                                                                                            |
| 1491 $app\{\tau_0\} v_0 v_1$                                                                               | $\triangleright_F$ InvariantErr                                                                                                                                                                            |
| 1492                                                                                                       | if $v_0 \notin (\lambda(x : \tau). e) \cup (\mathbb{G}(\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell) v)$                                                                        |
| 1493 $app\{\tau_0\} (\lambda(x_0 : \tau_1). e_0) v_0$                                                      | $\triangleright_F$ $e_0[x_0 \leftarrow v_0]$                                                                                                                                                               |
| 1494 $app\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) v_1$      | $\triangleright_F$ $\text{dyn } b_0 (app\{\mathcal{U}\} v_0 (stat b_1 v_1))$                                                                                                                               |
| 1495                                                                                                       | where $b_0 = (\ell_0 \blacktriangleleft cod(\tau_1) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)$                                              |
| 1496 $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$                          | $\triangleright_F$ $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$                                                                                                            |
| 1497                                                                                                       | if $shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$                                                                                                                                                       |
| 1498                                                                                                       | and $v_0 \in (\mathbb{T}_? \bar{b}(\lambda(x : \tau). e)) \cup (\mathbb{T}_? \bar{b}\langle v, v \rangle) \cup (\mathbb{T}_? \bar{b}(\mathbb{G}(\ell \blacktriangleleft \tau \blacktriangleleft \ell) v))$ |
| 1499 $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\mathbb{T}_? \bar{b}_0 i_0)$ | $\triangleright_F$ $i_0$                                                                                                                                                                                   |
| 1500                                                                                                       | if $shape\text{-}match(\lfloor \tau_0 \rfloor, i_0)$                                                                                                                                                       |
| 1501 $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$                          | $\triangleright_F$ BoundaryErr $((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \bar{b}_0, v_0)$                                                                                             |
| 1502                                                                                                       | if $\neg shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$ and $\bar{b}_0 = get\text{-}trace(v_0)$                                                                                                          |
| 1503                                                                                                       |                                                                                                                                                                                                            |
| 1504                                                                                                       |                                                                                                                                                                                                            |
| 1505                                                                                                       |                                                                                                                                                                                                            |
| 1506                                                                                                       |                                                                                                                                                                                                            |
| 1507                                                                                                       |                                                                                                                                                                                                            |
| 1508                                                                                                       |                                                                                                                                                                                                            |
| 1509                                                                                                       |                                                                                                                                                                                                            |
| 1510                                                                                                       |                                                                                                                                                                                                            |
| 1511                                                                                                       |                                                                                                                                                                                                            |
| 1512                                                                                                       |                                                                                                                                                                                                            |
| 1513                                                                                                       |                                                                                                                                                                                                            |
| 1514                                                                                                       |                                                                                                                                                                                                            |
| 1515                                                                                                       |                                                                                                                                                                                                            |
| 1516                                                                                                       |                                                                                                                                                                                                            |
| 1517                                                                                                       |                                                                                                                                                                                                            |
| 1518                                                                                                       |                                                                                                                                                                                                            |
| 1519                                                                                                       |                                                                                                                                                                                                            |

1520  $e \xrightarrow{F} e$

1521  $unop\{\mathcal{U}\} v_0 \quad \blacktriangleright_F \text{TagErr}$

1522 if  $v_1 = rem\text{-}trace(v_0)$  and  $v_1 \notin (\mathbb{G}(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell) v)$  and  $\delta(unop, v_1)$  is undefined

1523  $unop\{\mathcal{U}\} v_0 \quad \blacktriangleright_F add\text{-}trace(get\text{-}trace(v_0), \delta(unop, v_1))$

1524 if  $v_1 = rem\text{-}trace(v_0)$  and  $\delta(unop, v_1)$  is defined

1525  $fst\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) \quad \blacktriangleright_F trace \bar{b}_0 (stat b_0 (fst\{\tau_1\} v_0))$

1526 where  $\tau_1 = fst(\tau_0)$  and  $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$

1527  $snd\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) \quad \blacktriangleright_F trace \bar{b}_0 (stat b_0 (snd\{\tau_1\} v_0))$

1528 where  $\tau_1 = snd(\tau_0)$  and  $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$

1529  $binop\{\mathcal{U}\} v_0 v_1 \quad \blacktriangleright_F \text{TagErr}$

1530 if  $v_2 = rem\text{-}trace(v_0)$  and  $v_3 = rem\text{-}trace(v_1)$  and  $\delta(binop, v_2, v_3)$  is undefined

1531  $binop\{\mathcal{U}\} v_0 v_1 \quad \blacktriangleright_F \delta(binop, v_2, v_3)$

1532 if  $v_2 = rem\text{-}trace(v_0)$  and  $v_3 = rem\text{-}trace(v_1)$  and  $\delta(binop, v_2, v_3)$  is defined

1533  $app\{\mathcal{U}\} v_0 v_1 \quad \blacktriangleright_F \text{TagErr}$

1534 if  $v_0 \notin (\mathbb{T}_? \bar{b}(\lambda x. e)) \cup (\mathbb{T}_? \bar{b}(\mathbb{G}(\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell) v))$

1535  $app\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\lambda x_0. e_0)) v_0 \quad \blacktriangleright_F trace \bar{b}_0 (e_0[x_0 \leftarrow v_1])$

1536 where  $v_1 = add\text{-}trace(rev(\bar{b}_0), v_0)$

1537  $app\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) v_1 \quad \blacktriangleright_F trace \bar{b}_0 (stat b_0 (app\{\tau_1\} v_0 (dyn b_1 v_2)))$

1538 where  $\tau_1 = cod(\tau_0)$  and  $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$  and  $b_1 = (\ell_1 \blacktriangleleft dom(\tau_0) \blacktriangleleft \ell_0)$

1539 and  $v_2 = add\text{-}trace(rev(\bar{b}_0), v_1)$

1540  $stat(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \quad \blacktriangleright_F \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$

1541 if  $shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$  and  $v_0 \in (\lambda(x : \tau). e) \cup \langle v, v \rangle$

1542  $stat b_0 (\mathbb{G} b_1 (\mathbb{T}_? \bar{b}_0 v_0)) \quad \blacktriangleright_F trace(b_0 b_1 \bar{b}_0) v_0$

1543 if  $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$  and  $shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$

1544 and  $v_0 \in (\lambda x. e) \cup \langle v, v \rangle \cup (\mathbb{G} b (\lambda(x : \tau). e)) \cup (\mathbb{G} b \langle v, v \rangle)$

1545  $stat(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0 \quad \blacktriangleright_F i_0$

1546 if  $shape\text{-}match(\lfloor \tau_0 \rfloor, i_0)$

1547  $stat(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \quad \blacktriangleright_F \text{InvariantErr}$

1548 if  $\neg shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$

1549  $trace \bar{b}_0 v_0 \quad \blacktriangleright_F v_1$

1550 where  $v_1 = add\text{-}trace(\bar{b}_0, v_0)$

1551  $e \xrightarrow{F^*} e$  is the transitive, reflexive, compatible (with respect to evaluation contexts  $E$ , section 6.2)

1552 closure of the relation  $\bigcup\{\triangleright_F, \blacktriangleright_F\}$

1553  $F(e)$  holds for typed expressions with at most two guard wrappers and for untyped expressions

1554 with at most one guard wrapper. More precisely:

1555 
$$F(e_0) = \begin{cases} \text{True} & \text{if } \vdash_1 e_0 : \tau_0 \text{ and } \cdot \vdash_{FS} e_0 : \tau_0 \\ \text{True} & \text{if } \vdash_1 e_0 : \mathcal{U} \text{ and } \cdot \vdash_{FD} e_0 : \mathcal{U} \\ \text{False} & \text{otherwise} \end{cases}$$

1556

1557

1558

1559

1560

1561

1562

1563

1564

1565

1566

1567

1568



1569  $\boxed{\Gamma \vdash_{FS} e : \tau}$

1570

1571

1572

1573

1574

1575

1576

1577

1578

1579

1580

1581

1582

1583

1584

1585

1586

1587

1588

1589

1590

1591

1592

1593

1594

1594  $\boxed{\Gamma \vdash_{FD} e : \mathcal{U}}$

1595

1596

1597

1598

1599

1600

1601

1602

1603

1604

1605

1606

1607

1608

1609

1610

1611

1612

1613

1614

1615

1616

1617

$$\begin{array}{c}
\frac{}{\Gamma_0 \vdash_{FS} x_0 : \tau_0} \quad \frac{}{\Gamma_0 \vdash_{FS} n_0 : \text{Nat}} \quad \frac{}{\Gamma_0 \vdash_{FS} i_0 : \text{Int}} \quad \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 \quad \Gamma_0 \vdash_{FS} e_1 : \tau_1}{\Gamma_0 \vdash_{FS} \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma_0 \vdash_{FS} e_0 : \tau_1}{\Gamma_0 \vdash_{FS} \text{unop}\{\tau_0\} e_0 : \tau_0} \quad \frac{\Gamma_0 \vdash_{FS} e_0 : \tau_1 \quad \Gamma_0 \vdash_{FS} e_1 : \tau_2}{\Gamma_0 \vdash_{FS} \text{binop}\{\tau_0\} e_0 e_1 : \tau_0} \\
\frac{\Gamma_0 \vdash_{FS} e_0 : \tau_1 \Rightarrow \tau_2 \quad \Gamma_0 \vdash_{FS} e_1 : \tau_1}{\Gamma_0 \vdash_{FS} \text{app}\{\tau_0\} e_0 e_1 : \tau_0} \quad \frac{\Gamma_0 \vdash_{FD} e_0 : \mathcal{U}}{\Gamma_0 \vdash_{FS} \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) e_0 : \tau_0} \\
\frac{\Gamma_0 \vdash_{FS} e_0 : \tau_1 \quad \tau_1 \leq \tau_0}{\Gamma_0 \vdash_{FS} e_0 : \tau_0} \quad \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)} \quad \frac{}{\Gamma_0 \vdash_{FS} \text{Err} : \tau_0} \\
\frac{}{\Gamma_0 \vdash_{FD} x_0 : \mathcal{U}} \quad \frac{}{\Gamma_0 \vdash_{FD} i_0 : \mathcal{U}} \quad \frac{(x_0 : \mathcal{U}), \Gamma_0 \vdash_{FD} e_0 : \mathcal{U}}{\Gamma_0 \vdash_{FD} \lambda x_0. e_0 : \mathcal{U}} \quad \frac{\Gamma_0 \vdash_{FD} e_0 : \mathcal{U} \quad \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} \text{unop}\{\mathcal{U}\} e_0 : \mathcal{U}} \quad \frac{\Gamma_0 \vdash_{FD} e_0 : \mathcal{U} \quad \Gamma_0 \vdash_{FD} e_1 : \mathcal{U}}{\Gamma_0 \vdash_{FD} \text{binop}\{\mathcal{U}\} e_0 e_1 : \mathcal{U}} \\
\frac{\Gamma_0 \vdash_{FD} e_0 : \mathcal{U} \quad \Gamma_0 \vdash_{FD} e_1 : \mathcal{U}}{\Gamma_0 \vdash_{FD} \text{app}\{\mathcal{U}\} e_0 e_1 : \mathcal{U}} \quad \frac{\Gamma_0 \vdash_{FS} e_0 : \tau_0}{\Gamma_0 \vdash_{FD} \text{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}} \quad \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} \bar{b}_0 v_0 : \mathcal{U}} \quad \frac{\Gamma_0 \vdash_{FD} e_0 : \mathcal{U}}{\Gamma_0 \vdash_{FD} \text{trace} \bar{b}_0 e_0 : \mathcal{U}} \quad \frac{}{\Gamma_0 \vdash_{FD} \text{Err} : \mathcal{U}}
\end{array}$$

1618 THEOREM 6.33 (FORGETFUL TYPE SOUNDNESS). *Forgetful satisfies TS(1)*

1619 PROOF. By lemma 6.34, progress (lemma 6.35), and preservation (lemma 6.36). □

1621 LEMMA 6.34. *If  $e_0 : \tau/\mathcal{U}$  wf then  $F(e_0)$ .*

1622 PROOF. Wrappers are not part of the surface language. □

1624 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*  
 1625 *following holds:*

- 1626 •  $e_0 \in \nu \cup \text{Err}$
- 1627 •  $\tau/\mathcal{U} \in \tau$  and  $\exists e_1. e_0 \triangleright_{\mathbb{F}} e_1$
- 1628 •  $\tau/\mathcal{U} \in \mathcal{U}$  and  $\exists e_1. e_0 \blacktriangleright_{\mathbb{F}} e_1$

1630 PROOF SKETCH. By unique decomposition (lemma 6.1) and case analysis. More details in appen-  
 1631 dix: lemma A.14. □

1632 LEMMA 6.36 (FORGETFUL TYPE PRESERVATION).

1633 *If  $\cdot \vdash_1 E_0[e_0] : \tau/\mathcal{U}$  and  $F(E_0[e_0])$  and  $e_0(\triangleright_{\mathbb{F}} \cup \blacktriangleright_{\mathbb{F}})e_1$  then  $\cdot \vdash_1 E_0[e_1] : \tau/\mathcal{U}$  and  $F(E_0[e_1])$ .*

1634 PROOF SKETCH. By case analysis of each reduction relation. An interesting case is the  $\blacktriangleright_{\mathbb{F}}$  rule  
 1635 that removes a guard wrapper; the rule preserves soundness because it unwraps an untyped value  
 1636 in an untyped context. More details in appendix: lemma A.15. □

1638 LEMMA 6.37.

- 1639 • *If  $F(E_0[e_0])$  then  $F(e_0)$*
- 1640 • *If  $F(E_0[e_0])$  and  $F(e_1)$  then  $F(E_0[e_1])$*

1642 PROOF SKETCH. By induction on the structure of  $E_0$ . □

1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666

6.7.2 *Lifted Semantics, Complete Monitoring, Blame.*

|      |                                                                                                                                                                                                                                |                                                                                                                                                             |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1667 | $(e)^\ell \triangleright_{\mathbb{F}} (e)^\ell$ lifted version of $\triangleright_{\mathbb{F}}$                                                                                                                                |                                                                                                                                                             |
| 1668 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1669 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1670 | $(unop\{\tau_0\}((v_0))^{\bar{\ell}_0})^{\ell_0}$                                                                                                                                                                              | $\triangleright_{\mathbb{F}} (\text{InvariantErr})^{\ell_0}$                                                                                                |
| 1671 | if $v_0 \notin (v)^\ell \cup (\mathbb{G}(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell) v)$ and $\delta(unop, v_0)$ is undefined                                                                          |                                                                                                                                                             |
| 1672 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1673 | $(unop\{\tau_0\}((v_0))^{\bar{\ell}_0})^{\ell_0}$                                                                                                                                                                              | $\triangleright_{\mathbb{F}} (\delta(unop, v_0))^{\bar{\ell}_0 \ell_0}$                                                                                     |
| 1674 | if $\delta(unop, v_0)$ is defined                                                                                                                                                                                              |                                                                                                                                                             |
| 1675 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1676 | $(fst\{\tau_0\}(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)(v_0)^{\ell_2})^{\bar{\ell}_0})^{\ell_3}$                                                                                                | $\triangleright_{\mathbb{F}} (\text{dyn } b_0 (fst\{\mathcal{U}\}(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                                    |
| 1677 | where $\tau_2 = fst(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$                                                                                                                          |                                                                                                                                                             |
| 1678 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1679 | $(snd\{\tau_0\}(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)(v_0)^{\ell_2})^{\bar{\ell}_0})^{\ell_3}$                                                                                                | $\triangleright_{\mathbb{F}} (\text{dyn } b_0 (snd\{\mathcal{U}\}(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                                    |
| 1680 | where $\tau_2 = snd(\tau_1)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$                                                                                                                          |                                                                                                                                                             |
| 1681 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1682 | $(binop\{\tau_0\}((v_0))^{\bar{\ell}_0}((v_1))^{\bar{\ell}_1})^{\ell_0}$                                                                                                                                                       | $\triangleright_{\mathbb{F}} (\text{InvariantErr})^{\ell_0}$                                                                                                |
| 1683 | if $v_0 \notin (v)^\ell$ and $v_1 \notin (v)^\ell$ and $\delta(binop, v_0, v_1)$ is undefined                                                                                                                                  |                                                                                                                                                             |
| 1684 | $(binop\{\tau_0\}((v_0))^{\bar{\ell}_0}((v_1))^{\bar{\ell}_1})^{\ell_0}$                                                                                                                                                       | $\triangleright_{\mathbb{F}} (\delta(binop, v_0, v_1))^{\ell_0}$                                                                                            |
| 1685 | if $\delta(binop, v_0, v_1)$ is defined                                                                                                                                                                                        |                                                                                                                                                             |
| 1686 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1687 | $(app\{\tau_0\}((v_0))^{\bar{\ell}_0} v_1)^{\ell_0}$                                                                                                                                                                           | $\triangleright_{\mathbb{F}} (\text{InvariantErr})^{\ell_0}$                                                                                                |
| 1688 | if $v_0 \notin (v)^\ell \cup (\lambda(x : \tau). e) \cup (\mathbb{G} b v)$                                                                                                                                                     |                                                                                                                                                             |
| 1689 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1690 | $(app\{\tau_0\}((\lambda(x : \tau_1). e_0))^{\bar{\ell}_0} v_0)^{\ell_0}$                                                                                                                                                      | $\triangleright_{\mathbb{F}} (e_0[x_0 \leftarrow ((v_0))^{\ell_0 rev(\bar{\ell}_0)}])^{\bar{\ell}_0 \ell_0}$                                                |
| 1691 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1692 | $(app\{\tau_0\}(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)(v_0)^{\ell_2})^{\bar{\ell}_0} v_1)^{\ell_3}$                                                                                            | $\triangleright_{\mathbb{F}}$                                                                                                                               |
| 1693 | $(\text{dyn } b_0 (app\{\mathcal{U}\} v_0 (\text{stat } b_1 ((v_1))^{\ell_3 rev(\bar{\ell}_0)})^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                                                                              |                                                                                                                                                             |
| 1694 | where $b_0 = (\ell_0 \blacktriangleleft cod(\tau_1) \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)$                                                                  |                                                                                                                                                             |
| 1695 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1696 | $(\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2}$                                                                                                                   | $\triangleright_{\mathbb{F}} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2}$                      |
| 1697 | if <i>shape-match</i> ( $\lfloor \tau_0 \rfloor, v_0$ )                                                                                                                                                                        |                                                                                                                                                             |
| 1698 | and $v_0 \in (\mathbb{T}_? \bar{b}(\lambda(x : \tau). e)) \cup (\mathbb{T}_? \bar{b} \langle v, v \rangle) \cup (\mathbb{T}_? \bar{b}(\mathbb{G}(\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell) v))$ |                                                                                                                                                             |
| 1699 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1700 | $(\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((\mathbb{T}_? \bar{b}_0((i_0))^{\bar{\ell}_0})^{\bar{\ell}_1})^{\ell_2}$                                                                           | $\triangleright_{\mathbb{F}} (i_0)^{\ell_2}$                                                                                                                |
| 1701 | if <i>shape-match</i> ( $\lfloor \tau_0 \rfloor, i_0$ )                                                                                                                                                                        |                                                                                                                                                             |
| 1702 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1703 | $(\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_2})^{\ell_3}$                                                                                                                   | $\triangleright_{\mathbb{F}} (\text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \bar{b}_0, ((v_0))^{\bar{\ell}_2}))^{\ell_3}$ |
| 1704 | if $\neg \text{shape-match}(\lfloor \tau_0 \rfloor, v_0)$ and $\bar{b}_0 = \text{get-trace}(v_0)$                                                                                                                              |                                                                                                                                                             |
| 1705 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1706 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1707 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1708 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1709 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1710 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1711 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1712 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1713 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1714 |                                                                                                                                                                                                                                |                                                                                                                                                             |
| 1715 |                                                                                                                                                                                                                                |                                                                                                                                                             |

|                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1716<br>1717<br>1718<br>1719<br>1720<br>1721<br>1722<br>1723<br>1724<br>1725<br>1726<br>1727<br>1728<br>1729<br>1730<br>1731<br>1732<br>1733<br>1734<br>1735<br>1736<br>1737<br>1738<br>1739<br>1740<br>1741<br>1742<br>1743<br>1744<br>1745<br>1746<br>1747<br>1748<br>1749<br>1750<br>1751<br>1752<br>1753<br>1754<br>1755<br>1756<br>1757<br>1758<br>1759<br>1760<br>1761<br>1762<br>1763<br>1764 | $(e)^\ell \triangleright_{\mathbb{F}} (e)^\ell$ $\text{lifted version of } \triangleright_{\mathbb{F}}$ $(unop\{\mathcal{U}\}((v_0))^{\bar{\ell}_0})^{\ell_0} \triangleright_{\mathbb{F}} (\text{TagErr})^{\ell_0}$ <p style="margin-left: 2em;">if <math>v_0 \notin (v)^\ell \cup (\mathbb{G}(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell) v)</math> and <math>\delta(unop, v_0)</math> is undefined</p> $(unop\{\mathcal{U}\} v_0)^{\ell_0} \triangleright_{\mathbb{F}}$ <p style="margin-left: 2em;"><math>(add\text{-}trace(get\text{-}trace(v_0), \delta(unop, v_1)))^{\ell_0}</math></p> <p style="margin-left: 2em;">if <math>v_1 = rem\text{-}trace(v_0)</math> and <math>\delta(unop, v_1)</math> is defined</p> $(fst\{\mathcal{U}\}((\mathbb{T}_? \bar{b}_0((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)(v_0)^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4 \ell_5})) \triangleright_{\mathbb{F}} (\text{trace } \bar{b}_0((\text{stat } b_0(fst\{\tau_1\} v_0)^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4 \ell_5}))$ <p style="margin-left: 2em;">where <math>\tau_1 = fst(\tau_0)</math> and <math>b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)</math></p> $(snd\{\mathcal{U}\}((\mathbb{T}_? \bar{b}_0((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)(v_0)^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4 \ell_5})) \triangleright_{\mathbb{F}} (\text{trace } \bar{b}_0((\text{stat } b_0(snd\{\tau_1\} v_0)^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4 \ell_5}))$ <p style="margin-left: 2em;">where <math>\tau_1 = snd(\tau_0)</math> and <math>b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)</math></p> $(binop\{\mathcal{U}\}((v_0))^{\bar{\ell}_0}((v_1))^{\bar{\ell}_1})^{\ell_0} \triangleright_{\mathbb{F}} (\text{TagErr})^{\ell_0}$ <p style="margin-left: 2em;">if <math>v_2 = rem\text{-}trace(v_0)</math> and <math>v_3 = rem\text{-}trace(v_1)</math> and <math>\delta(binop, v_2, v_3)</math> is undefined</p> $(binop\{\mathcal{U}\}((v_0))^{\bar{\ell}_0}((v_1))^{\bar{\ell}_1})^{\ell_0} \triangleright_{\mathbb{F}} \delta(binop, v_2, v_3)$ <p style="margin-left: 2em;">if <math>v_2 = rem\text{-}trace(v_0)</math> and <math>v_3 = rem\text{-}trace(v_1)</math> and <math>\delta(binop, v_2, v_3)</math> is defined</p> $(app\{\mathcal{U}\}((v_0))^{\bar{\ell}_0} v_1)^{\ell_0} \triangleright_{\mathbb{F}} (\text{TagErr})^{\ell_0}$ <p style="margin-left: 2em;">if <math>v_0 \notin (\mathbb{T}_? \bar{b}(\lambda x. e)) \cup (\mathbb{T}_? \bar{b}(\mathbb{G}(\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell) v))</math></p> $(app\{\mathcal{U}\}((\mathbb{T}_? \bar{b}_0((\lambda x_0. e_0))^{\bar{\ell}_0})^{\bar{\ell}_1 \ell_2} v_0) \triangleright_{\mathbb{F}} (\text{trace } \bar{b}_0((e_0[x_0 \leftarrow v_1])^{\bar{\ell}_0})^{\bar{\ell}_1 \ell_2}))$ <p style="margin-left: 2em;">where <math>v_1 = add\text{-}trace(rev(\bar{b}_0), ((v_0))^{\ell_2 rev(\bar{\ell}_1) rev(\bar{\ell}_0)})</math></p> $(app\{\mathcal{U}\}((\mathbb{T}_? \bar{b}_0((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)(v_0)^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4 \ell_5} v_1) \triangleright_{\mathbb{F}}$ <p style="margin-left: 2em;"><math>(\text{trace } \bar{b}_0((\text{stat } b_0(app\{\tau_1\} v_0(dyn b_1 v_2))^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4 \ell_5}))</math></p> <p style="margin-left: 2em;">where <math>\tau_1 = cod(\tau_0)</math> and <math>b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)</math> and <math>b_1 = (\ell_1 \blacktriangleleft dom(\tau_0) \blacktriangleleft \ell_0)</math></p> <p style="margin-left: 2em;">and <math>v_2 = add\text{-}trace(rev(\bar{b}_0), ((v_1))^{\ell_5 rev(\bar{\ell}_3) \bar{\ell}_4})</math></p> $(\text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)^{\ell_2} \triangleright_{\mathbb{F}} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)^{\ell_2}$ <p style="margin-left: 2em;">if <math>shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)</math> and <math>v_0 \in ((\lambda(x : \tau). e))^{\bar{\ell}} \cup ((\langle v, v \rangle))^{\bar{\ell}}</math></p> $(\text{stat } b_0((\mathbb{G} b_1((\mathbb{T}_? \bar{b}_2 v_0))^{\bar{\ell}_0})^{\bar{\ell}_1 \ell_2}) \triangleright_{\mathbb{F}} (\text{trace } (b_0 b_1 \bar{b}_2)((v_0))^{\bar{\ell}_0 \bar{\ell}_1 \ell_2})^{\ell_2}$ <p style="margin-left: 2em;">if <math>b_0 = (\ell_3 \blacktriangleleft \tau_0 \blacktriangleleft \ell_4)</math> and <math>shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)</math></p> <p style="margin-left: 2em;">and <math>v_0 \in ((\lambda x. e))^{\bar{\ell}} \cup ((\langle v, v \rangle))^{\bar{\ell}} \cup ((\mathbb{G} b(\lambda(x : \tau). e))^{\bar{\ell}} \cup ((\mathbb{G} b \langle v, v \rangle))^{\bar{\ell}}</math></p> $(\text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((i_0))^{\bar{\ell}_2})^{\ell_3} \triangleright_{\mathbb{F}} (i_0)^{\ell_3}$ <p style="margin-left: 2em;">if <math>shape\text{-}match(\lfloor \tau_0 \rfloor, i_0)</math></p> $(\text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_2})^{\ell_3} \triangleright_{\mathbb{F}} (\text{InvariantErr})^{\ell_3}$ <p style="margin-left: 2em;">if <math>\neg shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)</math></p> $(\text{trace } \bar{b}_0 v_0)^{\ell_0} \triangleright_{\mathbb{F}} (v_1)^{\ell_0}$ <p style="margin-left: 2em;">where <math>v_1 = add\text{-}trace(\bar{b}_0, v_0)</math></p> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

1765 THEOREM 6.38 (FORGETFUL INCOMPLETE MONITORING). *Forgetful does not satisfy CM*

1766 PROOF. The stat rule that removes an outer guard breaks single-owner consistency. One way to  
1767 exercise this rule is to send an untyped function into typed code and back out again; on the way  
1768 out, the function loses a wrapper and gains an owner.  $\square$

1770 THEOREM 6.39 (FORGETFUL BLAME SOUNDNESS AND COMPLETENESS). *Forgetful satisfies BS and BC*

1771 PROOF SKETCH. By preservation of path-owner consistency ( $\Vdash_p$ ) for  $\triangleright_{\mathbb{F}}$  and  $\blacktriangleright_{\mathbb{F}}$ . More details in  
1772 appendix: lemma A.16.  $\square$

1774

1775

1776

1777

1778

1779

1780

1781

1782

1783

1784

1785

1786

1787

1788

1789

1790

1791

1792

1793

1794

1795

1796

1797

1798

1799

1800

1801

1802

1803

1804

1805

1806

1807

1808

1809

1810

1811

1812

1813

## 6.7.3 Relation to Co-Natural.

$$\boxed{v \lesssim v}$$

$$\frac{}{i_0 \lesssim i_0} \quad \frac{}{i_0 \lesssim \mathbb{T} \bar{b}_0 i_0} \quad \frac{v_0 \lesssim v_2 \quad v_1 \lesssim v_3}{\langle v_0, v_1 \rangle \lesssim \langle v_2, v_3 \rangle} \quad \frac{e_0 \lesssim e_1}{\lambda x_0. e_0 \lesssim \lambda x_0. e_1}$$

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

$$\frac{b_0 \leqslant b_2 \quad b_1 \leqslant b_3 \quad v_0 \lesssim \mathbb{T} \bar{b}_4 v_1}{\mathbb{G} b_0 (\mathbb{G} b_1 v_0) \lesssim \mathbb{T} b_2 b_3 \bar{b}_4 v_1} \quad \frac{b_0 \leqslant b_1 \quad v_0 \lesssim v_1}{\mathbb{G} b_0 v_0 \lesssim \mathbb{G} b_1 v_1}$$

$$\boxed{e \lesssim e}$$

$$\frac{}{x_0 \lesssim x_0} \quad \frac{e_0 \lesssim e_2 \quad e_1 \lesssim e_3}{\langle e_0, e_1 \rangle \lesssim \langle e_2, e_3 \rangle} \quad \frac{e_0 \lesssim e_2 \quad e_1 \lesssim e_3}{\text{app}\{\tau/\mathcal{U}\} e_0 e_1 \lesssim \text{app}\{\tau/\mathcal{U}\} e_2 e_3}$$

$$\frac{e_0 \lesssim e_1}{\text{unop}\{\tau/\mathcal{U}\} e_0 \lesssim \text{unop}\{\tau/\mathcal{U}\} e_1} \quad \frac{e_0 \lesssim e_2 \quad e_1 \lesssim e_3}{\text{binop}\{\tau/\mathcal{U}\} e_0 e_1 \lesssim \text{binop}\{\tau/\mathcal{U}\} e_2 e_3} \quad \frac{b_0 \leqslant b_1 \quad e_0 \lesssim e_1}{\text{dyn} b_0 e_0 \lesssim \text{dyn} b_1 e_1}$$

$$\frac{b_0 \leqslant b_1 \quad e_0 \lesssim e_1}{\text{stat} b_0 e_0 \lesssim \text{stat} b_1 e_1} \quad \frac{b_0 \leqslant b_2 \quad b_1 \leqslant b_3 \quad e_0 \lesssim \text{trace} \bar{b}_4 e_1}{\text{stat} b_0 (\text{dyn} b_1 e_0) \lesssim \text{trace} b_2 b_3 \bar{b}_4 e_1}$$

$$\frac{}{\text{InvariantErr} \lesssim \text{InvariantErr}}$$

$$\frac{}{\text{TagErr} \lesssim \text{TagErr}}$$

$$\frac{}{\text{DivErr} \lesssim \text{DivErr}}$$

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

$$\boxed{E \lesssim E}$$

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

$$\frac{v_0 \lesssim v_2 \quad E_1 \lesssim E_3}{\text{app}\{\tau/\mathcal{U}\} v_0 E_1 \lesssim \text{app}\{\tau/\mathcal{U}\} v_2 E_3}$$

$$\frac{E_0 \lesssim E_1}{\text{unop}\{\tau/\mathcal{U}\} E_0 \lesssim \text{unop}\{\tau/\mathcal{U}\} E_1}$$

$$\frac{E_0 \lesssim E_2 \quad e_1 \lesssim e_3}{\text{binop}\{\tau/\mathcal{U}\} E_0 e_1 \lesssim \text{binop}\{\tau/\mathcal{U}\} E_2 e_3}$$

$$\frac{v_0 \lesssim v_2 \quad E_1 \lesssim E_3}{\text{binop}\{\tau/\mathcal{U}\} v_0 E_1 \lesssim \text{binop}\{\tau/\mathcal{U}\} v_2 E_3}$$

$$\frac{b_0 \leqslant b_1 \quad E_0 \lesssim E_1}{\text{dyn} b_0 E_0 \lesssim \text{dyn} b_1 E_1} \quad \frac{b_0 \leqslant b_1 \quad E_0 \lesssim E_1}{\text{stat} b_0 E_0 \lesssim \text{stat} b_1 E_1} \quad \frac{b_0 \leqslant b_2 \quad b_1 \leqslant b_3 \quad E_0 \lesssim \text{trace} \bar{b}_4 E_1}{\text{stat} b_0 (\text{dyn} b_1 E_0) \lesssim \text{trace} b_2 b_3 \bar{b}_4 E_1}$$

1863 THEOREM 6.40 (CO-NATURAL FORGETFUL ERROR PREORDER).  $C \lesssim F$

1864 PROOF. By lemma 6.42 and that  $e_0 \lesssim \text{BoundaryErr}(\bar{b}_1, v_1)$  implies  $e_0 \in \text{BoundaryErr}(b, v)$ .  $\square$

1865  
1866 THEOREM 6.41.  $F \not\lesssim C$

1867 PROOF. If an untyped value travels to typed code and back again, Forgetful unwraps it but  
1868 Co-Natural continues to enforce the type.

1869 Let:

1870  $e_0 = \text{stat } b_0 (\text{dyn } (\ell_0 \blacktriangleleft (\text{Nat} \Rightarrow \text{Nat}) \blacktriangleleft \ell_1) (\lambda x_0. x_0))$

1871  $e_1 = \text{app}\{\mathcal{U}\} e_0 \langle 2, 8 \rangle$

1872 Then  $e_1 \rightarrow_F^* \langle 2, 8 \rangle$  and  $e_1 \rightarrow_C^* \text{BoundaryErr}(\dots)$ .  $\square$

1873  
1874 LEMMA 6.42.

- 1875 • If  $e_0 \lesssim e_2$  and  $e_0 \rightarrow_C e_1$  then  $\exists e_3, e_4$  such that  $e_1 \rightarrow_C^* e_3$  and  $e_2 \rightarrow_F^* e_4$  and  $e_3 \lesssim e_4$ .
- 1876 • If  $e_0 \lesssim e_2$  and  $e_2 \rightarrow_F e_3$  then  $\exists e_1, e_4$  such that  $e_3 \rightarrow_F^* e_4$  and  $e_0 \rightarrow_C^* e_1$  and  $e_1 \lesssim e_4$

1877  
1878 PROOF SKETCH. Co-Natural may take extra steps at elimination forms, to unwrap several layers.  
1879 Forgetful takes extra steps to combine boundaries in a trace wrapper. Otherwise, the two are  
1880 in sync modulo extra guard wrappers on the Co-Natural side of the  $\lesssim$  relation More details in  
1881 appendix: lemma A.17.  $\square$

1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911

## 6.8 Transient and its Properties

### 6.8.1 Semantics, Type Soundness.

|                                                                                                                                |                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| $e; \mathcal{H}; \mathcal{B} \triangleright_{\top} e; \mathcal{H}; \mathcal{B}$                                                |                                                                                                                                                 |
| $w_0; \mathcal{H}_0; \mathcal{B}_0$                                                                                            | $\triangleright_{\top} p_0; (\{p_0 \mapsto w_0\} \cup \mathcal{H}_0); (\{p_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$                           |
| where $p_0$ fresh in $\mathcal{H}_0$ and $\mathcal{B}_0$                                                                       |                                                                                                                                                 |
| $(unop\{\tau_0\} v_0); \mathcal{H}_0; \mathcal{B}_0$                                                                           | $\triangleright_{\top} \text{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$                                                                       |
| if $\delta(unop, \mathcal{H}_0(v_0))$ is undefined                                                                             |                                                                                                                                                 |
| $(unop\{\mathcal{U}\} v_0); \mathcal{H}_0; \mathcal{B}_0$                                                                      | $\triangleright_{\top} \text{TagErr}; \mathcal{H}_0; \mathcal{B}_0$                                                                             |
| if $\delta(unop, \mathcal{H}_0(v_0))$ is undefined                                                                             |                                                                                                                                                 |
| $(unop\{\tau/\mathcal{U}\} p_0); \mathcal{H}_0; \mathcal{B}_0$                                                                 | $\triangleright_{\top} (\text{check}\{\tau/\mathcal{U}\} \delta(unop, \mathcal{H}_0(p_0)) p_0); \mathcal{H}_0; \mathcal{B}_0$                   |
| if $\delta(unop, \mathcal{H}_0(p_0))$ is defined                                                                               |                                                                                                                                                 |
| $(binop\{\tau_0\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0$                                                                      | $\triangleright_{\top} \text{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$                                                                       |
| if $\delta(binop, v_0, v_1)$ is undefined                                                                                      |                                                                                                                                                 |
| $(binop\{\mathcal{U}\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0$                                                                 | $\triangleright_{\top} \text{TagErr}; \mathcal{H}_0; \mathcal{B}_0$                                                                             |
| if $\delta(binop, v_0, v_1)$ is undefined                                                                                      |                                                                                                                                                 |
| $(binop\{\tau/\mathcal{U}\} i_0 i_1); \mathcal{H}_0; \mathcal{B}_0$                                                            | $\triangleright_{\top} \delta(binop, i_0, i_1); \mathcal{H}_0; \mathcal{B}_0$                                                                   |
| if $\delta(binop, i_0, i_1)$ is defined                                                                                        |                                                                                                                                                 |
| $(app\{\tau_0\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0$                                                                        | $\triangleright_{\top} \text{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$                                                                       |
| if $\mathcal{H}_0(v_0) \notin (\lambda x. e) \cup (\lambda(x : \tau). e)$                                                      |                                                                                                                                                 |
| $(app\{\mathcal{U}\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0$                                                                   | $\triangleright_{\top} \text{TagErr}; \mathcal{H}_0; \mathcal{B}_0$                                                                             |
| if $\mathcal{H}_0(v_0) \notin (\lambda x. e) \cup (\lambda(x : \tau). e)$                                                      |                                                                                                                                                 |
| $(app\{\tau/\mathcal{U}\} p_0 v_0); \mathcal{H}_0; \mathcal{B}_0$                                                              | $\triangleright_{\top} (\text{check}\{\tau/\mathcal{U}\} e_0[x_0 \leftarrow v_0] p_0); \mathcal{H}_0; \mathcal{B}_1$                            |
| if $\mathcal{H}_0(p_0) = \lambda(x_0 : \tau_0). e_0$ and $\text{shape-match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$      |                                                                                                                                                 |
| and $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \text{rev}(\mathcal{B}_0(p_0))]$                                                   |                                                                                                                                                 |
| $(app\{\tau/\mathcal{U}\} p_0 v_0); \mathcal{H}_0; \mathcal{B}_0$                                                              | $\triangleright_{\top} \text{BoundaryErr}(\mathcal{B}_0(v_0) \cup \text{rev}(\mathcal{B}_0(p_0)), v_0); \mathcal{H}_0; \mathcal{B}_1$           |
| if $\mathcal{H}_0(p_0) = \lambda(x_0 : \tau_0). e_0$ and $\neg \text{shape-match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$ |                                                                                                                                                 |
| where $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \text{rev}(\mathcal{B}_0(p_0))]$                                                 |                                                                                                                                                 |
| $(app\{\tau_0\} p_0 v_0); \mathcal{H}_0; \mathcal{B}_0$                                                                        | $\triangleright_{\top} (\text{check}\{\tau_0\} e_0[x_0 \leftarrow v_0] p_0); \mathcal{H}_0; \mathcal{B}_1$                                      |
| if $\mathcal{H}_0(p_0) = \lambda x_0. e_0$                                                                                     |                                                                                                                                                 |
| and $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \text{rev}(\mathcal{B}_0(p_0))]$                                                   |                                                                                                                                                 |
| $(app\{\mathcal{U}\} p_0 v_0); \mathcal{H}_0; \mathcal{B}_0$                                                                   | $\triangleright_{\top} (e_0[x_0 \leftarrow v_0]); \mathcal{H}_0; \mathcal{B}_0$                                                                 |
| if $\mathcal{H}_0(p_0) = \lambda x_0. e_0$                                                                                     |                                                                                                                                                 |
| $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0); \mathcal{H}_0; \mathcal{B}_0$                   | $\triangleright_{\top} v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}])$          |
| if $\text{shape-match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$                                                            |                                                                                                                                                 |
| $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0); \mathcal{H}_0; \mathcal{B}_0$                   | $\triangleright_{\top} \text{BoundaryErr}(\{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}, v_0); \mathcal{H}_0; \mathcal{B}_0$ |
| if $\neg \text{shape-match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$                                                       |                                                                                                                                                 |
| $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0); \mathcal{H}_0; \mathcal{B}_0$                  | $\triangleright_{\top} v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}])$          |
| if $\text{shape-match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$                                                            |                                                                                                                                                 |
| $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0); \mathcal{H}_0; \mathcal{B}_0$                  | $\triangleright_{\top} \text{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$                                                                       |
| if $\neg \text{shape-match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$                                                       |                                                                                                                                                 |



1961  $(\text{check}\{\mathcal{U}\} v_0 p_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} v_0; \mathcal{H}_0; \mathcal{B}_0$   
 1962  $(\text{check}\{\tau_0\} v_0 p_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \mathcal{B}_0(p_0)])$   
 1963  $\text{if } \text{shape-match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$   
 1964  $(\text{check}\{\tau_0\} v_0 p_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \text{BoundaryErr}(\mathcal{B}_0(v_0) \cup \mathcal{B}_0(p_0), v_0); \mathcal{H}_0; \mathcal{B}_0$   
 1965  $\text{if } \neg \text{shape-match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$

1966  $e; \mathcal{H}; \mathcal{B} \rightarrow_{\top} e; \mathcal{H}; \mathcal{B}$  is the compatible closure of the relation  $\triangleright_{\top}$ . More precisely:

1967  $\text{if } e_0; \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} e_1; \mathcal{H}_1; \mathcal{B}_1$   
 1968  $\text{then } E[e_0]; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top} E[e_1]; \mathcal{H}_1; \mathcal{B}_1$

1970  $e; \mathcal{H}; \mathcal{B} \rightarrow_{\top}^* e; \mathcal{H}; \mathcal{B}$  is the transitive, reflexive closure of the relation  $\rightarrow_{\top}$

1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009

2010 THEOREM 6.43 (TRANSIENT UNSOUNDNESS). *Transient does not satisfy TS(1)*

2011 PROOF. Let  $e_0 = \text{dyn } (\ell_0 \blacktriangleleft (\text{Nat} \Rightarrow \text{Nat}) \blacktriangleleft \ell_1) (\lambda x_0. -4)$ .

- 2012 •  $\vdash e_0 : \text{Nat} \Rightarrow \text{Nat}$  in the surface language, but
- 2013 •  $e_0; \emptyset; \emptyset \rightarrow_{\top}^* p_0; \mathcal{H}_0; \mathcal{B}_0$ , where  $\mathcal{H}_0(p_0) = (\lambda x_0. -4)$

2014 and  $\not\vdash_1 (\lambda x_0. -4) : \text{Nat} \Rightarrow \text{Nat}$ . □

2016 THEOREM 6.44 (TRANSIENT SHAPE SOUNDNESS). *Transient satisfies TS(s)*

2017 PROOF. By progress (lemma 6.45) and preservation (lemma 6.46). □

2019 LEMMA 6.45 (TRANSIENT TYPE PROGRESS).

2020 *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:*

- 2021 •  $e_0 \in \nu \cup \text{Err}$
- 2022 •  $\exists e_1, \mathcal{H}_1, \mathcal{B}_1. e_0; \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} e_1; \mathcal{H}_1; \mathcal{B}_1$

2024 PROOF SKETCH. By unique decomposition (lemma 6.1) and case analysis. More details in appen-  
2025 dix: lemma A.24. □

2026 LEMMA 6.46 (TRANSIENT TYPE PRESERVATION).

2027 *If  $\mathcal{T}_0; \cdot \vdash_s e_0; \mathcal{H}_0; \mathcal{B}_0 : \tau/\mathcal{U}$  and  $e_0; \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} e_1; \mathcal{H}_1; \mathcal{B}_1$  then  $\exists \mathcal{T}_1. \mathcal{T}_0 \subseteq \mathcal{T}_1$  and  $\mathcal{T}_1; \cdot \vdash_s e_1; \mathcal{H}_1; \mathcal{B}_1 : \tau/\mathcal{U}$ .*

2029 PROOF SKETCH. By case analysis of the reduction relation. The new heap typing  $\mathcal{T}_1$  gains an  
2030 entry only when the value heap does; if  $\mathcal{H}_1 = \{p_0 \mapsto w_0\} \cup \mathcal{H}_0$  then  $\mathcal{T}_1 = \{(p_0 : s_0)\} \cup \mathcal{T}_0$ , where  $s_0$   
2031 is the shape of the pre-value (lemma 6.47). More details in appendix: lemma A.25. □

2032 LEMMA 6.47 (TRANSIENT SHAPE INFERENCE).

2033 *If  $\mathcal{T}_0; \cdot \vdash_s w_0; \mathcal{H}_0; \mathcal{B}_0 : \tau/\mathcal{U}$  then  $\exists s_0. \mathcal{T}_0; \cdot \vdash_s w_0; \mathcal{H}_0; \mathcal{B}_0 : s_0$ .*

2035 PROOF. By induction on the structure of the closed pre-value  $w_0$ . Note that lambdas are a base  
2036 case, thus the induction does not need to consider type environments ( $\Gamma$ ). □

6.8.2 *Lifted Semantics, Complete Monitoring, Blame.*

|      |                                                                                                                                                                                                                  |                                                                                                          |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| 2059 | $(e)^\ell; \mathcal{H}; \mathcal{B}; O \triangleright_{\overline{\tau}} (e)^\ell; \mathcal{H}; \mathcal{B}; O$                                                                                                   |                                                                                                          |
| 2060 |                                                                                                                                                                                                                  |                                                                                                          |
| 2061 |                                                                                                                                                                                                                  |                                                                                                          |
| 2062 | $(w_0)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$                                                                                                                                                              | $\triangleright_{\overline{\tau}} (p_0)^{\ell_0}; \mathcal{H}_1; \mathcal{B}_1; O_1$                     |
| 2063 | where $p_0$ fresh in $\mathcal{H}_0$ and $\mathcal{B}_0$ and $O_0$                                                                                                                                               |                                                                                                          |
| 2064 | and $\mathcal{H}_1 = \{p_0 \mapsto w_0\} \cup \mathcal{H}_0$ and $\mathcal{B}_1 = \{p_0 \mapsto \emptyset\} \cup \mathcal{B}_0$ and $O_1 = (\{p_0 \mapsto \{\ell_0\}\} \cup O_0)$                                |                                                                                                          |
| 2065 |                                                                                                                                                                                                                  |                                                                                                          |
| 2066 | $(unop\{\tau_0\} ((v_0))^{\overline{\ell}_0}{}^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$                                                                                                                      | $\triangleright_{\overline{\tau}} (\text{InvariantErr})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$     |
| 2067 | if $v_0 \notin (v)^\ell$ and $\delta(unop, \mathcal{H}_0(v_0))$ is undefined                                                                                                                                     |                                                                                                          |
| 2068 |                                                                                                                                                                                                                  |                                                                                                          |
| 2069 | $(unop\{\mathcal{U}\} ((v_0))^{\overline{\ell}_0}{}^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$                                                                                                                 | $\triangleright_{\overline{\tau}} (\text{TagErr})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$           |
| 2070 | if $v_0 \notin (v)^\ell$ and $\delta(unop, \mathcal{H}_0(v_0))$ is undefined                                                                                                                                     |                                                                                                          |
| 2071 |                                                                                                                                                                                                                  |                                                                                                          |
| 2072 | $(unop\{\tau/\mathcal{U}\} ((p_0))^{\overline{\ell}_0}{}^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$                                                                                                            | $\triangleright_{\overline{\tau}}$                                                                       |
| 2073 | $(\text{check}\{\tau/\mathcal{U}\} ((\delta(unop, \mathcal{H}_0(p_0))))^{\overline{\ell}_0} p_0)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0[p_0 \cup \overline{\ell}_0]$                                        |                                                                                                          |
| 2074 | if $\delta(unop, \mathcal{H}_0(p_0))$ is defined                                                                                                                                                                 |                                                                                                          |
| 2075 |                                                                                                                                                                                                                  |                                                                                                          |
| 2076 | $(binop\{\tau_0\} ((v_0))^{\overline{\ell}_0} ((v_1))^{\overline{\ell}_1}{}^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$                                                                                         | $\triangleright_{\overline{\tau}} (\text{InvariantErr})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$     |
| 2077 | if $v_0 \notin (v)^\ell$ and $v_1 \notin (v)^\ell$ and $\delta(binop, v_0, v_1)$ is undefined                                                                                                                    |                                                                                                          |
| 2078 |                                                                                                                                                                                                                  |                                                                                                          |
| 2079 | $(binop\{\mathcal{U}\} ((v_0))^{\overline{\ell}_0} ((v_1))^{\overline{\ell}_1}{}^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$                                                                                    | $\triangleright_{\overline{\tau}} (\text{TagErr})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$           |
| 2080 | if $v_0 \notin (v)^\ell$ and $v_1 \notin (v)^\ell$ and $\delta(binop, v_0, v_1)$ is undefined                                                                                                                    |                                                                                                          |
| 2081 |                                                                                                                                                                                                                  |                                                                                                          |
| 2082 | $(binop\{\tau/\mathcal{U}\} ((i_0))^{\overline{\ell}_0} ((i_1))^{\overline{\ell}_1}{}^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$                                                                               | $\triangleright_{\overline{\tau}} (\delta(binop, i_0, i_1))^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$ |
| 2083 | if $\delta(binop, i_0, i_1)$ is defined                                                                                                                                                                          |                                                                                                          |
| 2084 |                                                                                                                                                                                                                  |                                                                                                          |
| 2085 | $(app\{\tau_0\} ((v_0))^{\overline{\ell}_0} v_1)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$                                                                                                                    | $\triangleright_{\overline{\tau}} (\text{InvariantErr})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$     |
| 2086 | if $v_0 \notin (v)^\ell$ and $\mathcal{H}_0(v_0) \notin (\lambda x. e) \cup (\lambda(x : \tau). e)$                                                                                                              |                                                                                                          |
| 2087 |                                                                                                                                                                                                                  |                                                                                                          |
| 2088 | $(app\{\mathcal{U}\} ((v_0))^{\overline{\ell}_0} v_1)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$                                                                                                               | $\triangleright_{\overline{\tau}} (\text{TagErr})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$           |
| 2089 | if $v_0 \notin (v)^\ell$ and $\mathcal{H}_0(v_0) \notin (\lambda x. e) \cup (\lambda(x : \tau). e)$                                                                                                              |                                                                                                          |
| 2090 |                                                                                                                                                                                                                  |                                                                                                          |
| 2091 | $(app\{\tau/\mathcal{U}\} ((p_0))^{\overline{\ell}_0} ((v_0))^{\overline{\ell}_1}{}^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$                                                                                 | $\triangleright_{\overline{\tau}}$                                                                       |
| 2092 | $(\text{check}\{\tau/\mathcal{U}\} ((e_0[x_0 \leftarrow ((v_0))^{\overline{\ell}_1 \ell_0 \text{rev}(\overline{\ell}_0)})])^{\overline{\ell}_0} p_0)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_1; O_1$                |                                                                                                          |
| 2093 | if $\mathcal{H}_0(p_0) = \lambda(x_0 : \tau_0). e_0$ and <i>shape-match</i> ( $\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0)$ )                                                                                     |                                                                                                          |
| 2094 | where $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \text{rev}(\mathcal{B}_0(p_0))]$ and $O_1 = O_0[p_0 \cup \overline{\ell}_0 \ell_0][v_0 \cup \overline{\ell}_1 O_0(p_0) \cup \ell_0 \text{rev}(\overline{\ell}_0)]$ |                                                                                                          |
| 2095 |                                                                                                                                                                                                                  |                                                                                                          |
| 2096 | $(app\{\tau/\mathcal{U}\} ((p_0))^{\overline{\ell}_0} ((v_0))^{\overline{\ell}_1}{}^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$                                                                                 | $\triangleright_{\overline{\tau}}$                                                                       |
| 2097 | $(\text{BoundaryErr}(\mathcal{B}_0(v_0) \cup \text{rev}(\mathcal{B}_0(p_0)), ((v_0))^{\overline{\ell}_1 \ell_0 \text{rev}(\overline{\ell}_0)}))^{\ell_0}; \mathcal{H}_0; \mathcal{B}_1; O_1$                     |                                                                                                          |
| 2098 | if $\mathcal{H}_0(p_0) = \lambda(x_0 : \tau_0). e_0$ and $v_0 \notin (v)^\ell$ and $\neg \text{shape-match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$                                                         |                                                                                                          |
| 2099 | where $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \text{rev}(\mathcal{B}_0(p_0))]$ and $O_1 = O_0[p_0 \cup \overline{\ell}_0 \ell_0][v_0 \cup O_0(p_0) \cup \overline{\ell}_1 \ell_0 \text{rev}(\overline{\ell}_0)]$ |                                                                                                          |
| 2100 |                                                                                                                                                                                                                  |                                                                                                          |
| 2101 | $(app\{\tau_0\} ((p_0))^{\overline{\ell}_0} ((v_0))^{\overline{\ell}_1}{}^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; O_0$                                                                                           | $\triangleright_{\overline{\tau}}$                                                                       |
| 2102 | $(\text{check}\{\tau_0\} ((e_0[x_0 \leftarrow ((v_0))^{\overline{\ell}_1 \ell_0 \text{rev}(\overline{\ell}_0)})])^{\overline{\ell}_0} p_0)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_1; O_1$                          |                                                                                                          |
| 2103 | if $\mathcal{H}_0(p_0) = \lambda x_0. e_0$ and $v_0 \notin (v)^\ell$                                                                                                                                             |                                                                                                          |
| 2104 | where $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \text{rev}(\mathcal{B}_0(p_0))]$                                                                                                                                   |                                                                                                          |
| 2105 | and $O_1 = O_0[p_0 \cup \overline{\ell}_0 \ell_0][v_0 \cup O_0(p_0) \cup \overline{\ell}_1 \ell_0 \text{rev}(\overline{\ell}_0)]$                                                                                |                                                                                                          |
| 2106 |                                                                                                                                                                                                                  |                                                                                                          |
| 2107 |                                                                                                                                                                                                                  |                                                                                                          |

2108  $(\text{app}\{\mathcal{U}\}((p_0))^{\bar{\ell}_0}((v_0))^{\bar{\ell}_1})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \triangleright_{\bar{\Gamma}} ((e_0[x_0 \leftarrow ((v_0))^{\bar{\ell}_1 \ell_0 \text{rev}(\bar{\ell}_0)}])^{\bar{\ell}_0 \ell_0}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_1$   
 2109     if  $\mathcal{H}_0(p_0) = \lambda x_0. e_0$  and  $v_0 \notin (v)^{\ell}$   
 2110     and  $\mathcal{O}_1 = \mathcal{O}_0[p_0 \cup \bar{\ell}_0 \ell_0][v_0 \cup \mathcal{O}_0(p_0) \cup \bar{\ell}_1 \ell_0 \text{rev}(\bar{\ell}_0)]$   
 2111  
 2112  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)((v_0))^{\bar{\ell}_0})^{\ell_2}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \triangleright_{\bar{\Gamma}} ((v_0))^{\bar{\ell}_0 \ell_2}; \mathcal{H}_0; \mathcal{B}_1; \mathcal{O}_1$   
 2113     if *shape-match*( $\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0)$ )  
 2114     where  $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}]$  and  $\mathcal{O}_1 = \mathcal{O}_0[v_0 \cup \bar{\ell}_0 \ell_2]$   
 2115  
 2116  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)((v_0))^{\bar{\ell}_0})^{\ell_2}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \triangleright_{\bar{\Gamma}}$   
 2117      $(\text{BoundaryErr}(\{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}, ((v_0))^{\bar{\ell}_0})^{\ell_2}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0$   
 2118     if  $v_0 \notin (v)^{\ell}$  and  $\neg \text{shape-match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$   
 2119  
 2120  $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)((v_0))^{\bar{\ell}_0})^{\ell_2}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \triangleright_{\bar{\Gamma}} ((v_0))^{\bar{\ell}_0 \ell_2}; \mathcal{H}_0; \mathcal{B}_1; \mathcal{O}_1$   
 2121     if *shape-match*( $\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0)$ )  
 2122     where  $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}]$  and  $\mathcal{O}_1 = \mathcal{O}_0[v_0 \cup \bar{\ell}_0 \ell_2]$   
 2123  
 2124  $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)((v_0))^{\bar{\ell}_0})^{\ell_2}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \triangleright_{\bar{\Gamma}} (\text{InvariantErr})^{\ell_2}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0$   
 2125     if  $v_0 \notin (v)^{\ell}$  and  $\neg \text{shape-match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$   
 2126  
 2127  $(\text{check}\{\mathcal{U}\} v_0 p_0)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \triangleright_{\bar{\Gamma}} ((v_0))^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0$   
 2128  $(\text{check}\{\tau_0\}((v_0))^{\bar{\ell}_0} p_0)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \triangleright_{\bar{\Gamma}} ((v_0))^{\bar{\ell}_0 \ell_0}; \mathcal{H}_0; \mathcal{B}_1; \mathcal{O}_1$   
 2129     if  $v_0 \notin (v)^{\ell}$  and *shape-match*( $\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0)$ )  
 2130     where  $\mathcal{B}_1 = \mathcal{B}_0[v_0 \cup \mathcal{B}_0(p_0)]$  and  $\mathcal{O}_1 = \mathcal{O}_0[v_0 \cup \mathcal{O}_0(p_0) \cup \bar{\ell}_0 \ell_0]$   
 2131  
 2132  $(\text{check}\{\tau_0\}((v_0))^{\bar{\ell}_0} p_0)^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_0 \triangleright_{\bar{\Gamma}}$   
 2133      $(\text{BoundaryErr}(\mathcal{B}_0(v_0) \cup \mathcal{B}_0(p_0), ((v_0))^{\bar{\ell}_0})^{\ell_0}; \mathcal{H}_0; \mathcal{B}_0; \mathcal{O}_1$   
 2134     if  $v_0 \notin (v)^{\ell}$  and  $\neg \text{shape-match}(\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0))$   
 2135     where  $\mathcal{O}_1 = \mathcal{O}_0[v_0 \cup \mathcal{O}_0(p_0)]$   
 2136  
 2137  
 2138  
 2139  
 2140  
 2141  
 2142  
 2143  
 2144  
 2145  
 2146  
 2147  
 2148  
 2149  
 2150  
 2151  
 2152  
 2153  
 2154  
 2155  
 2156

2157 THEOREM 6.48 (TRANSIENT INCOMPLETE MONITORING). *Transient does not satisfy CM*

2158 PROOF. Whenever a pair or function crosses a boundary, Transient lets it across without adding  
 2159 a guard wrapper. Thus, the value gains an additional ownership label.  $\square$   
 2160

2161 THEOREM 6.49 (TRANSIENT BLAME UNSOUNDNESS). *Transient does not satisfy BS*

2162 PROOF. Let component  $\ell_0$  define a function  $f_0$  and export it to components  $\ell_1$  and  $\ell_2$ . If component  
 2163  $\ell_2$  triggers a type mismatch, then component  $\ell_1$  gets blamed even though there is no direct channel  
 2164 from  $\ell_1$  to  $\ell_2$ .

2165 The following term expresses the scenario above, using a let-expression to abbreviate untyped  
 2166 function application:

2167  $(\text{let } f_0 = (\lambda x_0. \langle x_0, x_0 \rangle) \text{ in}$   
 2168  $\text{let } f_1 = (\text{stat } (\ell_0 \blacktriangleleft (\text{Int} \Rightarrow \text{Int}) \blacktriangleleft \ell_1) (\text{dyn } (\ell_1 \blacktriangleleft (\text{Int} \Rightarrow \text{Int}) \blacktriangleleft \ell_0) (f_0)^{\ell_0})^{\ell_1} \text{ in}$   
 2169  $\text{stat } (\ell_0 \blacktriangleleft \text{Int} \blacktriangleleft \ell_2) (\text{app}\{\text{Int}\} (\text{dyn } (\ell_2 \blacktriangleleft (\text{Int} \Rightarrow \text{Int}) \blacktriangleleft \ell_0) (f_0)^{\ell_0}) 5)^{\ell_2})^{\ell_0}; \emptyset; \emptyset; \emptyset$

2170 Reduction ends in a boundary error that blames all three components.  $\square$   
 2171

2172 THEOREM 6.50 (TRANSIENT BLAME INCOMPLETENESS). *Transient does not satisfy BC.*

2173 PROOF. The rule for untyped function application does not update the blame map. The following  
 2174 term illustrates the problem by using an untyped identity function  $f_1$  to coerce the type of another  
 2175 function ( $f_0$ ). After the coercion, an application leads to type mismatch.

2176  $(\text{let } f_0 = \text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{dyn } (\ell_1 \blacktriangleleft \tau_0 \blacktriangleleft \ell_2) (\lambda x_0. x_0)) \text{ in}$   
 2177  $\text{let } f_1 = \text{stat } (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_3) (\text{dyn } (\ell_3 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_4) (\lambda x_1. x_1)) \text{ in}$   
 2178  $\text{stat } (\ell_0 \blacktriangleleft (\text{Int} \times \text{Int}) \blacktriangleleft \ell_5)$   
 2179  $(\text{app}\{\text{Int} \times \text{Int}\} (\text{dyn } (\ell_5 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) (\text{app}\{\mathcal{U}\} f_1 f_0)^{\ell_0}) 42)^{\ell_5})^{\ell_0}; \emptyset; \emptyset; \emptyset$

2180 Reduction ends in a boundary error that does not report the crucial labels  $\ell_3$  and  $\ell_4$ .  $\square$   
 2181

### 2182 6.8.3 Relation to Forgetful.

2183 THEOREM 6.51.  $F \lesssim T$ .

2184 PROOF. Indirectly, via  $T \approx A$  (theorem 6.59) and  $F \lesssim A$  (theorem 6.61). Both appear in the next  
 2185 section.  $\square$   
 2186

2187  
2188  
2189  
2190  
2191  
2192  
2193  
2194  
2195  
2196  
2197  
2198  
2199  
2200  
2201  
2202  
2203  
2204  
2205

## 6.9 Amnesic and its Properties

### 6.9.1 Semantics, Type Soundness.

$$\boxed{e \triangleright_A e}$$

|      |                                                                                                                                                                                                            |                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| 2206 | $unop\{\tau_0\} v_0$                                                                                                                                                                                       | $\triangleright_A$ InvariantErr                                                                                |
| 2207 | if $v_0 \notin (\mathbb{G}(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell) v)$ and $\delta(unop, v_0)$ is undefined                                                                    |                                                                                                                |
| 2208 | $unop\{\tau_0\} v_0$                                                                                                                                                                                       | $\triangleright_A \delta(unop, v_0)$                                                                           |
| 2209 | if $\delta(unop, v_0)$ is defined                                                                                                                                                                          |                                                                                                                |
| 2210 | $fst\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0)$                                                                                                               | $\triangleright_A$ dyn $b_0$ (fst{ $\mathcal{U}$ } $v_0$ )                                                     |
| 2211 | where $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$                                                                                                                                 |                                                                                                                |
| 2212 | $snd\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0)$                                                                                                               | $\triangleright_A$ dyn $b_0$ (snd{ $\mathcal{U}$ } $v_0$ )                                                     |
| 2213 | where $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$                                                                                                                                 |                                                                                                                |
| 2214 | $binop\{\tau_0\} v_0 v_1$                                                                                                                                                                                  | $\triangleright_A$ InvariantErr                                                                                |
| 2215 | if $\delta(binop, v_0, v_1)$ is undefined                                                                                                                                                                  |                                                                                                                |
| 2216 | $binop\{\tau_0\} v_0 v_1$                                                                                                                                                                                  | $\triangleright_A \delta(binop, v_0, v_1)$                                                                     |
| 2217 | if $\delta(binop, v_0, v_1)$ is defined                                                                                                                                                                    |                                                                                                                |
| 2218 | $app\{\tau_0\} v_0 v_1$                                                                                                                                                                                    | $\triangleright_A$ InvariantErr                                                                                |
| 2219 | if $v_0 \notin (\lambda(x : \tau). e) \cup (\mathbb{G}(\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell) v)$                                                                        |                                                                                                                |
| 2220 | $app\{\tau_0\} (\lambda(x_0 : \tau_1). e_0) v_0$                                                                                                                                                           | $\triangleright_A e_0[x_0 \leftarrow v_0]$                                                                     |
| 2221 | $app\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) v_1$                                                                                                           | $\triangleright_A$ dyn $b_0$ (app{ $\mathcal{U}$ } $v_0$ (stat $b_1$ $v_1$ ))                                  |
| 2222 | where $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft dom(\tau_1) \blacktriangleleft \ell_0)$                                                   |                                                                                                                |
| 2223 | $dyn(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$                                                                                                                                      | $\triangleright_A \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$                  |
| 2224 | if $shape-match(\lfloor \tau_0 \rfloor, v_0)$                                                                                                                                                              |                                                                                                                |
| 2225 | and $v_0 \in (\mathbb{T}_? \bar{b}(\lambda(x : \tau). e)) \cup (\mathbb{T}_? \bar{b}\langle v, v \rangle) \cup (\mathbb{T}_? \bar{b}(\mathbb{G}(\ell \blacktriangleleft \tau \blacktriangleleft \ell) v))$ |                                                                                                                |
| 2226 | $dyn(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\mathbb{T}_? \bar{b}_0 i_0)$                                                                                                             | $\triangleright_A i_0$                                                                                         |
| 2227 | if $shape-match(\lfloor \tau_0 \rfloor, i_0)$                                                                                                                                                              |                                                                                                                |
| 2228 | $dyn(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$                                                                                                                                      | $\triangleright_A$ BoundaryErr $((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \bar{b}_0, v_0)$ |
| 2229 | if $\neg shape-match(\lfloor \tau_0 \rfloor, v_0)$ and $\bar{b}_0 = get-trace(v_0)$                                                                                                                        |                                                                                                                |
| 2230 |                                                                                                                                                                                                            |                                                                                                                |
| 2231 |                                                                                                                                                                                                            |                                                                                                                |
| 2232 |                                                                                                                                                                                                            |                                                                                                                |
| 2233 |                                                                                                                                                                                                            |                                                                                                                |
| 2234 |                                                                                                                                                                                                            |                                                                                                                |
| 2235 |                                                                                                                                                                                                            |                                                                                                                |
| 2236 |                                                                                                                                                                                                            |                                                                                                                |
| 2237 |                                                                                                                                                                                                            |                                                                                                                |
| 2238 |                                                                                                                                                                                                            |                                                                                                                |
| 2239 |                                                                                                                                                                                                            |                                                                                                                |
| 2240 |                                                                                                                                                                                                            |                                                                                                                |
| 2241 |                                                                                                                                                                                                            |                                                                                                                |
| 2242 |                                                                                                                                                                                                            |                                                                                                                |
| 2243 |                                                                                                                                                                                                            |                                                                                                                |
| 2244 |                                                                                                                                                                                                            |                                                                                                                |
| 2245 |                                                                                                                                                                                                            |                                                                                                                |
| 2246 |                                                                                                                                                                                                            |                                                                                                                |
| 2247 |                                                                                                                                                                                                            |                                                                                                                |
| 2248 |                                                                                                                                                                                                            |                                                                                                                |
| 2249 |                                                                                                                                                                                                            |                                                                                                                |
| 2250 |                                                                                                                                                                                                            |                                                                                                                |
| 2251 |                                                                                                                                                                                                            |                                                                                                                |
| 2252 |                                                                                                                                                                                                            |                                                                                                                |
| 2253 |                                                                                                                                                                                                            |                                                                                                                |
| 2254 |                                                                                                                                                                                                            |                                                                                                                |

|      |                                |                                                                                                                                                                                                                                                            |
|------|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2255 | $e \xrightarrow{\mathbb{A}} e$ |                                                                                                                                                                                                                                                            |
| 2256 |                                | $\text{unop}\{\mathcal{U}\} v_0 \xrightarrow{\mathbb{A}} \text{TagErr}$                                                                                                                                                                                    |
| 2257 |                                | if $v_1 = \text{rem-trace}(v_0)$ and $v_1 \notin \mathbb{G}(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell) v$ and $\delta(\text{unop}, v_1)$ is undefined                                                                             |
| 2258 |                                | $\text{unop}\{\mathcal{U}\} v_0 \xrightarrow{\mathbb{A}} \text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, v_1))$                                                                                                                                |
| 2259 |                                | if $v_1 = \text{rem-trace}(v_0)$ and $\delta(\text{unop}, v_1)$ is defined                                                                                                                                                                                 |
| 2260 |                                | $\text{fst}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) \xrightarrow{\mathbb{A}} \text{trace } \bar{b}_0 (\text{stat } b_0 (\text{fst}\{\tau_1\} v_0))$                           |
| 2261 |                                | where $\tau_1 = \text{fst}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$                                                                                                                                               |
| 2262 |                                | $\text{snd}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) \xrightarrow{\mathbb{A}} \text{trace } \bar{b}_0 (\text{stat } b_0 (\text{snd}\{\tau_1\} v_0))$                           |
| 2263 |                                | where $\tau_1 = \text{snd}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$                                                                                                                                               |
| 2264 |                                | $\text{binop}\{\mathcal{U}\} v_0 v_1 \xrightarrow{\mathbb{A}} \text{TagErr}$                                                                                                                                                                               |
| 2265 |                                | if $v_2 = \text{rem-trace}(v_0)$ and $v_3 = \text{rem-trace}(v_1)$ and $\delta(\text{binop}, v_2, v_3)$ is undefined                                                                                                                                       |
| 2266 |                                | $\text{binop}\{\mathcal{U}\} v_0 v_1 \xrightarrow{\mathbb{A}} \delta(\text{binop}, v_2, v_3)$                                                                                                                                                              |
| 2267 |                                | if $v_2 = \text{rem-trace}(v_0)$ and $v_3 = \text{rem-trace}(v_1)$ and $\delta(\text{binop}, v_2, v_3)$ is defined                                                                                                                                         |
| 2268 |                                | $\text{app}\{\mathcal{U}\} v_0 v_1 \xrightarrow{\mathbb{A}} \text{TagErr}$                                                                                                                                                                                 |
| 2269 |                                | if $v_0 \notin (\mathbb{T}_? \bar{b}(\lambda x. e)) \cup (\mathbb{T}_? \bar{b}(\mathbb{G}(\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell) v))$                                                                                    |
| 2270 |                                | $\text{app}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\lambda x_0. e_0)) v_0 \xrightarrow{\mathbb{A}} \text{trace } \bar{b}_0 (e_0[x_0 \leftarrow v_1])$                                                                                                     |
| 2271 |                                | where $v_1 = \text{add-trace}(\text{rev}(\bar{b}_0), v_0)$                                                                                                                                                                                                 |
| 2272 |                                | $\text{app}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) v_1 \xrightarrow{\mathbb{A}} \text{trace } \bar{b}_0 (\text{stat } b_0 (\text{app}\{\tau_2\} v_0 (\text{dyn } b_1 v_2)))$ |
| 2273 |                                | where $\tau_2 = \text{cod}(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0)$                                                          |
| 2274 |                                | and $v_2 = \text{add-trace}(\text{rev}(\bar{b}_0), v_1)$                                                                                                                                                                                                   |
| 2275 |                                | $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \xrightarrow{\mathbb{A}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$                                                                          |
| 2276 |                                | if $\text{shape-match}(\lfloor \tau_0 \rfloor, v_0)$ and $v_0 \in (\lambda(x : \tau). e) \cup \langle v, v \rangle$                                                                                                                                        |
| 2277 |                                | $\text{stat } b_0 (\mathbb{G} b_1 (\mathbb{T}_? \bar{b}_0 v_0)) \xrightarrow{\mathbb{A}} \text{trace}(b_0 b_1 \bar{b}_0) v_0$                                                                                                                              |
| 2278 |                                | if $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$ and $\text{shape-match}(\lfloor \tau_0 \rfloor, v_0)$                                                                                                                              |
| 2279 |                                | and $v_0 \in (\lambda x. e) \cup \langle v, v \rangle \cup (\mathbb{G} b (\lambda(x : \tau). e)) \cup (\mathbb{G} b \langle v, v \rangle)$                                                                                                                 |
| 2280 |                                | $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0 \xrightarrow{\mathbb{A}} i_0$                                                                                                                                                 |
| 2281 |                                | if $\text{shape-match}(\lfloor \tau_0 \rfloor, i_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$                                                                                                                              |
| 2282 |                                | $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \xrightarrow{\mathbb{A}} \text{InvariantErr}$                                                                                                                                 |
| 2283 |                                | if $\neg \text{shape-match}(\lfloor \tau_0 \rfloor, v_0)$                                                                                                                                                                                                  |
| 2284 |                                | $\text{trace } \bar{b}_0 v_0 \xrightarrow{\mathbb{A}} v_1$                                                                                                                                                                                                 |
| 2285 |                                | where $v_1 = \text{add-trace}(\bar{b}_0, v_0)$                                                                                                                                                                                                             |
| 2286 |                                | $e \xrightarrow{\mathbb{A}}^* e$ is the transitive, reflexive, compatible (with respect to evaluation contexts $E$ , section 6.2)                                                                                                                          |
| 2287 |                                | closure of the relation $\bigcup \{\triangleright_{\mathbb{A}}, \blacktriangleright_{\mathbb{A}}\}$                                                                                                                                                        |
| 2288 |                                | $A(e) = F(e)$                                                                                                                                                                                                                                              |
| 2289 |                                | holds for typed expressions with at most two guard wrappers and for untyped expressions                                                                                                                                                                    |
| 2290 |                                | with at most one guard wrapper.                                                                                                                                                                                                                            |
| 2291 |                                |                                                                                                                                                                                                                                                            |
| 2292 |                                |                                                                                                                                                                                                                                                            |
| 2293 |                                |                                                                                                                                                                                                                                                            |
| 2294 |                                |                                                                                                                                                                                                                                                            |
| 2295 |                                |                                                                                                                                                                                                                                                            |
| 2296 |                                |                                                                                                                                                                                                                                                            |
| 2297 |                                |                                                                                                                                                                                                                                                            |
| 2298 |                                |                                                                                                                                                                                                                                                            |
| 2299 |                                |                                                                                                                                                                                                                                                            |
| 2300 |                                |                                                                                                                                                                                                                                                            |
| 2301 |                                |                                                                                                                                                                                                                                                            |
| 2302 |                                |                                                                                                                                                                                                                                                            |
| 2303 |                                |                                                                                                                                                                                                                                                            |

2304 THEOREM 6.52 (AMNESIC TYPE SOUNDNESS). *Amnesic satisfies TS(1)*

2305 PROOF. By lemma 6.53, progress (lemma 6.54), and preservation (lemma 6.55). □

2307 LEMMA 6.53. *If  $e_0 : \tau/\mathcal{U}$  wf then  $A(e_0)$ .*

2308 PROOF. Wrappers are not part of the surface language. □

2310 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*

- 2311 holds:
- 2312 •  $e_0 \in v \cup \text{Err}$
  - 2313 •  $\tau/\mathcal{U} \in \tau$  and  $\exists e_1. e_0 \triangleright_A e_1$
  - 2314 •  $\tau/\mathcal{U} \in \mathcal{U}$  and  $\exists e_1. e_0 \blacktriangleright_A e_1$

2316 PROOF SKETCH. By unique decomposition (lemma 6.1) and case analysis. More details in appendix: lemma A.26. □

2318 LEMMA 6.55 (AMNESIC TYPE PRESERVATION).

2319 *If  $\cdot \vdash_1 E_0[e_0] : \tau/\mathcal{U}$  and  $A(E_0[e_0])$  and  $e_0(\triangleright_A \cup \blacktriangleright_A)e_1$  then  $\cdot \vdash_1 E_0[e_1] : \tau/\mathcal{U}$  and  $A(E_0[e_1])$ .*

2320 PROOF SKETCH. By case analysis of each reduction relation. More details in appendix: lemma A.27. □

2322 LEMMA 6.56.

- 2324 • *If  $A(E_0[e_0])$  then  $A(e_0)$*
- 2325 • *If  $A(E_0[e_0])$  and  $A(e_1)$  then  $A(E_0[e_1])$*

2327 PROOF SKETCH. By lemma 6.37. □

2328

2329

2330

2331

2332

2333

2334

2335

2336

2337

2338

2339

2340

2341

2342

2343

2344

2345

2346

2347

2348

2349

2350

2351

2352



6.9.2 *Lifted Semantics, Complete Monitoring, Blame.*

|      |                                                                                                                                                                                                                               |                                                                                                                                                           |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2353 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2354 | $(e)^\ell \triangleright_{\bar{A}} (e)^\ell$                                                                                                                                                                                  | lifted version of $\triangleright_A$                                                                                                                      |
| 2355 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2356 | $(unop\{\tau_0\}((v_0))^{\bar{\ell}_0})^{\ell_0}$                                                                                                                                                                             | $\triangleright_{\bar{A}} (\text{InvariantErr})^{\ell_0}$                                                                                                 |
| 2357 | if $v_0 \notin (v)^\ell \cup (\mathbb{G}(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell) v)$ and $\delta(unop, v_0)$ is undefined                                                                         |                                                                                                                                                           |
| 2358 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2359 | $(unop\{\tau_0\}((v_0))^{\bar{\ell}_0})^{\ell_0}$                                                                                                                                                                             | $\triangleright_{\bar{A}} (\delta(unop, v_0))^{\bar{\ell}_0 \ell_0}$                                                                                      |
| 2360 | if $\delta(unop, v_0)$ is defined                                                                                                                                                                                             |                                                                                                                                                           |
| 2361 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2362 | $(fst\{\tau_0\}(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                                                                                 | $\triangleright_{\bar{A}} (\text{dyn } b_0 (\text{fst}\{\mathcal{U}\}(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                              |
| 2363 | where $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$                                                                                                                                                    |                                                                                                                                                           |
| 2364 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2365 | $(snd\{\tau_0\}(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                                                                                 | $\triangleright_{\bar{A}} (\text{dyn } b_0 (\text{snd}\{\mathcal{U}\}(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                              |
| 2366 | where $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$                                                                                                                                                    |                                                                                                                                                           |
| 2367 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2368 | $(binop\{\tau_0\}((v_0))^{\bar{\ell}_0}((v_1))^{\bar{\ell}_1})^{\ell_0}$                                                                                                                                                      | $\triangleright_{\bar{A}} (\text{InvariantErr})^{\ell_0}$                                                                                                 |
| 2369 | if $v_0 \notin (v)^\ell$ and $v_1 \notin (v)^\ell$ and $\delta(binop, v_0, v_1)$ is undefined                                                                                                                                 |                                                                                                                                                           |
| 2370 | $(binop\{\tau_0\}((v_0))^{\bar{\ell}_0}((v_1))^{\bar{\ell}_1})^{\ell_0}$                                                                                                                                                      | $\triangleright_{\bar{A}} (\delta(binop, v_0, v_1))^{\ell_0}$                                                                                             |
| 2371 | if $\delta(binop, v_0, v_1)$ is defined                                                                                                                                                                                       |                                                                                                                                                           |
| 2372 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2373 | $(app\{\tau_0\}((v_0))^{\bar{\ell}_0} v_1)^{\ell_0}$                                                                                                                                                                          | $\triangleright_{\bar{A}} (\text{InvariantErr})^{\ell_0}$                                                                                                 |
| 2374 | if $v_0 \notin (v)^\ell \cup (\lambda(x : \tau). e) \cup (\mathbb{G} b v)$                                                                                                                                                    |                                                                                                                                                           |
| 2375 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2376 | $(app\{\tau_0\}((\lambda(x_0 : \tau_1). e_0))^{\bar{\ell}_0} v_0)^{\ell_0}$                                                                                                                                                   | $\triangleright_{\bar{A}} ((e_0[x_0 \leftarrow ((v_0))^{\ell_0 \text{rev}(\bar{\ell}_0)}]))^{\bar{\ell}_0 \ell_0}$                                        |
| 2377 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2378 | $(app\{\tau_0\}(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)(v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3} v_1$                                                                                             | $\triangleright_{\bar{A}}$                                                                                                                                |
| 2379 | $(\text{dyn } b_0 (\text{app}\{\mathcal{U}\} v_0 (\text{stat } b_1 ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)})^{\ell_2}))^{\bar{\ell}_0 \ell_3}$                                                                               |                                                                                                                                                           |
| 2380 | where $b_0 = (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0)$                                                               |                                                                                                                                                           |
| 2381 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2382 | $(\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2}$                                                                                                                  | $\triangleright_{\bar{A}} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2}$                       |
| 2383 | if <i>shape-match</i> ( $\lfloor \tau_0 \rfloor, v_0$ )                                                                                                                                                                       |                                                                                                                                                           |
| 2384 | and $v_0 \in (\mathbb{T}_? \bar{b}(\lambda(x : \tau). e)) \cup (\mathbb{T}_? \bar{b}\langle v, v \rangle) \cup (\mathbb{T}_? \bar{b}(\mathbb{G}(\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell) v))$ |                                                                                                                                                           |
| 2385 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2386 | $(\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((\mathbb{T}_? \bar{b}_0((i_0))^{\bar{\ell}_0})^{\bar{\ell}_1})^{\ell_2}$                                                                          | $\triangleright_{\bar{A}} (i_0)^{\ell_2}$                                                                                                                 |
| 2387 | if <i>shape-match</i> ( $\lfloor \tau_0 \rfloor, i_0$ )                                                                                                                                                                       |                                                                                                                                                           |
| 2388 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2389 | $(\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_2})^{\ell_3}$                                                                                                                  | $\triangleright_{\bar{A}} (\text{BoundaryErr}(((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \bar{b}_0, ((v_0))^{\bar{\ell}_2}))^{\ell_3}$ |
| 2390 | if $\neg \text{shape-match}(\lfloor \tau_0 \rfloor, v_0)$ and $\bar{b}_0 = \text{get-trace}(v_0)$                                                                                                                             |                                                                                                                                                           |
| 2391 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2392 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2393 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2394 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2395 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2396 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2397 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2398 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2399 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2400 |                                                                                                                                                                                                                               |                                                                                                                                                           |
| 2401 |                                                                                                                                                                                                                               |                                                                                                                                                           |

|                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2402<br>2403<br>2404<br>2405<br>2406<br>2407<br>2408<br>2409<br>2410<br>2411<br>2412<br>2413<br>2414<br>2415<br>2416<br>2417<br>2418<br>2419<br>2420<br>2421<br>2422<br>2423<br>2424<br>2425<br>2426<br>2427<br>2428<br>2429<br>2430<br>2431<br>2432<br>2433<br>2434<br>2435<br>2436<br>2437<br>2438<br>2439<br>2440<br>2441<br>2442<br>2443<br>2444<br>2445<br>2446<br>2447<br>2448<br>2449<br>2450 | <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-bottom: 10px;"> <math>(e)^\ell \xrightarrow{\bar{\Lambda}} (e)^\ell</math> </div> lifted version of $\xrightarrow{\Lambda}$<br>$(unop\{\mathcal{U}\}((v_0))^{\bar{\ell}_0})^{\ell_0} \xrightarrow{\bar{\Lambda}} (TagErr)^{\ell_0}$<br>if $v_0 \notin (v)^\ell \cup (\mathbb{G}(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell) v)$ and $\delta(unop, v_0)$ is undefined<br>$(unop\{\mathcal{U}\} v_0)^{\ell_0} \xrightarrow{\bar{\Lambda}}$<br>$(add\text{-}trace(get\text{-}trace(v_0), \delta(unop, v_1)))^{\ell_0}$<br>if $v_1 = rem\text{-}trace(v_0)$ and $\delta(unop, v_1)$ is defined<br>$(fst\{\mathcal{U}\}((\mathbb{T}_? \bar{b}_0((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)(v_0)^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4} \ell_5))) \xrightarrow{\bar{\Lambda}} (trace \bar{b}_0((stat b_0(fst\{\tau_1\} v_0)^{\ell_2}))^{\bar{\ell}_3})^{\bar{\ell}_4 \ell_5}$<br>where $\tau_1 = fst(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$<br>$(snd\{\mathcal{U}\}((\mathbb{T}_? \bar{b}_0((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)(v_0)^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4} \ell_5))) \xrightarrow{\bar{\Lambda}} (trace \bar{b}_0((stat b_0(snd\{\tau_1\} v_0)^{\ell_2}))^{\bar{\ell}_3})^{\bar{\ell}_4 \ell_5}$<br>where $\tau_1 = snd(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$<br>$(binop\{\mathcal{U}\}((v_0))^{\bar{\ell}_0}((v_1))^{\bar{\ell}_1})^{\ell_0} \xrightarrow{\bar{\Lambda}} (TagErr)^{\ell_0}$<br>if $v_2 = rem\text{-}trace(v_0)$ and $v_3 = rem\text{-}trace(v_1)$ and $\delta(binop, v_2, v_3)$ is undefined<br>$(binop\{\mathcal{U}\}((v_0))^{\bar{\ell}_0}((v_1))^{\bar{\ell}_1})^{\ell_0} \xrightarrow{\bar{\Lambda}} \delta(binop, v_2, v_3)$<br>if $v_2 = rem\text{-}trace(v_0)$ and $v_3 = rem\text{-}trace(v_1)$ and $\delta(binop, v_2, v_3)$ is defined<br>$(app\{\mathcal{U}\}((v_0))^{\bar{\ell}_0} v_1)^{\ell_0} \xrightarrow{\bar{\Lambda}} (TagErr)^{\ell_0}$<br>if $v_0 \notin (\mathbb{T}_? \bar{b}(\lambda x. e)) \cup (\mathbb{T}_? \bar{b}(\mathbb{G}(\ell \blacktriangleleft (\tau \Rightarrow \tau) \blacktriangleleft \ell) v))$<br>$(app\{\mathcal{U}\}((\mathbb{T}_? \bar{b}_0((\lambda x_0. e_0))^{\bar{\ell}_0})^{\bar{\ell}_1} \ell_2) v_0) \xrightarrow{\bar{\Lambda}} (trace \bar{b}_0((e_0[x_0 \leftarrow v_1]))^{\bar{\ell}_0})^{\bar{\ell}_1 \ell_2}$<br>where $v_1 = add\text{-}trace(rev(\bar{b}_0), ((v_0))^{\ell_2 rev(\bar{\ell}_1) rev(\bar{\ell}_0)})$<br>$(app\{\mathcal{U}\}((\mathbb{T}_? \bar{b}_0((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)(v_0)^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4} \ell_5) v_1) \xrightarrow{\bar{\Lambda}}$<br>$((trace \bar{b}_0((stat b_0(app\{\tau_1\} v_0(dyn b_1 v_2))^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4 \ell_5}))$<br>where $\tau_1 = cod(\tau_0)$ and $b_0 = (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)$ and $b_1 = (\ell_1 \blacktriangleleft dom(\tau_0) \blacktriangleleft \ell_0)$<br>and $v_2 = add\text{-}trace(rev(\bar{b}_0), ((v_1))^{\ell_5 rev(\bar{\ell}_3 \bar{\ell}_4)})$<br>$(stat(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)^{\ell_2} \xrightarrow{\bar{\Lambda}} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)^{\ell_2}$<br>if $shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$ and $v_0 \in ((\lambda(x : \tau). e))^{\bar{\ell}} \cup ((\langle v, v \rangle))^{\bar{\ell}}$<br>$(stat b_0((\mathbb{G} b_1((\mathbb{T}_? \bar{b}_2 v_0))^{\bar{\ell}_0})^{\bar{\ell}_1} \ell_2)) \xrightarrow{\bar{\Lambda}} (trace(b_0 b_1 \bar{b}_2)((v_0))^{\bar{\ell}_0 \bar{\ell}_1 \ell_2})^{\ell_2}$<br>if $b_0 = (\ell_3 \blacktriangleleft \tau_0 \blacktriangleleft \ell_4)$ and $shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$<br>and $v_0 \in ((\lambda x. e))^{\bar{\ell}} \cup ((\langle v, v \rangle))^{\bar{\ell}} \cup ((\mathbb{G} b(\lambda(x : \tau). e))^{\bar{\ell}} \cup ((\mathbb{G} b \langle v, v \rangle))^{\bar{\ell}}$<br>$(stat(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)((i_0))^{\bar{\ell}_2})^{\ell_3} \xrightarrow{\bar{\Lambda}} (i_0)^{\ell_3}$<br>if $shape\text{-}match(\lfloor \tau_0 \rfloor, i_0)$<br>$(stat(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)((v_0))^{\bar{\ell}_2})^{\ell_3} \xrightarrow{\bar{\Lambda}} (InvariantErr)^{\ell_3}$<br>if $\neg shape\text{-}match(\lfloor \tau_0 \rfloor, v_0)$<br>$(trace \bar{b}_0 v_0)^{\ell_0} \xrightarrow{\bar{\Lambda}} (v_1)^{\ell_0}$<br>where $v_1 = add\text{-}trace(\bar{b}_0, v_0)$ |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

2451 THEOREM 6.57 (AMNESIC INCOMPLETE MONITORING). *Amnesic does not satisfy CM*

2452

2453

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

2454

2455

$(\text{stat } (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) (\text{dyn } (\ell_1 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_2) (\lambda x_0. x_0)^{\ell_2})^{\ell_1})^{\ell_0}$

2456

$\rightarrow_A (\text{stat } (\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) (\mathbb{G} (\ell_1 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_2) (\lambda x_0. x_0)^{\ell_2})^{\ell_1})^{\ell_0}$

2457

$\rightarrow_A ((\text{trace } ((\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1)(\ell_1 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_2) (\lambda x_0. x_0)^{\ell_2}))^{\ell_2 \ell_1 \ell_0})$

2458

□

2459

2460

THEOREM 6.58 (AMNESIC BLAME SOUNDNESS AND COMPLETENESS). *Amnesic satisfies BS and BC*

2461

2462

PROOF SKETCH. By preservation of path-owner consistency ( $\Vdash_p$ ) for  $\triangleright_{\bar{A}}$  and  $\blacktriangleright_{\bar{A}}$ . More details in appendix: lemma A.28.

2463

□

2464

2465

2466

2467

2468

2469

2470

2471

2472

2473

2474

2475

2476

2477

2478

2479

2480

2481

2482

2483

2484

2485

2486

2487

2488

2489

2490

2491

2492

2493

2494

2495

2496

2497

2498

2499

## 6.9.3 Relation to Transient.

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

$$\frac{v_0 \approx v_1; \mathcal{H}_0; \mathcal{B}_0}{\text{trace } \bar{b}_0 v_0 \approx v_1; \mathcal{H}_0; \mathcal{B}_0} \quad \frac{v_0 \approx \mathcal{H}_0(p_0); \mathcal{H}_0; \mathcal{B}_0}{v_0 \approx p_0; \mathcal{H}_0; \mathcal{B}_0} \quad \frac{}{i_0 \approx i_0; \mathcal{H}_0; \mathcal{B}_0} \quad \frac{}{\mathbb{T} \bar{b}_0 i_0 \approx i_0; \mathcal{H}_0; \mathcal{B}_0}$$

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

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

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

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

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

$$\frac{e_0 \approx e_2; \mathcal{H}_0; \mathcal{B}_0 \quad e_1 \approx e_3; \mathcal{H}_0; \mathcal{B}_0}{\langle e_0, e_1 \rangle \approx \langle e_2, e_3 \rangle; \mathcal{H}_0; \mathcal{B}_0} \quad \frac{e_0 \approx e_2; \mathcal{H}_0; \mathcal{B}_0 \quad e_1 \approx e_3; \mathcal{H}_0; \mathcal{B}_0}{\text{app}\{\tau/\mathcal{U}\} e_0 e_1 \approx \text{app}\{\tau/\mathcal{U}\} e_2 e_3; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\text{unop}\{\tau/\mathcal{U}\} e_0 \approx \text{unop}\{\tau/\mathcal{U}\} e_1; \mathcal{H}_0; \mathcal{B}_0} \quad \frac{e_0 \approx e_2; \mathcal{H}_0; \mathcal{B}_0 \quad e_1 \approx e_3; \mathcal{H}_0; \mathcal{B}_0}{\text{binop}\{\tau/\mathcal{U}\} e_0 e_1 \approx \text{binop}\{\tau/\mathcal{U}\} e_2 e_3; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\text{dyn } b_0 e_0 \approx \text{dyn } b_0 e_1; \mathcal{H}_0; \mathcal{B}_0} \quad \frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\text{stat } b_0 e_0 \approx \text{stat } b_0 e_1; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) e_0 \approx \text{check}\{\tau_0\} e_1 p_0; \mathcal{H}_0; \mathcal{B}_0} \quad \frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) e_0 \approx \text{check}\{\mathcal{U}\} e_1 p_0; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{\tau_1 \leq \tau_0 \quad e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{stat } (\ell_2 \blacktriangleleft \tau_1 \blacktriangleleft \ell_3) e_0) \approx \text{check}\{\tau_0\} e_1 p_0; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0}{\text{check}\{\tau/\mathcal{U}\} e_0 \bullet \approx \text{check}\{\tau/\mathcal{U}\} e_1 p_0; \mathcal{H}_0; \mathcal{B}_0} \quad \frac{}{\text{InvariantErr} \approx \text{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{}{\text{TagErr} \approx \text{TagErr}; \mathcal{H}_0; \mathcal{B}_0} \quad \frac{}{\text{DivErr} \approx \text{DivErr}; \mathcal{H}_0; \mathcal{B}_0}$$

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

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

$$\frac{E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0}{\text{trace } \bar{b}_0 E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0} \quad \frac{}{[\ ] \approx [\ ]; \mathcal{H}_0; \mathcal{B}_0} \quad \frac{E_0 \approx E_2; \mathcal{H}_0; \mathcal{B}_0 \quad e_1 \approx e_3; \mathcal{H}_0; \mathcal{B}_0}{\langle E_0, e_1 \rangle \approx \langle E_2, e_3 \rangle; \mathcal{H}_0; \mathcal{B}_0}$$

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

$$\frac{v_0 \approx v_2; \mathcal{H}_0; \mathcal{B}_0 \quad E_1 \approx E_3; \mathcal{H}_0; \mathcal{B}_0}{\text{app}\{\tau/\mathcal{U}\} v_0 E_1 \approx \text{app}\{\tau/\mathcal{U}\} v_2 E_3; \mathcal{H}_0; \mathcal{B}_0} \quad \frac{E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0}{\text{unop}\{\tau/\mathcal{U}\} E_0 \approx \text{unop}\{\tau/\mathcal{U}\} E_1; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{E_0 \approx E_2; \mathcal{H}_0; \mathcal{B}_0 \quad e_1 \approx e_3; \mathcal{H}_0; \mathcal{B}_0}{\text{binop}\{\tau/\mathcal{U}\} E_0 e_1 \approx \text{binop}\{\tau/\mathcal{U}\} E_2 e_3; \mathcal{H}_0; \mathcal{B}_0} \quad \frac{v_0 \approx v_2; \mathcal{H}_0; \mathcal{B}_0 \quad E_1 \approx E_3; \mathcal{H}_0; \mathcal{B}_0}{\text{binop}\{\tau/\mathcal{U}\} v_0 E_1 \approx \text{binop}\{\tau/\mathcal{U}\} v_2 E_3; \mathcal{H}_0; \mathcal{B}_0}$$

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

$$\frac{E_0 \notin \text{stat } b E \quad E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0}{\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) E_0 \approx \text{check}\{\tau_0\} E_1 p_0; \mathcal{H}_0; \mathcal{B}_0} \quad \frac{E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0}{\text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) E_0 \approx \text{check}\{\mathcal{U}\} E_1 p_0; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{\tau_1 \leq \tau_0 \quad E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0}{\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{stat } (\ell_2 \blacktriangleleft \tau_1 \blacktriangleleft \ell_3) E_0) \approx \text{check}\{\tau_0\} E_1 p_0; \mathcal{H}_0; \mathcal{B}_0}$$

$$\frac{E_0 \approx E_1; \mathcal{H}_0; \mathcal{B}_0}{\text{check}\{\tau/\mathcal{U}\} E_0 \bullet \approx \text{check}\{\tau/\mathcal{U}\} E_1 p_0; \mathcal{H}_0; \mathcal{B}_0}$$

2598 THEOREM 6.59 (TRANSIENT AMNESIC ERROR EQUIVALENCE).  $T \approx A$

2599 PROOF. By lemma 6.60. □

2600 LEMMA 6.60. *If  $e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0$  then:*

- 2602 • if  $e_0 \rightarrow_A e_2$  then  $e_2 \rightarrow_A^* e_3$  and  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* e_4; \mathcal{H}_1; \mathcal{B}_1$  and  $e_3 \approx e_4; \mathcal{H}_1; \mathcal{B}_1$
- 2603 • if  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T e_3; \mathcal{H}_1; \mathcal{B}_1$  then  $e_0 \rightarrow_A^* e_2$  and  $e_2 \approx e_3; \mathcal{H}_1; \mathcal{B}_1$

2604 PROOF SKETCH. Amnesic may take extra steps at an elimination form and to combine traces into  
 2605 one wrapper. Transient takes extra steps to place pre-values on the heap and to conservatively  
 2606 check the result of elimination forms. The extra checks in Transient are problematic, however,  
 2607 because they may appear alongside any expression on the Amnesic side. A direct simulation would  
 2608 be messy; thus the  $\approx$  relations above assume a variant of Amnesic that inserts check expressions  
 2609 after the application of an unwrapped function. Type preservation guarantees that such checks  
 2610 never fail. More details in appendix: lemma A.29. □

2612

2613

2614

2615

2616

2617

2618

2619

2620

2621

2622

2623

2624

2625

2626

2627

2628

2629

2630

2631

2632

2633

2634

2635

2636

2637

2638

2639

2640

2641

2642

2643

2644

2645

2646

## 6.9.4 Relation to Forgetful.

$$\boxed{v \lesssim v}$$

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

$$\frac{b_0 \leqslant b_1 \quad v_0 \lesssim v_1}{\mathbb{G} b_0 v_0 \lesssim \mathbb{G} b_1 v_1} \quad \frac{b_0 \leqslant b_1 \quad v_0 \lesssim v_1}{\mathbb{T} b_0 v_0 \lesssim \mathbb{T} b_1 v_1} \quad \frac{b_0 \leqslant b_1 \quad \mathbb{T} \bar{b}_0 v_0 \lesssim \mathbb{T} \bar{b}_1 v_1}{\mathbb{T} b_0 \bar{b}_0 v_0 \lesssim \mathbb{T} b_1 \bar{b}_1 v_1}$$

$$\boxed{e \lesssim e}$$

$$\frac{}{x_0 \lesssim x_0} \quad \frac{e_0 \lesssim e_2 \quad e_1 \lesssim e_3}{\langle e_0, e_1 \rangle \lesssim \langle e_2, e_3 \rangle} \quad \frac{e_0 \lesssim e_2 \quad e_1 \lesssim e_3}{\text{app}\{\tau/\mathcal{U}\} e_0 e_1 \lesssim \text{app}\{\tau/\mathcal{U}\} e_2 e_3}$$

$$\frac{e_0 \lesssim e_1}{\text{unop}\{\tau/\mathcal{U}\} e_0 \lesssim \text{unop}\{\tau/\mathcal{U}\} e_1} \quad \frac{e_0 \lesssim e_2 \quad e_1 \lesssim e_3}{\text{binop}\{\tau/\mathcal{U}\} e_0 e_1 \lesssim \text{binop}\{\tau/\mathcal{U}\} e_2 e_3} \quad \frac{b_0 \leqslant b_1 \quad e_0 \lesssim e_1}{\text{dyn} b_0 e_0 \lesssim \text{dyn} b_1 e_1}$$

$$\frac{b_0 \leqslant b_1 \quad e_0 \lesssim e_1}{\text{stat} b_0 e_0 \lesssim \text{stat} b_1 e_1} \quad \frac{b_0 \leqslant b_1 \quad e_0 \lesssim e_1}{\text{trace} b_0 e_0 \lesssim \text{trace} b_1 e_1} \quad \frac{b_0 \leqslant b_1 \quad \text{trace} \bar{b}_0 e_0 \lesssim \text{trace} \bar{b}_1 e_1}{\text{trace} b_0 \bar{b}_0 e_0 \lesssim \text{trace} b_1 \bar{b}_1 e_1}$$

$$\frac{}{\text{TagErr} \lesssim \text{TagErr}} \quad \frac{}{\text{DivErr} \lesssim \text{DivErr}} \quad \frac{}{\text{BoundaryErr}(b_0, v_0) \lesssim e_1}$$

$$\boxed{E \lesssim E}$$

2696

2697

2698

2699

2700

2701

2702

2703

2704

2705

2706

2707

2708

2709

2710

2711

2712

2713

2714

2715

2716

2717

2718

2719

2720

2721

2722

2723

2724

2725

2726

2727

2728

2729

2730

2731

2732

2733

2734

2735

2736

2737

2738

2739

2740

2741

2742

2743

2744

$$\frac{}{[] \lesssim []}$$

$$\frac{E_0 \lesssim E_2 \quad e_1 \lesssim e_3}{\langle E_0, e_1 \rangle \lesssim \langle E_2, e_3 \rangle}$$

$$\frac{v_0 \lesssim v_2 \quad E_1 \lesssim E_3}{\langle v_0, E_1 \rangle \lesssim \langle v_2, E_3 \rangle}$$

$$\frac{E_0 \lesssim E_2 \quad e_1 \lesssim e_3}{\text{app}\{\tau/\mathcal{U}\} E_0 e_1 \lesssim \text{app}\{\tau/\mathcal{U}\} E_2 e_3}$$

$$\frac{v_0 \lesssim v_2 \quad E_1 \lesssim E_3}{\text{app}\{\tau/\mathcal{U}\} v_0 E_1 \lesssim \text{app}\{\tau/\mathcal{U}\} v_2 E_3}$$

$$\frac{E_0 \lesssim E_1}{\text{unop}\{\tau/\mathcal{U}\} E_0 \lesssim \text{unop}\{\tau/\mathcal{U}\} E_1}$$

$$\frac{E_0 \lesssim E_2 \quad e_1 \lesssim e_3}{\text{binop}\{\tau/\mathcal{U}\} E_0 e_1 \lesssim \text{binop}\{\tau/\mathcal{U}\} E_2 e_3}$$

$$\frac{v_0 \lesssim v_2 \quad E_1 \lesssim E_3}{\text{binop}\{\tau/\mathcal{U}\} v_0 E_1 \lesssim \text{binop}\{\tau/\mathcal{U}\} v_2 E_3}$$

$$\frac{b_0 \leqslant b_1 \quad E_0 \lesssim E_1}{\text{dyn } b_0 E_0 \lesssim \text{dyn } b_1 E_1}$$

$$\frac{b_0 \leqslant b_1 \quad E_0 \lesssim E_1}{\text{stat } b_0 E_0 \lesssim \text{stat } b_1 E_1}$$

$$\frac{b_0 \leqslant b_1 \quad E_0 \lesssim E_1}{\text{trace } b_0 E_0 \lesssim \text{trace } b_1 E_1}$$

$$\frac{b_0 \leqslant b_1 \quad \text{trace } \bar{b}_0 E_0 \lesssim \text{trace } \bar{b}_1 E_1}{\text{trace } b_0 \bar{b}_0 E_0 \lesssim \text{trace } b_1 \bar{b}_1 E_1}$$



2745 THEOREM 6.61 (FORGETFUL AMNESIC ERROR PREORDER).  $F \lesssim A$

2746 PROOF SKETCH. By showing that  $e \lesssim e$  is a lock-step bisimulation. More details in appen-  
 2747 dix: lemma A.36. □

2748 THEOREM 6.62.  $A \not\lesssim F$

2749 PROOF. Forgetful checks the types that come from boundaries, but Amnesic checks local annota-  
 2750 tions. The annotations may be supertypes of the boundary types.

2751  $e_0 = \text{fst}\{\text{Int}\}(\text{dyn}(\ell_0 \blacktriangleleft (\text{Nat} \times \text{Nat}) \blacktriangleleft \ell_1) \langle -4, 4 \rangle)$

2752 Since  $-4$  is an integer, Amnesic reduces to a value. Forgetful detects an error. □

2755

2756

2757

2758

2759

2760

2761

2762

2763

2764

2765

2766

2767

2768

2769

2770

2771

2772

2773

2774

2775

2776

2777

2778

2779

2780

2781

2782

2783

2784

2785

2786

2787

2788

2789

2790

2791

2792

2793

## 6.10 Erasure and its Properties

### 6.10.1 Semantics, Type Soundness.

|                                                                              |                                                       |
|------------------------------------------------------------------------------|-------------------------------------------------------|
| $e \triangleright_E e$                                                       |                                                       |
| $unop\{\tau_0\} v_0$                                                         | $\triangleright_E \text{BoundaryErr}(\emptyset, v_0)$ |
| if $\delta(unop, v_0)$ is undefined                                          |                                                       |
| $unop\{\mathcal{U}\} v_0$                                                    | $\triangleright_E \text{TagErr}$                      |
| if $\delta(unop, v_0)$ is undefined                                          |                                                       |
| $unop\{\tau/\mathcal{U}\} v_0$                                               | $\triangleright_E \delta(unop, v_0)$                  |
| if $\delta(unop, v_0)$ is defined                                            |                                                       |
| $binop\{\tau_0\} v_0 v_1$                                                    | $\triangleright_E \text{BoundaryErr}(\emptyset, v_0)$ |
| if $\delta(binop, v_0, v_1)$ is undefined and $v_0 \notin i$                 |                                                       |
| $binop\{\tau_0\} v_0 v_1$                                                    | $\triangleright_E \text{BoundaryErr}(\emptyset, v_1)$ |
| if $\delta(binop, v_0, v_1)$ is undefined and $v_0 \in i$ and $v_1 \notin i$ |                                                       |
| $binop\{\mathcal{U}\} v_0 v_1$                                               | $\triangleright_E \text{TagErr}$                      |
| if $\delta(binop, v_0, v_1)$ is undefined                                    |                                                       |
| $binop\{\tau/\mathcal{U}\} v_0 v_1$                                          | $\triangleright_E \delta(binop, v_0, v_1)$            |
| if $\delta(binop, v_0, v_1)$ is defined                                      |                                                       |
| $app\{\tau_0\} v_0 v_1$                                                      | $\triangleright_E \text{BoundaryErr}(\emptyset, v_0)$ |
| if $v_0 \notin (\lambda x. e) \cup (\lambda(x : \tau). e)$                   |                                                       |
| $app\{\mathcal{U}\} v_0 v_1$                                                 | $\triangleright_E \text{TagErr}$                      |
| if $v_0 \notin (\lambda x. e) \cup (\lambda(x : \tau). e)$                   |                                                       |
| $app\{\tau/\mathcal{U}\} (\lambda(x_0 : \tau_0). e_0) v_0$                   | $\triangleright_E e_0[x_0 \leftarrow v_0]$            |
| $app\{\tau/\mathcal{U}\} (\lambda x_0. e_0) v_0$                             | $\triangleright_E e_0[x_0 \leftarrow v_0]$            |
| $dyn(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$        | $\triangleright_E v_0$                                |
| $stat(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$       | $\triangleright_E v_0$                                |

$e \rightarrow_E^* e$  is the transitive, reflexive, compatible (with respect to evaluation contexts  $E$ , section 6.2) closure of the relation  $\triangleright_E$

2843 THEOREM 6.63 (ERASURE UNSOUNDNESS). *Erasure satisfies neither TS(1) nor TS(s)*

2844

2845

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

2846

$\text{dyn}(\ell_0 \blacktriangleleft \text{Int} \blacktriangleleft \ell_1)(\lambda x_0. 42) \triangleright_E (\lambda x_0. 42)$

2848

□

2849

THEOREM 6.64 (ERASURE DYN SOUNDNESS). *Erasure satisfies TS(0)*

2850

2851

PROOF. By progress (lemma 6.65) and preservation (lemma 6.66).

□

2852

LEMMA 6.65 (ERASURE TYPE PROGRESS). *If  $\cdot \vdash_0 E_0[e_0] : \mathcal{U}$  then one of the following holds:*

2853

•  $e_0 \in v \cup \text{Err}$

2854

•  $\exists e_1. e_0 \triangleright_E e_1$

2855

2856

PROOF SKETCH. By unique decomposition (lemma 6.1) and case analysis. More details in appendix: lemma A.43.

2857

□

2858

LEMMA 6.66 (ERASURE TYPE PRESERVATION).

2859

*If  $\cdot \vdash_0 e_0 : \mathcal{U}$  and  $e_0 \triangleright_E e_1$  then  $\cdot \vdash_0 e_1 : \mathcal{U}$ .*

2860

2861

PROOF SKETCH. By case analysis of the reduction relation. More details in appendix: lemma A.44.

2862

□

2863

2864

2865

2866

2867

2868

2869

2870

2871

2872

2873

2874

2875

2876

2877

2878

2879

2880

2881

2882

2883

2884

2885

2886

2887

2888

2889

2890

2891

6.10.2 *Lifted Semantics, Complete Monitoring, Blame.*

|      |                                                                                                                                  |                                                                                                                    |
|------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| 2892 | $(e)^\ell \triangleright_{\bar{E}} (e)^\ell$ lifted version of $\triangleright_{\bar{E}}$                                        |                                                                                                                    |
| 2893 |                                                                                                                                  |                                                                                                                    |
| 2894 |                                                                                                                                  |                                                                                                                    |
| 2895 | $(unop\{\tau_0\} ((v_0))^{\bar{\ell}_0})^{\ell_0}$                                                                               | $\triangleright_{\bar{E}} (\text{BoundaryErr}(\emptyset, ((v_0))^{\bar{\ell}_0}))^{\ell_0}$                        |
| 2896 | if $v_0 \notin (v)^\ell$ and $\delta(unop, v_0)$ is undefined                                                                    |                                                                                                                    |
| 2897 |                                                                                                                                  |                                                                                                                    |
| 2898 | $(unop\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0})^{\ell_0}$                                                                          | $\triangleright_{\bar{E}} (\text{TagErr})^{\ell_0}$                                                                |
| 2899 | if $v_0 \notin (v)^\ell$ and $\delta(unop, v_0)$ is undefined                                                                    |                                                                                                                    |
| 2900 |                                                                                                                                  |                                                                                                                    |
| 2901 | $(unop\{\tau/\mathcal{U}\} ((v_0))^{\bar{\ell}_0})^{\ell_0}$                                                                     | $\triangleright_{\bar{E}} (\delta(unop, v_0))^{\bar{\ell}_0 \ell_0}$                                               |
| 2902 | if $\delta(unop, v_0)$ is defined                                                                                                |                                                                                                                    |
| 2903 |                                                                                                                                  |                                                                                                                    |
| 2904 | $(binop\{\tau_0\} ((v_0))^{\bar{\ell}_0} ((v_1))^{\bar{\ell}_1})^{\ell_0}$                                                       | $\triangleright_{\bar{E}} (\text{BoundaryErr}(\emptyset, v_0))^{\ell_0}$                                           |
| 2905 | if $v_0 \notin (v)^\ell$ and $v_1 \notin (v)^\ell$ and $\delta(binop, v_0, v_1)$ is undefined and $v_0 \notin i$                 |                                                                                                                    |
| 2906 | $(binop\{\tau_0\} ((v_0))^{\bar{\ell}_0} ((v_1))^{\bar{\ell}_1})^{\ell_0}$                                                       | $\triangleright_{\bar{E}} (\text{BoundaryErr}(\emptyset, v_1))^{\ell_0}$                                           |
| 2907 | if $v_0 \notin (v)^\ell$ and $v_1 \notin (v)^\ell$ and $\delta(binop, v_0, v_1)$ is undefined and $v_0 \in i$ and $v_1 \notin i$ |                                                                                                                    |
| 2908 |                                                                                                                                  |                                                                                                                    |
| 2909 | $(binop\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0} ((v_1))^{\bar{\ell}_1})^{\ell_0}$                                                  | $\triangleright_{\bar{E}} (\text{TagErr})^{\ell_0}$                                                                |
| 2910 | if $v_0 \notin (v)^\ell$ and $v_1 \notin (v)^\ell$ and $\delta(binop, v_0, v_1)$ is undefined                                    |                                                                                                                    |
| 2911 |                                                                                                                                  |                                                                                                                    |
| 2912 | $(binop\{\tau/\mathcal{U}\} ((v_0))^{\bar{\ell}_0} ((v_1))^{\bar{\ell}_1})^{\ell_0}$                                             | $\triangleright_{\bar{E}} (\delta(binop, v_0, v_1))^{\ell_0}$                                                      |
| 2913 | if $\delta(binop, v_0, v_1)$ is defined                                                                                          |                                                                                                                    |
| 2914 | $(app\{\tau_0\} ((v_0))^{\bar{\ell}_0} v_1)^{\ell_0}$                                                                            | $\triangleright_{\bar{E}} (\text{BoundaryErr}(\emptyset, ((v_0))^{\bar{\ell}_0}))^{\ell_0}$                        |
| 2915 | if $v_0 \notin (v)^\ell \cup (\lambda x. e) \cup (\lambda(x : \tau). e)$                                                         |                                                                                                                    |
| 2916 |                                                                                                                                  |                                                                                                                    |
| 2917 | $(app\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0} v_1)^{\ell_0}$                                                                       | $\triangleright_{\bar{E}} (\text{TagErr})^{\ell_0}$                                                                |
| 2918 | if $v_0 \notin (v)^\ell \cup (\lambda x. e) \cup (\lambda(x : \tau). e)$                                                         |                                                                                                                    |
| 2919 |                                                                                                                                  |                                                                                                                    |
| 2920 | $(app\{\tau/\mathcal{U}\} ((\lambda(x_0 : \tau_0). e_0))^{\bar{\ell}_0} v_0)^{\ell_0}$                                           | $\triangleright_{\bar{E}} ((e_0[x_0 \leftarrow ((v_0))^{\ell_0 \text{rev}(\bar{\ell}_0)}]))^{\bar{\ell}_0 \ell_0}$ |
| 2921 |                                                                                                                                  |                                                                                                                    |
| 2922 | $(app\{\tau/\mathcal{U}\} ((\lambda x_0. e_0))^{\bar{\ell}_0} v_0)^{\ell_0}$                                                     | $\triangleright_{\bar{E}} ((e_0[x_0 \leftarrow ((v_0))^{\ell_0 \text{rev}(\bar{\ell}_0)}]))^{\bar{\ell}_0 \ell_0}$ |
| 2923 | $(dyn (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)^{\ell_0}$                                                | $\triangleright_{\bar{E}} (v_0)^{\ell_0}$                                                                          |
| 2924 | $(stat (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)^{\ell_0}$                                               | $\triangleright_{\bar{E}} (v_0)^{\ell_0}$                                                                          |
| 2925 |                                                                                                                                  |                                                                                                                    |
| 2926 |                                                                                                                                  |                                                                                                                    |
| 2927 |                                                                                                                                  |                                                                                                                    |
| 2928 |                                                                                                                                  |                                                                                                                    |
| 2929 |                                                                                                                                  |                                                                                                                    |
| 2930 |                                                                                                                                  |                                                                                                                    |
| 2931 |                                                                                                                                  |                                                                                                                    |
| 2932 |                                                                                                                                  |                                                                                                                    |
| 2933 |                                                                                                                                  |                                                                                                                    |
| 2934 |                                                                                                                                  |                                                                                                                    |
| 2935 |                                                                                                                                  |                                                                                                                    |
| 2936 |                                                                                                                                  |                                                                                                                    |
| 2937 |                                                                                                                                  |                                                                                                                    |
| 2938 |                                                                                                                                  |                                                                                                                    |
| 2939 |                                                                                                                                  |                                                                                                                    |
| 2940 |                                                                                                                                  |                                                                                                                    |

2941 THEOREM 6.67 (ERASURE INCOMPLETE MONITORING). *Erasure does not satisfy CM*

2942 PROOF. The evaluation of a boundary term adds a new owner, breaking single-owner consistency.

2943 For example,  $(\text{dyn } (\ell_0 \blacktriangleleft (\text{Int} \Rightarrow \text{Nat}) \blacktriangleleft \ell_1) (\lambda x_0. x_0)^{\ell_1})^{\ell_0} \not\triangleright_{\mathbb{E}} ((\lambda x_0. x_0))^{\ell_0 \ell_1}$ . □

2945 THEOREM 6.68 (ERASURE BLAME SOUNDNESS). *Erasure satisfies BS*

2946 PROOF. By inspection, the only Erasure rules that raise a boundary error blame the empty set.

2947 An empty set is trivially blame sound. □

2948 THEOREM 6.69 (ERASURE BLAME INCOMPLETENESS). *Erasure does not satisfy BC*

2949 PROOF. The empty set is trivially incomplete, because every value has at least one label for its  
2950 context. □

2953

2954

2955

2956

2957

2958

2959

2960

2961

2962

2963

2964

2965

2966

2967

2968

2969

2970

2971

2972

2973

2974

2975

2976

2977

2978

2979

2980

2981

2982

2983

2984

2985

2986

2987

2988

2989

## 6.10.3 Relation to Amnesic.

$$\boxed{v \lesssim v}$$

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

$$\frac{v_0 \lesssim v_1}{\mathbb{G} b_0 v_0 \lesssim v_1} \quad \frac{v_0 \lesssim v_1}{\mathbb{T} \bar{b}_0 v_0 \lesssim v_1}$$

$$\boxed{e \lesssim e}$$

$$\frac{}{x_0 \lesssim x_0} \quad \frac{e_0 \lesssim e_2 \quad e_1 \lesssim e_3}{\langle e_0, e_1 \rangle \lesssim \langle e_2, e_3 \rangle} \quad \frac{e_0 \lesssim e_2 \quad e_1 \lesssim e_3}{\text{app}\{\tau/\mathcal{U}\} e_0 e_1 \lesssim \text{app}\{\tau/\mathcal{U}\} e_2 e_3}$$

$$\frac{e_0 \lesssim e_1}{\text{unop}\{\tau/\mathcal{U}\} e_0 \lesssim \text{unop}\{\tau/\mathcal{U}\} e_1} \quad \frac{e_0 \lesssim e_2 \quad e_1 \lesssim e_3}{\text{binop}\{\tau/\mathcal{U}\} e_0 e_1 \lesssim \text{binop}\{\tau/\mathcal{U}\} e_2 e_3} \quad \frac{e_0 \lesssim e_1}{\text{dyn } b_0 e_0 \lesssim \text{dyn } b_0 e_1}$$

$$\frac{e_0 \lesssim e_1}{\text{stat } b_0 e_0 \lesssim \text{stat } b_0 e_1} \quad \frac{e_0 \lesssim e_1}{\text{dyn } b_0 e_0 \lesssim e_1} \quad \frac{e_0 \lesssim e_1}{\text{stat } b_0 e_0 \lesssim e_1} \quad \frac{e_0 \lesssim e_1}{\text{trace } \bar{b}_0 e_0 \lesssim e_1}$$

$$\frac{}{\text{TagErr} \lesssim \text{TagErr}}$$

$$\frac{}{\text{DivErr} \lesssim \text{DivErr}}$$

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

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

$$\boxed{E \lesssim E}$$

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

$$\frac{v_0 \lesssim v_2 \quad E_1 \lesssim E_3}{\text{app}\{\tau/\mathcal{U}\} v_0 E_1 \lesssim \text{app}\{\tau/\mathcal{U}\} v_2 E_3} \quad \frac{E_0 \lesssim E_1}{\text{unop}\{\tau/\mathcal{U}\} E_0 \lesssim \text{unop}\{\tau/\mathcal{U}\} E_1}$$

$$\frac{E_0 \lesssim E_2 \quad e_1 \lesssim e_3}{\text{binop}\{\tau/\mathcal{U}\} E_0 e_1 \lesssim \text{binop}\{\tau/\mathcal{U}\} E_2 e_3} \quad \frac{v_0 \lesssim v_2 \quad E_1 \lesssim E_3}{\text{binop}\{\tau/\mathcal{U}\} v_0 E_1 \lesssim \text{binop}\{\tau/\mathcal{U}\} v_2 E_3}$$

$$\frac{E_0 \lesssim E_1}{\text{dyn } b_0 E_0 \lesssim \text{dyn } b_0 E_1} \quad \frac{E_0 \lesssim E_1}{\text{stat } b_0 E_0 \lesssim \text{stat } b_0 E_1} \quad \frac{E_0 \lesssim E_1}{\text{trace } \bar{b}_0 E_0 \lesssim E_1}$$

3039 THEOREM 6.70 (AMNESIC ERASURE ERROR PREORDER).  $A \lesssim E$

3040 PROOF. By lemma 6.72 and that  $e_0 \lesssim \text{BoundaryErr}(\bar{b}_1, v_1)$  implies  $e_0 \in \text{BoundaryErr}(b, v)$ .  $\square$

3042 THEOREM 6.71.  $E \not\lesssim A$

3043 PROOF. Because Amnesic enforces types at boundaries. For example,  $\text{dyn}(\ell_0 \blacktriangleleft \text{Nat} \blacktriangleleft \ell_1) - 1$  raises  
3044 a boundary error in Amnesic and computes a negative number in Erasure.  $\square$

3046 LEMMA 6.72.

3047 *There is a stuttering simulation between Amnesic and Erasure. More precisely, the following two results*  
3048 *hold:*

- 3049 • If  $e_0 \lesssim e_2$  and  $e_0 \rightarrow_A e_1$  then  $\exists e_3, e_4$  such that  $e_1 \rightarrow_A^* e_3$  and  $e_2 \rightarrow_E e_4$  and  $e_3 \lesssim e_4$ .
- 3050 • If  $e_0 \lesssim e_2$  and  $e_2 \rightarrow_E e_3$  then  $\exists e_1$  and  $e_0 \rightarrow_A^* e_1$  and  $e_1 \lesssim e_4$

3052 PROOF SKETCH. Amnesic takes extra steps to unwrap at elimination forms and to combine traces  
3053 into a single wrapper. More details in appendix: lemma A.45.  $\square$

3054

3055

3056

3057

3058

3059

3060

3061

3062

3063

3064

3065

3066

3067

3068

3069

3070

3071

3072

3073

3074

3075

3076

3077

3078

3079

3080

3081

3082

3083

3084

3085

3086

3087

## 3088 A PROOFS

### 3089 A.1 Natural

3090 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*  
 3091 *holds:*

- 3092 •  $e_0 \in v \cup \text{Err}$
- 3093 •  $\tau/\mathcal{U} \in \tau$  and  $\exists e_1. e_0 \triangleright_N e_1$
- 3094 •  $\tau/\mathcal{U} \in \mathcal{U}$  and  $\exists e_1. e_0 \blacktriangleright_N e_1$

3096 PROOF. By unique decomposition (lemma 6.1) and case analysis:

3098 **Case:**  $\cdot \vdash_1 n_0 : \text{Nat}$

3099 Immediate.

3100 **Case:**  $\cdot \vdash_1 i_0 : \text{Int}$

3101 Immediate.

3102 **Case:**  $\cdot \vdash_1 \lambda(x_0 : \tau_0). e_1 : \tau_0 \Rightarrow \tau_1$

3103 Immediate.

3104 **Case:**  $\cdot \vdash_1 \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$

3105 Immediate.

3106 **Case:**  $\cdot \vdash_1 \text{unop}\{\tau_0\} v_0 : \tau_0$

3107 -  $\triangleright_N \delta(\text{unop}, v_0)$  if defined

3108 -  $\triangleright_N \text{Err}$  otherwise

3109 **Case:**  $\cdot \vdash_1 \text{binop}\{\tau_0\} v_0 v_1 : \tau_0$

3110 -  $\triangleright_N \delta(\text{binop}, v_0, v_1)$  if defined

3111 -  $\triangleright_N \text{Err}$  otherwise

3112 **Case:**  $\cdot \vdash_1 \text{app}\{\tau_0\} v_0 v_1 : \tau_0$

3113 -  $\triangleright_N e_1[x_0 \leftarrow v_1]$

3114 if  $v_0 = \lambda(\tau_1 : x_0). e_1$

3115 -  $\triangleright_N \text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_2 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1))$

3116 if  $v_0 = \mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1) v_2$

3117 -  $\triangleright_N \text{Err}$  otherwise

3118 **Case:**  $\cdot \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 : \tau_0$

3119 -  $\triangleright_N \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$

3120 if  $\tau_0 \in \tau \Rightarrow \tau$  and *shape-match*( $\lfloor \tau_0 \rfloor, v_0$ )

3121 -  $\triangleright_N \langle (\text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1), (\text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) v_2) \rangle$

3122 if  $\tau_0 = \tau_1 \times \tau_2$  and  $v_0 = \langle v_1, v_2 \rangle$

3123 -  $\triangleright_N v_0$

3124 if  $v_0 \in i$  and  $\tau_0 \in \text{Int}$

3125 -  $\triangleright_N v_0$

3126 if  $v_0 \in n$  and  $\tau_0 \in \text{Nat}$

3127 -  $\triangleright_N \text{Err}$  otherwise

3128 **Case:**  $\cdot \vdash_1 \mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1) v_0 : \tau_0$

3129 Immediate.

3130 **Case:**  $\cdot \vdash_1 \text{Err} : \tau_0$

3131 Immediate.

3132 **Case:**  $\cdot \vdash_1 i : \mathcal{U}$

3133 Immediate.

3134 **Case:**  $\cdot \vdash_1 \lambda x_0. e_0 : \mathcal{U}$

3135 Immediate.

3136



3137 **Case:**  $\cdot \vdash_1 \langle v_0, v_1 \rangle : \mathcal{U}$   
 3138 Immediate.

3139 **Case:**  $\cdot \vdash_1 \text{unop}\{\mathcal{U}\} v_0 : \mathcal{U}$   
 3140 -  $\blacktriangleright_N \delta(\text{unop}, v_0)$  if defined  
 3141 -  $\blacktriangleright_N \text{Err}$  otherwise

3142 **Case:**  $\cdot \vdash_1 \text{binop}\{\mathcal{U}\} v_0 v_1 : \mathcal{U}$   
 3143 -  $\blacktriangleright_N \delta(\text{binop}, v_0, v_1)$  if defined  
 3144 -  $\blacktriangleright_N \text{Err}$  otherwise

3145 **Case:**  $\cdot \vdash_1 \text{app}\{\mathcal{U}\} v_0 v_1 : \mathcal{U}$   
 3146 -  $\blacktriangleright_N e_1[x_0 \leftarrow v_1]$   
 3147 if  $v_0 = \lambda x_0. e_1$   
 3148 -  $\blacktriangleright_N \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\tau_0\} v_2 (\text{dyn}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1))$   
 3149 if  $v_0 = \mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1) v_2$   
 3150 -  $\blacktriangleright_N \text{Err}$  otherwise

3151 **Case:**  $\cdot \vdash_1 \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 : \mathcal{U}$   
 3152 -  $\blacktriangleright_N \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
 3153 if  $\tau_0 \in \tau \Rightarrow \tau$  and  $\text{shape-match}(\lfloor \tau_0 \rfloor, v_0)$   
 3154 -  $\blacktriangleright_N \langle (\text{stat}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1), (\text{stat}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) v_2) \rangle$   
 3155 if  $\tau_0 = \tau_1 \times \tau_2$  and  $v_0 = \langle v_1, v_2 \rangle$   
 3156 -  $\blacktriangleright_N v_0$   
 3157 if  $v_0 \in i$  and  $\tau_0 \in \text{Int}$   
 3158 -  $\blacktriangleright_N v_0$   
 3159 if  $v_0 \in n$  and  $\tau_0 \in \text{Nat}$   
 3160 -  $\blacktriangleright_N \text{Err}$  otherwise

3161 **Case:**  $\cdot \vdash_1 \mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1) v_0 : \mathcal{U}$   
 3162 Immediate.

3163 **Case:**  $\cdot \vdash_1 \text{Err} : \mathcal{U}$   
 3164 Immediate.

□

3165  
3166  
3167  
3168  
3169  
3170  
3171  
3172  
3173  
3174  
3175  
3176  
3177  
3178  
3179  
3180  
3181  
3182  
3183  
3184  
3185

3186 LEMMA A.2 (NATURAL TYPE PRESERVATION).

3187 *If  $\cdot \vdash_1 E_0[e_0] : \tau/\mathcal{U}$  and  $N(E_0[e_0])$  and  $e_0 \triangleright_{\mathbb{N}} \cup \blacktriangleright_{\mathbb{N}} e_1$  then  $\cdot \vdash_1 E_0[e_1] : \tau/\mathcal{U}$  and  $N(E_0[e_1])$ .*

3188

3189 PROOF. By case analysis of each reduction relation:

3190

**Case:**  $unop\{\tau_0\} v_0 \triangleright_{\mathbb{N}}$  InvariantErr

Immediate.

3191

**Case:**  $unop\{\tau_0\} v_0 \triangleright_{\mathbb{N}} \delta(unop, v_0)$

By lemma 6.2.

3192

**Case:**  $binop\{\tau_0\} v_0 v_1 \triangleright_{\mathbb{N}}$  InvariantErr

Immediate.

3193

**Case:**  $binop\{\tau_0\} v_0 v_1 \triangleright_{\mathbb{N}} \delta(binop, v_0, v_1)$

By lemma 6.2.

3194

**Case:**  $app\{\tau_0\} v_0 v_1 \triangleright_{\mathbb{N}}$  InvariantErr

Immediate.

3195

**Case:**  $app\{\tau_0\} (\lambda(x_0 : \tau_1). e_0) v_0 \triangleright_{\mathbb{N}} e_0[x_0 \leftarrow v_0]$

By substitution lemmas for typed functions and for  $N(\cdot)$ .

3196

**Case:**  $app\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_2) \blacktriangleleft \ell_1) v_0) v_1 \triangleright_{\mathbb{N}} \text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1))$

(1)  $\cdot \vdash_1 v_0 : \mathcal{U}$

By  $\vdash_1$  on the redex

3204

(2)  $\cdot \vdash_1 v_1 : \tau_1$

By  $\vdash_1$  on the redex

3205

(3)  $\cdot \vdash_1 \text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1 : \mathcal{U}$

By (2)

3206

(4)  $\cdot \vdash_1 \text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1) : \mathcal{U}$

By (1) and (3)

3207

(5)  $\tau_2 \leq \tau_0$

By  $\vdash_1$  on the redex

3208

(6)  $\cdot \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1)) : \tau_0$

By (4) and (5)

3209

(7)  $N(\text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1)))$

By similar reasoning

3210

**Case:**  $\text{dyn}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) v_0 \triangleright_{\mathbb{N}} \mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) v_0$

(1)  $\cdot \vdash_1 v_0 : \mathcal{U}$

By  $\vdash_1$  on the redex

3211

(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)

3212

**Case:**  $\text{dyn}(\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1) \langle v_0, v_1 \rangle \triangleright_{\mathbb{N}} \langle \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0, \text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1 \rangle$

(1)  $\cdot \vdash_1 v_0 : \mathcal{U}$

By  $\vdash_1$  on the redex

3213

(2)  $\cdot \vdash_1 v_1 : \mathcal{U}$

By  $\vdash_1$  on the redex

3214

(3)  $\cdot \vdash_1 \langle \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0, \text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1 \rangle : \tau_0 \times \tau_1$

By (1) and (2)

3215

**Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \text{Int} \blacktriangleleft \ell_1) i_0 \triangleright_{\mathbb{N}} i_0$

Immediate.

3216

**Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \text{Nat} \blacktriangleleft \ell_1) n_0 \triangleright_{\mathbb{N}} n_0$

Immediate.

3217

- 3235 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_{\mathbb{N}} \text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), v_0)$   
 3236 Immediate.
- 3237 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \triangleright_{\mathbb{N}} \text{TagErr}$   
 3238 Immediate.
- 3239 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \triangleright_{\mathbb{N}} \delta(\text{unop}, v_0)$   
 3240 Immediate.
- 3241 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \triangleright_{\mathbb{N}} \text{TagErr}$   
 3242 Immediate.
- 3243 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \triangleright_{\mathbb{N}} \delta(\text{binop}, v_0, v_1)$   
 3244 Immediate.
- 3245 **Case:**  $\text{app}\{\mathcal{U}\} v_0 v_1 \triangleright_{\mathbb{N}} \text{TagErr}$   
 3246 Immediate.
- 3247 **Case:**  $\text{app}\{\mathcal{U}\} (\lambda x_0. e_0) v_0 \triangleright_{\mathbb{N}} e_0[x_0 \leftarrow v_0]$   
 3248 By substitution lemmas for untyped functions and for  $N(\cdot)$ .
- 3249 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_2) \blacktriangleleft \ell_1) v_0) v_1 \triangleright_{\mathbb{N}} \text{stat}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\tau_2\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1))$   
 3250 (1)  $\cdot \vdash_1 v_0 : \tau_1 \Rightarrow \tau_2$   
 3251 By  $\vdash_1$  on the redex
- 3252 (2)  $\cdot \vdash_1 v_1 : \mathcal{U}$   
 3253 By  $\vdash_1$  on the redex
- 3254 (3)  $\cdot \vdash_1 \text{dyn}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1 : \tau_1$   
 3255 By (2)
- 3256 (4)  $\cdot \vdash_1 \text{app}\{\tau_2\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1) : \tau_2$   
 3257 By (1) and (3)
- 3258 (5)  $\cdot \vdash_1 \text{stat}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\tau_2\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1)) : \mathcal{U}$   
 3259 By (4)
- 3260 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) v_0 \triangleright_{\mathbb{N}} \mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) v_0$   
 3261 (1)  $\cdot \vdash_1 v_0 : \tau_0 \Rightarrow \tau_1$   
 3262 By  $\vdash_1$  on the redex
- 3263 (2)  $\cdot \vdash_1 \mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) v_0 : \mathcal{U}$   
 3264 By (1)
- 3265 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1) \langle v_0, v_1 \rangle \triangleright_{\mathbb{N}} \langle \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0, \text{stat}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1 \rangle$   
 3266 (1)  $\cdot \vdash_1 v_0 : \tau_0$   
 3267 By  $\vdash_1$  on the redex
- 3268 (2)  $\cdot \vdash_1 v_1 : \tau_1$   
 3269 By  $\vdash_1$  on the redex
- 3270 (3)  $\cdot \vdash_1 \langle \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0, \text{stat}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1 \rangle : \mathcal{U}$   
 3271 By (1) and (2)
- 3272 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \text{Int} \blacktriangleleft \ell_1) i_0 \triangleright_{\mathbb{N}} i_0$   
 3273 Immediate.
- 3274 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \text{Nat} \blacktriangleleft \ell_1) n_0 \triangleright_{\mathbb{N}} n_0$   
 3275 Immediate.
- 3276 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_{\mathbb{N}} \text{InvariantErr}$   
 3277 Immediate.

□

3278  
 3279  
 3280  
 3281  
 3282  
 3283

THEOREM A.3 (NATURAL COMPLETE MONITORING). *Natural satisfies CM*

PROOF. By preservation of single-owner consistency ( $\Vdash$ ) for  $\triangleright_{\mathbb{N}}$  and  $\blacktriangleright_{\mathbb{N}}$ .

**Case:**  $(unop\{\tau_0\} ((v_0))^{\bar{\ell}_0})^{\ell_0} \triangleright_{\mathbb{N}} (\text{InvariantErr})^{\ell_0}$

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

**Case:**  $(unop\{\tau_0\} ((v_0))^{\bar{\ell}_0})^{\ell_0} \triangleright_{\mathbb{N}} (\delta(unop, v_0))^{\bar{\ell}_0 \ell_0}$

(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:**  $(binop\{\tau_0\} ((v_0))^{\bar{\ell}_0} ((v_1))^{\bar{\ell}_1})^{\ell_0} \triangleright_{\mathbb{N}} (\text{InvariantErr})^{\ell_0}$

Immediate.

**Case:**  $(binop\{\tau_0\} ((v_0))^{\bar{\ell}_0} ((v_1))^{\bar{\ell}_1})^{\ell_0} \triangleright_{\mathbb{N}} (\delta(binop, v_0, v_1))^{\ell_0}$

(1)  $\delta(binop, v_0, v_1) \in i$

By definition of  $\delta$

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

By (1)

**Case:**  $(app\{\tau_0\} ((v_0))^{\bar{\ell}_0} v_1)^{\ell_0} \triangleright_{\mathbb{N}} (\text{InvariantErr})^{\ell_0}$

Immediate.

**Case:**  $(app\{\tau_0\} ((\lambda(x_0 : \tau_1). e_0))^{\bar{\ell}_0} v_1)^{\ell_0} \triangleright_{\mathbb{N}} ((e_0[x_0 \leftarrow ((v_1))^{\ell_0 \text{rev}(\bar{\ell}_0)}]))^{\bar{\ell}_0 \ell_0}$

(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)  $\ell_0; \cdot \Vdash ((v_0))^{\ell_0 \text{rev}(\bar{\ell}_0)}$

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)  $\ell_0; \cdot \Vdash ((e_0[x_0 \leftarrow ((v_1))^{\ell_0 \text{rev}(\bar{\ell}_0)}]))^{\bar{\ell}_0 \ell_0}$

By (3) and (4)

**Case:**  $(app\{\tau_0\} ((\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (v_0))^{\ell_2})^{\bar{\ell}_0} v_1)^{\ell_3} \triangleright_{\mathbb{N}}$

$((\text{dyn}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (app\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)})))^{\ell_2})^{\bar{\ell}_0 \ell_3}$

(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)  $\ell_3; \cdot \Vdash ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)}$

By (2) and  $\Vdash$  on the redex

- 3333 (4)  $\ell_2; \cdot \Vdash \text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)}$   
 3334 By (3) and  $\Vdash$  on the redex  
 3335  
 3336 (5)  $\ell_3; \cdot \Vdash ((\text{dyn}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)})))^{\ell_2})^{\bar{\ell}_0 \ell_3}$   
 3337 By (1) and (4)  
 3338 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2} \triangleright_{\mathbb{N}} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2}$   
 3339 Immediate.  
 3340 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\langle v_0, v_1 \rangle))^{\bar{\ell}_0})^{\ell_2} \triangleright_{\mathbb{N}}$   
 3341  $(\langle \text{dyn}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0}, \text{dyn}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) ((v_1))^{\bar{\ell}_0} \rangle)^{\ell_2}$   
 3342 (1)  $\ell_1; \cdot \Vdash ((v_0))^{\bar{\ell}_0}$  and  $\ell_1; \cdot \Vdash ((v_1))^{\bar{\ell}_0}$   
 3343 By  $\Vdash$  on the redex  
 3344 (2)  $\ell_2; \cdot \Vdash \langle \text{dyn}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0}, \text{dyn}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) ((v_1))^{\bar{\ell}_0} \rangle$   
 3345 By (1) and  $\Vdash$  on the redex  
 3346 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((i_0))^{\bar{\ell}_0})^{\ell_2} \triangleright_{\mathbb{N}} (i_0)^{\ell_2}$   
 3347 Immediate.  
 3348 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2} \triangleright_{\mathbb{N}} (\text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), ((v_0))^{\bar{\ell}_0}))^{\ell_2}$   
 3349 Immediate.  
 3350 **Case:**  $(\text{unop}\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0})^{\ell_0} \blacktriangleright_{\mathbb{N}} (\text{TagErr})^{\ell_0}$   
 3351 Immediate.  
 3352 **Case:**  $(\text{unop}\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0})^{\ell_0} \blacktriangleright_{\mathbb{N}} (\delta(\text{unop}, v_0))^{\bar{\ell}_0 \ell_0}$   
 3353 (1)  $v_0 = \langle v_1, v_2 \rangle$  and  $\delta(\text{unop}, v_0) \in \{v_1, v_2\}$   
 3354 By definition  
 3355 (2)  $\ell_0; \cdot \Vdash v_0$   
 3356 By  $\Vdash$  on the redex  
 3357 (3)  $\ell_0; \cdot \Vdash v_1$  and  $\ell_0; \cdot \Vdash v_2$   
 3358 By (2)  
 3359 (4)  $\ell_0; \cdot \Vdash \delta(\text{unop}, v_0)$   
 3360 By (1) and (3)  
 3361 **Case:**  $(\text{binop}\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0} ((v_1))^{\bar{\ell}_1})^{\ell_0} \blacktriangleright_{\mathbb{N}} (\text{TagErr})^{\ell_0}$   
 3362 Immediate.  
 3363 **Case:**  $(\text{binop}\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0} ((v_1))^{\bar{\ell}_1})^{\ell_0} \blacktriangleright_{\mathbb{N}} (\delta(\text{binop}, v_0, v_1))^{\ell_0}$   
 3364 (1)  $\delta(\text{binop}, v_0, v_1) \in i$   
 3365 By definition of  $\delta$   
 3366 (2)  $\ell_0; \cdot \Vdash \delta(\text{binop}, v_0, v_1)$   
 3367 By (1)  
 3368 **Case:**  $(\text{app}\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0} v_1)^{\ell_0} \blacktriangleright_{\mathbb{N}} (\text{TagErr})^{\ell_0}$   
 3369 Immediate.  
 3370 **Case:**  $(\text{app}\{\mathcal{U}\} ((\lambda x_0. e_0))^{\bar{\ell}_0} v_1)^{\ell_0} \blacktriangleright_{\mathbb{N}} ((e_0[x_0 \leftarrow ((v_1))^{\ell_0 \text{rev}(\bar{\ell}_0)}]))^{\bar{\ell}_0 \ell_0}$   
 3371 (1)  $\ell_0; \cdot \Vdash \lambda x_0. e_0$   
 3372 By  $\Vdash$  on the redex  
 3373 (2)  $\ell_0; \cdot \Vdash v_0$   
 3374 By  $\Vdash$  on the redex  
 3375  
 3376  
 3377  
 3378  
 3379  
 3380  
 3381

3382 (3)  $\ell_0; \cdot \Vdash ((v_0))^{\ell_0 \text{rev}(\bar{\ell}_0)}$   
 3383 By (1) and (2)  
 3384 (4)  $\ell_0; \cdot \Vdash x_0$  for each occurrence of  $x_0$  in  $e_0$   
 3385 By  $\Vdash$  on the redex  
 3386 (5)  $\ell_0; \cdot \Vdash ((e_0[x_0 \leftarrow ((v_1))^{\ell_0 \text{rev}(\bar{\ell}_0)}]))^{\bar{\ell}_0 \ell_0}$   
 3387 By (3) and (4)  
 3388  
 3389 **Case:**  $(\text{app}\{\mathcal{U}\} ((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0))^{\ell_2})^{\bar{\ell}_0} v_1)^{\ell_3} \blacktriangleright_{\bar{N}}$   
 3390  
 3391  $((\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)}))^{\ell_2})^{\bar{\ell}_0 \ell_3})$   
 3392 (1)  $\ell_2; \cdot \Vdash v_0$   
 3393 By  $\Vdash$  on the redex  
 3394 (2)  $\ell_3; \cdot \Vdash v_1$   
 3395 By  $\Vdash$  on the redex  
 3396 (3)  $\ell_3; \cdot \Vdash ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)}$   
 3397 By (2) and  $\Vdash$  on the redex  
 3398 (4)  $\ell_2; \cdot \Vdash \text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)}$   
 3399 By (3) and  $\Vdash$  on the redex  
 3400  
 3401 (5)  $\ell_3; \cdot \Vdash ((\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)}))^{\ell_2})^{\bar{\ell}_0 \ell_3})$   
 3402 By (1) and (4)  
 3403 **Case:**  $(\text{stat}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2} \blacktriangleright_{\bar{N}} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2}$   
 3404 Immediate.  
 3405 **Case:**  $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((\langle v_0, v_1 \rangle))^{\bar{\ell}_0})^{\ell_2} \blacktriangleright_{\bar{N}}$   
 3406  $(\langle \text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0}, \text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) ((v_1))^{\bar{\ell}_0} \rangle)^{\ell_2}$   
 3407 (1)  $\ell_1; \cdot \Vdash ((v_0))^{\bar{\ell}_0}$  and  $\ell_1; \cdot \Vdash ((v_1))^{\bar{\ell}_0}$   
 3408 By  $\Vdash$  on the redex  
 3409 (2)  $\ell_2; \cdot \Vdash \langle \text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0}, \text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) ((v_1))^{\bar{\ell}_0} \rangle$   
 3410 By (1) and  $\Vdash$  on the redex  
 3411 **Case:**  $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((i_0))^{\bar{\ell}_2})^{\ell_3} \blacktriangleright_{\bar{N}} (i_0)^{\ell_3}$   
 3412 Immediate.  
 3413 **Case:**  $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_2})^{\ell_2} \blacktriangleright_{\bar{N}} (\text{InvariantErr})^{\ell_2}$   
 3414 Immediate.  
 3415  
 3416  
 3417  
 3418  
 3419  
 3420  
 3421  
 3422  
 3423  
 3424  
 3425  
 3426  
 3427  
 3428  
 3429  
 3430

□

## 3431 A.2 Co-Natural

3432 LEMMA A.4 (CO-NATURAL TYPE PROGRESS).

3433 If  $\cdot \vdash_1 E_0[e_0] : \tau/\mathcal{U}$  and  $C(E_0[e_0])$  then one of the following holds:

- 3434 •  $e_0 \in v \cup \text{Err}$
- 3435 •  $\tau/\mathcal{U} \in \tau$  and  $\exists e_1. e_0 \triangleright_C e_1$
- 3436 •  $\tau/\mathcal{U} \in \mathcal{U}$  and  $\exists e_1. e_0 \blacktriangleright_C e_1$

3438 PROOF. By unique decomposition (lemma 6.1) and case analysis:

3439 **Case:**  $\cdot \vdash_1 n_0 : \text{Nat}$

3440 Immediate.

3441 **Case:**  $\cdot \vdash_1 i_0 : \text{Int}$

3442 Immediate.

3443 **Case:**  $\cdot \vdash_1 \lambda(x_0 : \tau_0). e_1 : \tau_0 \Rightarrow \tau_1$

3444 Immediate.

3445 **Case:**  $\cdot \vdash_1 \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$

3446 Immediate.

3447 **Case:**  $\cdot \vdash_1 \text{unop}\{\tau_0\} v_0 : \tau_0$

- 3448 -  $\triangleright_C \text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_1)$
- 3449 if  $\text{unop} = \text{fst}$  and  $v_0 = \mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_1$
- 3450 -  $\triangleright_C \text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{snd}\{\mathcal{U}\} v_1)$
- 3451 if  $\text{unop} = \text{snd}$  and  $v_0 = \mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_1$
- 3452 -  $\triangleright_C \delta(\text{unop}, v_0)$  if defined
- 3453 -  $\triangleright_C \text{Err}$  otherwise

3454 **Case:**  $\cdot \vdash_1 \text{binop}\{\tau_0\} v_0 v_1 : \tau_0$

- 3455 -  $\triangleright_C \delta(\text{binop}, v_0, v_1)$  if defined
- 3456 -  $\triangleright_C \text{Err}$  otherwise

3457 **Case:**  $\cdot \vdash_1 \text{app}\{\tau_0\} v_0 v_1 : \tau_0$

- 3458 -  $\triangleright_C e_1[x_0 \leftarrow v_1]$
- 3459 if  $v_0 = \lambda(\tau_1 : x_0). e_1$
- 3460 -  $\triangleright_C \text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_2 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1))$
- 3461 if  $v_0 = \mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1) v_2$
- 3462 -  $\triangleright_C \text{Err}$  otherwise

3463 **Case:**  $\cdot \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 : \tau_0$

- 3464 -  $\triangleright_C \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$
- 3465 if  $\tau_0 \in \tau \Rightarrow \tau \cup \tau \times \tau$  and  $\text{shape-match}([\tau_0], v_0)$
- 3466 -  $\triangleright_C v_0$
- 3467 if  $v_0 \in i$  and  $\tau_0 \in \text{Int}$
- 3468 -  $\triangleright_C v_0$
- 3469 if  $v_0 \in n$  and  $\tau_0 \in \text{Nat}$
- 3470 -  $\triangleright_C \text{Err}$  otherwise

3471 **Case:**  $\cdot \vdash_1 \mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) v_0 : \tau_0$

3472 Immediate.

3473 **Case:**  $\cdot \vdash_1 \mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1) v_0 : \tau_0$

3474 Immediate.

3475 **Case:**  $\cdot \vdash_1 \text{Err} : \tau_0$

3476 Immediate.

3477 **Case:**  $\cdot \vdash_1 i : \mathcal{U}$

3478 Immediate.

3479

3480 **Case:**  $\cdot \vdash_1 \lambda x_0. e_0 : \mathcal{U}$   
 3481 Immediate.

3482 **Case:**  $\cdot \vdash_1 \langle v_0, v_1 \rangle : \mathcal{U}$   
 3483 Immediate.

3484 **Case:**  $\cdot \vdash_1 \text{unop}\{\mathcal{U}\} v_0 : \mathcal{U}$   
 3485 -  $\blacktriangleright_{\mathbb{C}}$   $\text{stat}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) (\text{fst}\{\tau_1\} v_1)$   
 3486 if  $\text{unop} = \text{fst}$  and  $v_0 = \mathbb{G}(\ell_0 \blacktriangleright (\tau_1 \times \tau_2) \blacktriangleright \ell_1) v_1$   
 3487 -  $\blacktriangleright_{\mathbb{C}}$   $\text{stat}(\ell_0 \blacktriangleright \tau_2 \blacktriangleright \ell_1) (\text{snd}\{\tau_2\} v_1)$   
 3488 if  $\text{unop} = \text{snd}$  and  $v_0 = \mathbb{G}(\ell_0 \blacktriangleright (\tau_1 \times \tau_2) \blacktriangleright \ell_1) v_1$   
 3489 -  $\blacktriangleright_{\mathbb{C}}$   $\delta(\text{unop}, v_0)$  if defined  
 3490 -  $\blacktriangleright_{\mathbb{C}}$  Err otherwise

3491 **Case:**  $\cdot \vdash_1 \text{binop}\{\mathcal{U}\} v_0 v_1 : \mathcal{U}$   
 3492 -  $\blacktriangleright_{\mathbb{C}}$   $\delta(\text{binop}, v_0, v_1)$  if defined  
 3493 -  $\blacktriangleright_{\mathbb{C}}$  Err otherwise

3494 **Case:**  $\cdot \vdash_1 \text{app}\{\mathcal{U}\} v_0 v_1 : \mathcal{U}$   
 3495 -  $\blacktriangleright_{\mathbb{C}}$   $e_1[x_0 \leftarrow v_1]$   
 3496 if  $v_0 = \lambda x_0. e_1$   
 3497 -  $\blacktriangleright_{\mathbb{C}}$   $\text{stat}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) (\text{app}\{\tau_0\} v_2 (\text{dyn}(\ell_1 \blacktriangleright \tau_1 \blacktriangleright \ell_0) v_1))$   
 3498 if  $v_0 = \mathbb{G}(\ell_0 \blacktriangleright (\tau_1 \Rightarrow \tau_0) \blacktriangleright \ell_1) v_2$   
 3499 -  $\blacktriangleright_{\mathbb{C}}$  Err otherwise

3500 **Case:**  $\cdot \vdash_1 \text{stat}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0 : \mathcal{U}$   
 3501 -  $\blacktriangleright_{\mathbb{C}}$   $\mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0$   
 3502 if  $\tau_0 \in \tau \Rightarrow \tau \cup \tau \times \tau$  and  $\text{shape-match}(\lfloor \tau_0 \rfloor, v_0)$   
 3503 -  $\blacktriangleright_{\mathbb{C}}$   $v_0$   
 3504 if  $v_0 \in i$  and  $\tau_0 \in \text{Int}$   
 3505 -  $\blacktriangleright_{\mathbb{C}}$   $v_0$   
 3506 if  $v_0 \in n$  and  $\tau_0 \in \text{Nat}$   
 3507 -  $\blacktriangleright_{\mathbb{C}}$  Err otherwise

3508 **Case:**  $\cdot \vdash_1 \mathbb{G}(\ell_0 \blacktriangleright (\tau_1 \Rightarrow \tau_0) \blacktriangleright \ell_1) v_0 : \mathcal{U}$   
 3509 Immediate.

3510 **Case:**  $\cdot \vdash_1 \mathbb{G}(\ell_0 \blacktriangleright (\tau_1 \times \tau_0) \blacktriangleright \ell_1) v_0 : \mathcal{U}$   
 3511 Immediate.

3512 **Case:**  $\cdot \vdash_1 \text{Err} : \mathcal{U}$   
 3513 Immediate.

□

3514  
 3515  
 3516  
 3517  
 3518  
 3519  
 3520  
 3521  
 3522  
 3523  
 3524  
 3525  
 3526  
 3527  
 3528



3529 LEMMA A.5 (CO-NATURAL TYPE PRESERVATION).  
 3530 If  $\cdot \vdash_1 E_0[e_0] : \tau/\mathcal{U}$  and  $C(E_0[e_0])$  and  $e_0 \triangleright_C \cup \blacktriangleright_C e_1$  then  $\cdot \vdash_1 E_0[e_1] : \tau/\mathcal{U}$  and  $C(E_0[e_1])$ .  
 3531

3532 PROOF. By case analysis of each reduction relation.

3533 **Case:**  $unop\{\tau_0\} v_0 \triangleright_C \text{InvariantErr}$   
 3534 Immediate.

3535 **Case:**  $unop\{\tau_0\} v_0 \triangleright_C \delta(unop, v_0)$   
 3536 By lemma 6.2.

3537 **Case:**  $\text{fst}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_0) \triangleright_C \text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_0)$   
 3538 (1)  $\cdot \vdash_1 v_0 : \mathcal{U}$

3539 By  $\vdash_1$  on the redex

3540 (2)  $\cdot \vdash_1 \text{fst}\{\mathcal{U}\} v_0 : \mathcal{U}$

3541 By (1)

3542 (3)  $\tau_1 \leqslant \tau_0$

3543 By  $\vdash_1$  on the redex

3544 (4)  $\cdot \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_0) : \tau_0$

3545 By (2) and (3)

3546 (5)  $C(\text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_0))$

3547 By similar reasoning

3548 **Case:**  $\text{snd}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_0) \triangleright_C \text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{snd}\{\mathcal{U}\} v_0)$

3549 (1)  $\cdot \vdash_1 v_0 : \mathcal{U}$

3550 By  $\vdash_1$  on the redex

3551 (2)  $\cdot \vdash_1 \text{snd}\{\mathcal{U}\} v_0 : \mathcal{U}$

3552 By (1)

3553 (3)  $\tau_2 \leqslant \tau_0$

3554 By  $\vdash_1$  on the redex

3555 (4)  $\cdot \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{snd}\{\mathcal{U}\} v_0) : \tau_0$

3556 By (2) and (3)

3557 **Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_C \text{InvariantErr}$

3558 Immediate.

3559 **Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_C \delta(\text{binop}, v_0, v_1)$

3560 By lemma 6.2.

3561 **Case:**  $\text{app}\{\tau_0\} v_0 v_1 \triangleright_C \text{InvariantErr}$

3562 Immediate.

3563 **Case:**  $\text{app}\{\tau_0\} (\lambda(x_0 : \tau_1). e_0) v_0 \triangleright_C e_0[x_0 \leftarrow v_0]$

3564 By substitution lemmas for typed functions and for  $C(\cdot)$ .

3565 **Case:**  $\text{app}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) v_1 \triangleright_C \text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1))$

3566 (1)  $\cdot \vdash_1 v_0 : \mathcal{U}$

3567 By  $\vdash_1$  on the redex

3568 (2)  $\cdot \vdash_1 v_1 : \tau_1$

3569 By  $\vdash_1$  on the redex

3570 (3)  $\cdot \vdash_1 \text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1 : \mathcal{U}$

3571 By (2)

3572 (4)  $\cdot \vdash_1 \text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1) : \mathcal{U}$

3573 By (1) and (3)

3574 (5)  $\tau_2 \leqslant \tau_0$

3575 By  $\vdash_1$  on the redex  
 3576  
 3577

3578 (6)  $\cdot \vdash_1 \text{dyn } (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat } (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1)) : \tau_0$   
3579 By (4) and (5)  
3580 (7)  $C(\text{dyn } (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat } (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1)))$   
3581 By similar reasoning  
3582 **Case:**  $\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_C \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
3583 Immediate.  
3584 **Case:**  $\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0 \triangleright_C i_0$   
3585 Immediate.  
3586 **Case:**  $\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_C \text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), v_0)$   
3587 Immediate.  
3588 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_C \text{TagErr}$   
3589 Immediate.  
3590 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_C \delta(\text{unop}, v_0)$   
3591 Immediate.  
3592 **Case:**  $\text{fst}\{\mathcal{U}\} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_0) \blacktriangleright_C \text{stat } (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{fst}\{\tau_1\} v_0)$   
3593 (1)  $\cdot \vdash_1 v_0 : \tau_1 \times \tau_2$   
3594 By  $\vdash_1$  on the redex  
3595 (2)  $\cdot \vdash_1 \text{fst}\{\tau_1\} v_0 : \tau_1$   
3596 By (1)  
3597 (3)  $\cdot \vdash_1 \text{stat } (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{fst}\{\tau_1\} v_0) : \mathcal{U}$   
3598 By (2)  
3599 **Case:**  $\text{snd}\{\mathcal{U}\} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_0) \blacktriangleright_C \text{stat } (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{snd}\{\tau_2\} v_0)$   
3600 (1)  $\cdot \vdash_1 v_0 : \tau_1 \times \tau_2$   
3601 By  $\vdash_1$  on the redex  
3602 (2)  $\cdot \vdash_1 \text{snd}\{\tau_2\} v_0 : \tau_2$   
3603 By (1)  
3604 (3)  $\cdot \vdash_1 \text{stat } (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{snd}\{\tau_2\} v_0) : \mathcal{U}$   
3605 By (2)  
3606 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_C \text{TagErr}$   
3607 Immediate.  
3608 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_C \delta(\text{binop}, v_0, v_1)$   
3609 Immediate.  
3610 **Case:**  $\text{app}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_C \text{TagErr}$   
3611 Immediate.  
3612 **Case:**  $\text{app}\{\mathcal{U}\} (\lambda x_0. e_0) v_0 \blacktriangleright_C e_0[x_0 \leftarrow v_0]$   
3613 By substitution lemmas for untyped functions and for  $C(\cdot)$ .  
3614 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_2) \blacktriangleleft \ell_1) v_0) v_1 \blacktriangleright_C \text{stat } (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\tau_2\} v_0 (\text{dyn } (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1))$   
3615 (1)  $\cdot \vdash_1 v_0 : \tau_1 \Rightarrow \tau_2$   
3616 By  $\vdash_1$  on the redex  
3617 (2)  $\cdot \vdash_1 v_1 : \mathcal{U}$   
3618 By  $\vdash_1$  on the redex  
3619 (3)  $\cdot \vdash_1 \text{dyn } (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1 : \tau_1 \Rightarrow \tau_2$   
3620 By (2)  
3621 (4)  $\cdot \vdash_1 \text{app}\{\tau_2\} v_0 (\text{dyn } (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1) : \tau_2$   
3622 By (1) and (3)  
3623 (5)  $\cdot \vdash_1 \text{stat } (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\tau_2\} v_0 (\text{dyn } (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1)) : \mathcal{U}$   
3624 By (4)  
3625  
3626

3627 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{C}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$

3628 Immediate.

3629 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0 \blacktriangleright_{\mathbb{C}} i_0$

3630 Immediate.

3631 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{C}} \text{InvariantErr}$

3632 Immediate.

3633

□

3634

3635

3636

3637

3638

3639

3640

3641

3642

3643

3644

3645

3646

3647

3648

3649

3650

3651

3652

3653

3654

3655

3656

3657

3658

3659

3660

3661

3662

3663

3664

3665

3666

3667

3668

3669

3670

3671

3672

3673

3674

3675

THEOREM A.6 (CO-NATURAL COMPLETE MONITORING). *Co-Natural satisfies CM*

PROOF. By preservation of single-owner consistency ( $\Vdash$ ) for  $\triangleright_{\bar{c}}$  and  $\blacktriangleright_{\bar{c}}$ .

**Case:**  $(unop\{\tau_0\} \langle (v_0) \rangle^{\bar{\ell}_0})^{\ell_0} \triangleright_{\bar{c}} (InvariantErr)^{\ell_0}$

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

**Case:**  $(unop\{\tau_0\} \langle (v_0) \rangle^{\bar{\ell}_0})^{\ell_0} \triangleright_{\bar{c}} (\delta(unop, v_0))^{\bar{\ell}_0 \ell_0}$

(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:**  $(fst\{\tau_0\} \langle (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) (v_0)^{\ell_2}) \rangle^{\bar{\ell}_0})^{\ell_3} \triangleright_{\bar{c}} (\text{dyn}(\ell_0 \blacktriangleright fst(\tau_1) \blacktriangleright \ell_1) (fst\{\mathcal{U}\} (v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$

(1)  $\ell_1; \cdot \Vdash (v_0)^{\ell_2}$

By  $\Vdash$  on the redex

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

By (1)

(3)  $\ell_3; \cdot \Vdash (\text{dyn}(\ell_0 \blacktriangleright fst(\tau_1) \blacktriangleright \ell_1) (fst\{\mathcal{U}\} (v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$

By (1) and  $\Vdash$  on the redex

**Case:**  $(snd\{\tau_0\} \langle (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) (v_0)^{\ell_2}) \rangle^{\bar{\ell}_0})^{\ell_3} \triangleright_{\bar{c}} (\text{dyn}(\ell_0 \blacktriangleright snd(\tau_1) \blacktriangleright \ell_1) (snd\{\mathcal{U}\} (v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$

(1)  $\ell_1; \cdot \Vdash (v_0)^{\ell_2}$

By  $\Vdash$  on the redex

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

By (1)

(3)  $\ell_3; \cdot \Vdash (\text{dyn}(\ell_0 \blacktriangleright snd(\tau_1) \blacktriangleright \ell_1) (snd\{\mathcal{U}\} (v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$

By (1) and  $\Vdash$  on the redex

**Case:**  $(binop\{\tau_0\} \langle (v_0) \rangle^{\bar{\ell}_0} \langle (v_1) \rangle^{\bar{\ell}_1})^{\ell_0} \triangleright_{\bar{c}} (InvariantErr)^{\ell_0}$

Immediate.

**Case:**  $(binop\{\tau_0\} \langle (v_0) \rangle^{\bar{\ell}_0} \langle (v_1) \rangle^{\bar{\ell}_1})^{\ell_0} \triangleright_{\bar{c}} (\delta(binop, v_0, v_1))^{\ell_0}$

(1)  $\delta(binop, v_0, v_1) \in i$

By definition of  $\delta$

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

By (1)

**Case:**  $(app\{\tau_0\} \langle (v_0) \rangle^{\bar{\ell}_0} v_1)^{\ell_0} \triangleright_{\bar{c}} (InvariantErr)^{\ell_0}$

Immediate.

**Case:**  $(app\{\tau_0\} \langle (\lambda(x_0 : \tau_1). e_0) \rangle^{\bar{\ell}_0} v_0)^{\ell_0} \triangleright_{\bar{c}} (e_0[x_0 \leftarrow \langle (v_0) \rangle^{\ell_0 rev(\bar{\ell}_0)}])^{\bar{\ell}_0 \ell_0}$

(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

- 3725 (3)  $\ell_0; \cdot \Vdash \langle (v_0) \rangle^{\ell_0 \text{rev}(\bar{\ell}_0)}$   
 3726 By (1) and (2)  
 3727 (4)  $\ell_0; \cdot \Vdash x_0$  for each occurrence of  $x_0$  in  $e_0$   
 3728 By  $\Vdash$  on the redex  
 3729 (5)  $\ell_0; \cdot \Vdash \langle (e_0[x_0 \leftarrow (v_1)]^{\ell_0 \text{rev}(\bar{\ell}_0)}) \rangle^{\bar{\ell}_0 \ell_0}$   
 3730 By (3) and (4)  
 3731 **Case:**  $(\text{app}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (v_0)^{\ell_2})^{\bar{\ell}_0} v_1)^{\ell_3} \triangleright_{\bar{c}}^{\ell_3}$   
 3732  $(\text{dyn}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) \langle (v_1) \rangle^{\ell_3 \text{rev}(\bar{\ell}_0)}))^{\ell_2})^{\bar{\ell}_0 \ell_3}$   
 3733 (1)  $\ell_2; \cdot \Vdash v_0$   
 3734 By  $\Vdash$  on the redex  
 3735 (2)  $\ell_3; \cdot \Vdash v_1$   
 3736 By  $\Vdash$  on the redex  
 3737 (3)  $\ell_3; \cdot \Vdash \langle (v_1) \rangle^{\ell_3 \text{rev}(\bar{\ell}_0)}$   
 3738 By (2) and  $\Vdash$  on the redex  
 3739 (4)  $\ell_2; \cdot \Vdash \text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) \langle (v_1) \rangle^{\ell_3 \text{rev}(\bar{\ell}_0)}$   
 3740 By (3) and  $\Vdash$  on the redex  
 3741 (5)  $\ell_3; \cdot \Vdash \langle \text{dyn}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) \langle (v_1) \rangle^{\ell_3 \text{rev}(\bar{\ell}_0)}))^{\ell_2} \rangle^{\bar{\ell}_0 \ell_3}$   
 3742 By (1) and (4)  
 3743 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \langle (v_0) \rangle^{\bar{\ell}_0})^{\ell_2} \triangleright_{\bar{c}}^{\ell_2} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \langle (v_0) \rangle^{\bar{\ell}_0})^{\ell_2}$   
 3744 Immediate.  
 3745 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \langle (i_0) \rangle^{\bar{\ell}_0})^{\ell_2} \triangleright_{\bar{c}}^{\ell_2} (i_0)^{\ell_2}$   
 3746 Immediate.  
 3747 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \langle (v_0) \rangle^{\bar{\ell}_0})^{\ell_2} \triangleright_{\bar{c}}^{\ell_2} (\text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), \langle (v_0) \rangle^{\bar{\ell}_0}))^{\ell_2}$   
 3748 Immediate.  
 3749 **Case:**  $(\text{unop}\{\mathcal{U}\} \langle (v_0) \rangle^{\bar{\ell}_0})^{\ell_0} \blacktriangleright_{\bar{c}}^{\ell_0} (\text{TagErr})^{\ell_0}$   
 3750 Immediate.  
 3751 **Case:**  $(\text{unop}\{\mathcal{U}\} \langle (v_0) \rangle^{\bar{\ell}_0})^{\ell_0} \blacktriangleright_{\bar{c}}^{\ell_0} (\delta(\text{unop}, v_0))^{\bar{\ell}_0 \ell_0}$   
 3752 (1)  $v_0 = \langle v_1, v_2 \rangle$  and  $\delta(\text{unop}, v_0) \in \{v_1, v_2\}$   
 3753 By definition  
 3754 (2)  $\ell_0; \cdot \Vdash v_0$   
 3755 By  $\Vdash$  on the redex  
 3756 (3)  $\ell_0; \cdot \Vdash v_1$  and  $\ell_0; \cdot \Vdash v_2$   
 3757 By (2)  
 3758 (4)  $\ell_0; \cdot \Vdash \delta(\text{unop}, v_0)$   
 3759 By (1) and (3)  
 3760 **Case:**  $(\text{fst}\{\mathcal{U}\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0)^{\ell_2})^{\bar{\ell}_0})^{\ell_3} \blacktriangleright_{\bar{c}}^{\ell_3} (\text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} (v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$   
 3761 (1)  $\ell_1; \cdot \Vdash (v_0)^{\ell_2}$   
 3762 By  $\Vdash$  on the redex  
 3763 (2)  $\ell_1; \cdot \Vdash \text{fst}\{\mathcal{U}\} (v_0)^{\ell_2}$   
 3764 By (1)  
 3765 (3)  $\ell_3; \cdot \Vdash \langle \text{dyn}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} (v_0)^{\ell_2}) \rangle^{\bar{\ell}_0 \ell_3}$   
 3766 By (1) and  $\Vdash$  on the redex  
 3767  
 3768  
 3769  
 3770  
 3771  
 3772  
 3773

3774 **Case:**  $(\text{snd}\{\mathcal{U}\} \llbracket (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0)^{\ell_2}) \rrbracket^{\bar{\ell}_0})^{\ell_3} \blacktriangleright_{\bar{C}} (\text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) (\text{snd}\{\tau_1\} (v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$

3775 (1)  $\ell_1; \cdot \Vdash (v_0)^{\ell_2}$

3776 By  $\Vdash$  on the redex

3777 (2)  $\ell_1; \cdot \Vdash \text{snd}\{\mathcal{U}\} (v_0)^{\ell_2}$

3778 By (1)

3779 (3)  $\ell_3; \cdot \Vdash (\text{dyn}(\ell_0 \blacktriangleleft \text{snd}(\tau_1) \blacktriangleleft \ell_1) (\text{snd}\{\mathcal{U}\} (v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$

3780 By (1) and  $\Vdash$  on the redex

3781 **Case:**  $(\text{binop}\{\mathcal{U}\} \llbracket (v_0) \rrbracket^{\bar{\ell}_0} \llbracket (v_1) \rrbracket^{\bar{\ell}_1})^{\ell_0} \blacktriangleright_{\bar{C}} (\text{TagErr})^{\ell_0}$

3782 Immediate.

3783 **Case:**  $(\text{binop}\{\mathcal{U}\} \llbracket (v_0) \rrbracket^{\bar{\ell}_0} \llbracket (v_1) \rrbracket^{\bar{\ell}_1})^{\ell_0} \blacktriangleright_{\bar{C}} (\delta(\text{binop}, v_0, v_1))^{\ell_0}$

3784 (1)  $\delta(\text{binop}, v_0, v_1) \in i$

3785 By definition of  $\delta$

3786 (2)  $\ell_0; \cdot \Vdash \delta(\text{binop}, v_0, v_1)$

3787 By (1)

3788 **Case:**  $(\text{app}\{\mathcal{U}\} \llbracket (v_0) \rrbracket^{\bar{\ell}_0} v_1)^{\ell_0} \blacktriangleright_{\bar{C}} (\text{TagErr})^{\ell_0}$

3789 Immediate.

3790 **Case:**  $(\text{app}\{\mathcal{U}\} \llbracket (\lambda x_0. e_0) \rrbracket^{\bar{\ell}_0} v_1)^{\ell_0} \blacktriangleright_{\bar{C}} ((e_0[x_0 \leftarrow \llbracket (v_1) \rrbracket^{\ell_0 \text{rev}(\bar{\ell}_0)}])^{\bar{\ell}_0 \ell_0})^{\ell_0}$

3791 (1)  $\ell_0; \cdot \Vdash \lambda x_0. e_0$

3792 By  $\Vdash$  on the redex

3793 (2)  $\ell_0; \cdot \Vdash v_1$

3794 By  $\Vdash$  on the redex

3795 (3)  $\ell_0; \cdot \Vdash \llbracket (v_0) \rrbracket^{\ell_0 \text{rev}(\bar{\ell}_0)}$

3796 By (1) and (2)

3797 (4)  $\ell_0; \cdot \Vdash x_0$  for each occurrence of  $x_0$  in  $e_0$

3798 By  $\Vdash$  on the redex

3799 (5)  $\ell_0; \cdot \Vdash \llbracket (e_0[x_0 \leftarrow \llbracket (v_1) \rrbracket^{\ell_0 \text{rev}(\bar{\ell}_0)}]) \rrbracket^{\bar{\ell}_0 \ell_0}$

3800 By (3) and (4)

3801 **Case:**  $(\text{app}\{\mathcal{U}\} \llbracket (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0)^{\ell_2}) \rrbracket^{\bar{\ell}_0} v_1)^{\ell_3} \blacktriangleright_{\bar{C}}$

3802  $(\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) \llbracket (v_1) \rrbracket^{\ell_3 \text{rev}(\bar{\ell}_0)}))^{\ell_2})^{\bar{\ell}_0 \ell_3}$

3803 (1)  $\ell_2; \cdot \Vdash v_0$

3804 By  $\Vdash$  on the redex

3805 (2)  $\ell_3; \cdot \Vdash v_1$

3806 By  $\Vdash$  on the redex

3807 (3)  $\ell_3; \cdot \Vdash \llbracket (v_1) \rrbracket^{\ell_3 \text{rev}(\bar{\ell}_0)}$

3808 By (2) and  $\Vdash$  on the redex

3809 (4)  $\ell_2; \cdot \Vdash \text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) \llbracket (v_1) \rrbracket^{\ell_3 \text{rev}(\bar{\ell}_0)}$

3810 By (3) and  $\Vdash$  on the redex

3811 (5)  $\ell_3; \cdot \Vdash (\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) \llbracket (v_1) \rrbracket^{\ell_3 \text{rev}(\bar{\ell}_0)}))^{\ell_2})^{\bar{\ell}_0 \ell_3}$

3812 By (1) and (4)

3813 **Case:**  $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \llbracket (v_0) \rrbracket^{\bar{\ell}_0})^{\ell_2} \blacktriangleright_{\bar{C}} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \llbracket (v_0) \rrbracket^{\bar{\ell}_0})^{\ell_2}$

3814 Immediate.

3815

3816

3823 **Case:**  $(\text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((i_0))^{\bar{\ell}_2})^{\ell_3} \blacktriangleright_{\bar{c}} (i_0)^{\ell_3}$

3824 Immediate.

3825 **Case:**  $(\text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_2})^{\ell_2} \blacktriangleright_{\bar{c}} (\text{InvariantErr})^{\ell_2}$

3826 Immediate.

3827

3828

3829

3830

3831

3832

3833

3834

3835

3836

3837

3838

3839

3840

3841

3842

3843

3844

3845

3846

3847

3848

3849

3850

3851

3852

3853

3854

3855

3856

3857

3858

3859

3860

3861

3862

3863

3864

3865

3866

3867

3868

3869

3870

3871

□

LEMMA A.7 ( $N \lesssim C$ ).

- If  $e_0 \lesssim e_2$  and  $e_0 \rightarrow_N e_1$  then  $\exists e_3, e_4$  such that  $e_1 \rightarrow_N^* e_3$  and  $e_2 \rightarrow_C^* e_4$  and  $e_3 \lesssim e_4$ .
- If  $e_0 \lesssim e_2$  and  $e_2 \rightarrow_C e_3$  then  $\exists e_1, e_4$  such that  $e_3 \rightarrow_C^* e_4$  and  $e_0 \rightarrow_N^* e_1$  and  $e_1 \lesssim e_4$

PROOF. By lemma A.8 and lemma A.9. □

$\text{wfr}_{NC}(e_0, e_1)$  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  $e_2 \rightarrow_N^* e_0$  and  $e_2 \rightarrow_C^* e_1$

LEMMA A.8.

If  $\text{wfr}_{NC}(e_0, e_2)$  and  $e_0 \lesssim e_2$  and  $e_0 \rightarrow_N e_1$  then  $\exists e_3, e_4$  such that  $e_1 \rightarrow_N^* e_3$  and  $e_2 \rightarrow_C^* e_4$  and  $e_3 \lesssim e_4$ .

PROOF. By lemma A.10, lemma A.13, and case analysis of  $\triangleright_N \cup \blacktriangleright_N$ .

**Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_N \text{InvariantErr}$

Impossible, by type soundness

**Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_N \delta(\text{unop}, v_0)$

(1)  $e_1 = \text{unop}\{\tau_0\} v_1$  and  $v_0 \lesssim v_1$

By  $\lesssim$  on the redex

(2) If  $v_1 \in \langle v, v \rangle$  then  $\delta(\text{unop}, v_1)$  is defined and  $\delta(\text{unop}, v_0) \lesssim \delta(\text{unop}, v_1)$

(3) Otherwise  $v_1 \in \mathbb{G} b v$  and  $e_1 \rightarrow_C^* v_2$  where  $\delta(\text{unop}, v_0) \lesssim v_2$

**Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_N \text{InvariantErr}$

Impossible, by type soundness

**Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_N \delta(\text{binop}, v_0, v_1)$

(1)  $e_1 = \text{binop}\{\tau_0\} v_2 v_3$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$

By  $\lesssim$  on the redex

(2)  $\delta(\text{binop}, v_2, v_3)$  is defined

By (1)

(3)  $\delta(\text{binop}, v_0, v_1) \lesssim \delta(\text{binop}, v_2, v_3)$

By  $\delta$

**Case:**  $\text{app}\{\tau_0\} v_0 v_1 \triangleright_N \text{InvariantErr}$

Impossible, by type soundness

**Case:**  $\text{app}\{\tau_0\} (\lambda(x_0 : \tau_1). e_0) v_0 \triangleright_N e_0[x_0 \leftarrow v_0]$

(1)  $e_1 = \text{app}\{\tau_0\} v_1 v_2$  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:**  $\text{app}\{\tau_0\} (\mathbb{G} (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) v_1 \triangleright_N$

$\text{dyn} (\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat} (\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_1))$

(1)  $e_1 = \text{app}\{\tau_0\} v_2 v_3$  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)  $e_1 \triangleright_C \text{dyn} (\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat} (\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_3))$

By (2)

(4)  $\text{dyn} (\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat} (\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_1)) \lesssim$

$\text{dyn} (\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat} (\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_3))$



- 3921 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) v_0 \triangleright_N \mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) v_0$   
 3922 (1)  $e_1 = \text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) v_1$  and  $v_0 \lesssim v_1$  and  $\tau_0 \Rightarrow \tau_1 = \tau_2$   
 3923 By  $\lesssim$   
 3924 (2)  $e_1 \triangleright_C \mathbb{G}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) v_1$   
 3925 By  $\triangleright_C$   
 3926 (3)  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \Rightarrow \tau_1 \blacktriangleleft \ell_1) v_0 \lesssim \mathbb{G}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) v_1$   
 3927 By (1)
- 3928 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \langle v_0, v_1 \rangle \triangleright_N \langle \text{dyn}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) v_0, \text{dyn}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) v_1 \rangle$   
 3929 (1)  $e_1 = \text{dyn}(\ell_0 \blacktriangleleft \tau_1 \times \tau_2 \blacktriangleleft \ell_1) v_1$  and  $v_0 \lesssim v_1$  and  $\tau_0 = \tau_1 \times \tau_2$   
 3930 By  $\lesssim$   
 3931 (2)  $e_1 \triangleright_C \mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \times \tau_2 \blacktriangleleft \ell_1) v_1$   
 3932 By  $\triangleright_C$   
 3933 (3) Either  $e_0 \rightarrow_N^* \text{BoundaryErr}(\bar{b}, v)$   
 3934 or  $e_0 \rightarrow_N^* \langle v_2, v_3 \rangle$  and  $\langle v_2, v_3 \rangle \lesssim \mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \times \tau_2 \blacktriangleleft \ell_1) v_1$
- 3935 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0 \triangleright_N i_0$   
 3936 (1)  $e_1 = \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0$   
 3937 By  $\lesssim$   
 3938 (2)  $i_0 \lesssim i_0$
- 3939 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_N \text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), v_0)$   
 3940 Immediate
- 3941 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_N \text{TagErr}$   
 3942 (1)  $e_1 = \text{unop}\{\mathcal{U}\} v_1$  and  $v_0 \lesssim v_1$   
 3943 By  $\lesssim$  on the redex  
 3944 (2)  $\delta(\text{unop}, v_1)$  is undefined  
 3945 By (1)  
 3946 (3)  $\text{TagErr} \lesssim \text{TagErr}$
- 3947 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_N \delta(\text{unop}, v_0)$   
 3948 (1)  $e_1 = \text{unop}\{\mathcal{U}\} v_1$  and  $v_0 \lesssim v_1$   
 3949 By  $\lesssim$  on the redex  
 3950 (2) If  $v_1 \in \langle v, v \rangle$  then  $\delta(\text{unop}, v_1)$  is defined  
 3951 By (1)  
 3952 (3) Otherwise  $v_1 \in \mathbb{G} b v$  and  $e_1 \rightarrow_C^* 2$  where  $\delta(\text{unop}, v_0) \lesssim v_2$
- 3953 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_N \text{TagErr}$   
 3954 (1)  $e_1 = \text{binop}\{\mathcal{U}\} v_2 v_3$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$   
 3955 By  $\lesssim$  on the redex  
 3956 (2)  $\delta(\text{binop}, v_2, v_3)$  is undefined  
 3957 By (1)  
 3958 (3)  $\text{TagErr} \lesssim \text{TagErr}$
- 3959 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_N \delta(\text{binop}, v_0, v_1)$   
 3960 (1)  $e_1 = \text{binop}\{\mathcal{U}\} v_2 v_3$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$   
 3961 By  $\lesssim$  on the redex  
 3962 (2)  $\delta(\text{binop}, v_2, v_3)$  is defined  
 3963 By (1)  
 3964 (3)  $\delta(\text{binop}, v_0, v_1) \lesssim \delta(\text{binop}, v_2, v_3)$   
 3965 By  $\delta$
- 3966 **Case:**  $\text{app}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_N \text{TagErr}$   
 3967  
 3968  
 3969

3970 (1)  $e_1 = \text{app}\{\mathcal{U}\} v_2 v_3$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$   
 3971 By  $\lesssim$  on the redex  
 3972 (2)  $v_2 \notin \lambda x. e \cup \mathbb{G} b v$   
 3973 By (1)  
 3974 (3)  $\text{TagErr} \lesssim \text{TagErr}$   
 3975 **Case:**  $\text{app}\{\mathcal{U}\} (\lambda x_0. e_0) v_0 \blacktriangleright_{\mathbb{N}} e_0[x_0 \leftarrow v_0]$   
 3976 (1)  $e_1 = \text{app}\{\mathcal{U}\} v_1 v_2$  and  $(\lambda x_0. e_4) \lesssim v_1$  and  $v_0 \lesssim v_2$   
 3977 By  $\lesssim$  on the redex  
 3978 (2)  $v_1 = (\lambda x_0. e_5)$   
 3979 By (1)  
 3980 (3)  $(e_4[x_0 \leftarrow v_1]) \lesssim (e_5[x_0 \leftarrow v_2])$   
 3981 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{G} (\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0) v_1 \blacktriangleright_{\mathbb{N}}$   
 3982  $\text{stat} (\ell_0 \blacktriangleright \text{cod}(\tau_0) \blacktriangleright \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 (\text{dyn} (\ell_1 \blacktriangleright \text{dom}(\tau_0) \blacktriangleright \ell_0) v_1))$   
 3983 (1)  $e_1 = \text{app}\{\mathcal{U}\} v_2 v_3$  and  $(\mathbb{G} (\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0) \lesssim v_2$  and  $v_1 \lesssim v_3$   
 3984 By  $\lesssim$  on the redex  
 3985 (2)  $v_2 = (\mathbb{G} (\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_4)$  and  $\tau_0 = \tau_1$   
 3986 By (1)  
 3987 (3)  $e_1 \blacktriangleright_{\mathbb{C}} \text{stat} (\ell_0 \blacktriangleright \text{cod}(\tau_1) \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat} (\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_3))$   
 3988 By (2)  
 3989 (4)  $\text{stat} (\ell_0 \blacktriangleright \text{cod}(\tau_0) \blacktriangleright \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 (\text{dyn} (\ell_1 \blacktriangleright \text{dom}(\tau_0) \blacktriangleright \ell_0) v_1)) \lesssim$   
 3990  $\text{stat} (\ell_0 \blacktriangleright \text{cod}(\tau_1) \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat} (\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_3))$   
 3991 **Case:**  $\text{stat} (\ell_0 \blacktriangleright (\tau_0 \Rightarrow \tau_1) \blacktriangleright \ell_1) v_0 \blacktriangleright_{\mathbb{N}} \mathbb{G} (\ell_0 \blacktriangleright (\tau_0 \Rightarrow \tau_1) \blacktriangleright \ell_1) v_0$   
 3992 (1)  $e_1 = \text{stat} (\ell_0 \blacktriangleright \tau_0 \Rightarrow \tau_1 \blacktriangleright \ell_1) v_1$  and  $v_0 \lesssim v_1$   
 3993 By  $\lesssim$   
 3994 (2)  $e_1 \blacktriangleright_{\mathbb{C}} \mathbb{G} (\ell_0 \blacktriangleright \tau_0 \Rightarrow \tau_1 \blacktriangleright \ell_1) v_1$   
 3995 By  $\blacktriangleright_{\mathbb{C}}$   
 3996 (3)  $\mathbb{G} (\ell_0 \blacktriangleright \tau_0 \Rightarrow \tau_1 \blacktriangleright \ell_1) v_0 \lesssim \mathbb{G} (\ell_0 \blacktriangleright \tau_0 \Rightarrow \tau_1 \blacktriangleright \ell_1) v_1$   
 3997 By (1)  
 3998 **Case:**  $\text{stat} (\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) \langle v_0, v_1 \rangle \blacktriangleright_{\mathbb{N}} \langle \text{stat} (\ell_0 \blacktriangleright \text{fst}(\tau_0) \blacktriangleright \ell_1) v_0, \text{stat} (\ell_0 \blacktriangleright \text{snd}(\tau_0) \blacktriangleright \ell_1) v_1 \rangle$   
 3999 (1)  $e_1 = \text{dyn} (\ell_0 \blacktriangleright \tau_1 \times \tau_2 \blacktriangleright \ell_1) v_1$  and  $v_0 \lesssim v_1$  and  $\tau_0 = \tau_1 \times \tau_2$   
 4000 By  $\lesssim$   
 4001 (2)  $e_1 \blacktriangleright_{\mathbb{C}} \mathbb{G} (\ell_0 \blacktriangleright \tau_1 \times \tau_2 \blacktriangleright \ell_1) v_1$   
 4002 By  $\blacktriangleright_{\mathbb{C}}$   
 4003 (3) Either  $e_0 \rightarrow_{\mathbb{N}}^* \text{BoundaryErr} (\bar{b}, v)$   
 4004 or  $e_0 \rightarrow_{\mathbb{N}}^* \langle v_2, v_3 \rangle$  and  $\langle v_2, v_3 \rangle \lesssim \mathbb{G} (\ell_0 \blacktriangleright \tau_1 \times \tau_2 \blacktriangleright \ell_1) v_1$   
 4005 **Case:**  $\text{stat} (\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) i_0 \blacktriangleright_{\mathbb{N}} i_0$   
 4006 (1)  $e_1 = \text{stat} (\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) i_0$   
 4007 By  $\lesssim$   
 4008 (2)  $i_0 \lesssim i_0$   
 4009 **Case:**  $\text{stat} (\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0 \blacktriangleright_{\mathbb{N}} \text{InvariantErr}$   
 4010 Impossible, by type soundness  
 4011  
 4012  
 4013  
 4014  
 4015  
 4016  
 4017  
 4018

□

LEMMA A.9.

If  $\text{wfr}_{NC}(e_0, e_2)$  and  $e_0 \lesssim e_2$  and  $e_2 \rightarrow_C e_3$  then  $\exists e_1, e_4$  such that  $e_3 \rightarrow_C^* e_4$  and  $e_0 \rightarrow_N^* e_1$  and  $e_1 \lesssim e_4$

PROOF. By lemma A.10, lemma A.13, and case analysis of  $\triangleright_C \cup \blacktriangleright_C$ .

**Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_C \text{InvariantErr}$

Impossible, by type soundness

**Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_C \delta(\text{unop}, v_0)$

(1)  $e_0 = \text{unop}\{\tau_0\} v_1$  and  $v_1 \lesssim v_0$

By  $\lesssim$  on the redex

(2)  $v_1 \in \langle v, v \rangle$  and  $\delta(\text{unop}, v_1)$  is defined

By (1)

(3)  $\delta(\text{unop}, v_1) \lesssim \delta(\text{unop}, v_0)$

**Case:**  $\text{fst}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \triangleright_C \text{dyn}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_0)$

(1)  $e_0 = \text{fst}\{\tau_0\} v_1$  and  $v_1 \lesssim v_0$

By  $\lesssim$  on the redex

(2)  $v_1 \in \langle v, v \rangle$  and  $\delta(\text{unop}, v_1)$  is defined

By (1)

(3)  $\text{dyn } b_0 (\text{fst}\{\mathcal{U}\} v_0) \rightarrow_C^* v_2$

By (2)

(4)  $\delta(\text{fst}, v_1) \lesssim v_2$

**Case:**  $\text{snd}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \triangleright_C \text{dyn}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) (\text{snd}\{\mathcal{U}\} v_0)$

(1)  $e_0 = \text{snd}\{\tau_0\} v_1$  and  $v_1 \lesssim v_0$

By  $\lesssim$  on the redex

(2)  $v_1 \in \langle v, v \rangle$  and  $\delta(\text{unop}, v_1)$  is defined

By (1)

(3)  $\text{dyn } b_0 (\text{snd}\{\mathcal{U}\} v_0) \rightarrow_C^* v_2$

By (2)

(4)  $\delta(\text{snd}, v_1) \lesssim v_2$

**Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_C \text{InvariantErr}$

Impossible, by type soundness

**Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_C \delta(\text{binop}, v_0, v_1)$

(1)  $e_0 = \text{binop}\{\tau_0\} v_2 v_3$  and  $v_2 \lesssim v_0$  and  $v_3 \lesssim v_1$

By  $\lesssim$  on the redex

(2)  $\delta(\text{binop}, v_2, v_3)$  is defined

By (1)

(3)  $\delta(\text{binop}, v_2, v_3) \lesssim \delta(\text{binop}, v_0, v_1)$

By  $\delta$

**Case:**  $\text{app}\{\tau_0\} v_0 v_1 \triangleright_C \text{InvariantErr}$

Impossible, by type soundness

**Case:**  $\text{app}\{\tau_0\} (\lambda(x_0 : \tau_1). e_0) v_0 \triangleright_C e_0[x_0 \leftarrow v_0]$

(1)  $e_0 = \text{app}\{\tau_0\} v_1 v_2$  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:**  $\text{app}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) v_1 \triangleright_C$

$\text{dyn}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_1))$

- 4068 (1)  $e_0 = \text{app}\{\tau_0\} v_2 v_3$  and  $v_2 \lesssim (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0)$  and  $v_3 \lesssim v_1$   
 4069 By  $\lesssim$  on the redex
- 4070 (2)  $v_2 = \mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_4$   
 4071 By (1)
- 4072 (3)  $e_0 \triangleright_{\mathbb{N}} \text{dyn}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_3))$   
 4073 By (2)
- 4074 (4)  $\text{dyn}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_3)) \lesssim$   
 4075  $\text{dyn}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_1))$
- 4076 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_{\mathbb{C}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$
- 4077 (1)  $e_0 = \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $v_1 \lesssim v_0$   
 4078 By  $\lesssim$
- 4079 (2) If  $\tau_0 \in \tau \Rightarrow \tau$  then  $e_0 \triangleright_{\mathbb{N}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$
- 4080 (3) If  $\tau_0 \in \tau \times \tau$  then either  $e_0 \triangleright_{\mathbb{N}} \text{BoundaryErr}(\bar{b}, v)$  or  $e_0 \rightarrow_{\mathbb{N}}^* \langle v_2, v_3 \rangle$  where  $\langle v_2, v_3 \rangle \lesssim$   
 4081  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$
- 4082 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0 \triangleright_{\mathbb{C}} i_0$
- 4083 (1)  $e_0 = \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0$   
 4084 By  $\lesssim$
- 4085 (2)  $i_0 \lesssim i_0$
- 4086 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_{\mathbb{C}} \text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1), v_0)$
- 4087 (1)  $e_0 = \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $v_1 \lesssim v_0$   
 4088 By  $\lesssim$
- 4089 (2)  $e_0 \triangleright_{\mathbb{N}} \text{BoundaryErr}(\bar{b}, v_1)$
- 4090 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_{\mathbb{C}} \text{TagErr}$
- 4091 (1)  $e_0 = \text{unop}\{\mathcal{U}\} v_1$  and  $v_1 \lesssim v_0$   
 4092 By  $\lesssim$  on the redex
- 4093 (2)  $\delta(\text{unop}, v_1)$  is undefined  
 4094 By (1)
- 4095 (3)  $\text{TagErr} \lesssim \text{TagErr}$
- 4096 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_{\mathbb{C}} \delta(\text{unop}, v_0)$
- 4097 (1)  $e_0 = \text{unop}\{\mathcal{U}\} v_1$  and  $v_1 \lesssim v_0$   
 4098 By  $\lesssim$  on the redex
- 4099 (2)  $\delta(\text{unop}, v_1)$  is defined  
 4100 By (1)
- 4101 (3)  $\delta(\text{unop}, v_1) \lesssim \delta(\text{unop}, v_0)$
- 4102 **Case:**  $\text{fst}\{\mathcal{U}\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0) \blacktriangleright_{\mathbb{C}} \text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) (\text{fst}\{\tau_1\} v_0)$
- 4103 (1)  $e_0 = \text{fst}\{\tau_0\} v_1$  and  $v_1 \lesssim v_0$   
 4104 By  $\lesssim$  on the redex
- 4105 (2)  $v_1 \in \langle v, v \rangle$  and  $\delta(\text{unop}, v_1)$  is defined  
 4106 By (1)
- 4107 (3)  $\text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_0) \rightarrow_{\mathbb{C}}^* v_2$   
 4108 By (2)
- 4109 (4)  $\delta(\text{fst}, v_1) \lesssim v_2$
- 4110 **Case:**  $\text{snd}\{\mathcal{U}\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0) \blacktriangleright_{\mathbb{C}} \text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) (\text{snd}\{\tau_1\} v_0)$
- 4111 (1)  $e_0 = \text{snd}\{\tau_0\} v_1$  and  $v_1 \lesssim v_0$   
 4112 By  $\lesssim$  on the redex
- 4113 (2)  $v_1 \in \langle v, v \rangle$  and  $\delta(\text{unop}, v_1)$  is defined  
 4114 By (1)
- 4115
- 4116

- 4117 (3)  $\text{stat}(\ell_0 \blacktriangleright \text{snd}(\tau_0) \blacktriangleright \ell_1) (\text{snd}\{\mathcal{U}\} v_0) \rightarrow_{\mathbb{C}}^* v_2$   
 4118 By (2)  
 4119 (4)  $\delta(\text{snd}, v_1) \lesssim v_2$   
 4120 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{C}} \text{TagErr}$   
 4121 (1)  $e_0 = \text{binop}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim v_0$  and  $v_3 \lesssim v_1$   
 4122 By  $\lesssim$  on the redex  
 4123 (2)  $\delta(\text{binop}, v_2, v_3)$  is undefined  
 4124 By (1)  
 4125 (3)  $\text{TagErr} \lesssim \text{TagErr}$   
 4126 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{C}} \delta(\text{binop}, v_0, v_1)$   
 4127 (1)  $e_0 = \text{binop}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim v_0$  and  $v_3 \lesssim v_1$   
 4128 By  $\lesssim$  on the redex  
 4129 (2)  $\delta(\text{binop}, v_2, v_3)$  is defined  
 4130 By (1)  
 4131 (3)  $\delta(\text{binop}, v_2, v_3) \lesssim \delta(\text{binop}, v_0, v_1)$   
 4132 By  $\delta$   
 4133 **Case:**  $\text{app}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{C}} \text{TagErr}$   
 4134 (1)  $e_0 = \text{app}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim v_0$  and  $v_3 \lesssim v_1$   
 4135 By  $\lesssim$  on the redex  
 4136 (2)  $v_2 \notin \lambda x. e \cup \mathbb{G} b v$   
 4137 By (1)  
 4138 (3)  $\text{TagErr} \lesssim \text{TagErr}$   
 4139 **Case:**  $\text{app}\{\mathcal{U}\} (\lambda x_0. e_0) v_0 \blacktriangleright_{\mathbb{C}} e_0[x_0 \leftarrow v_0]$   
 4140 (1)  $e_0 = \text{app}\{\mathcal{U}\} v_1 v_2$  and  $v_1 \lesssim (\lambda x_0. e_4)$  and  $v_2 \lesssim v_0$   
 4141 By  $\lesssim$  on the redex  
 4142 (2)  $v_1 = (\lambda x_0. e_5)$   
 4143 By (1)  
 4144 (3)  $(e_5[x_0 \leftarrow v_2]) \lesssim (e_4[x_0 \leftarrow v_1])$   
 4145 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0) v_1 \blacktriangleright_{\mathbb{C}}$   
 4146  $\text{stat}(\ell_0 \blacktriangleright \text{cod}(\tau_0) \blacktriangleright \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 (\text{dyn}(\ell_1 \blacktriangleright \text{dom}(\tau_0) \blacktriangleright \ell_0) v_1))$   
 4147 (1)  $e_0 = \text{app}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim (\mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0)$  and  $v_3 \lesssim v_1$   
 4148 By  $\lesssim$  on the redex  
 4149 (2)  $v_2 = (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_4)$  and  $\tau_0 = \tau_1$   
 4150 By (1)  
 4151 (3)  $e_0 \blacktriangleright_{\mathbb{N}} \text{stat}(\ell_0 \blacktriangleright \text{cod}(\tau_1) \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_3))$   
 4152 By (2)  
 4153 (4)  $\text{stat}(\ell_0 \blacktriangleright \text{cod}(\tau_1) \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_3)) \lesssim$   
 4154  $\text{stat}(\ell_0 \blacktriangleright \text{cod}(\tau_0) \blacktriangleright \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 (\text{dyn}(\ell_1 \blacktriangleright \text{dom}(\tau_0) \blacktriangleright \ell_0) v_1))$   
 4155 **Case:**  $\text{stat}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0 \blacktriangleright_{\mathbb{C}} \mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0$   
 4156 (1)  $e_0 = \text{stat}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_1$  and  $v_1 \lesssim v_0$  and  $\tau_1 = \tau_0$   
 4157 By  $\lesssim$   
 4158 (2) If  $\tau_0 \in \tau \Rightarrow \tau$  then  $e_1 \blacktriangleright_{\mathbb{N}} \mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_1$   
 4159 (3) Otherwise  $\tau_0 \in \tau \times \tau$  and either  $e_0 \rightarrow_{\mathbb{N}}^* \text{BoundaryErr}(\bar{b}, v)$  or  $e_0 \rightarrow_{\mathbb{N}}^* \langle v_2, v_3 \rangle$  where  
 4160  $\langle v_2, v_3 \rangle \lesssim \mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0$   
 4161 By  $\rightarrow_{\mathbb{N}}^*$   
 4162 **Case:**  $\text{stat}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) i_0 \blacktriangleright_{\mathbb{C}} i_0$   
 4163  
 4164  
 4165

4166 (1)  $e_0 = \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0$

4167 By  $\lesssim$

4168 (2)  $i_0 \lesssim i_0$

4169 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{C}} \text{InvariantErr}$

4170 Impossible, by type soundness

4171

□

4172

LEMMA A.10.

4173

4174 *If  $\text{wfr}_{NC}(e_0, e_1)$  and  $e_0 \lesssim e_1$  and either  $e_0 \rightarrow_{\mathbb{N}} e_2$  or  $e_1 \rightarrow_{\mathbb{C}} e_3$  then the following results hold:*

4175 •  $e_0 = E_0[e_4]$

4176 •  $e_1 = E_1[e_5]$

4177 •  $E_0 \lesssim E_1$

4178 •  $e_4 \lesssim e_5$ .

4179

PROOF. By lemma A.11 and lemma A.12.

4180

□

4181

LEMMA A.11.

4182 *If  $\text{wfr}_{NC}(E_0[e_0], e_1)$  and  $E_0[e_0] \lesssim e_1$  and  $e_0 (\triangleright_{\mathbb{N}} \cup \blacktriangleright_{\mathbb{N}}) e_2$  then the following results hold:*

4183 •  $e_1 = E_1[e_3]$

4184 •  $E_0 \lesssim E_1$

4185 •  $e_0 \lesssim e_3$ .

4186

PROOF. By induction on  $E_0[e_0] \lesssim e_1$ , proceeding by case analysis of  $E_0[e_0]$ .

4187

□

4188

LEMMA A.12.

4189 *If  $\text{wfr}_{NC}(e_0, E_1[e_1])$  and  $e_0 \lesssim E_1[e_1]$  and  $e_1 (\triangleright_{\mathbb{C}} \cup \blacktriangleright_{\mathbb{C}}) e_3$  then the following results hold:*

4190 •  $e_0 = E_0[e_2]$

4191 •  $E_0 \lesssim E_1$

4192 •  $e_2 \lesssim e_1$ .

4193

PROOF. By induction on  $e_0 \lesssim E_1[e_1]$ , proceeding by case analysis of  $E_1[e_1]$ .

4194

□

4195

LEMMA A.13.

4196 *If  $E_0 \lesssim E_1$  and  $e_2 \lesssim e_3$  then  $E_0[e_2] \lesssim E_1[e_3]$ .*

4197

PROOF. By induction on  $E_0 \lesssim E_1$ .

4198

□

4199

4200

4201

4202

4203

4204

4205

4206

4207

4208

4209

4210

4211

4212

4213

4214

4215 **A.3 Forgetful**

4216 **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*  
 4217 *following holds:*

- 4218 •  $e_0 \in v \cup \text{Err}$
- 4219 •  $\tau/\mathcal{U} \in \tau$  and  $\exists e_1. e_0 \triangleright_{\mathbb{F}} e_1$
- 4220 •  $\tau/\mathcal{U} \in \mathcal{U}$  and  $\exists e_1. e_0 \blacktriangleright_{\mathbb{F}} e_1$

4222 **PROOF.** By unique decomposition (lemma 6.1) and case analysis:

4224 **Case:**  $\cdot \vdash_1 n_0 : \text{Nat}$

4225 Immediate.

4226 **Case:**  $\cdot \vdash_1 i_0 : \text{Int}$

4227 Immediate.

4228 **Case:**  $\cdot \vdash_1 \lambda(x_0 : \tau_0). e_1 : \tau_0 \Rightarrow \tau_1$

4229 Immediate.

4230 **Case:**  $\cdot \vdash_1 \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$

4231 Immediate.

4232 **Case:**  $\cdot \vdash_1 \text{unop}\{\tau_0\} v_0 : \tau_0$

- 4233 -  $\triangleright_{\mathbb{F}}$   $\text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_1)$
- 4234 if  $\text{unop} = \text{fst}$  and  $v_0 = \mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_1$
- 4235 -  $\triangleright_{\mathbb{F}}$   $\text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{snd}\{\mathcal{U}\} v_1)$
- 4236 if  $\text{unop} = \text{snd}$  and  $v_0 = \mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_1$
- 4237 -  $\triangleright_{\mathbb{F}}$   $\delta(\text{unop}, v_0)$  if defined
- 4238 -  $\triangleright_{\mathbb{F}}$  Err otherwise

4239 **Case:**  $\cdot \vdash_1 \text{binop}\{\tau_0\} v_0 v_1 : \tau_0$

- 4240 -  $\triangleright_{\mathbb{F}}$   $\delta(\text{binop}, v_0, v_1)$  if defined
- 4241 -  $\triangleright_{\mathbb{F}}$  Err otherwise

4242 **Case:**  $\cdot \vdash_1 \text{app}\{\tau_0\} v_0 v_1 : \tau_0$

- 4243 -  $\triangleright_{\mathbb{F}}$   $e_1[x_0 \leftarrow v_1]$
- 4244 if  $v_0 = \lambda(\tau_1 : x_0). e_1$
- 4245 -  $\triangleright_{\mathbb{F}}$   $\text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_2 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1))$
- 4246 if  $v_0 = \mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1) v_2$
- 4247 -  $\triangleright_{\mathbb{F}}$  Err otherwise

4248 **Case:**  $\cdot \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 : \tau_0$

- 4249 -  $\triangleright_{\mathbb{F}}$   $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$
- 4250 if  $\tau_0 \in \tau \Rightarrow \tau \cup \tau \times \tau$  and  $\text{shape-match}([\tau_0], v_0)$
- 4251 -  $\triangleright_{\mathbb{F}}$   $v_0$
- 4252 if  $v_0 \in \mathbb{T} \text{? } \bar{b}_0 i$  and  $\tau_0 \in \text{Int}$
- 4253 -  $\triangleright_{\mathbb{F}}$   $v_0$
- 4254 if  $v_0 \in \mathbb{T} \text{? } \bar{b}_0 n$  and  $\tau_0 \in \text{Nat}$
- 4255 -  $\triangleright_{\mathbb{F}}$  Err otherwise

4256 **Case:**  $\cdot \vdash_1 \mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \Rightarrow \tau_1) \blacktriangleleft \ell_1) v_0 : \tau_0$

4257 Immediate.

4258 **Case:**  $\cdot \vdash_1 \mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1) v_0 : \tau_0$

4259 Immediate.

4260 **Case:**  $\cdot \vdash_1 \text{Err} : \tau_0$

4261 Immediate.

4262

4263

4264 **Case:**  $\cdot \vdash_1 i : \mathcal{U}$   
 4265 Immediate.

4266 **Case:**  $\cdot \vdash_1 \lambda x_0. e_0 : \mathcal{U}$   
 4267 Immediate.

4268 **Case:**  $\cdot \vdash_1 \langle v_0, v_1 \rangle : \mathcal{U}$   
 4269 Immediate.

4270 **Case:**  $\cdot \vdash_1 \text{unop}\{\mathcal{U}\} v_0 : \mathcal{U}$   
 4271 -  $\blacktriangleright_{\text{F}}$   $\text{trace } \bar{b}_0 (\text{stat } (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{fst}\{\tau_1\} v_1))$   
 4272 if  $\text{unop} = \text{fst}$  and  $v_0 = \mathbb{T}_? \bar{b}_0 (\mathbb{G} (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_1)$   
 4273 -  $\blacktriangleright_{\text{F}}$   $\text{trace } \bar{b}_0 (\text{stat } (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{snd}\{\tau_2\} v_1))$   
 4274 if  $\text{unop} = \text{snd}$  and  $v_0 = \mathbb{T}_? \bar{b}_0 (\mathbb{G} (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_1)$   
 4275 -  $\blacktriangleright_{\text{F}}$   $\text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, \text{rem-trace}(v_0)))$  if defined  
 4276 -  $\blacktriangleright_{\text{F}}$  Err otherwise

4277 **Case:**  $\cdot \vdash_1 \text{binop}\{\mathcal{U}\} v_0 v_1 : \mathcal{U}$   
 4278 -  $\blacktriangleright_{\text{F}}$   $\delta(\text{binop}, \text{rem-trace}(v_0), \text{rem-trace}(v_1))$  if defined  
 4279 -  $\blacktriangleright_{\text{F}}$  Err otherwise

4280 **Case:**  $\cdot \vdash_1 \text{app}\{\mathcal{U}\} v_0 v_1 : \mathcal{U}$   
 4281 -  $\blacktriangleright_{\text{F}}$   $\text{trace } \bar{b}_0 (e_1[x_0 \leftarrow (\text{add-trace}(\text{rev}(\bar{b}_0), v_1)])$   
 4282 if  $v_0 = \mathbb{T}_? \bar{b}_0 (\lambda x_0. e_1)$   
 4283 -  $\blacktriangleright_{\text{F}}$   $\text{trace } \bar{b}_0 (\text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\tau_0\} v_2 (\text{dyn } (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) \text{add-trace}(\text{rev}(\bar{b}_0), v_1))))$   
 4284 if  $v_0 = \mathbb{T}_? \bar{b}_0 (\mathbb{G} (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1) v_2)$   
 4285 -  $\blacktriangleright_{\text{F}}$  Err otherwise

4286 **Case:**  $\cdot \vdash_1 \text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 : \mathcal{U}$   
 4287 -  $\blacktriangleright_{\text{F}}$   $\mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
 4288 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  $\text{shape-match}(\lfloor \tau_0 \rfloor, v_0)$   
 4289 -  $\blacktriangleright_{\text{F}}$   $\text{trace } (b_0 b_1 \bar{b}_0) v_1$   
 4290 if  $\tau_0 \in \tau \Rightarrow \tau \cup \tau \times \tau$  and  $v_0 = \mathbb{G} b_1 (\mathbb{T}_? \bar{b}_0 v_1)$  and  $\text{shape-match}(\lfloor \tau_0 \rfloor, v_0)$   
 4291 -  $\blacktriangleright_{\text{F}}$   $v_0$   
 4292 if  $v_0 \in i$  and  $\tau_0 \in \text{Int}$   
 4293 -  $\blacktriangleright_{\text{F}}$   $v_0$   
 4294 if  $v_0 \in n$  and  $\tau_0 \in \text{Nat}$   
 4295 -  $\blacktriangleright_{\text{F}}$  Err otherwise

4296 **Case:**  $\cdot \vdash_1 \mathbb{G} (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1) v_0 : \mathcal{U}$   
 4297 Immediate.

4298 **Case:**  $\cdot \vdash_1 \mathbb{G} (\ell_0 \blacktriangleleft (\tau_1 \times \tau_0) \blacktriangleleft \ell_1) v_0 : \mathcal{U}$   
 4299 Immediate.

4300 **Case:**  $\cdot \vdash_1 \mathbb{T} \bar{b}_0 v_0 : \mathcal{U}$   
 4301 Immediate.

4302 **Case:**  $\cdot \vdash_1 \text{trace } \bar{b}_0 v_0 : \mathcal{U}$   
 4303 -  $\blacktriangleright_{\text{F}}$   $\text{add-trace}(\bar{b}_0, v_0)$

4304 **Case:**  $\cdot \vdash_1 \text{Err} : \mathcal{U}$   
 4305 Immediate.

□



LEMMA A.15 (FORGETFUL TYPE PRESERVATION).

If  $\cdot \vdash_1 E_0[e_0] : \tau/\mathcal{U}$  and  $F(E_0[e_0])$  and  $e_0 \triangleright_{\mathbb{F}} \cup \blacktriangleright_{\mathbb{F}} e_1$  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  $\blacktriangleright_{\mathbb{F}}$  rule that removes a guard wrapper; the rule preserves soundness because it unwraps an untyped value in an untyped context.

**Case:**  $unop\{\tau_0\} v_0 \triangleright_{\mathbb{F}}$  InvariantErr

Immediate.

**Case:**  $unop\{\tau_0\} v_0 \triangleright_{\mathbb{F}} \delta(unop, v_0)$

By lemma 6.2.

**Case:**  $fst\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_0) \triangleright_{\mathbb{F}} \text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (fst\{\mathcal{U}\} v_0)$

(1)  $\cdot \vdash_1 v_0 : \mathcal{U}$

By  $\vdash_1$  on the redex

(2)  $\cdot \vdash_1 fst\{\mathcal{U}\} v_0 : \mathcal{U}$

By (1)

(3)  $\tau_1 \leq \tau_0$

By  $\vdash_1$  on the redex

(4)  $\cdot \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (fst\{\mathcal{U}\} v_0) : \tau_0$

By (2) and (3)

(5)  $F(\text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (fst\{\mathcal{U}\} v_0))$

By similar reasoning

**Case:**  $snd\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_0) \triangleright_{\mathbb{F}} \text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (snd\{\mathcal{U}\} v_0)$

(1)  $\cdot \vdash_1 v_0 : \mathcal{U}$

By  $\vdash_1$  on the redex

(2)  $\cdot \vdash_1 snd\{\mathcal{U}\} v_0 : \mathcal{U}$

By (1)

(3)  $\tau_2 \leq \tau_0$

By  $\vdash_1$  on the redex

(4)  $\cdot \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (snd\{\mathcal{U}\} v_0) : \tau_0$

By (2) and (3)

**Case:**  $binop\{\tau_0\} v_0 v_1 \triangleright_{\mathbb{F}}$  InvariantErr

Immediate.

**Case:**  $binop\{\tau_0\} v_0 v_1 \triangleright_{\mathbb{F}} \delta(binop, v_0, v_1)$

Immediate.

**Case:**  $app\{\tau_0\} v_0 v_1 \triangleright_{\mathbb{F}}$  InvariantErr

Immediate.

**Case:**  $app\{\tau_0\} (\lambda(x_0 : \tau_1). e_0) v_0 \triangleright_{\mathbb{F}} e_0[x_0 \leftarrow v_0]$

By substitution lemmas for typed functions and for  $F(\cdot)$ .

**Case:**  $app\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) v_1 \triangleright_{\mathbb{F}} \text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (app\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1))$

(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)  $\cdot \vdash_1 \text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1 : \mathcal{U}$

By (2)

(4)  $\cdot \vdash_1 app\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1) : \mathcal{U}$

By (1) and (3)

4362 (5)  $\tau_2 \leq \tau_0$   
 4363 By  $\vdash_1$  on the redex  
 4364 (6)  $\cdot \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1)) : \tau_0$   
 4365 By (4) and (5)  
 4366 (7)  $F(\text{dyn}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1)))$   
 4367 By similar reasoning  
 4368 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_{\mathbb{F}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
 4369 Immediate.  
 4370 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\mathbb{T}_? \bar{b}_0 i_0) \triangleright_{\mathbb{F}} i_0$   
 4371 Immediate.  
 4372 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_{\mathbb{F}} \text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \bar{b}_0, v_0)$   
 4373 Immediate.  
 4374 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_{\mathbb{F}} \text{TagErr}$   
 4375 Immediate.  
 4376 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_{\mathbb{F}} \text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, v_1))$   
 4377 Immediate.  
 4378 **Case:**  $\text{fst}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_0)) \blacktriangleright_{\mathbb{F}} \text{trace} \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{fst}\{\tau_1\} v_0))$   
 4379 (1)  $\cdot \vdash_1 v_0 : \tau_1 \times \tau_2$   
 4380 By  $\vdash_1$  on the redex  
 4381 (2)  $\cdot \vdash_1 \text{fst}\{\tau_1\} v_0 : \tau_1$   
 4382 By (1)  
 4383 (3)  $\cdot \vdash_1 \text{trace} \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{fst}\{\tau_1\} v_0)) : \mathcal{U}$   
 4384 By (2)  
 4385 **Case:**  $\text{snd}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_0)) \blacktriangleright_{\mathbb{F}} \text{trace} \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{snd}\{\tau_2\} v_0))$   
 4386 (1)  $\cdot \vdash_1 v_0 : \tau_1 \times \tau_2$   
 4387 By  $\vdash_1$  on the redex  
 4388 (2)  $\cdot \vdash_1 \text{snd}\{\tau_2\} v_0 : \tau_2$   
 4389 By (1)  
 4390 (3)  $\cdot \vdash_1 \text{stat}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{snd}\{\tau_2\} v_0) : \mathcal{U}$   
 4391 By (2)  
 4392 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{F}} \text{TagErr}$   
 4393 Immediate.  
 4394 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{F}} \delta(\text{binop}, v_2, v_3)$   
 4395 Immediate.  
 4396 **Case:**  $\text{app}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{F}} \text{TagErr}$   
 4397 Immediate.  
 4398 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\lambda x_0. e_0)) v_0 \blacktriangleright_{\mathbb{F}} \text{trace} \bar{b}_0 (e_0[x_0 \leftarrow v_1])$   
 4399 By substitution lemmas for untyped functions and for  $F(\cdot)$ .  
 4400 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_2) \blacktriangleleft \ell_1) v_0)) v_1 \blacktriangleright_{\mathbb{F}}$   
 4401  $\text{trace} \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\tau_2\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_2)))$   
 4402 (1)  $\cdot \vdash_1 v_0 : \tau_1 \Rightarrow \tau_2$   
 4403 By  $\vdash_1$  on the redex  
 4404 (2)  $\cdot \vdash_1 v_1 : \mathcal{U}$   
 4405 By  $\vdash_1$  on the redex  
 4406 (3)  $\cdot \vdash_1 \text{dyn}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1 : \tau_1 \Rightarrow \tau_2$   
 4407 By (2)  
 4408  
 4409  
 4410

4411 (4)  $\cdot \vdash_1 \text{app}\{\tau_2\} v_0 (\text{dyn} (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1) : \tau_2$   
 4412 By (1) and (3)  
 4413 (5)  $\cdot \vdash_1 \text{trace} \bar{b}_0 (\text{stat} (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\tau_2\} v_0 (\text{dyn} (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_2))) : \mathcal{U}$   
 4414 By (4)  
 4415 **Case:**  $\text{stat} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{F}} \mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
 4416 Immediate.  
 4417 **Case:**  $\text{stat} b_0 (\mathbb{G} b_1 (\mathbb{T} \bar{b}_0 v_0)) \blacktriangleright_{\mathbb{F}} \text{trace} (b_0 b_1 \bar{b}_0) v_0$   
 4418 (1)  $\cdot \vdash_1 v_0 : \mathcal{U}$   
 4419 By  $\vdash_1$  on the redex  
 4420 (2)  $\cdot \vdash_1 \text{trace} (b_0 b_1 \bar{b}_0) v_0 : \mathcal{U}$   
 4421 By (1)  
 4422 **Case:**  $\text{stat} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0 \blacktriangleright_{\mathbb{F}} i_0$   
 4423 Immediate.  
 4424 **Case:**  $\text{stat} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{F}} \text{InvariantErr}$   
 4425 Immediate.  
 4426 **Case:**  $\text{trace} \bar{b}_0 v_0 \blacktriangleright_{\mathbb{F}} \text{add-trace} (\bar{b}_0, v_0)$   
 4427 Immediate.

□

4428  
4429  
4430  
4431  
4432  
4433  
4434  
4435  
4436  
4437  
4438  
4439  
4440  
4441  
4442  
4443  
4444  
4445  
4446  
4447  
4448  
4449  
4450  
4451  
4452  
4453  
4454  
4455  
4456  
4457  
4458  
4459

4460 THEOREM A.16 (FORGETFUL BLAME SOUNDNESS AND COMPLETENESS). *Forgetful satisfies BS and*  
 4461 *BC.*

4462 PROOF. By preservation of path-owner consistency ( $\Vdash_p$ ) for  $\triangleright_{\overline{\mathbb{F}}}$  and  $\blacktriangleright_{\overline{\mathbb{F}}}$ .

4463 **Case:**  $(unop\{\tau_0\}((v_0))^{\overline{\ell}_0}) \triangleright_{\overline{\mathbb{F}}} (InvariantErr)^{\ell_0}$

4464 Immediate.

4465 **Case:**  $(unop\{\tau_0\}((v_0))^{\overline{\ell}_0}) \triangleright_{\overline{\mathbb{F}}} (\delta(unop, v_0))^{\overline{\ell}_0 \ell_0}$

4466 (1)  $v_0 = \langle v_1, v_2 \rangle$  and  $\delta(unop, v_0) \in \{v_1, v_2\}$

4467 By definition

4468 (2)  $\ell_0; \cdot \Vdash_p v_0$

4469 By  $\Vdash_p$  on the redex

4470 (3)  $\ell_0; \cdot \Vdash_p v_1$  and  $\ell_0; \cdot \Vdash_p v_2$

4471 By (2) and (3)

4472 (4)  $\ell_0; \cdot \Vdash_p \delta(unop, v_0)$

4473 By (1) and (3)

4474 **Case:**  $(fst\{\tau_0\}(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)(v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3} \triangleright_{\overline{\mathbb{F}}} (dyn(\ell_0 \blacktriangleleft fst(\tau_1) \blacktriangleleft \ell_1)(fst\{\mathcal{U}\}(v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$

4475 (1)  $\ell_1; \cdot \Vdash_p (v_0)^{\ell_2}$

4476 By  $\Vdash_p$  on the redex

4477 (2)  $\ell_1; \cdot \Vdash_p fst\{\mathcal{U}\}(v_0)^{\ell_2}$

4478 By (1)

4479 (3)  $\ell_3; \cdot \Vdash_p (dyn(\ell_0 \blacktriangleleft fst(\tau_1) \blacktriangleleft \ell_1)(fst\{\mathcal{U}\}(v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$

4480 By (1) and  $\Vdash_p$  on the redex

4481 **Case:**  $(snd\{\tau_0\}(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1)(v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3} \triangleright_{\overline{\mathbb{F}}} (dyn(\ell_0 \blacktriangleleft snd(\tau_1) \blacktriangleleft \ell_1)(snd\{\mathcal{U}\}(v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$

4482 (1)  $\ell_1; \cdot \Vdash_p (v_0)^{\ell_2}$

4483 By  $\Vdash_p$  on the redex

4484 (2)  $\ell_1; \cdot \Vdash_p snd\{\mathcal{U}\}(v_0)^{\ell_2}$

4485 By (1)

4486 (3)  $\ell_3; \cdot \Vdash_p (dyn(\ell_0 \blacktriangleleft snd(\tau_1) \blacktriangleleft \ell_1)(snd\{\mathcal{U}\}(v_0)^{\ell_2}))^{\overline{\ell}_0 \ell_3}$

4487 By (1) and  $\Vdash_p$  on the redex

4488 **Case:**  $(binop\{\tau_0\}((v_0))^{\overline{\ell}_0}((v_1))^{\overline{\ell}_1})^{\ell_0} \triangleright_{\overline{\mathbb{F}}} (InvariantErr)^{\ell_0}$

4489 Immediate.

4490 **Case:**  $(binop\{\tau_0\}((v_0))^{\overline{\ell}_0}((v_1))^{\overline{\ell}_1})^{\ell_0} \triangleright_{\overline{\mathbb{F}}} (\delta(binop, v_0, v_1))^{\ell_0}$

4491 (1)  $\delta(binop, v_0, v_1) \in i$

4492 By definition of  $\delta$

4493 (2)  $\ell_0; \cdot \Vdash_p \delta(binop, v_0, v_1)$

4494 By (1)

4495 **Case:**  $(app\{\tau_0\}((v_0))^{\overline{\ell}_0} v_1)^{\ell_0} \triangleright_{\overline{\mathbb{F}}} (InvariantErr)^{\ell_0}$

4496 Immediate.

4497 **Case:**  $(app\{\tau_0\}((\lambda(x_0 : \tau_1). e_0))^{\overline{\ell}_0} v_0)^{\ell_0} \triangleright_{\overline{\mathbb{F}}} ((e_0[x_0 \leftarrow ((v_0))^{\ell_0 rev(\overline{\ell}_0)}]))^{\overline{\ell}_0 \ell_0}$

4498 (1)  $\ell_0; \cdot \Vdash_p \lambda(x_0 : \tau_1). e_0$

4499 By  $\Vdash_p$  on the redex

4509 (2)  $\ell_0; \cdot \Vdash_p v_0$   
 4510 By  $\Vdash_p$  on the redex  
 4511 (3)  $\ell_0; \cdot \Vdash_p ((v_0))^{\ell_0 \text{rev}(\bar{\ell}_0)}$   
 4512 By (1) and (2)  
 4513 (4)  $\ell_0; \cdot \Vdash_p x_0$  for each occurrence of  $x_0$  in  $e_0$   
 4514 By  $\Vdash_p$  on the redex  
 4515 (5)  $\ell_0; \cdot \Vdash_p ((e_0[x_0 \leftarrow ((v_1))^{\ell_0 \text{rev}(\bar{\ell}_0)}]))^{\bar{\ell}_0 \ell_0}$   
 4516 By (3) and (4)  
 4517 **Case:**  $(\text{app}\{\tau_0\} ((\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (v_0))^{\ell_2})^{\bar{\ell}_0} v_1)^{\ell_3} \triangleright_{\mathbb{F}}$   
 4518  $((\text{dyn}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)}))^{\ell_2})^{\bar{\ell}_0 \ell_3})$   
 4519  
 4520 (1)  $\ell_2; \cdot \Vdash_p v_0$   
 4521 By  $\Vdash_p$  on the redex  
 4522 (2)  $\ell_3; \cdot \Vdash_p v_1$   
 4523 By  $\Vdash_p$  on the redex  
 4524 (3)  $\ell_3; \cdot \Vdash_p ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)}$   
 4525 By (2) and  $\Vdash_p$  on the redex  
 4526 (4)  $\ell_2; \cdot \Vdash_p \text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)}$   
 4527 By (3) and  $\Vdash_p$  on the redex  
 4528 (5)  $\ell_3; \cdot \Vdash_p ((\text{dyn}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)}))^{\ell_2})^{\bar{\ell}_0 \ell_3})$   
 4529 By (1) and (4)  
 4530 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2} \triangleright_{\mathbb{F}} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2}$   
 4531 Immediate.  
 4532 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((\mathbb{T}_? \bar{b}_0 ((i_0))^{\bar{\ell}_0}))^{\bar{\ell}_1})^{\ell_2} \triangleright_{\mathbb{F}} (i_0)^{\ell_2}$   
 4533 Immediate.  
 4534 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_2})^{\ell_3} \triangleright_{\mathbb{F}} (\text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \bar{b}_0, ((v_0))^{\bar{\ell}_2}))^{\ell_3}$   
 4535 Immediate.  
 4536 **Case:**  $(\text{unop}\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0})^{\ell_0} \triangleright_{\mathbb{F}} (\text{TagErr})^{\ell_0}$   
 4537 Immediate.  
 4538 **Case:**  $(\text{unop}\{\mathcal{U}\} v_0)^{\ell_0} \triangleright_{\mathbb{F}}$   
 4539  $(\text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, \text{rem-trace}(v_0))))^{\ell_0}$   
 4540 (1)  $v_0 = \mathbb{T}_? \bar{b}_0 \langle v_1, v_2 \rangle$  and  $\delta(\text{unop}, \text{rem-trace}(v_0)) \in \{v_1, v_2\}$   
 4541 By definition  
 4542 (2)  $\ell_0; \cdot \Vdash_p v_0$  and  $\ell_n; \cdot \Vdash_p \text{rem-trace}(v_0)$   
 4543 By  $\Vdash_p$  on the redex  
 4544 (3)  $\ell_n; \cdot \Vdash_p v_1$  and  $\ell_n; \cdot \Vdash_p v_2$   
 4545 By (2)  
 4546 (4)  $\ell_0; \cdot \Vdash_p \text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, \text{rem-trace}(v_0)))$   
 4547 By (1) and (3)  
 4548 **Case:**  $(\text{fst}\{\mathcal{U}\} ((\mathbb{T}_? \bar{b}_0 ((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0))^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4})^{\ell_5} \triangleright_{\mathbb{F}}$   
 4549  $(\text{trace} \bar{b}_0 ((\text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_0))^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4 \ell_5})$   
 4550  
 4551  
 4552  
 4553  
 4554  
 4555  
 4556  
 4557

4558 (1)  $\ell_5; \cdot \Vdash_p \mathbb{T} \bar{b}_0 ((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)(v_0))^{\ell_2})^{\bar{\ell}_3}$   
 4559 By  $\Vdash_p$  on the redex  
 4560 (2)  $\ell_0; \cdot \Vdash_p \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)(v_0)^{\ell_2}$   
 4561 By (1)  
 4562 (3)  $\ell_1; \cdot \Vdash_p v_0$   
 4563 By (2)  
 4564 (4)  $\ell_1; \cdot \Vdash_p \text{fst}\{\text{fst}(\tau_0)\} v_0$   
 4565 By (3)  
 4566 (5)  $\ell_0; \cdot \Vdash_p \text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1)(\text{fst}\{\text{fst}(\tau_0)\} v_0)^{\ell_2}$   
 4567 By (4)  
 4568 (6)  $\ell_5; \cdot \Vdash_p \text{trace } \bar{b}_0 ((\text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1)(\text{fst}\{\text{fst}(\tau_0)\} v_0)^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_3}$   
 4569 By (1) and (5)  
 4570  
 4571 **Case:**  $(\text{snd}\{\mathcal{U}\} ((\mathbb{T} \bar{b}_0 ((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)(v_0))^{\ell_2})^{\bar{\ell}_3}))^{\bar{\ell}_4} \ell_5) \blacktriangleright_{\mathbb{F}}$   
 4572  $(\text{trace } \bar{b}_0 ((\text{stat } b_0 (\text{snd}\{\text{snd}(\tau_0)\} v_0)^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4} \ell_5)$   
 4573 (1)  $\ell_5; \cdot \Vdash_p \mathbb{T} \bar{b}_0 ((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)(v_0))^{\ell_2})^{\bar{\ell}_3}$   
 4574 By  $\Vdash_p$  on the redex  
 4575 (2)  $\ell_0; \cdot \Vdash_p \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)(v_0)^{\ell_2}$   
 4576 By (1)  
 4577 (3)  $\ell_1; \cdot \Vdash_p v_0$   
 4578 By (2)  
 4579 (4)  $\ell_1; \cdot \Vdash_p \text{snd}\{\text{snd}(\tau_0)\} v_0$   
 4580 By (3)  
 4581 (5)  $\ell_0; \cdot \Vdash_p \text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1)(\text{snd}\{\text{snd}(\tau_0)\} v_0)^{\ell_2}$   
 4582 By (4)  
 4583 (6)  $\ell_5; \cdot \Vdash_p \text{trace } \bar{b}_0 ((\text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1)(\text{snd}\{\text{snd}(\tau_0)\} v_0)^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_3}$   
 4584 By (1) and (5)  
 4585 **Case:**  $(\text{binop}\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0} ((v_1))^{\bar{\ell}_1} \ell_0) \blacktriangleright_{\mathbb{F}} (\text{TagErr})^{\ell_0}$   
 4586 Immediate.  
 4587 **Case:**  $(\text{binop}\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0} ((v_1))^{\bar{\ell}_1} \ell_0) \blacktriangleright_{\mathbb{F}} \delta(\text{binop}, v_2, v_3)$   
 4588 Immediate.  
 4589 **Case:**  $(\text{app}\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0} v_1 \ell_0) \blacktriangleright_{\mathbb{F}} (\text{TagErr})^{\ell_0}$   
 4590 Immediate.  
 4591 **Case:**  $(\text{app}\{\mathcal{U}\} ((\mathbb{T} \bar{b}_0 ((\lambda x_0. e_0))^{\bar{\ell}_0}))^{\bar{\ell}_1} v_0) \ell_2 \blacktriangleright_{\mathbb{F}}$   
 4592  $(\text{trace } \bar{b}_0 ([e_0[x_0 \leftarrow \text{add-trace}(\text{rev}(\bar{b}_0), ((v_0))^{\ell_2 \text{rev}(\bar{\ell}_1) \text{rev}(\bar{\ell}_0)})])^{\bar{\ell}_0} \bar{\ell}_1 \ell_2)$   
 4593 (1)  $\ell_2; \cdot \Vdash_p \mathbb{T} \bar{b}_0 ((\lambda x_0. e_0))^{\bar{\ell}_0}$   
 4594 By  $\Vdash_p$  on the redex  
 4595 (2)  $\ell_n; \cdot \Vdash_p \lambda x_0. e_0$   
 4596 By (1)  
 4597 (3)  $\ell_2; \cdot \Vdash_p v_0$   
 4598 By  $\Vdash_p$  on the redex  
 4599  
 4600  
 4601  
 4602  
 4603  
 4604  
 4605  
 4606

- 4607 (4)  $\ell_2; \cdot \Vdash_p v_0$   
 4608 By  $\Vdash_p$  on the redex
- 4609 (5)  $\ell_n; \cdot \Vdash_p \text{add-trace}(\text{rev}(\bar{b}_0), ((v_0))^{\ell_2 \text{rev}(\bar{\ell}_1) \text{rev}(\bar{\ell}_0)})$   
 4610 By (2) and (4)
- 4611 (6)  $\ell_n; \cdot \Vdash_p x_0$  for each occurrence of  $x_0$  in  $e_0$   
 4612 By  $\Vdash_p$  on the redex
- 4613 (7)  $\ell_2; \cdot \Vdash_p \text{trace } \bar{b}_0 \left( (e_0[x_0 \leftarrow \text{add-trace}(\text{rev}(\bar{b}_0), ((v_0))^{\ell_2 \text{rev}(\bar{\ell}_1) \text{rev}(\bar{\ell}_0)})]) \right)^{\bar{\ell}_0}$   
 4614 By (5) and (6)
- 4615 **Case:**  $(\text{app}\{\mathcal{U}\} \left( (\mathbb{T}_? \bar{b}_0 \left( (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0)^{\ell_2} \right)^{\bar{\ell}_3} \right)^{\bar{\ell}_4} v_1 \right)^{\ell_5} \right) \blacktriangleright_{\bar{F}}$   
 4616  $\left( (\text{trace } \bar{b}_0 \left( (\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 v_2)^{\ell_2} \right)^{\bar{\ell}_3} \right)^{\bar{\ell}_4 \ell_5} \right)$   
 4617 where  $v_2 = \text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) \text{add-trace}(\text{rev}(\bar{b}_0), ((v_1))^{\ell_5 \text{rev}(\bar{\ell}_3 \bar{\ell}_4)})$
- 4618 (1)  $\ell_5; \cdot \Vdash_p \mathbb{T}_? \bar{b}_0 \left( (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0)^{\ell_2} \right)^{\bar{\ell}_3} \right)^{\bar{\ell}_4}$   
 4619 By  $\Vdash_p$  on the redex
- 4620 (2)  $\ell_0; \cdot \Vdash_p \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0)^{\ell_2}$  and  $\ell_1; \cdot \Vdash_p v_0$   
 4621 By (1)
- 4622 (3)  $\ell_5; \cdot \Vdash_p v_1$   
 4623 By  $\Vdash_p$  on the redex
- 4624 (4)  $\ell_0; \cdot \Vdash_p \text{add-trace}(\text{rev}(\bar{b}_0), ((v_1))^{\ell_5 \text{rev}(\bar{\ell}_3 \bar{\ell}_4)})$   
 4625 By (1) and (3)
- 4626 (5)  $\ell_1; \cdot \Vdash_p \text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) \text{add-trace}(\text{rev}(\bar{b}_0), ((v_1))^{\ell_5 \text{rev}(\bar{\ell}_3 \bar{\ell}_4)})$   
 4627 By (4)
- 4628 (6)  $\ell_5; \cdot \Vdash_p \text{trace } \bar{b}_0 \left( (\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 v_2)^{\ell_2} \right)^{\bar{\ell}_3} \right)^{\bar{\ell}_4}$   
 4629 where  $v_2 = \text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) \text{add-trace}(\text{rev}(\bar{b}_0), ((v_1))^{\ell_5 \text{rev}(\bar{\ell}_3 \bar{\ell}_4)})$   
 4630 By (1) and (5)
- 4631 **Case:**  $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)^{\ell_2} \blacktriangleright_{\bar{F}} \left( (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)^{\ell_2} \right)$   
 4632 Immediate.
- 4633 **Case:**  $(\text{stat } b_0 \left( (\mathbb{G} b_1 \left( (\mathbb{T}_? \bar{b}_2 v_0 \right)^{\bar{\ell}_0} \right)^{\bar{\ell}_1} \right)^{\bar{\ell}_2} \right) \blacktriangleright_{\bar{F}} \left( \text{trace}(b_0 b_1 \bar{b}_2) \left( (v_0) \right)^{\bar{\ell}_0 \bar{\ell}_1 \ell_2} \right)^{\ell_2}$
- 4634 (1)  $b_0 = (\ell_2 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$  and  $b_1 = (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)$   
 4635 By  $\Vdash_p$  on the redex
- 4636 (2)  $\ell_1; \cdot \Vdash_p \left( (\mathbb{G} b_1 \left( (\mathbb{T}_? \bar{b}_2 v_0 \right)^{\bar{\ell}_0} \right)^{\bar{\ell}_1} \right)$   
 4637 By  $\Vdash_p$  on the redex and (1)
- 4638 (3)  $\ell_0; \cdot \Vdash_p \left( (\mathbb{T}_? \bar{b}_2 v_0 \right)^{\bar{\ell}_0}$   
 4639 By  $\Vdash_p$  on the redex and (1)
- 4640 (4)  $\ell_2; \cdot \Vdash_p \text{trace}(b_0 b_1 \bar{b}_2) \left( (v_0) \right)^{\bar{\ell}_0 \bar{\ell}_1 \ell_2}$   
 4641 By (2) and (3)
- 4642 **Case:**  $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((i_0))^{\bar{\ell}_2} \right)^{\ell_3} \blacktriangleright_{\bar{F}} (i_0)^{\ell_3}$   
 4643 Immediate.
- 4644 **Case:**  $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_2} \right)^{\ell_3} \blacktriangleright_{\bar{F}} (\text{InvariantErr})^{\ell_3}$   
 4645 Immediate.
- 4646
- 4647
- 4648
- 4649
- 4650
- 4651
- 4652
- 4653
- 4654
- 4655

4656 **Case:**  $(\text{trace } \bar{b}_0 v_0)^{\ell_0} \triangleright_{\mathbb{F}} (\text{add-trace}(\bar{b}_0, v_0))^{\ell_0}$   
4657 Immediate.

4658

4659

4660

4661

4662

4663

4664

4665

4666

4667

4668

4669

4670

4671

4672

4673

4674

4675

4676

4677

4678

4679

4680

4681

4682

4683

4684

4685

4686

4687

4688

4689

4690

4691

4692

4693

4694

4695

4696

4697

4698

4699

4700

4701

4702

4703

4704

□



LEMMA A.17 ( $C \lesssim F$ ).

- If  $e_0 \lesssim e_2$  and  $e_0 \rightarrow_C e_1$  then  $\exists e_3, e_4$  such that  $e_1 \rightarrow_C^* e_3$  and  $e_2 \rightarrow_F^* e_4$  and  $e_3 \lesssim e_4$ .
- If  $e_0 \lesssim e_2$  and  $e_2 \rightarrow_F e_3$  then  $\exists e_1, e_4$  such that  $e_3 \rightarrow_F^* e_4$  and  $e_0 \rightarrow_C^* e_1$  and  $e_1 \lesssim e_4$

PROOF. By lemma A.18 and lemma A.19.

□

$\boxed{\text{wfr}_{CF}(e_0, e_1)}$  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  $e_2 \rightarrow_C^* e_0$  and  $e_2 \rightarrow_F^* e_1$

LEMMA A.18.

If  $\text{wfr}_{CF}(e_0, e_2)$  and  $e_0 \lesssim e_2$  and  $e_0 \rightarrow_C e_1$  then  $\exists e_3, e_4$  such that  $e_1 \rightarrow_C^* e_3$  and  $e_2 \rightarrow_F^* e_4$  and  $e_3 \lesssim e_4$ .

PROOF. By lemma A.20, lemma A.23, and case analysis of  $\triangleright_C \cup \blacktriangleright_C$ .

**Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_C \text{InvariantErr}$

Impossible, by type soundness

**Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_C \delta(\text{unop}, v_0)$

(1)  $e_1 = \text{unop}\{\tau_0\} v_1$  and  $v_0 \lesssim v_1$

By  $\lesssim$  on the redex

(2)  $\delta(\text{unop}, v_1)$  is defined

By (1)

(3)  $\delta(\text{unop}, v_0) \lesssim \delta(\text{unop}, v_1)$

**Case:**  $\text{fst}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \triangleright_C \text{dyn}(\ell_0 \blacktriangleleft \text{fst}(\tau_1) \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_0)$

(1)  $e_1 = \text{fst}\{\tau_0\} v_1$  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)  $e_1 \triangleright_F \text{dyn}(\ell_0 \blacktriangleleft \text{fst}(\tau_1) \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_1)$

and  $\text{dyn}(\ell_0 \blacktriangleleft \text{fst}(\tau_1) \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_5) \lesssim \text{dyn}(\ell_0 \blacktriangleleft \text{fst}(\tau_1) \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_1)$

**Case:**  $\text{snd}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \triangleright_C \text{dyn}(\ell_0 \blacktriangleleft \text{snd}(\tau_1) \blacktriangleleft \ell_1) (\text{snd}\{\mathcal{U}\} v_0)$

(1)  $e_1 = \text{snd}\{\tau_0\} v_1$  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)  $e_1 \triangleright_F \text{dyn}(\ell_0 \blacktriangleleft \text{snd}(\tau_1) \blacktriangleleft \ell_1) (\text{snd}\{\mathcal{U}\} v_1)$

and  $\text{dyn}(\ell_0 \blacktriangleleft \text{snd}(\tau_1) \blacktriangleleft \ell_1) (\text{snd}\{\mathcal{U}\} v_5) \lesssim \text{dyn}(\ell_0 \blacktriangleleft \text{snd}(\tau_1) \blacktriangleleft \ell_1) (\text{snd}\{\mathcal{U}\} v_1)$

**Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_C \text{InvariantErr}$

Impossible, by type soundness

**Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_C \delta(\text{binop}, v_0, v_1)$

(1)  $e_1 = \text{binop}\{\tau_0\} v_2 v_3$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$

By  $\lesssim$  on the redex

(2)  $\delta(\text{binop}, v_2, v_3)$  is defined

By (1)

(3)  $\delta(\text{binop}, v_0, v_1) \lesssim \delta(\text{binop}, v_2, v_3)$

By  $\delta$

**Case:**  $\text{app}\{\tau_0\} v_0 v_1 \triangleright_C \text{InvariantErr}$

Impossible, by type soundness

**Case:**  $\text{app}\{\tau_0\} (\lambda(x_0 : \tau_1). e_0) v_0 \triangleright_C e_0[x_0 \leftarrow v_0]$

(1)  $e_1 = \text{app}\{\tau_0\} v_1 v_2$  and  $(\lambda(x_0 : \tau_1). e_4) \lesssim v_1$  and  $v_0 \lesssim v_2$

By  $\lesssim$  on the redex

- 4754 (2)  $v_1 = \lambda(x_0 : \tau_1). e_5$   
 4755 By (1)  
 4756 (3)  $e_4[x_0 \leftarrow v_0] \lesssim e_5[x_0 \leftarrow v_2]$   
 4757 **Case:**  $\text{app}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_0) v_1 \triangleright_{\mathbb{C}}$   
 4758  $\text{dyn}(\ell_0 \blacktriangleright \text{cod}(\tau_1) \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_1))$   
 4759 (1)  $e_1 = \text{app}\{\tau_0\} v_2 v_3$  and  $(\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_0) \lesssim v_2$  and  $v_1 \lesssim v_3$   
 4760 By  $\lesssim$  on the redex  
 4761 (2)  $v_2 = \mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_4$   
 4762 (3)  $e_1 \triangleright_{\mathbb{F}} \text{dyn}(\ell_0 \blacktriangleright \text{cod}(\tau_1) \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_3))$   
 4763 (4)  $\text{dyn}(\ell_0 \blacktriangleright \text{cod}(\tau_1) \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_1)) \lesssim$   
 4764  $\text{dyn}(\ell_0 \blacktriangleright \text{cod}(\tau_1) \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_3))$   
 4765 **Case:**  $\text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0 \triangleright_{\mathbb{C}} \mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0$   
 4766 (1)  $e_1 = \text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_1$  and  $v_0 \lesssim v_1$   
 4767 By  $\lesssim$   
 4768 (2)  $e_1 \triangleright_{\mathbb{F}} \mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_1$   
 4769 By  $\triangleright_{\mathbb{F}}$   
 4770 (3)  $\mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0 \lesssim \mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_1$   
 4771 **Case:**  $\text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) i_0 \triangleright_{\mathbb{C}} i_0$   
 4772 (1)  $e_1 = \text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_1$  and  $i_0 \lesssim v_1$   
 4773 By  $\lesssim$   
 4774 (2)  $\text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_1 \triangleright_{\mathbb{F}} v_1$  and  $i_0 \lesssim v_1$   
 4775 **Case:**  $\text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0 \triangleright_{\mathbb{C}} \text{BoundaryErr}((\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1), v_0)$   
 4776 Immediate  
 4777 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_{\mathbb{C}} \text{TagErr}$   
 4778 (1)  $e_1 = \text{unop}\{\mathcal{U}\} v_1$  and  $v_0 \lesssim v_1$   
 4779 By  $\lesssim$  on the redex  
 4780 (2)  $\delta(\text{unop}, v_1)$  is undefined  
 4781 By (1)  
 4782 (3)  $\text{TagErr} \lesssim \text{TagErr}$   
 4783 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_{\mathbb{C}} \delta(\text{unop}, v_0)$   
 4784 (1)  $e_1 = \text{unop}\{\tau_0\} v_1$  and  $v_0 \lesssim v_1$   
 4785 By  $\lesssim$  on the redex  
 4786 (2)  $\delta(\text{unop}, v_1)$  is defined  
 4787 By (1)  
 4788 (3)  $\delta(\text{unop}, v_0) \lesssim \delta(\text{unop}, v_1)$   
 4789 **Case:**  $\text{fst}\{\mathcal{U}\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0) \blacktriangleright_{\mathbb{C}} \text{stat}(\ell_0 \blacktriangleright \text{fst}(\tau_0) \blacktriangleright \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_0)$   
 4790 (1)  $e_1 = \text{fst}\{\tau_0\} v_1$  and  $v_0 \lesssim v_1$   
 4791 By  $\lesssim$  on the redex  
 4792 (2) If  $v_1 \in \mathbb{T} \bar{b}_0 v_2$  then either  $\text{stat}(\ell_0 \blacktriangleright \text{fst}(\tau_0) \blacktriangleright \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_0) \rightarrow_{\mathbb{C}}^* \text{BoundaryErr}(\bar{b}, v)$  or  
 4793  $\text{stat}(\ell_0 \blacktriangleright \text{fst}(\tau_0) \blacktriangleright \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_0) \rightarrow_{\mathbb{C}}^* v_3$  and  $e_1 \rightarrow_{\mathbb{F}}^* v_4$  and  $v_3 \lesssim v_4$   
 4794 (3) Otherwise  $v_1 \in \mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_5$  and  $e_1 \blacktriangleright_{\mathbb{F}} \text{stat}(\ell_0 \blacktriangleright \text{fst}(\tau_0) \blacktriangleright \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_1)$   
 4795 and  $\text{stat}(\ell_0 \blacktriangleright \text{fst}(\tau_0) \blacktriangleright \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_5) \lesssim \text{stat}(\ell_0 \blacktriangleright \text{fst}(\tau_1) \blacktriangleright \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_1)$   
 4796 **Case:**  $\text{snd}\{\mathcal{U}\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0) \blacktriangleright_{\mathbb{C}} \text{stat}(\ell_0 \blacktriangleright \text{snd}(\tau_0) \blacktriangleright \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_0)$   
 4797 (1)  $e_1 = \text{snd}\{\tau_0\} v_1$  and  $v_0 \lesssim v_1$   
 4798 By  $\lesssim$  on the redex  
 4799 (2) If  $v_1 \in \mathbb{T} \bar{b}_0 v_2$  then either  $\text{stat}(\ell_0 \blacktriangleright \text{snd}(\tau_0) \blacktriangleright \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_0) \rightarrow_{\mathbb{C}}^* \text{BoundaryErr}(\bar{b}, v)$   
 4800 or  $\text{stat}(\ell_0 \blacktriangleright \text{snd}(\tau_0) \blacktriangleright \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_0) \rightarrow_{\mathbb{C}}^* v_3$  and  $e_1 \rightarrow_{\mathbb{F}}^* v_4$  and  $v_3 \lesssim v_4$   
 4801  
 4802

- 4803 (3) Otherwise  $v_1 \in \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_5$  and  $e_1 \blacktriangleright_{\mathbb{F}} \text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_1)$  and  
4804  $\text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_5) \lesssim \text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_1) \blacktriangleleft \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_1)$
- 4805 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{C}} \text{TagErr}$   
4806 (1)  $e_1 = \text{binop}\{\mathcal{U}\} v_2 v_3$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$   
4807 By  $\lesssim$  on the redex  
4808 (2)  $\delta(\text{binop}, \text{rem-trace}(v_2), \text{rem-trace}(v_3))$  is undefined  
4809 By (1)  
4810 (3)  $\text{TagErr} \lesssim \text{TagErr}$
- 4811 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{C}} \delta(\text{binop}, v_0, v_1)$   
4812 (1)  $e_1 = \text{binop}\{\mathcal{U}\} v_2 v_3$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$   
4813 By  $\lesssim$  on the redex  
4814 (2)  $\delta(\text{binop}, \text{rem-trace}(v_2), \text{rem-trace}(v_3))$  is defined  
4815 By (1)  
4816 (3)  $\delta(\text{binop}, v_0, v_1) \lesssim \delta(\text{binop}, \text{rem-trace}(v_2), \text{rem-trace}(v_3))$   
4817 By  $\delta$
- 4818 **Case:**  $\text{app}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{C}} \text{TagErr}$   
4819 (1)  $e_1 = \text{app}\{\mathcal{U}\} v_2 v_3$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$   
4820 By  $\lesssim$  on the redex  
4821 (2)  $v_2 \notin \lambda x. e \cup \mathbb{G} b v$   
4822 By (1)  
4823 (3)  $\text{TagErr} \lesssim \text{TagErr}$
- 4824 **Case:**  $\text{app}\{\mathcal{U}\} (\lambda x_0. e_0) v_0 \blacktriangleright_{\mathbb{C}} e_0[x_0 \leftarrow v_0]$   
4825 (1)  $e_1 = \text{app}\{\mathcal{U}\} v_1 v_2$  and  $(\lambda x_0. e_4) \lesssim v_1$  and  $v_0 \lesssim v_2$   
4826 By  $\lesssim$  on the redex  
4827 (2)  $v_1 = (\lambda x_0. e_5)$   
4828 By (1)  
4829 (3)  $(e_4[x_0 \leftarrow v_1]) \lesssim (e_5[x_0 \leftarrow v_2])$
- 4830 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0) v_1 \blacktriangleright_{\mathbb{C}}$   
4831  $\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_1))$   
4832 (1)  $e_1 = \text{app}\{\mathcal{U}\} v_2 v_3$  and  $(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \lesssim v_2$  and  $v_1 \lesssim v_3$   
4833 By  $\lesssim$  on the redex  
4834 (2) If  $v_2 = \mathbb{T} \bar{b}_0 v_4$  then either  
4835  $\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_1)) \rightarrow_{\mathbb{C}}^* \text{BoundaryErr}(\bar{b}, v)$   
4836 or  $\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_1)) \rightarrow_{\mathbb{C}}^* v_5$   
4837 and  $e_1 \rightarrow_{\mathbb{F}}^* v_6$  and  $v_5 \lesssim v_6$   
4838 (3) Otherwise  $v_2 \in \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_7$   
4839 and  $e_1 \blacktriangleright_{\mathbb{F}} \text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_7 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_3))$   
4840 and  $\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_1)) \lesssim$   
4841  $\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_7 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_3))$
- 4842 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{C}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
4843 (1)  $e_1 = \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $v_0 \lesssim v_1$   
4844 By  $\lesssim$   
4845 (2) If  $e_1 \notin \mathbb{G} b v$  then  $e_1 \blacktriangleright_{\mathbb{F}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \lesssim \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$   
4846 By  $\blacktriangleright_{\mathbb{F}}$   
4847 (3) Otherwise  $e_1 = \mathbb{G} b_1 (\mathbb{T} \bar{b}_0 v_2)$  and  $e_1 \rightarrow_{\mathbb{F}}^* \mathbb{T} b_0 b_1 \bar{b}_0 v_2$  and  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \lesssim \mathbb{T} b_0 b_1 \bar{b}_0 v_2$
- 4848 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0 \blacktriangleright_{\mathbb{C}} i_0$   
4849  
4850  
4851

4852 (1)  $e_1 = \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $i_0 \lesssim v_1$   
 4853 By  $\lesssim$   
 4854 (2)  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1 \blacktriangleright_{\mathbb{F}} v_1$  and  $i_0 \lesssim v_1$   
 4855 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{C}} \text{InvariantErr}$   
 4856 Impossible, by type soundness  
 4857  
 4858  
 4859  
 4860  
 4861  
 4862  
 4863  
 4864  
 4865  
 4866  
 4867  
 4868  
 4869  
 4870  
 4871  
 4872  
 4873  
 4874  
 4875  
 4876  
 4877  
 4878  
 4879  
 4880  
 4881  
 4882  
 4883  
 4884  
 4885  
 4886  
 4887  
 4888  
 4889  
 4890  
 4891  
 4892  
 4893  
 4894  
 4895  
 4896  
 4897  
 4898  
 4899  
 4900

□

LEMMA A.19.

If  $\text{wfr}_{CF}(e_0, e_2)$  and  $e_0 \lesssim e_2$  and  $e_2 \rightarrow_F e_3$  then  $\exists e_1, e_4$  such that  $e_3 \rightarrow_F^* e_4$  and  $e_0 \rightarrow_C^* e_1$  and  $e_1 \lesssim e_4$

PROOF. By lemma A.20, lemma A.23, and case analysis of  $\triangleright_F \cup \blacktriangleright_F$ .

**Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_F \text{InvariantErr}$

Impossible, by type soundness

**Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_F \delta(\text{unop}, v_0)$

(1)  $e_0 = \text{unop}\{\tau_0\} v_1$  and  $v_1 \lesssim v_0$

By  $\lesssim$  on the redex

(2)  $\delta(\text{unop}, v_1)$  is defined

By (1)

(3)  $\delta(\text{unop}, v_1) \lesssim \delta(\text{unop}, v_0)$

**Case:**  $\text{fst}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_0) \triangleright_F \text{dyn}(\ell_0 \blacktriangleright \text{fst}(\tau_1) \blacktriangleright \ell_1) (\text{fst}\{\mathcal{U}\} v_0)$

(1)  $e_0 = \text{fst}\{\tau_0\} v_1$  and  $v_1 \lesssim v_0$

By  $\lesssim$  on the redex

(2)  $v_1 \in \mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_5$

(3)  $e_1 \triangleright_C \text{dyn}(\ell_0 \blacktriangleright \text{fst}(\tau_1) \blacktriangleright \ell_1) (\text{fst}\{\mathcal{U}\} v_1)$

and  $\text{dyn}(\ell_0 \blacktriangleright \text{fst}(\tau_1) \blacktriangleright \ell_1) (\text{fst}\{\mathcal{U}\} v_5) \lesssim \text{dyn}(\ell_0 \blacktriangleright \text{fst}(\tau_1) \blacktriangleright \ell_1) (\text{fst}\{\mathcal{U}\} v_1)$

**Case:**  $\text{snd}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_0) \triangleright_F \text{dyn}(\ell_0 \blacktriangleright \text{snd}(\tau_1) \blacktriangleright \ell_1) (\text{snd}\{\mathcal{U}\} v_0)$

(1)  $e_0 = \text{snd}\{\tau_0\} v_1$  and  $v_1 \lesssim v_0$

By  $\lesssim$  on the redex

(2)  $v_1 \in \mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_5$

(3)  $e_1 \triangleright_C \text{dyn}(\ell_0 \blacktriangleright \text{snd}(\tau_1) \blacktriangleright \ell_1) (\text{snd}\{\mathcal{U}\} v_1)$

and  $\text{dyn}(\ell_0 \blacktriangleright \text{snd}(\tau_1) \blacktriangleright \ell_1) (\text{snd}\{\mathcal{U}\} v_5) \lesssim \text{dyn}(\ell_0 \blacktriangleright \text{snd}(\tau_1) \blacktriangleright \ell_1) (\text{snd}\{\mathcal{U}\} v_1)$

**Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_F \text{InvariantErr}$

Impossible, by type soundness

**Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_F \delta(\text{binop}, v_0, v_1)$

(1)  $e_0 = \text{binop}\{\tau_0\} v_2 v_3$  and  $v_2 \lesssim v_0$  and  $v_3 \lesssim v_1$

By  $\lesssim$  on the redex

(2)  $\delta(\text{binop}, v_2, v_3)$  is defined

By (1)

(3)  $\delta(\text{binop}, v_2, v_3) \lesssim \delta(\text{binop}, v_0, v_1)$

By  $\delta$

**Case:**  $\text{app}\{\tau_0\} v_0 v_1 \triangleright_F \text{InvariantErr}$

Impossible, by type soundness

**Case:**  $\text{app}\{\tau_0\} (\lambda(x_0 : \tau_1). e_0) v_0 \triangleright_F e_0[x_0 \leftarrow v_0]$

(1)  $e_0 = \text{app}\{\tau_0\} v_1 v_2$  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:**  $\text{app}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_0) v_1 \triangleright_F$

$\text{dyn}(\ell_0 \blacktriangleright \text{cod}(\tau_1) \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_1))$

(1)  $e_0 = \text{app}\{\tau_0\} v_2 v_3$  and  $v_2 \lesssim (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_0)$  and  $v_3 \lesssim v_1$

By  $\lesssim$  on the redex

(2)  $v_2 \in \mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_4$

(3)  $e_0 \triangleright_C \text{dyn}(\ell_0 \blacktriangleright \text{cod}(\tau_1) \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_3))$

4950 (4)  $\text{dyn}(\ell_0 \blacktriangleright \text{cod}(\tau_1) \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_3)) \lesssim$   
4951  $\text{dyn}(\ell_0 \blacktriangleright \text{cod}(\tau_1) \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_1))$

4952 **Case:**  $\text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0 \triangleright_{\mathbb{F}} \mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0$

4953 (1)  $e_0 = \text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_1$  and  $v_1 \lesssim v_0$   
4954 By  $\lesssim$

4955 (2)  $e_0 \triangleright_{\mathbb{C}} \mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_1$   
4956 By  $\triangleright_{\mathbb{C}}$

4957 (3)  $\mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_1 \lesssim \mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0$

4958 **Case:**  $\text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) (\mathbb{T} \bar{b}_0 i_0) \triangleright_{\mathbb{F}} i_0$

4959 (1)  $e_0 = \text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) i_1$  and  $i_1 \lesssim i_0$   
4960 By  $\lesssim$

4961 (2)  $\text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) i_1 \triangleright_{\mathbb{C}} i_1$  and  $i_1 \lesssim i_0$

4962 **Case:**  $\text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0 \triangleright_{\mathbb{F}} \text{BoundaryErr}((\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) \bar{b}_0, v_0)$

4963 (1)  $e_0 = \text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_1$  and  $v_1 \lesssim v_0$   
4964 By  $\lesssim$

4965 (2)  $\text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_1 \triangleright_{\mathbb{C}} \text{BoundaryErr}(\bar{b}, v)$

4966 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_{\mathbb{F}} \text{TagErr}$

4967 (1)  $e_0 = \text{unop}\{\mathcal{U}\} v_1$  and  $v_1 \lesssim v_0$   
4968 By  $\lesssim$  on the redex

4969 (2)  $\delta(\text{unop}, v_1)$  is undefined  
4970 By (1)

4971 (3)  $\text{TagErr} \lesssim \text{TagErr}$

4972 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_{\mathbb{F}} \text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, v_1))$

4973 (1)  $e_0 = \text{unop}\{\tau_0\} v_1$  and  $v_1 \lesssim v_0$   
4974 By  $\lesssim$  on the redex

4975 (2)  $\delta(\text{unop}, v_1)$  is defined  
4976 By (1)

4977 (3)  $\delta(\text{unop}, v_1) \lesssim \delta(\text{unop}, v_0)$

4978 **Case:**  $\text{fst}\{\mathcal{U}\} (\mathbb{T} \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0)) \blacktriangleright_{\mathbb{F}} \text{trace } \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleright \text{fst}(\tau_0) \blacktriangleright \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_0))$

4979 (1)  $e_0 = \text{fst}\{\tau_0\} v_1$  and  $v_1 \lesssim v_0$   
4980 By  $\lesssim$  on the redex

4981 (2) If  $\bar{b}_0$  is not empty then either  $\text{fst}\{\tau_0\} v_1 \rightarrow_{\mathbb{C}}^* \text{BoundaryErr}(\bar{b}, v)$  or  $\text{fst}\{\tau_0\} v_1 \rightarrow_{\mathbb{C}}^* v_3$  and  
4982  $e_1 \rightarrow_{\mathbb{F}}^* v_4$  (unfolding guards and collecting traces) and  $v_3 \lesssim v_4$

4983 (3) Otherwise  $\bar{b}_0$  is empty and  $\text{fst}\{\tau_0\} v_1 \blacktriangleright_{\mathbb{C}} \text{stat}(\ell_0 \blacktriangleright \text{fst}(\tau_0) \blacktriangleright \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_1)$   
4984 and  $e_0 \blacktriangleright_{\mathbb{F}} \text{stat}(\ell_0 \blacktriangleright \text{fst}(\tau_0) \blacktriangleright \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_0)$   
4985 and  $\text{stat}(\ell_0 \blacktriangleright \text{fst}(\tau_0) \blacktriangleright \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_1) \lesssim \text{stat}(\ell_0 \blacktriangleright \text{fst}(\tau_0) \blacktriangleright \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_0)$

4986 **Case:**  $\text{snd}\{\mathcal{U}\} (\mathbb{T} \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0)) \blacktriangleright_{\mathbb{F}} \text{trace } \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleright \text{snd}(\tau_0) \blacktriangleright \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_0))$

4987 (1)  $e_0 = \text{snd}\{\tau_0\} v_1$  and  $v_1 \lesssim v_0$   
4988 By  $\lesssim$  on the redex

4989 (2) If  $\bar{b}_0$  is not empty then either  $\text{snd}\{\tau_0\} v_1 \rightarrow_{\mathbb{C}}^* \text{BoundaryErr}(\bar{b}, v)$  or  $\text{snd}\{\tau_0\} v_1 \rightarrow_{\mathbb{C}}^* v_3$  and  
4990  $e_1 \rightarrow_{\mathbb{F}}^* v_4$  (unfolding guards and collecting traces) and  $v_3 \lesssim v_4$

4991 (3) Otherwise  $\bar{b}_0$  is empty and  $\text{snd}\{\tau_0\} v_1 \blacktriangleright_{\mathbb{C}} \text{stat}(\ell_0 \blacktriangleright \text{snd}(\tau_0) \blacktriangleright \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_1)$   
4992 and  $e_0 \blacktriangleright_{\mathbb{F}} \text{stat}(\ell_0 \blacktriangleright \text{snd}(\tau_0) \blacktriangleright \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_0)$   
4993 and  $\text{stat}(\ell_0 \blacktriangleright \text{snd}(\tau_0) \blacktriangleright \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_1) \lesssim \text{stat}(\ell_0 \blacktriangleright \text{snd}(\tau_0) \blacktriangleright \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_0)$

4994 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{F}} \text{TagErr}$

4995 (1)  $e_0 = \text{binop}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim v_0$  and  $v_3 \lesssim v_1$   
4996 By  $\lesssim$  on the redex

4997

4998

- 4999 (2)  $\delta(\text{binop}, \text{rem-trace}(v_2), \text{rem-trace}(v_3))$  is undefined  
5000 By (1)  
5001 (3)  $\text{TagErr} \lesssim \text{TagErr}$   
5002 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{F}} \delta(\text{binop}, v_2, v_3)$   
5003 (1)  $e_0 = \text{binop}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim v_0$  and  $v_3 \lesssim v_1$   
5004 By  $\lesssim$  on the redex  
5005 (2)  $\delta(\text{binop}, \text{rem-trace}(v_2), \text{rem-trace}(v_3))$  is defined  
5006 By (1)  
5007 (3)  $\delta(\text{binop}, \text{rem-trace}(v_2), \text{rem-trace}(v_3)) \lesssim \delta(\text{binop}, v_0, v_1)$   
5008 By  $\delta$   
5009 **Case:**  $\text{app}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{F}} \text{TagErr}$   
5010 (1)  $e_0 = \text{app}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim v_0$  and  $v_3 \lesssim v_1$   
5011 By  $\lesssim$  on the redex  
5012 (2)  $v_2 \notin \lambda x. e \cup \mathbb{G} b v$   
5013 By (1)  
5014 (3)  $\text{TagErr} \lesssim \text{TagErr}$   
5015 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\lambda x_0. e_0)) v_0 \blacktriangleright_{\mathbb{F}} \text{trace } \bar{b}_0 (e_0[x_0 \leftarrow v_1])$   
5016 (1)  $e_1 = \text{app}\{\mathcal{U}\} v_1 v_2$  and  $v_1 \lesssim (\lambda x_0. e_4)$  and  $v_2 \lesssim v_0$  and  $\bar{b}_0$  is empty  
5017 By  $\lesssim$  on the redex  
5018 (2)  $v_1 = (\lambda x_0. e_5)$   
5019 By (1)  
5020 (3)  $(e_5[x_0 \leftarrow v_2]) \lesssim (e_4[x_0 \leftarrow v_1])$   
5021 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) v_1 \blacktriangleright_{\mathbb{F}} \text{trace } \bar{b}_0 (\text{stat } b_0 (\text{app}\{\mathcal{U}\} v_0 (\text{dyn } b_1 v_1)))$   
5022 (1)  $e_0 = \text{app}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim (\mathbb{G} (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0)$  and  $v_3 \lesssim v_1$   
5023 By  $\lesssim$  on the redex  
5024 (2) If  $\bar{b}_0$  is not empty then either  $\text{app}\{\mathcal{U}\} v_2 v_3 \rightarrow_{\mathbb{C}}^* \text{BoundaryErr}(\bar{b}, v)$   
5025 or  $\text{app}\{\mathcal{U}\} v_2 v_3 \rightarrow_{\mathbb{C}}^* v_5$   
5026 and  $e_1 \rightarrow_{\mathbb{F}}^* v_6$  (unfolding guards and collecting traces) and  $v_5 \lesssim v_6$   
5027 (3) Otherwise  $\bar{b}_0$  is empty  
5028 and  $e_1 \blacktriangleright_{\mathbb{F}} \text{stat } (\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_7 (\text{stat } (\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_1))$   
5029 and  $e_0 \blacktriangleright_{\mathbb{C}} \text{stat } (\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_8 (\text{stat } (\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_3))$   
5030 and  $\text{stat } (\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_8 (\text{stat } (\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_3)) \lesssim$   
5031  $\text{stat } (\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_7 (\text{stat } (\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_1))$   
5032 **Case:**  $\text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{F}} \mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
5033 (1)  $e_0 = \text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $v_1 \lesssim v_0$   
5034 By  $\lesssim$   
5035 (2)  $e_1 \blacktriangleright_{\mathbb{C}} \mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
5036 (3)  $\mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \lesssim \mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
5037 **Case:**  $\text{stat } b_0 (\mathbb{G} b_1 (\mathbb{T}_? \bar{b}_0 v_0)) \blacktriangleright_{\mathbb{F}} \text{trace } (b_0 b_1 \bar{b}_0) v_0$   
5038 (1)  $e_0 = \text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $v_1 \lesssim \mathbb{G} b_1 (\mathbb{T}_? \bar{b}_0 v_0)$   
5039 By  $\lesssim$   
5040 (2)  $v_1 = \mathbb{G} b_1 v_2$  and  $v_2 \lesssim \mathbb{T}_? \bar{b}_0 v_0$   
5041 By (1)  
5042 (3)  $e_0 \blacktriangleright_{\mathbb{C}} \mathbb{G} b_0 (\mathbb{G} b_1 v_2)$   
5043 By (2)  
5044 (4)  $e_1 \blacktriangleright_{\mathbb{F}} \mathbb{T} (b_0 b_1 \bar{b}_0) v_0$   
5045 By  $\blacktriangleright_{\mathbb{F}}$   
5046  
5047

5048 (5)  $\mathbb{G} b_0 (\mathbb{G} b_1 v_2) \lesssim \mathbb{T} (b_0 b_1 \bar{b}_0) v_0$

5049 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0 \blacktriangleright_{\mathbb{F}} i_0$

5050 (1)  $e_0 = \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_1$  and  $i_1 \lesssim i_0$

5051 By  $\lesssim$

5052 (2)  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_1 \blacktriangleright_{\mathbb{F}} i_1$  and  $i_1 \lesssim i_0$

5053 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{F}} \text{InvariantErr}$

5054 Impossible, by type soundness

5055 **Case:**  $\text{trace} \bar{b}_0 v_0 \blacktriangleright_{\mathbb{F}} \text{add-trace}(\bar{b}_0, v_0)$

5056 (1)  $e_0 = \text{stat} b_0 (\text{dyn} b_1 v_1)$  and  $\bar{b}_0 = b_0 b_1 \bar{b}_0$

5057 By  $\lesssim$

5058 (2)  $\text{add-trace}(\bar{b}_0, v_0) = \mathbb{T} \bar{b}_0 v_0$

5059 By (1)

5060 (3) Either  $e_0 \rightarrow_{\mathbb{C}}^* \text{BoundaryErr}(\bar{b}, v)$  or  $e_0 \rightarrow_{\mathbb{C}}^* v_2$  and  $v_2 \lesssim \mathbb{T} \bar{b}_0 v_0$

5061

5062

5063 LEMMA A.20.

5064 *If  $\text{wfr}_{CF}(e_0, e_1)$  and  $e_0 \lesssim e_1$  and either  $e_0 \rightarrow_{\mathbb{C}} e_2$  or  $e_1 \rightarrow_{\mathbb{F}} e_3$  then the following results hold:*

5065 •  $e_0 = E_0[e_4]$

5066 •  $e_1 = E_1[e_5]$

5067 •  $E_0 \lesssim E_1$

5068 •  $e_4 \lesssim e_5$ .

5069

5070 **PROOF.** By lemma A.21 and lemma A.22. □

5071 LEMMA A.21.

5072 *If  $\text{wfr}_{CF}(E_0[e_0], e_1)$  and  $E_0[e_0] \lesssim e_1$  and  $e_0 (\triangleright_{\mathbb{C}} \cup \blacktriangleright_{\mathbb{C}}) e_2$  then the following results hold:*

5073 •  $e_1 = E_1[e_3]$

5074 •  $E_0 \lesssim E_1$

5075 •  $e_0 \lesssim e_3$ .

5076

5077 **PROOF.** By induction on  $E_0[e_0] \lesssim e_1$ , proceeding by case analysis of  $E_0[e_0]$ . □

5078 LEMMA A.22.

5079 *If  $\text{wfr}_{CF}(e_0, E_1[e_1])$  and  $e_0 \lesssim E_1[e_1]$  and  $e_1 (\triangleright_{\mathbb{F}} \cup \blacktriangleright_{\mathbb{F}}) e_3$  then the following results hold:*

5080 •  $e_0 = E_0[e_2]$

5081 •  $E_0 \lesssim E_1$

5082 •  $e_2 \lesssim e_1$ .

5083

5084 **PROOF.** By induction on  $e_0 \lesssim E_1[e_1]$ , proceeding by case analysis of  $E_1[e_1]$ . □

5085 LEMMA A.23.

5086 *If  $E_0 \lesssim E_1$  and  $e_2 \lesssim e_3$  then  $E_0[e_2] \lesssim E_1[e_3]$ .*

5087

5088 **PROOF.** By induction on  $E_0 \lesssim E_1$ . □

5089

5090

5091

5092

5093

5094

5095

5096



5097 **A.4 Transient**

5098 LEMMA A.24 (TRANSIENT TYPE PROGRESS).

5099 *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:*

- 5100 •  $e_0 \in v \cup \text{Err}$
- 5101 •  $\exists e_1, \mathcal{H}_1, \mathcal{B}_1. e_0; \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} e_1; \mathcal{H}_1; \mathcal{B}_1$

5103 PROOF. By unique decomposition (lemma 6.1) and case analysis:

5104 **Case:**  $\mathcal{T}_0; \cdot \vdash_s i_0; \mathcal{H}_0; \mathcal{B}_0 : \text{Int}$ 

5105 Immediate.

5106 **Case:**  $\mathcal{T}_0; \cdot \vdash_s n_0; \mathcal{H}_0; \mathcal{B}_0 : \text{Nat}$ 

5107 Immediate.

5108 **Case:**  $\mathcal{T}_0; \cdot \vdash_s (\lambda x_0. e_0); \mathcal{H}_0; \mathcal{B}_0 : \text{Fun}$ 5109  $\triangleright_{\top} p_0; (\{p_0 \mapsto (\lambda x_0. e_0)\} \cup \mathcal{H}_0); (\{p_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$ 5110 **Case:**  $\mathcal{T}_0; \cdot \vdash_s (\lambda(x_0 : \tau_0). e_0); \mathcal{H}_0; \mathcal{B}_0 : \text{Fun}$ 5111  $\triangleright_{\top} p_0; (\{p_0 \mapsto (\lambda(x_0 : \tau_0). e_0)\} \cup \mathcal{H}_0); (\{p_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$ 5112 **Case:**  $\mathcal{T}_0; \cdot \vdash_s \langle v_0, v_1 \rangle; \mathcal{H}_0; \mathcal{B}_0 : \text{Pair}$ 5113  $\triangleright_{\top} p_0; (\{p_0 \mapsto \langle v_0, v_1 \rangle\} \cup \mathcal{H}_0); (\{p_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$ 5114 **Case:**  $\mathcal{T}_0; \cdot \vdash_s (\text{app}\{\tau_0\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0 : \lfloor \tau_0 \rfloor$ 5115 -  $\triangleright_{\top} (\text{check}\{\tau_0\} (e_0[x_0 \leftarrow v_1]) v_0; \mathcal{H}_0; \mathcal{B}_0[v_1 \cup \text{rev}(\mathcal{B}_0(v_0))])$ 5116 if  $\mathcal{H}_0(v_0) = \lambda(x_0 : \tau_1). e_0$  and *shape-match*( $\lfloor \tau_1 \rfloor, v_1$ )5117 -  $\triangleright_{\top} (\text{check}\{\tau_0\} (e_0[x_0 \leftarrow v_1]) v_0; \mathcal{H}_0; \mathcal{B}_0[v_1 \cup \text{rev}(\mathcal{B}_0(v_0))])$ 5118 if  $\mathcal{H}_0(v_0) = \lambda x_0. e_0$ 5119 -  $\triangleright_{\top} \text{Err}$  otherwise5120 **Case:**  $\mathcal{T}_0; \cdot \vdash_s (\text{unop}\{\tau_0\} v_0); \mathcal{H}_0; \mathcal{B}_0 : \lfloor \tau_0 \rfloor$ 5121 -  $\triangleright_{\top} \text{check}\{\tau_0\} \delta(\text{unop}, \mathcal{H}_0(v_0)) v_0; \mathcal{H}_0; \mathcal{B}_0$  if defined5122 -  $\triangleright_{\top} \text{Err}$  otherwise5123 **Case:**  $\mathcal{T}_0; \cdot \vdash_s (\text{binop}\{\tau_0\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0 : \lfloor \tau_0 \rfloor$ 5124 -  $\triangleright_{\top} \delta(\text{binop}, v_0, v_1); \mathcal{H}_0; \mathcal{B}_0$  if defined5125 -  $\triangleright_{\top} \text{Err}$  otherwise5126 **Case:**  $\mathcal{T}_0; \cdot \vdash_s (\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0); \mathcal{H}_0; \mathcal{B}_0 : \lfloor \tau_0 \rfloor$ 5127 -  $\triangleright_{\top} v_0; \mathcal{H}_0; \mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}]$ 5128 if *shape-match*( $\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0)$ )5129 -  $\triangleright_{\top} \text{Err}$  otherwise5130 **Case:**  $\mathcal{T}_0; \cdot \vdash_s (\text{check}\{\tau_0\} v_0 p_0); \mathcal{H}_0; \mathcal{B}_0 : \lfloor \tau_0 \rfloor$ 5131 -  $\triangleright_{\top} v_0; \mathcal{H}_0; \mathcal{B}_0[v_0 \cup \mathcal{B}_0(p_0)]$ 5132 if *shape-match*( $\lfloor \tau_0 \rfloor, v_0$ )5133 -  $\triangleright_{\top} \text{Err}$  otherwise5134 **Case:**  $\mathcal{T}_0; \cdot \vdash_s p_0; \mathcal{H}_0; \mathcal{B}_0 : s_0$ 

5135 Immediate.

5136 **Case:**  $\mathcal{T}_0; \cdot \vdash_s \text{Err}; \mathcal{H}_0; \mathcal{B}_0 : s_0$ 

5137 Immediate.

5138 **Case:**  $\mathcal{T}_0; \cdot \vdash_s i_0; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$ 

5139 Immediate.

5140 **Case:**  $\mathcal{T}_0; \cdot \vdash_s n_0; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$ 

5141 Immediate.

5142 **Case:**  $\mathcal{T}_0; \cdot \vdash_s (\lambda x_0. e_0); \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$ 5143  $\triangleright_{\top} p_0; (\{p_0 \mapsto (\lambda x_0. e_0)\} \cup \mathcal{H}_0); (\{p_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$ 

5144

5145

5146 **Case:**  $\mathcal{T}_0; \cdot \vdash_s (\lambda(x_0 : \tau_0). e_0); \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$   
5147  $\triangleright_{\top} p_0; (\{p_0 \mapsto (\lambda(x_0 : \tau_0). e_0)\} \cup \mathcal{H}_0); (\{p_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$   
5148 **Case:**  $\mathcal{T}_0; \cdot \vdash_s \langle v_0, v_1 \rangle; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$   
5149  $\triangleright_{\top} p_0; (\{p_0 \mapsto \langle v_0, v_1 \rangle\} \cup \mathcal{H}_0); (\{p_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$   
5150 **Case:**  $\mathcal{T}_0; \cdot \vdash_s (\text{app}\{\mathcal{U}\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$   
5151 -  $\triangleright_{\top} (\text{check}\{\mathcal{U}\} (e_0[x_0 \leftarrow v_1]) v_0; \mathcal{H}_0; \mathcal{B}_0[v_1 \cup \text{rev}(\mathcal{B}_0(v_0))])$   
5152 if  $\mathcal{H}_0(v_0) = \lambda(x_0 : \tau_1). e_0$  and *shape-match*( $\lfloor \tau_1 \rfloor, v_1$ )  
5153 -  $\triangleright_{\top} (e_0[x_0 \leftarrow v_1]); \mathcal{H}_0; \mathcal{B}_0$   
5154 if  $\mathcal{H}_0(v_0) = \lambda x_0. e_0$   
5155 -  $\triangleright_{\top}$  Err otherwise  
5156 **Case:**  $\mathcal{T}_0; \cdot \vdash_s (\text{unop}\{\mathcal{U}\} v_0); \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$   
5157 -  $\triangleright_{\top} \text{check}\{\mathcal{U}\} \delta(\text{unop}, \mathcal{H}_0(v_0)) v_0; \mathcal{H}_0; \mathcal{B}_0$  if defined  
5158 -  $\triangleright_{\top}$  Err otherwise  
5159 **Case:**  $\mathcal{T}_0; \cdot \vdash_s (\text{binop}\{\mathcal{U}\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$   
5160 -  $\triangleright_{\top} \delta(\text{binop}, v_0, v_1); \mathcal{H}_0; \mathcal{B}_0$  if defined  
5161 -  $\triangleright_{\top}$  Err otherwise  
5162 **Case:**  $\mathcal{T}_0; \cdot \vdash_s (\text{stat} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0); \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$   
5163 -  $\triangleright_{\top} v_0; \mathcal{H}_0; \mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}]$   
5164 if *shape-match*( $\lfloor \tau_0 \rfloor, \mathcal{H}_0(v_0)$ )  
5165 -  $\triangleright_{\top}$  Err otherwise  
5166 **Case:**  $\mathcal{T}_0; \cdot \vdash_s (\text{check}\{\mathcal{U}\} v_0 p_0); \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$   
5167  $\triangleright_{\top} v_0; \mathcal{H}_0; \mathcal{B}_0$   
5168 **Case:**  $\mathcal{T}_0; \cdot \vdash_s p_0; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$   
5169 Immediate.  
5170 **Case:**  $\mathcal{T}_0; \cdot \vdash_s \text{Err}; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$   
5171 Immediate.

□

5172  
5173  
5174  
5175  
5176  
5177  
5178  
5179  
5180  
5181  
5182  
5183  
5184  
5185  
5186  
5187  
5188  
5189  
5190  
5191  
5192  
5193  
5194

5195 LEMMA A.25 (TRANSIENT TYPE PRESERVATION).

5196 If  $\mathcal{T}_0; \cdot \vdash_s e_0; \mathcal{H}_0; \mathcal{B}_0 : \tau/\mathcal{U}$  and  $e_0; \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\tau} e_1; \mathcal{H}_1; \mathcal{B}_1$  then  $\exists \mathcal{T}_1. \mathcal{T}_0 \subseteq \mathcal{T}_1$  and  $\mathcal{T}_1; \cdot \vdash_s e_1; \mathcal{H}_1; \mathcal{B}_1 : \tau/\mathcal{U}$ .

5197

5198 PROOF. By case analysis of the reduction relation. The new heap typing  $\mathcal{T}_1$  gains an entry only  
 5199 when the value heap does; if  $\mathcal{H}_1 = \{p_0 \mapsto w_0\} \cup \mathcal{H}_0$  then  $\mathcal{T}_1 = \{(p_0 : s_0)\} \cup \mathcal{T}_0$ , where  $s_0$  is the shape  
 5200 of the pre-value (lemma 6.47).

5201 **Case:**  $w_0; \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\tau} p_0; (\{p_0 \mapsto w_0\} \cup \mathcal{H}_0); (\{p_0 \mapsto \emptyset\} \cup \mathcal{B}_0)$

5202 (1)  $\mathcal{T}_0; \cdot \vdash_s w_0; \mathcal{H}_0; \mathcal{B}_0 : s_0$

5203 By  $\vdash_s$  on the redex

5204 (2)  $\mathcal{T}_1 = (p_0 : s_0), \mathcal{T}_0$

5205 (3)  $\mathcal{T}_1; \cdot \vdash_s p_0; (\{p_0 \mapsto w_0\} \cup \mathcal{H}_0); (\{p_0 \mapsto \emptyset\} \cup \mathcal{B}_0) : s_0$

5206 By (1) and (2)

5207 **Case:**  $(unop\{\tau_0\} v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\tau} \text{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$

5208 Impossible for a well-typed redex

5209 **Case:**  $(unop\{\mathcal{U}\} v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\tau} \text{TagErr}; \mathcal{H}_0; \mathcal{B}_0$

5210  $\mathcal{T}_1 = \mathcal{T}_0$

5211 **Case:**  $(unop\{\tau/\mathcal{U}\} p_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\tau} (\text{check}\{\tau/\mathcal{U}\} \delta(unop, \mathcal{H}_0(p_0)) p_0); \mathcal{H}_0; \mathcal{B}_0$

5212 (1)  $\mathcal{T}_1 = \mathcal{T}_0$

5213 (2)  $\mathcal{T}_1; \cdot \vdash_s \delta(unop, \mathcal{H}_0(p_0)); \mathcal{H}_0; \mathcal{B}_0 : s_1$

5214 By a variant of lemma 6.2 for  $\vdash_s$ .

5215 (3)  $\mathcal{T}_1; \cdot \vdash_s (\text{check}\{\tau/\mathcal{U}\} \delta(unop, \mathcal{H}_0(p_0)) p_0); \mathcal{H}_0; \mathcal{B}_0 : \tau/\mathcal{U}$

5216 By (2)

5217 **Case:**  $(binop\{\tau_0\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\tau} \text{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$

5218 Impossible for a well-typed redex

5219 **Case:**  $(binop\{\mathcal{U}\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\tau} \text{TagErr}; \mathcal{H}_0; \mathcal{B}_0$

5220  $\mathcal{T}_1 = \mathcal{T}_0$

5221 **Case:**  $(binop\{\tau/\mathcal{U}\} i_0 i_1); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\tau} \delta(binop, i_0, i_1); \mathcal{H}_0; \mathcal{B}_0$

5222 (1)  $\mathcal{T}_1 = \mathcal{T}_0$

5223 (2)  $\mathcal{T}_1; \cdot \vdash_s \delta(binop, i_0, i_1); \mathcal{H}_0; \mathcal{B}_0 : \tau/\mathcal{U}$

5224 By lemma 6.2 (restated for tags rather than types)

5225 **Case:**  $(app\{\tau_0\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\tau} \text{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$

5226 Impossible for a well-typed redex

5227 **Case:**  $(app\{\mathcal{U}\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\tau} \text{TagErr}; \mathcal{H}_0; \mathcal{B}_0$

5228  $\mathcal{T}_1 = \mathcal{T}_0$

5229 **Case:**  $(app\{\tau/\mathcal{U}\} p_0 v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\tau} (\text{check}\{\tau/\mathcal{U}\} e_0[x_0 \leftarrow v_0] p_0); \mathcal{H}_0; \mathcal{B}_1$

5230 (1)  $\mathcal{T}_1 = \mathcal{T}_0$

5231 (2)  $\mathcal{T}_0; \cdot \vdash_s e_0[x_0 \leftarrow v_0]; \mathcal{H}_0; \mathcal{B}_0 : s_1$

5232 By a substitution lemma for  $\vdash_s$

5233 (3)  $\mathcal{T}_1; \cdot \vdash_s e_0[x_0 \leftarrow v_0]; \mathcal{H}_0; \mathcal{B}_1 : s_1$

5234 By a store extension lemma and (2)

5235 (4)  $\mathcal{T}_1; \cdot \vdash_s (\text{check}\{\tau/\mathcal{U}\} e_0[x_0 \leftarrow v_0] p_0); \mathcal{H}_0; \mathcal{B}_1 : \lfloor \tau/\mathcal{U} \rfloor$

5236 By (3)

5237 **Case:**  $(app\{\tau/\mathcal{U}\} p_0 v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\tau} \text{BoundaryErr}(\text{rev}(\mathcal{B}_0(p_0)), v_0); \mathcal{H}_0; \mathcal{B}_1$

5238  $\mathcal{T}_1 = \mathcal{T}_0$

5239 **Case:**  $(app\{\tau_0\} p_0 v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\tau} (\text{check}\{\tau_0\} e_0[x_0 \leftarrow v_0] p_0); \mathcal{H}_0; \mathcal{B}_1$

5240 (1)  $\mathcal{T}_1 = \mathcal{T}_0$

5241 (2)  $\mathcal{T}_0; \cdot \vdash_s e_0[x_0 \leftarrow v_0]; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$

5242 By a substitution lemma for  $\vdash_s$

5243

5244 (3)  $\mathcal{T}_1; \cdot \vdash_s e_0[x_0 \leftarrow v_0]; \mathcal{H}_0; \mathcal{B}_1 : \mathcal{U}$   
 5245 By a store extension lemma and (2)  
 5246 (4)  $\mathcal{T}_1; \cdot \vdash_s (\text{check}\{\tau_0\} e_0[x_0 \leftarrow v_0] p_0); \mathcal{H}_0; \mathcal{B}_1 : \lfloor \tau/\mathcal{U} \rfloor$   
 5247 By (3)  
 5248 **Case:**  $(\text{app}\{\mathcal{U}\} p_0 v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} (e_0[x_0 \leftarrow v_0]); \mathcal{H}_0; \mathcal{B}_0$   
 5249 (1)  $\mathcal{T}_1 = \mathcal{T}_0$   
 5250 (2)  $\mathcal{T}_1; \cdot \vdash_s e_0[x_0 \leftarrow v_0]; \mathcal{H}_0; \mathcal{B}_0 : \mathcal{U}$   
 5251 By a substitution lemma for  $\vdash_s$   
 5252 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}])$   
 5253 (1)  $\mathcal{T}_1 = \mathcal{T}_0$   
 5254 (2)  $\mathcal{T}_1; \cdot \vdash_s v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}]) : \lfloor \tau_0 \rfloor$   
 5255 By a lemma for *shape-match*( $\lfloor \tau_0 \rfloor, \cdot$ ) and  $\vdash_s$   
 5256 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \text{BoundaryErr}(\{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}, v_0); \mathcal{H}_0; \mathcal{B}_0$   
 5257  $\mathcal{T}_1 = \mathcal{T}_0$   
 5258 **Case:**  $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}])$   
 5259 (1)  $\mathcal{T}_1 = \mathcal{T}_0$   
 5260 (2)  $\mathcal{T}_1; \cdot \vdash_s v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}]) : \lfloor \tau_0 \rfloor$   
 5261 By a lemma for *shape-match*( $\lfloor \tau_0 \rfloor, \cdot$ ) and  $\vdash_s$   
 5262 **Case:**  $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \text{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$   
 5263 Impossible for a well-typed redex  
 5264 **Case:**  $(\text{check}\{\mathcal{U}\} v_0 p_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} v_0; \mathcal{H}_0; \mathcal{B}_0$   
 5265  $\mathcal{T}_1 = \mathcal{T}_0$   
 5266 **Case:**  $(\text{check}\{\tau_0\} v_0 p_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \mathcal{B}_0(p_0)])$   
 5267 (1)  $\mathcal{T}_1 = \mathcal{T}_0$   
 5268 (2)  $\mathcal{T}_1; \cdot \vdash_s v_0; \mathcal{H}_0; (\mathcal{B}_0[v_0 \cup \{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}]) : \lfloor \tau_0 \rfloor$   
 5269 By a lemma for *shape-match*( $\lfloor \tau_0 \rfloor, \cdot$ ) and  $\vdash_s$   
 5270 **Case:**  $(\text{check}\{\tau_0\} v_0 p_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \text{BoundaryErr}(\mathcal{B}_0(v_0) \cup \mathcal{B}_0(p_0), v_0); \mathcal{H}_0; \mathcal{B}_0$   
 5271  $\mathcal{T}_1 = \mathcal{T}_0$

□

5272  
5273  
5274  
5275  
5276  
5277  
5278  
5279  
5280  
5281  
5282  
5283  
5284  
5285  
5286  
5287  
5288  
5289  
5290  
5291  
5292

5293 **A.5 Amnesic**

5294 **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*  
 5295 *holds:*

- 5296
- 5297 •  $e_0 \in \nu \cup \text{Err}$
  - 5298 •  $\tau/\mathcal{U} \in \tau$  and  $\exists e_1. e_0 \triangleright_A e_1$
  - 5299 •  $\tau/\mathcal{U} \in \mathcal{U}$  and  $\exists e_1. e_0 \blacktriangleright_A e_1$

5300

5301 **PROOF.** By unique decomposition (lemma 6.1) and case analysis:

5302

**Case:**  $\cdot \vdash_1 n_0 : \text{Nat}$

Immediate.

5303

**Case:**  $\cdot \vdash_1 i_0 : \text{Int}$

Immediate.

5304

**Case:**  $\cdot \vdash_1 \lambda(x_0 : \tau_0). e_1 : \tau_0 \Rightarrow \tau_1$

Immediate.

5305

**Case:**  $\cdot \vdash_1 \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$

Immediate.

5306

**Case:**  $\cdot \vdash_1 \text{unop}\{\tau_0\} v_0 : \tau_0$

- 5311 -  $\triangleright_A \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_1)$
- 5312 if  $\text{unop} = \text{fst}$  and  $v_0 = \mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_1$
- 5313 -  $\triangleright_A \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{snd}\{\mathcal{U}\} v_1)$
- 5314 if  $\text{unop} = \text{snd}$  and  $v_0 = \mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_1$
- 5315 -  $\triangleright_A \delta(\text{unop}, v_0)$  if defined
- 5316 -  $\triangleright_A \text{Err}$  otherwise

5317

**Case:**  $\cdot \vdash_1 \text{binop}\{\tau_0\} v_0 v_1 : \tau_0$

- 5318 -  $\triangleright_A \delta(\text{binop}, v_0, v_1)$  if defined
- 5319 -  $\triangleright_A \text{Err}$  otherwise

5320

**Case:**  $\cdot \vdash_1 \text{app}\{\tau_0\} v_0 v_1 : \tau_0$

- 5321 -  $\triangleright_A e_1[x_0 \leftarrow v_1]$
- 5322 if  $v_0 = \lambda(\tau_1 : x_0). e_1$
- 5323 -  $\triangleright_A \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_2 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1))$
- 5324 if  $v_0 = \mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_2) \blacktriangleleft \ell_1) v_2$
- 5325 -  $\triangleright_A \text{Err}$  otherwise

5326

**Case:**  $\cdot \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 : \tau_0$

- 5327 -  $\triangleright_A \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$
- 5328 if  $\tau_0 \in \tau \Rightarrow \tau \cup \tau \times \tau$  and  $\text{shape-match}([\tau_0], v_0)$
- 5329 -  $\triangleright_A v_0$
- 5330 if  $v_0 \in \mathbb{T}_? \bar{b}_0 i$  and  $\tau_0 \in \text{Int}$
- 5331 -  $\triangleright_A v_0$
- 5332 if  $v_0 \in \mathbb{T}_? \bar{b}_0 n$  and  $\tau_0 \in \text{Nat}$
- 5333 -  $\triangleright_A \text{Err}$  otherwise

5334

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

Immediate.

5335

**Case:**  $\cdot \vdash_1 \mathbb{G}(\ell_0 \blacktriangleleft (\tau_0 \times \tau_1) \blacktriangleleft \ell_1) v_0 : \tau_0$

Immediate.

5336

**Case:**  $\cdot \vdash_1 \text{Err} : \tau_0$

Immediate.

5337

5338

5339

5340

5341

5342 **Case:**  $\cdot \vdash_1 i : \mathcal{U}$   
 5343 Immediate.

5344 **Case:**  $\cdot \vdash_1 \lambda x_0. e_0 : \mathcal{U}$   
 5345 Immediate.

5346 **Case:**  $\cdot \vdash_1 \langle v_0, v_1 \rangle : \mathcal{U}$   
 5347 Immediate.

5348 **Case:**  $\cdot \vdash_1 \mathit{unop}\{\mathcal{U}\} v_0 : \mathcal{U}$   
 5349 -  $\blacktriangleright_A \text{trace } \bar{b}_0 (\text{stat } (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{fst}\{\tau_1\} v_1))$   
 5350 if  $\mathit{unop} = \text{fst}$  and  $v_0 = \mathbb{T}_? \bar{b}_0 (\mathbb{G} (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_1)$   
 5351 -  $\blacktriangleright_A \text{trace } \bar{b}_0 (\text{stat } (\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{snd}\{\tau_2\} v_1))$   
 5352 if  $\mathit{unop} = \text{snd}$  and  $v_0 = \mathbb{T}_? \bar{b}_0 (\mathbb{G} (\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_1)$   
 5353 -  $\blacktriangleright_A \text{add-trace}(\text{get-trace}(v_0), \delta(\mathit{unop}, \text{rem-trace}(v_0)))$  if defined  
 5354 -  $\blacktriangleright_A \text{Err}$  otherwise

5355 **Case:**  $\cdot \vdash_1 \mathit{binop}\{\mathcal{U}\} v_0 v_1 : \mathcal{U}$   
 5356 -  $\blacktriangleright_A \delta(\mathit{binop}, \text{rem-trace}(v_0), \text{rem-trace}(v_1))$  if defined  
 5357 -  $\blacktriangleright_A \text{Err}$  otherwise

5358 **Case:**  $\cdot \vdash_1 \mathit{app}\{\mathcal{U}\} v_0 v_1 : \mathcal{U}$   
 5359 -  $\blacktriangleright_A \text{trace } \bar{b}_0 (e_1[x_0 \leftarrow (\text{add-trace}(\text{rev}(\bar{b}_0), v_1)])$   
 5360 if  $v_0 = \mathbb{T}_? \bar{b}_0 (\lambda x_0. e_1)$   
 5361 -  $\blacktriangleright_A \text{trace } \bar{b}_0 \text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\mathit{app}\{\tau_0\} v_2 (\text{dyn } (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) \text{add-trace}(\text{rev}(\bar{b}_0), v_1)))$   
 5362 if  $v_0 = \mathbb{T}_? \bar{b}_0 (\mathbb{G} (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1) v_2)$   
 5363 -  $\blacktriangleright_A \text{Err}$  otherwise

5364 **Case:**  $\cdot \vdash_1 \text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 : \mathcal{U}$   
 5365 -  $\blacktriangleright_A \mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
 5366 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  $\text{shape-match}(\lfloor \tau_0 \rfloor, v_0)$   
 5367 -  $\blacktriangleright_A \text{trace } (b_0 b_1 \bar{b}_0) v_1$   
 5368 if  $\tau_0 \in \tau \Rightarrow \tau \cup \tau \times \tau$  and  $v_0 = \mathbb{G} b_1 (\mathbb{T}_? \bar{b}_0 v_1)$  and  $\text{shape-match}(\lfloor \tau_0 \rfloor, v_0)$   
 5369 -  $\blacktriangleright_A v_0$   
 5370 if  $v_0 \in i$  and  $\tau_0 \in \text{Int}$   
 5371 -  $\blacktriangleright_A v_0$   
 5372 if  $v_0 \in n$  and  $\tau_0 \in \text{Nat}$   
 5373 -  $\blacktriangleright_A \text{Err}$  otherwise

5374 **Case:**  $\cdot \vdash_1 \mathbb{G} (\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_0) \blacktriangleleft \ell_1) v_0 : \mathcal{U}$   
 5375 Immediate.

5376 **Case:**  $\cdot \vdash_1 \mathbb{G} (\ell_0 \blacktriangleleft (\tau_1 \times \tau_0) \blacktriangleleft \ell_1) v_0 : \mathcal{U}$   
 5377 Immediate.

5378 **Case:**  $\cdot \vdash_1 \mathbb{T} \bar{b}_0 v_0 : \mathcal{U}$   
 5379 Immediate.

5380 **Case:**  $\cdot \vdash_1 \text{trace } \bar{b}_0 v_0 : \mathcal{U}$   
 5381 -  $\blacktriangleright_A \text{add-trace}(\bar{b}_0, v_0)$

5382 **Case:**  $\cdot \vdash_1 \text{Err} : \mathcal{U}$   
 5383 Immediate.

□

5385  
 5386  
 5387  
 5388  
 5389  
 5390

5391 LEMMA A.27 (AMNESIC TYPE PRESERVATION).  
 5392 If  $\cdot \vdash_1 E_0[e_0] : \tau/\mathcal{U}$  and  $A(E_0[e_0])$  and  $e_0 \triangleright_A \cup \blacktriangleright_A e_1$  then  $\cdot \vdash_1 E_0[e_1] : \tau/\mathcal{U}$  and  $A(E_0[e_1])$ .  
 5393

5394 PROOF. By case analysis of each reduction relation.

5395 **Case:**  $unop\{\tau_0\} v_0 \triangleright_A \text{InvariantErr}$   
 5396 Immediate.

5397 **Case:**  $unop\{\tau_0\} v_0 \triangleright_A \delta(unop, v_0)$   
 5398 By lemma 6.2.

5400 **Case:**  $\text{fst}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_0) \triangleright_A \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_0)$

5401 (1)  $\cdot \vdash_1 v_0 : \mathcal{U}$

5402 By  $\vdash_1$  on the redex

5403 (2)  $\cdot \vdash_1 \text{fst}\{\mathcal{U}\} v_0 : \mathcal{U}$

5404 By (1)

5405 (3)  $\cdot \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_0) : \tau_0$

5406 By (2)

5407 (4)  $A(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_0))$

5408 By similar reasoning

5409 **Case:**  $\text{snd}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_0) \triangleright_A \text{dyn}(\ell_0 \blacktriangleleft (\tau_0 \times \tau_2) \blacktriangleleft \ell_1) (\text{snd}\{\mathcal{U}\} v_0)$

5410 (1)  $\cdot \vdash_1 v_0 : \mathcal{U}$

5411 By  $\vdash_1$  on the redex

5412 (2)  $\cdot \vdash_1 \text{snd}\{\mathcal{U}\} v_0 : \mathcal{U}$

5413 By (1)

5414 (3)  $\cdot \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{snd}\{\mathcal{U}\} v_0) : \tau_0$

5415 By (2)

5416 **Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_A \text{InvariantErr}$

5417 Immediate.

5418 **Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_A \delta(\text{binop}, v_0, v_1)$

5419 Immediate.

5420 **Case:**  $\text{app}\{\tau_0\} v_0 v_1 \triangleright_A \text{InvariantErr}$

5421 Immediate.

5422 **Case:**  $\text{app}\{\tau_0\} (\lambda(x_0 : \tau_1). e_0) v_0 \triangleright_A e_0[x_0 \leftarrow v_0]$

5423 By substitution lemmas for typed functions and for  $A(\cdot)$ .

5424 **Case:**  $\text{app}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_2) \blacktriangleleft \ell_1) v_0) v_1 \triangleright_A \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1))$

5425 (1)  $\cdot \vdash_1 v_0 : \mathcal{U}$

5426 By  $\vdash_1$  on the redex

5427 (2)  $\cdot \vdash_1 v_1 : \tau_1$

5428 By  $\vdash_1$  on the redex

5429 (3)  $\cdot \vdash_1 \text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1 : \mathcal{U}$

5430 By (2)

5431 (4)  $\cdot \vdash_1 \text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1) : \mathcal{U}$

5432 By (1) and (3)

5433 (5)  $\cdot \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1)) : \tau_0$

5434 By (4)

5435 (6)  $A(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1)))$

5436 By similar reasoning

5437 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_A \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$

5438 Immediate.

5439

5440 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\mathbb{T} \bar{b}_0 i_0) \triangleright_{\mathbb{A}} i_0$   
 5441 Immediate.

5442 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_{\mathbb{A}} \text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \bar{b}_0, v_0)$   
 5443 Immediate.

5444 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \triangleright_{\mathbb{A}} \text{TagErr}$   
 5445 Immediate.

5446 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \triangleright_{\mathbb{A}} \text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, v_1))$   
 5447 Immediate.

5448 **Case:**  $\text{fst}\{\mathcal{U}\} (\mathbb{T} \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_0)) \triangleright_{\mathbb{A}} \text{trace} \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{fst}\{\tau_1\} v_0))$   
 5449 (1)  $\cdot \vdash_1 v_0 : \tau_1 \times \tau_2$   
 5450 By  $\vdash_1$  on the redex  
 5451 (2)  $\cdot \vdash_1 \text{fst}\{\tau_1\} v_0 : \tau_1$   
 5452 By (1)  
 5453 (3)  $\cdot \vdash_1 \text{trace} \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (\text{fst}\{\tau_1\} v_0)) : \mathcal{U}$   
 5454 By (2)

5455 **Case:**  $\text{snd}\{\mathcal{U}\} (\mathbb{T} \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \times \tau_2) \blacktriangleleft \ell_1) v_0)) \triangleright_{\mathbb{A}} \text{trace} \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{snd}\{\tau_2\} v_0))$   
 5456 (1)  $\cdot \vdash_1 v_0 : \tau_1 \times \tau_2$   
 5457 By  $\vdash_1$  on the redex  
 5458 (2)  $\cdot \vdash_1 \text{snd}\{\tau_2\} v_0 : \tau_2$   
 5459 By (1)  
 5460 (3)  $\cdot \vdash_1 \text{stat}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{snd}\{\tau_2\} v_0) : \mathcal{U}$   
 5461 By (2)

5462 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \triangleright_{\mathbb{A}} \text{TagErr}$   
 5463 Immediate.

5464 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \triangleright_{\mathbb{A}} \delta(\text{binop}, v_2, v_3)$   
 5465 Immediate.

5466 **Case:**  $\text{app}\{\mathcal{U}\} v_0 v_1 \triangleright_{\mathbb{A}} \text{TagErr}$   
 5467 Immediate.

5468 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{T} \bar{b}_0 (\lambda x_0. e_0)) v_0 \triangleright_{\mathbb{A}} \text{trace} \bar{b}_0 (e_0[x_0 \leftarrow v_1])$   
 5469 By substitution lemmas for untyped functions and for  $A(\cdot)$ .

5470 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{T} \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft (\tau_1 \Rightarrow \tau_2) \blacktriangleleft \ell_1) v_0)) v_1 \triangleright_{\mathbb{A}}$   
 5471  $\text{trace} \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\tau_2\} v_0 (\text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_2)))$   
 5472 (1)  $\cdot \vdash_1 v_0 : \tau_1 \Rightarrow \tau_2$   
 5473 By  $\vdash_1$  on the redex  
 5474 (2)  $\cdot \vdash_1 v_1 : \mathcal{U}$   
 5475 By  $\vdash_1$  on the redex  
 5476 (3)  $\cdot \vdash_1 \text{dyn}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1 : \tau_1 \Rightarrow \tau_2$   
 5477 By (2)  
 5478 (4)  $\cdot \vdash_1 \text{app}\{\tau_2\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_1) : \tau_2$   
 5479 By (1) and (3)  
 5480 (5)  $\cdot \vdash_1 \text{trace} \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) (\text{app}\{\tau_2\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0) v_2))) : \mathcal{U}$   
 5481 By (4)

5482 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_{\mathbb{A}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
 5483 Immediate.

5484 **Case:**  $\text{stat} b_0 (\mathbb{G} b_1 (\mathbb{T} \bar{b}_0 v_0)) \triangleright_{\mathbb{A}} \text{trace}(b_0 b_1 \bar{b}_0) v_0$   
 5485 (1)  $\cdot \vdash_1 v_0 : \mathcal{U}$   
 5486 By  $\vdash_1$  on the redex  
 5487  
 5488



5489  $(2) \cdot \vdash_1 \text{trace}(b_0 b_1 \bar{b}_0) v_0 : \mathcal{U}$

5490 By (1)

5491 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0 \blacktriangleright_{\Lambda} i_0$

5492 Immediate.

5493 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\Lambda} \text{InvariantErr}$

5494 Immediate.

5495 **Case:**  $\text{trace} \bar{b}_0 v_0 \blacktriangleright_{\Lambda} v_1$

5496 Immediate.

5497

□

5498

5499

5500

5501

5502

5503

5504

5505

5506

5507

5508

5509

5510

5511

5512

5513

5514

5515

5516

5517

5518

5519

5520

5521

5522

5523

5524

5525

5526

5527

5528

5529

5530

5531

5532

5533

5534

5535

5536

5537

THEOREM A.28 (AMNESIC BLAME SOUNDNESS AND COMPLETENESS). *Amnesic satisfies BS and BC*

PROOF. By preservation of path-owner consistency ( $\Vdash_p$ ) for  $\triangleright_{\bar{A}}$  and  $\blacktriangleright_{\bar{A}}$ .

**Case:**  $(unop\{\tau_0\} \langle (v_0) \rangle^{\bar{\ell}_0})^{\ell_0} \triangleright_{\bar{A}} (\text{InvariantErr})^{\ell_0}$

Immediate.

**Case:**  $(unop\{\tau_0\} \langle (v_0) \rangle^{\bar{\ell}_0})^{\ell_0} \triangleright_{\bar{A}} (\delta(unop, v_0))^{\bar{\ell}_0 \ell_0}$

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

By definition

(2)  $\ell_0; \cdot \Vdash_p v_0$

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)  $\ell_0; \cdot \Vdash_p \delta(unop, v_0)$

By (1) and (3)

**Case:**  $(fst\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3} \triangleright_{\bar{A}} (\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (fst\{\mathcal{U}\} (v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$

(1)  $\ell_1; \cdot \Vdash_p (v_0)^{\ell_2}$

By  $\Vdash_p$  on the redex

(2)  $\ell_1; \cdot \Vdash_p fst\{\mathcal{U}\} (v_0)^{\ell_2}$

By (1)

(3)  $\ell_3; \cdot \Vdash_p (\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (fst\{\mathcal{U}\} (v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$

By (1) and  $\Vdash_p$  on the redex

**Case:**  $(snd\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3} \triangleright_{\bar{A}} (\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (snd\{\mathcal{U}\} (v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$

(1)  $\ell_1; \cdot \Vdash_p (v_0)^{\ell_2}$

By  $\Vdash_p$  on the redex

(2)  $\ell_1; \cdot \Vdash_p snd\{\mathcal{U}\} (v_0)^{\ell_2}$

By (1)

(3)  $\ell_3; \cdot \Vdash_p (\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (snd\{\mathcal{U}\} (v_0)^{\ell_2}))^{\bar{\ell}_0 \ell_3}$

By (1) and  $\Vdash_p$  on the redex

**Case:**  $(binop\{\tau_0\} \langle (v_0) \rangle^{\bar{\ell}_0} \langle (v_1) \rangle^{\bar{\ell}_1})^{\ell_0} \triangleright_{\bar{A}} (\text{InvariantErr})^{\ell_0}$

Immediate.

**Case:**  $(binop\{\tau_0\} \langle (v_0) \rangle^{\bar{\ell}_0} \langle (v_1) \rangle^{\bar{\ell}_1})^{\ell_0} \triangleright_{\bar{A}} (\delta(binop, v_0, v_1))^{\ell_0}$

(1)  $\delta(binop, v_0, v_1) \in i$

By definition of  $\delta$

(2)  $\ell_0; \cdot \Vdash_p \delta(binop, v_0, v_1)$

By (1)

**Case:**  $(app\{\tau_0\} \langle (v_0) \rangle^{\bar{\ell}_0} v_1)^{\ell_0} \triangleright_{\bar{A}} (\text{InvariantErr})^{\ell_0}$

Immediate.

**Case:**  $(app\{\tau_0\} (\lambda(x_0 : \tau_1). e_0))^{\bar{\ell}_0} v_0)^{\ell_0} \triangleright_{\bar{A}} (e_0[x_0 \leftarrow \langle (v_0) \rangle^{\ell_0 rev(\bar{\ell}_0)}])^{\bar{\ell}_0 \ell_0}$

(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

- 5587 (3)  $\ell_0; \cdot \Vdash_P ((v_0))^{\ell_0 \text{rev}(\bar{\ell}_0)}$   
 5588 By (1) and (2)
- 5589 (4)  $\ell_0; \cdot \Vdash_P x_0$  for each occurrence of  $x_0$  in  $e_0$   
 5590 By  $\Vdash_P$  on the redex
- 5591 (5)  $\ell_0; \cdot \Vdash_P ((e_0[x_0 \leftarrow ((v_1))^{\ell_0 \text{rev}(\bar{\ell}_0)}]))^{\bar{\ell}_0 \ell_0}$   
 5592 By (3) and (4)
- 5593 **Case:**  $(\text{app}\{\tau_0\} ((\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) (v_0))^{\ell_2})^{\bar{\ell}_0} v_1)^{\ell_3} \triangleright_{\bar{A}}$   
 5594  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)}))^{\ell_2})^{\bar{\ell}_0 \ell_3}$   
 5595  
 5596 (1)  $\ell_2; \cdot \Vdash_P v_0$   
 5597 By  $\Vdash_P$  on the redex
- 5598 (2)  $\ell_3; \cdot \Vdash_P v_1$   
 5600 By  $\Vdash_P$  on the redex
- 5601 (3)  $\ell_3; \cdot \Vdash_P ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)}$   
 5602 By (2) and  $\Vdash_P$  on the redex
- 5603 (4)  $\ell_2; \cdot \Vdash_P \text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)}$   
 5604 By (3) and  $\Vdash_P$  on the redex
- 5605 (5)  $\ell_3; \cdot \Vdash_P ((\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) ((v_1))^{\ell_3 \text{rev}(\bar{\ell}_0)}))^{\ell_2})^{\bar{\ell}_0 \ell_3})$   
 5606 By (1) and (4)
- 5607 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2} \triangleright_{\bar{A}} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_0})^{\ell_2}$   
 5608 Immediate.
- 5609 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((\mathbb{T}; \bar{b}_0((i_0))^{\bar{\ell}_0})^{\bar{\ell}_1})^{\ell_2}) \triangleright_{\bar{A}} (i_0)^{\ell_2}$   
 5610 Immediate.
- 5611 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\ell}_2})^{\ell_3} \triangleright_{\bar{A}} (\text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \bar{b}_0, ((v_0))^{\bar{\ell}_2}))^{\ell_3}$   
 5612 Immediate.
- 5613 **Case:**  $(\text{unop}\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0})^{\ell_0} \blacktriangleright_{\bar{A}} (\text{TagErr})^{\ell_0}$   
 5614 Immediate.
- 5615 **Case:**  $(\text{unop}\{\mathcal{U}\} v_0)^{\ell_0} \blacktriangleright_{\bar{A}} (\text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, v_1)))^{\ell_0}$   
 5616 (1)  $v_0 = \mathbb{T}; \bar{b}_0 \langle v_1, v_2 \rangle$  and  $\delta(\text{unop}, \text{rem-trace}(v_0)) \in \{v_1, v_2\}$   
 5617 By definition
- 5618 (2)  $\ell_0; \cdot \Vdash_P v_0$  and  $\ell_n; \cdot \Vdash_P \text{rem-trace}(v_0)$   
 5619 By  $\Vdash_P$  on the redex
- 5620 (3)  $\ell_n; \cdot \Vdash_P v_1$  and  $\ell_n; \cdot \Vdash_P v_2$   
 5621 By (2)
- 5622 (4)  $\ell_0; \cdot \Vdash_P \text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, \text{rem-trace}(v_0)))$   
 5623 By (1) and (3)
- 5624 **Case:**  $(\text{fst}\{\mathcal{U}\} ((\mathbb{T}; \bar{b}_0((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0))^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4})^{\ell_5} \blacktriangleright_{\bar{A}}$   
 5625  $(\text{trace} \bar{b}_0 ((\text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_0)^{\ell_2})^{\bar{\ell}_3})^{\bar{\ell}_4})^{\ell_5}$   
 5626 (1)  $\ell_5; \cdot \Vdash_P \mathbb{T}; \bar{b}_0((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0))^{\ell_2})^{\bar{\ell}_3}$   
 5627 By  $\Vdash_P$  on the redex
- 5628  
 5629  
 5630  
 5631  
 5632  
 5633  
 5634  
 5635

- 5636 (2)  $\ell_0; \cdot \Vdash_p \mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0)^{\ell_2}$   
 5637 By (1)
- 5638 (3)  $\ell_1; \cdot \Vdash_p v_0$   
 5639 By (2)
- 5640 (4)  $\ell_1; \cdot \Vdash_p \text{fst}\{\text{fst}(\tau_0)\} v_0$   
 5641 By (3)
- 5642 (5)  $\ell_0; \cdot \Vdash_p \text{stat} (\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_0)^{\ell_2}$   
 5643 By (4)
- 5644 (6)  $\ell_5; \cdot \Vdash_p \text{trace } \bar{b}_0 ((\text{stat} (\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_0)^{\ell_2}))^{\bar{\ell}_3}$   
 5645 By (1) and (5)
- 5646
- 5647 **Case:**  $(\text{snd}\{\mathcal{U}\} ((\mathbb{T}_? \bar{b}_0 ((\mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0)^{\ell_2}))^{\bar{\ell}_3}))^{\bar{\ell}_4} \ell_5) \blacktriangleright_{\bar{A}}$   
 5648  $(\text{trace } \bar{b}_0 ((\text{stat} (\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_0)^{\ell_2}))^{\bar{\ell}_3})^{\bar{\ell}_4} \ell_5)$   
 5649
- 5650 (1)  $\ell_5; \cdot \Vdash_p \mathbb{T}_? \bar{b}_0 ((\mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0)^{\ell_2}))^{\bar{\ell}_3}$   
 5651 By  $\Vdash_p$  on the redex
- 5652 (2)  $\ell_0; \cdot \Vdash_p \mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0)^{\ell_2}$   
 5653 By (1)
- 5654 (3)  $\ell_1; \cdot \Vdash_p v_0$   
 5655 By (2)
- 5656 (4)  $\ell_1; \cdot \Vdash_p \text{snd}\{\text{snd}(\tau_0)\} v_0$   
 5657 By (3)
- 5658 (5)  $\ell_0; \cdot \Vdash_p \text{stat} (\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_0)^{\ell_2}$   
 5659 By (4)
- 5660 (6)  $\ell_5; \cdot \Vdash_p \text{trace } \bar{b}_0 ((\text{stat} (\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_0)^{\ell_2}))^{\bar{\ell}_3}$   
 5661 By (1) and (5)
- 5662
- 5663 **Case:**  $(\text{binop}\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0} ((v_1))^{\bar{\ell}_1} \ell_0) \blacktriangleright_{\bar{A}} (\text{TagErr})^{\ell_0}$   
 5664 Immediate.
- 5665 **Case:**  $(\text{binop}\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0} ((v_1))^{\bar{\ell}_1} \ell_0) \blacktriangleright_{\bar{A}} \delta(\text{binop}, v_2, v_3)$   
 5666 Immediate.
- 5667 **Case:**  $(\text{app}\{\mathcal{U}\} ((v_0))^{\bar{\ell}_0} v_1) \blacktriangleright_{\bar{A}} (\text{TagErr})^{\ell_0}$   
 5668 Immediate.
- 5669
- 5670 **Case:**  $(\text{app}\{\mathcal{U}\} ((\mathbb{T}_? \bar{b}_0 ((\lambda x_0. e_0))^{\bar{\ell}_0}))^{\bar{\ell}_1} v_0) \blacktriangleright_{\bar{A}}$   
 5671  $(\text{trace } \bar{b}_0 ((e_0[x_0 \leftarrow \text{add-trace}(\text{rev}(\bar{b}_0), ((v_0))^{\ell_2 \text{rev}(\bar{\ell}_1) \text{rev}(\bar{\ell}_0)})]))^{\bar{\ell}_0} \bar{\ell}_1 \ell_2)$   
 5672
- 5673 (1)  $\ell_2; \cdot \Vdash_p \mathbb{T}_? \bar{b}_0 ((\lambda x_0. e_0))^{\bar{\ell}_0}$   
 5674 By  $\Vdash_p$  on the redex
- 5675 (2)  $\ell_n; \cdot \Vdash_p \lambda x_0. e_0$   
 5676 By (1)
- 5677 (3)  $\ell_2; \cdot \Vdash_p v_0$   
 5678 By  $\Vdash_p$  on the redex
- 5679 (4)  $\ell_2; \cdot \Vdash_p v_0$   
 5680 By  $\Vdash_p$  on the redex
- 5681 (5)  $\ell_n; \cdot \Vdash_p \text{add-trace}(\text{rev}(\bar{b}_0), ((v_0))^{\ell_2 \text{rev}(\bar{\ell}_1) \text{rev}(\bar{\ell}_0)})$   
 5682 By (2) and (4)
- 5683
- 5684

5685 (6)  $\ell_n; \cdot \Vdash_p x_0$  for each occurrence of  $x_0$  in  $e_0$   
 5686 By  $\Vdash_p$  on the redex

5687 (7)  $\ell_2; \cdot \Vdash_p \text{trace } \bar{b}_0 ((e_0[x_0 \leftarrow \text{add-trace}(\text{rev}(\bar{b}_0), ((v_0))^{\ell_2 \text{rev}(\bar{\tau}_1) \text{rev}(\bar{\tau}_0)})]))^{\bar{\tau}_0}$   
 5688 By (5) and (6)

5689 **Case:**  $(\text{app}\{\mathcal{U}\} ((\mathbb{T}_? \bar{b}_0 ((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0))^{\ell_2})^{\bar{\tau}_3})^{\bar{\tau}_4} v_1))^{\ell_5} \blacktriangleright_{\bar{A}}$

5692  $((\text{trace } \bar{b}_0 ((\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_2))^{\ell_2})^{\bar{\tau}_3})^{\bar{\tau}_4} \ell_5$   
 5693 where  $v_2 = \text{add-trace}(\text{rev}(\bar{b}_0), ((v_1))^{\ell_5 \text{rev}(\bar{\tau}_3 \bar{\tau}_4)})$

5694 (1)  $\ell_5; \cdot \Vdash_p \mathbb{T}_? \bar{b}_0 ((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0))^{\ell_2})^{\bar{\tau}_3}$   
 5695 By  $\Vdash_p$  on the redex

5696 (2)  $\ell_0; \cdot \Vdash_p \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (v_0)^{\ell_2}$  and  $\ell_1; \cdot \Vdash_p v_0$   
 5697 By (1)

5698 (3)  $\ell_5; \cdot \Vdash_p v_1$   
 5699 By  $\Vdash_p$  on the redex

5700 (4)  $\ell_0; \cdot \Vdash_p \text{add-trace}(\text{rev}(\bar{b}_0), ((v_1))^{\ell_5 \text{rev}(\bar{\tau}_3 \bar{\tau}_4)})$   
 5701 By (1) and (3)

5702 (5)  $\ell_1; \cdot \Vdash_p \text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) \text{add-trace}(\text{rev}(\bar{b}_0), ((v_1))^{\ell_5 \text{rev}(\bar{\tau}_3 \bar{\tau}_4)})$   
 5703 By (4)

5704 (6)  $\ell_5; \cdot \Vdash_p \text{trace } \bar{b}_0 ((\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 v_2))^{\ell_2})^{\bar{\tau}_3}$   
 5705 where  $v_2 = \text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) \text{add-trace}(\text{rev}(\bar{b}_0), ((v_1))^{\ell_5 \text{rev}(\bar{\tau}_3 \bar{\tau}_4)})$   
 5706 By (1) and (5)

5707 **Case:**  $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)^{\ell_2} \blacktriangleright_{\bar{A}} ((\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0))^{\ell_2}$   
 5708 Immediate.

5709 **Case:**  $(\text{stat } b_0 ((\mathbb{G} b_1 ((\mathbb{T}_? \bar{b}_2 v_0))^{\bar{\tau}_0})^{\bar{\tau}_1} \ell_2))^{\bar{\tau}_0} \blacktriangleright_{\bar{A}} (\text{trace}(b_0 b_1 \bar{b}_2) ((v_0))^{\bar{\tau}_0 \bar{\tau}_1 \ell_2})^{\ell_2}$

5710 (1)  $b_0 = (\ell_2 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$  and  $b_1 = (\ell_1 \blacktriangleleft \tau_1 \blacktriangleleft \ell_0)$   
 5711 By  $\Vdash_p$  on the redex

5712 (2)  $\ell_1; \cdot \Vdash_p ((\mathbb{G} b_1 ((\mathbb{T}_? \bar{b}_2 v_0))^{\bar{\tau}_0})^{\bar{\tau}_1})$   
 5713 By  $\Vdash_p$  on the redex and (1)

5714 (3)  $\ell_0; \cdot \Vdash_p ((\mathbb{T}_? \bar{b}_2 v_0))^{\bar{\tau}_0}$   
 5715 By  $\Vdash_p$  on the redex and (1)

5716 (4)  $\ell_2; \cdot \Vdash_p \text{trace}(b_0 b_1 \bar{b}_2) ((v_0))^{\bar{\tau}_0 \bar{\tau}_1 \ell_2}$   
 5717 By (2) and (3)

5718 **Case:**  $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((i_0))^{\bar{\tau}_2})^{\ell_3} \blacktriangleright_{\bar{A}} (i_0)^{\ell_3}$   
 5719 Immediate.

5720 **Case:**  $(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) ((v_0))^{\bar{\tau}_2})^{\ell_3} \blacktriangleright_{\bar{A}} (\text{InvariantErr})^{\ell_3}$   
 5721 Immediate.

5722 **Case:**  $(\text{trace } \bar{b}_0 v_0)^{\ell_0} \blacktriangleright_{\bar{A}} (\text{add-trace}(\bar{b}_0, v_0))^{\ell_0}$   
 5723 Immediate.

5724

5725

5726

5727

5728

5729

5730

5731

5732

5733

□

5734 LEMMA A.29 ( $A \approx T$ ). If  $e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0$  then:

- 5735 • if  $e_0 \rightarrow_A e_2$  then  $e_2 \rightarrow_A^* e_3$  and  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* e_4; \mathcal{H}_1; \mathcal{B}_1$  and  $e_3 \approx e_4; \mathcal{H}_1; \mathcal{B}_1$   
 5736 • if  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T e_3; \mathcal{H}_1; \mathcal{B}_1$  then  $e_0 \rightarrow_A^* e_2$  and  $e_2 \approx e_3; \mathcal{H}_1; \mathcal{B}_1$   
 5737

5738 PROOF. By lemma A.30 and lemma A.31.

5739

5740

5741  $\boxed{\text{wfr}_{AT}(e_0, e_1)}$  holds for well-formed residuals of a common term; that is, pairs such that there  
 5742 exists an  $e_2$  where  $e_2 : \tau/\mathcal{U}$  wf and  $e_2 \rightarrow_A^* e_0$  and  $e_2; \cdot \rightarrow_T^* e_1; \mathcal{H}_1; \mathcal{B}_1$   
 5743

5744 LEMMA A.30. If  $\text{wfr}_{AT}(e_0, e_1)$  and  $e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0$  and  $e_0 \rightarrow_A e_2$  then  $e_2 \rightarrow_A^* e_3$  and  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^*$   
 5745  $e_4; \mathcal{H}_1; \mathcal{B}_1$  and  $e_3 \approx e_4; \mathcal{H}_1; \mathcal{B}_1$   
 5746

5747

PROOF. By lemma A.32, lemma A.35, and case analysis of  $\triangleright_A \cup \blacktriangleright_A$ .

5748 **Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_A \text{InvariantErr}$

5749 Impossible, by type soundness

5750 **Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_A \delta(\text{unop}, v_0)$

5751 (1)  $e_1 = \text{unop}\{\tau_0\} e_5$  and  $v_0 \lesssim e_5$

5752 By  $\lesssim$  on the redex

5753 (2) If  $e_5$  is a pre-value, it gets allocated. If not,  $e_5$  must be a value. Either way  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^*$   
 5754  $\text{unop}\{\tau_0\} v_1; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \lesssim v_1$

5755 (3)  $\delta(\text{unop}, v_1)$  is defined  
 5756 By (2)

5757 (4)  $\delta(\text{unop}, v_0) \approx \delta(\text{unop}, v_1); \mathcal{H}_1; \mathcal{B}_1$   
 5758 By  $\delta$

5759 **Case:**  $\text{fst}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \triangleright_A \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{fst}\{\mathcal{U}\} v_0)$

5760 (1)  $e_1 = \text{fst}\{\tau_0\} e_5$  and  $v_0 \lesssim e_5$

5761 By  $\lesssim$  on the redex

5762 (2) If  $e_5$  is a pre-value, it gets allocated. If not,  $e_5$  must be a value. Either way  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^*$   
 5763  $\text{fst}\{\tau_0\} v_1; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \lesssim v_1$

5764 (3)  $\text{fst}\{\tau_0\} v_1; \mathcal{H}_1; \mathcal{B}_1 \rightarrow_T^* \text{check}\{\tau_0\} \delta(\text{fst}, v_1) v_1; \mathcal{H}_1; \mathcal{B}_1$   
 5765 By  $\rightarrow_T^*$

5766 (4) If  $v_0 = \langle v_2, v_3 \rangle$  then  $e_0 \rightarrow_A^* \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_2$   
 5767 and  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_2 \approx \text{check}\{\tau_0\} \delta(\text{fst}, v_1) v_1; \mathcal{H}_1; \mathcal{B}_1$   
 5768 By (3)

5769 (5) Otherwise  $v_0 = \mathbb{G} b_1 \langle v_2, v_3 \rangle$  and  $e_0 \rightarrow_A^* \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{stat } b_1 v_2)$   
 5770 and  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{stat } b_1 v_2) \approx \text{check}\{\tau_0\} \delta(\text{fst}, v_1) v_1; \mathcal{H}_1; \mathcal{B}_1$

5771 **Case:**  $\text{snd}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \triangleright_A \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{snd}\{\mathcal{U}\} v_0)$   
 5772

5773 (1)  $e_1 = \text{snd}\{\tau_0\} e_5$  and  $v_0 \lesssim e_5$

5774 By  $\lesssim$  on the redex

5775 (2) If  $e_5$  is a pre-value, it gets allocated. If not,  $e_5$  must be a value. Either way  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^*$   
 5776  $\text{snd}\{\tau_0\} v_1; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \lesssim v_1$

5777 (3)  $\text{snd}\{\tau_0\} v_1; \mathcal{H}_1; \mathcal{B}_1 \rightarrow_T^* \text{check}\{\tau_0\} \delta(\text{snd}, v_1) v_1; \mathcal{H}_1; \mathcal{B}_1$   
 5778 By  $\rightarrow_T^*$

5779 (4) If  $v_0 = \langle v_2, v_3 \rangle$  then  $e_0 \rightarrow_A^* \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_2$   
 5780 and  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_2 \approx \text{check}\{\tau_0\} \delta(\text{snd}, v_1) v_1; \mathcal{H}_1; \mathcal{B}_1$   
 5781 By (3)

5782

- 5783 (5) Otherwise  $v_0 = \mathbb{G} b_1 \langle v_2, v_3 \rangle$  and  $e_0 \rightarrow_A^* \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$  (stat  $b_1 v_2$ )  
 5784 and  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)$  (stat  $b_1 v_2$ )  $\approx \text{check}\{\tau_0\} \delta(\text{snd}, v_1) v_1; \mathcal{H}_1; \mathcal{B}_1$   
 5785 **Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_A \text{InvariantErr}$   
 5786 Impossible, by type soundness  
 5787 **Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_A \delta(\text{binop}, v_0, v_1)$   
 5788 (1)  $e_1 = \text{binop}\{\tau_0\} e_5 e_6$  and  $v_0 \lesssim e_5$  and  $v_1 \lesssim e_6$   
 5789 By  $\lesssim$  on the redex  
 5790 (2) If  $e_5$  a pre-value, it gets allocated. If not,  $e_5$  must be a value. Similarly for  $e_6$ . Either way  
 5791  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* \text{binop}\{\tau_0\} v_2 v_3; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$   
 5792 (3)  $\delta(\text{binop}, v_2, v_3)$  is defined  
 5793 By (2)  
 5794 (4)  $\delta(\text{binop}, v_0, v_1) \approx \delta(\text{binop}, v_2, v_3); \mathcal{H}_1; \mathcal{B}_1$   
 5795 By  $\delta$   
 5796 **Case:**  $\text{app}\{\tau_0\} v_0 v_1 \triangleright_A \text{InvariantErr}$   
 5797 Impossible, by type soundness  
 5798 **Case:**  $\text{app}\{\tau_0\} (\lambda(x_0 : \tau_1). e_0) v_0 \triangleright_A \text{check}\{\tau_0\} e_0[x_0 \leftarrow v_0] \bullet$   
 5799 (1)  $e_1 = \text{app}\{\tau_0\} e_5 e_6$  and  $(\lambda(x_0 : \tau_1). e_4) \lesssim e_5$  and  $v_0 \lesssim e_6$   
 5800 By  $\lesssim$  on the redex  
 5801 (2) If  $e_5$  a pre-value, it gets allocated. If not,  $e_5$  must be a value. Similarly for  $e_6$ . Either way  
 5802  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* \text{app}\{\tau_0\} v_2 v_3; \mathcal{H}_1; \mathcal{B}_1$  and  $(\lambda(x_0 : \tau_1). e_4) \lesssim v_2$  and  $v_0 \lesssim v_3$   
 5803 (3)  $e_1; \mathcal{H}_1; \mathcal{B}_1 \rightarrow_T^* \text{check}\{\tau_0\} e_7[x_0 \leftarrow 3] v_2; \mathcal{H}_2; \mathcal{B}_2$   
 5804 By (2)  
 5805 (4)  $\text{check}\{\tau_0\} e_0[x_0 \leftarrow v_0] \bullet \approx \text{check}\{\tau_0\} e_7[x_0 \leftarrow 3] v_2; \mathcal{H}_2; \mathcal{B}_2$   
 5806 By (3) and a substitution lemma  
 5807 **Case:**  $\text{app}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) v_1 \triangleright_A$   
 5808  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_1))$   
 5809 (1)  $e_1 = \text{app}\{\tau_0\} e_5 e_6$  and  $(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \lesssim e_5$  and  $v_1 \lesssim e_6$   
 5810 By  $\lesssim$  on the redex  
 5811 (2) If  $e_5$  a pre-value, it gets allocated. If not,  $e_5$  must be a value. Similarly for  $e_6$ . Either way  
 5812  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* \text{app}\{\tau_0\} v_2 v_3; \mathcal{H}_1; \mathcal{B}_1$  and  $(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \lesssim v_2$  and  $v_1 \lesssim v_3$   
 5813 (3)  $\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_1 \rightarrow_A^* v_4$   
 5814 By  $v_1 \lesssim v_3$   
 5815 (4)  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 v_4) \approx \text{app}\{\tau_0\} v_2 v_3; \mathcal{H}_1; \mathcal{B}_1$   
 5816 By (3)  
 5817 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_A \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
 5818 (1) If  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1; \mathcal{H}_1; \mathcal{B}_1$  then  $v_0 \lesssim v_1$  and  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* v_1; \mathcal{H}_2; \mathcal{B}_2$  and  
 5819  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \lesssim v_1; \mathcal{H}_2; \mathcal{B}_2$   
 5820 (2) Otherwise  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* \text{check}\{\tau_0\} v_1 p_0; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \approx v_1; \mathcal{H}_1; \mathcal{B}_1$   
 5821 (3)  $\text{check}\{\tau_0\} v_1 p_0; \mathcal{H}_1; \mathcal{B}_1 \rightarrow_T^* v_1; \mathcal{H}_2; \mathcal{B}_2$   
 5822 By (2)  
 5823 (4)  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \approx v_1; \mathcal{H}_2; \mathcal{B}_2$   
 5824 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\mathbb{T} \bar{b}_0 i_0) \triangleright_A i_0$   
 5825 (1) If  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1; \mathcal{H}_1; \mathcal{B}_1$  then  $i_0 \lesssim v_1$  and  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* v_1; \mathcal{H}_2; \mathcal{B}_2$  and  
 5826  $i_0 \lesssim v_1; \mathcal{H}_2; \mathcal{B}_2$   
 5827 (2) Otherwise  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* \text{check}\{\tau_0\} v_1 p_0; \mathcal{H}_1; \mathcal{B}_1$  and  $i_0 \approx v_1; \mathcal{H}_1; \mathcal{B}_1$   
 5828  
 5829  
 5830  
 5831

- 5832 (3)  $\text{check}\{\tau_0\} v_1 p_0; \mathcal{H}_1; \mathcal{B}_1 \rightarrow_{\top}^* v_1; \mathcal{H}_2; \mathcal{B}_2$   
 5833 By (2)  
 5834 (4)  $i_0 \approx v_1; \mathcal{H}_2; \mathcal{B}_2$   
 5835 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_{\mathbb{A}} \text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \bar{b}_0, v_0)$   
 5836 (1) If  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^* \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1; \mathcal{H}_1; \mathcal{B}_1$  then  $v_0 \lesssim v_1$   
 5837 and  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^* \text{BoundaryErr}(\bar{b}, v); \mathcal{H}_2; \mathcal{B}_2$   
 5838 and  $\text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \bar{b}_0, v_0) \lesssim \text{BoundaryErr}(\bar{b}, v); \mathcal{H}_2; \mathcal{B}_2$   
 5839 (2) Otherwise  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^* \text{check}\{\tau_0\} v_1 p_0; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \approx v_1; \mathcal{H}_1; \mathcal{B}_1$  and  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^*$   
 5840  $\text{BoundaryErr}(\bar{b}, v); \mathcal{H}_2; \mathcal{B}_2$  and  $\text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \bar{b}_0, v_0) \lesssim \text{BoundaryErr}(\bar{b}, v); \mathcal{H}_2; \mathcal{B}_2$   
 5841 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_{\mathbb{A}} \text{TagErr}$   
 5842 (1)  $e_1 = \text{unop}\{\mathcal{U}\} e_5$  and  $v_0 \lesssim e_5$   
 5843 By  $\lesssim$  on the redex  
 5844 (2) If  $e_5$  is a pre-value, it gets allocated. If not,  $e_5$  must be a value. Either way  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^*$   
 5845  $\text{unop}\{\mathcal{U}\} v_1; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \lesssim v_1$   
 5846 (3)  $\delta(\text{unop}, v_1)$  is undefined  
 5847 By  $v_0 \lesssim v_1$   
 5848 (4)  $\text{TagErr} \approx \text{TagErr}; \mathcal{H}_1; \mathcal{B}_1$   
 5849 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_{\mathbb{A}} \text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, v_1))$   
 5850 (1)  $e_1 = \text{unop}\{\mathcal{U}\} e_5$  and  $v_0 \lesssim e_5$   
 5851 By  $\lesssim$  on the redex  
 5852 (2) If  $e_5$  is a pre-value, it gets allocated. If not,  $e_5$  must be a value. Either way  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^*$   
 5853  $\text{unop}\{\mathcal{U}\} v_1; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \lesssim v_1$   
 5854 (3)  $\delta(\text{unop}, v_1)$  is undefined  
 5855 By  $v_0 \lesssim v_1$   
 5856 (4)  $\text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, \text{rem-trace}(v_0))) \approx \delta(\text{unop}, v_1); \mathcal{H}_1; \mathcal{B}_1$   
 5857 **Case:**  $\text{fst}\{\mathcal{U}\} (\mathbb{T}?, \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) \blacktriangleright_{\mathbb{A}} \text{trace } \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) (\text{fst}\{\tau_1\} v_0))$   
 5858 (1)  $e_1 = \text{fst}\{\mathcal{U}\} e_5$  and  $v_0 \lesssim e_5$   
 5859 By  $\lesssim$  on the redex  
 5860 (2) If  $e_5$  is a pre-value, it gets allocated. If not,  $e_5$  must be a value. Either way  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^*$   
 5861  $\text{fst}\{\mathcal{U}\} v_1; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \lesssim v_1$   
 5862 (3)  $\text{fst}\{\mathcal{U}\} v_1; \mathcal{H}_1; \mathcal{B}_1 \rightarrow_{\top}^* \text{check}\{\tau_0\} \delta(\text{fst}, v_1) v_1; \mathcal{H}_1; \mathcal{B}_1$   
 5863 By  $\rightarrow_{\top}^*$   
 5864 (4) If  $v_0 = \langle v_2, v_3 \rangle$  then  $e_0 \rightarrow_{\mathbb{A}}^* \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_2$   
 5865 and  $\text{trace } \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) (\text{fst}\{\tau_1\} v_0)) \approx \text{check}\{\tau_0\} \delta(\text{fst}, v_1) v_1; \mathcal{H}_1; \mathcal{B}_1$   
 5866 By (3)  
 5867 (5) Otherwise  $v_0 = \mathbb{G} b_1 \langle v_2, v_3 \rangle$  and  $e_0 \rightarrow_{\mathbb{A}}^* \text{trace } \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{dyn } b_1 v_2))$   
 5868 and  $\text{trace } \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{dyn } b_1 v_2)) \approx \text{check}\{\tau_0\} \delta(\text{fst}, v_1) v_1; \mathcal{H}_1; \mathcal{B}_1$   
 5869 **Case:**  $\text{snd}\{\mathcal{U}\} (\mathbb{T}?, \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) \blacktriangleright_{\mathbb{A}} \text{trace } \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) (\text{snd}\{\tau_1\} v_0))$   
 5870 (1)  $e_1 = \text{snd}\{\mathcal{U}\} e_5$  and  $v_0 \lesssim e_5$   
 5871 By  $\lesssim$  on the redex  
 5872 (2) If  $e_5$  is a pre-value, it gets allocated. If not,  $e_5$  must be a value. Either way  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^*$   
 5873  $\text{snd}\{\mathcal{U}\} v_1; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \lesssim v_1$   
 5874 (3)  $\text{snd}\{\mathcal{U}\} v_1; \mathcal{H}_1; \mathcal{B}_1 \rightarrow_{\top}^* \text{check}\{\tau_0\} \delta(\text{snd}, v_1) v_1; \mathcal{H}_1; \mathcal{B}_1$   
 5875 By  $\rightarrow_{\top}^*$   
 5876  
 5877  
 5878  
 5879  
 5880



- 5881 (4) If  $v_0 = \langle v_2, v_3 \rangle$  then  $e_0 \rightarrow_A^* \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_2$   
 5882 and  $\text{trace } \bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) (\text{snd}\{\tau_1\} v_0)) \approx \text{check}\{\tau_0\} \delta(\text{snd}, v_1) v_1; \mathcal{H}_1; \mathcal{B}_1$   
 5883 By (3)
- 5884 (5) Otherwise  $v_0 = \mathbb{G} b_1 \langle v_2, v_3 \rangle$  and  $e_0 \rightarrow_A^* \text{trace } \bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{dyn } b_1 v_2))$   
 5885 and  $\text{trace } \bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{dyn } b_1 v_2)) \approx \text{check}\{\tau_0\} \delta(\text{snd}, v_1) v_1; \mathcal{H}_1; \mathcal{B}_1$   
 5886 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_A \text{TagErr}$   
 5887 (1)  $e_1 = \text{binop}\{\tau_0\} e_5 e_6$  and  $v_0 \lesssim e_5$  and  $v_1 \lesssim e_6$   
 5888 By  $\lesssim$  on the redex  
 5889 (2) If  $e_5$  a pre-value, it gets allocated. If not,  $e_5$  must be a value. Similarly for  $e_6$ . Either way  
 5890  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* \text{binop}\{\tau_0\} v_2 v_3; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$   
 5891 (3)  $\delta(\text{binop}, v_2, v_3)$  is undefined  
 5892 By (2)  
 5893 (4)  $\text{TagErr} \approx \text{TagErr}; \mathcal{H}_1; \mathcal{B}_1$   
 5894 By  $\delta$   
 5895 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_A \delta(\text{binop}, v_2, v_3)$   
 5896 (1)  $e_1 = \text{binop}\{\tau_0\} e_5 e_6$  and  $v_0 \lesssim e_5$  and  $v_1 \lesssim e_6$   
 5897 By  $\lesssim$  on the redex  
 5898 (2) If  $e_5$  a pre-value, it gets allocated. If not,  $e_5$  must be a value. Similarly for  $e_6$ . Either way  
 5899  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* \text{binop}\{\tau_0\} v_2 v_3; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$   
 5900 (3)  $\delta(\text{binop}, v_2, v_3)$  is defined  
 5901 By (2)  
 5902 (4)  $\delta(\text{binop}, \text{rem-trace}(v_0), \text{rem-trace}(v_1)) \approx \delta(\text{binop}, v_2, v_3); \mathcal{H}_1; \mathcal{B}_1$   
 5903 By  $\delta$   
 5904 **Case:**  $\text{app}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_A \text{TagErr}$   
 5905 (1)  $e_1 = \text{app}\{\tau_0\} e_5 e_6$  and  $v_0 \lesssim e_5$  and  $v_1 \lesssim e_6$   
 5906 By  $\lesssim$  on the redex  
 5907 (2) If  $e_5$  a pre-value, it gets allocated. If not,  $e_5$  must be a value. Similarly for  $e_6$ . Either way  
 5908  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* \text{app}\{\tau_0\} v_2 v_3; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$   
 5909 (3)  $v_2$  is not a function  
 5910 By (2)  
 5911 (4)  $\text{TagErr} \approx \text{TagErr}; \mathcal{H}_1; \mathcal{B}_1$   
 5912 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{T}; \bar{b}_0(\lambda x_0. e_0)) v_0 \blacktriangleright_A \text{check}\{\mathcal{U}\} \text{trace } \bar{b}_0(e_0[x_0 \leftarrow v_1]) \bullet$   
 5913 (1)  $e_1 = \text{app}\{\mathcal{U}\} e_5 e_6$  and  $(\lambda(x_0 : \tau_1). e_4) \lesssim e_5$  and  $v_0 \lesssim e_6$   
 5914 By  $\lesssim$  on the redex  
 5915 (2) If  $e_5$  a pre-value, it gets allocated. If not,  $e_5$  must be a value. Similarly for  $e_6$ . Either way  
 5916  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* \text{app}\{\mathcal{U}\} v_2 v_3; \mathcal{H}_1; \mathcal{B}_1$  and  $(\lambda(x_0 : \tau_1). e_4) \lesssim v_2$  and  $v_0 \lesssim v_3$   
 5917 (3)  $e_1; \mathcal{H}_1; \mathcal{B}_1 \rightarrow_T^* \text{check}\{\tau_0\} e_7[x_0 \leftarrow 3] v_2; \mathcal{H}_2; \mathcal{B}_2$   
 5918 By (2)  
 5919 (4)  $\text{check}\{\mathcal{U}\} \text{trace } \bar{b}_0(e_0[x_0 \leftarrow v_1]) \bullet \approx \text{check}\{\tau_0\} e_7[x_0 \leftarrow 3] v_2; \mathcal{H}_2; \mathcal{B}_2$   
 5920 By (3) and a substitution lemma  
 5921 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{T}; \bar{b}_0(\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) v_1 \blacktriangleright_A$   
 5922  $\text{trace } \bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\tau_2\} v_0 (\text{dyn } (\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_2)))$   
 5923 (1)  $e_1 = \text{app}\{\tau_0\} e_5 e_6$  and  $(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \lesssim e_5$  and  $v_1 \lesssim e_6$   
 5924 By  $\lesssim$  on the redex  
 5925 (2) If  $e_5$  a pre-value, it gets allocated. If not,  $e_5$  must be a value. Similarly for  $e_6$ . Either way  
 5926  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_T^* \text{app}\{\tau_0\} v_2 v_3; \mathcal{H}_1; \mathcal{B}_1$  and  $(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \lesssim v_2$  and  $v_1 \lesssim v_3$   
 5927  
 5928  
 5929

5930 (3) Either  $\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_1 \rightarrow_{\mathbb{A}}^* \text{BoundaryErr}(\bar{b}, v)$  or  $\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_1 \rightarrow_{\mathbb{A}}^* v_4$   
5931 and trace  $\bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\tau_2\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_2)))$   
5932  $\approx \text{app}\{\tau_0\} v_2 v_3; \mathcal{H}_1; \mathcal{B}_1$   
5933 By  $v_1 \lesssim v_3$   
5934 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{A}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
5935 (1) If  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^* \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1; \mathcal{H}_1; \mathcal{B}_1$  then  $v_0 \lesssim v_1$  and  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^* v_1; \mathcal{H}_2; \mathcal{B}_2$  and  
5936  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \lesssim v_1; \mathcal{H}_2; \mathcal{B}_2$   
5937 (2) Otherwise  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^* \text{check}\{\tau_0\} v_1 p_0; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \approx v_1; \mathcal{H}_1; \mathcal{B}_1$   
5938 (3)  $\text{check}\{\tau_0\} v_1 p_0; \mathcal{H}_1; \mathcal{B}_1 \rightarrow_{\top}^* v_1; \mathcal{H}_2; \mathcal{B}_2$   
5939 By (2)  
5940 (4)  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \approx v_1; \mathcal{H}_2; \mathcal{B}_2$   
5941 **Case:**  $\text{stat} b_0 (\mathbb{G} b_1 (\mathbb{T} \bar{b}_0 v_0)) \blacktriangleright_{\mathbb{A}} \text{trace}(b_0 b_1 \bar{b}_0) v_0$   
5942 (1) If  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^* \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1; \mathcal{H}_1; \mathcal{B}_1$  then  $v_0 \lesssim v_1$  and  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^* v_1; \mathcal{H}_2; \mathcal{B}_2$  and  
5943  $\text{trace}(b_0 b_1 \bar{b}_0) v_0 \lesssim v_1; \mathcal{H}_2; \mathcal{B}_2$   
5944 (2) Otherwise  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^* \text{check}\{\tau_0\} v_1 p_0; \mathcal{H}_1; \mathcal{B}_1$  and  $v_0 \approx v_1; \mathcal{H}_1; \mathcal{B}_1$   
5945 (3)  $\text{check}\{\tau_0\} v_1 p_0; \mathcal{H}_1; \mathcal{B}_1 \rightarrow_{\top}^* v_1; \mathcal{H}_2; \mathcal{B}_2$   
5946 By (2)  
5947 (4)  $\text{trace}(b_0 b_1 \bar{b}_0) v_0 \approx v_1; \mathcal{H}_2; \mathcal{B}_2$   
5948 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0 \blacktriangleright_{\mathbb{A}} i_0$   
5949 (1) If  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^* \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1; \mathcal{H}_1; \mathcal{B}_1$  then  $i_0 \lesssim v_1$  and  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^* v_1; \mathcal{H}_2; \mathcal{B}_2$  and  
5950  $i_0 \lesssim v_1; \mathcal{H}_2; \mathcal{B}_2$   
5951 (2) Otherwise  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top}^* \text{check}\{\tau_0\} v_1 p_0; \mathcal{H}_1; \mathcal{B}_1$  and  $i_0 \approx v_1; \mathcal{H}_1; \mathcal{B}_1$   
5952 (3)  $\text{check}\{\tau_0\} v_1 p_0; \mathcal{H}_1; \mathcal{B}_1 \rightarrow_{\top}^* v_1; \mathcal{H}_2; \mathcal{B}_2$   
5953 By (2)  
5954 (4)  $i_0 \approx v_1; \mathcal{H}_2; \mathcal{B}_2$   
5955 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{A}} \text{InvariantErr}$   
5956 Impossible, by type soundness  
5957 **Case:**  $\text{trace} \bar{b}_0 v_0 \blacktriangleright_{\mathbb{A}} v_1$   
5958 Immediate  
5959  
5960  
5961  
5962  
5963  
5964  
5965  
5966  
5967  
5968  
5969  
5970  
5971  
5972  
5973  
5974  
5975  
5976  
5977  
5978

□

LEMMA A.31. *If  $\text{wfr}_{AT}(e_0, e_1)$  and  $e_0 \approx e_1; \mathcal{H}_0; \mathcal{B}_0$  then: and  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top} e_3; \mathcal{H}_1; \mathcal{B}_1$  then  $e_0 \rightarrow_{\Delta}^* e_2$  and  $e_2 \approx e_3; \mathcal{H}_1; \mathcal{B}_1$*

PROOF. By lemma A.32, lemma A.35, and case analysis of  $\triangleright_{\top}$ .

**Case:**  $w_0; \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} p_0; \mathcal{H}_1; \mathcal{B}_1$

Immediate

**Case:**  $(\text{unop}\{\tau_0\} v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \text{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$

Impossible, by type soundness

**Case:**  $(\text{unop}\{\mathcal{U}\} v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \text{TagErr}; \mathcal{H}_0; \mathcal{B}_0$

(1)  $e_0 = \text{unop}\{\mathcal{U}\} v_1$  and  $v_1 \lesssim v_0$

By  $\lesssim$  on the redex

(2)  $\delta(\text{unop}, \text{rem-trace}(v_1))$  is undefined

By (1)

(3)  $\text{TagErr} \approx \text{TagErr}; \mathcal{H}_0; \mathcal{B}_0$

By  $\delta$

**Case:**  $(\text{unop}\{\tau/\mathcal{U}\} p_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} (\text{check}\{\tau/\mathcal{U}\} \delta(\text{unop}, \mathcal{H}_0(p_0)) p_0); \mathcal{H}_0; \mathcal{B}_0$

(1)  $e_0 = \text{unop}\{\tau/\mathcal{U}\} v_1$  and  $v_1 \lesssim p_0$

By  $\lesssim$  on the redex

(2) If  $v_1$  is a pair then  $\delta(\text{unop}, \text{rem-trace}(v_1))$  is defined

and  $\text{check}\{\tau/\mathcal{U}\} \text{add-trace}(\text{get-trace}(v_1), \delta(\text{unop}, v_1)) \bullet \approx$

$;\text{check}\{\tau/\mathcal{U}\} \delta(\text{unop}, \mathcal{H}_0(p_0)) p_0; \mathcal{H}_0 \mathcal{B}_0$

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  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \delta(\text{unop}, v_2) \approx \text{check}\{\tau_0\} \delta(\text{unop}, p_0) p_0; \mathcal{H}_1; \mathcal{B}_1$

By  $\delta$

(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  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{stat } b_1 v_2) \approx \text{check}\{\tau_0\} \delta(\text{unop}, p_0) p_0; \mathcal{H}_1; \mathcal{B}_1$

By  $\delta$

**Case:**  $(\text{binop}\{\tau_0\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \text{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$

Impossible, by type soundness

**Case:**  $(\text{binop}\{\mathcal{U}\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \text{TagErr}; \mathcal{H}_0; \mathcal{B}_0$

(1)  $e_0 = \text{binop}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim v_0$  and  $v_3 \lesssim v_1$

By  $\lesssim$  on the redex

(2)  $\delta(\text{binop}, \text{rem-trace}(v_2), \text{rem-trace}(v_3))$  is undefined

By (1)

(3)  $\text{TagErr} \approx \text{TagErr}; \mathcal{H}_0; \mathcal{B}_0$

By  $\delta$

**Case:**  $(\text{binop}\{\tau/\mathcal{U}\} i_0 i_1); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \delta(\text{binop}, i_0, i_1); \mathcal{H}_0; \mathcal{B}_0$

(1)  $e_0 = \text{binop}\{\tau/\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim i_0$  and  $v_3 \lesssim i_1$

By  $\lesssim$  on the redex

(2)  $\delta(\text{binop}, \text{rem-trace}(v_2), \text{rem-trace}(v_3))$  is defined

By (1)

(3)  $\delta(\text{binop}, v_2, v_3) \approx \delta(\text{binop}, \mathcal{H}_0(p_0), \mathcal{H}_0(p_1); \mathcal{H}_0; \mathcal{B}_0$

By  $\delta$

**Case:**  $(\text{app}\{\tau_0\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \text{InvariantErr}; \mathcal{H}_0; \mathcal{B}_0$

Impossible, by type soundness

**Case:**  $(\text{app}\{\mathcal{U}\} v_0 v_1); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \text{TagErr}; \mathcal{H}_0; \mathcal{B}_0$

- 6028 (1)  $e_0 = \text{app}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim v_0$  and  $v_3 \lesssim v_1$   
6029 By  $\lesssim$  on the redex  
6030 (2)  $v_2$  is not a function  
6031 By (1)  
6032 (3)  $\text{TagErr} \approx \text{TagErr}; \mathcal{H}_0; \mathcal{B}_0$   
6033 **Case:**  $(\text{app}\{\tau/\mathcal{U}\} p_0 v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} (\text{check}\{\tau/\mathcal{U}\} e_0[x_0 \leftarrow v_0] p_0); \mathcal{H}_0; \mathcal{B}_1$   
6034 (1)  $e_0 = \text{app}\{\tau/\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim p_0$  and  $v_3 \lesssim v_0$   
6035 By  $\lesssim$  on the redex  
6036 (2) If  $v_2$  is a function, then  $e_0 \rightarrow_{\Delta}^* \text{check}\{\tau/\mathcal{U}\} e_1[x_0 \leftarrow v_3] \bullet$   
6037 and  $\text{check}\{\tau/\mathcal{U}\} e_1[x_0 \leftarrow v_3] \bullet \approx (\text{check}\{\tau/\mathcal{U}\} e_0[x_0 \leftarrow v_0] p_0); \mathcal{H}_0; \mathcal{B}_1$   
6038 By (1)  
6039 (3) Otherwise  $v_2 \in \mathbb{G} b v_4$  and unfolds to a dyn/stat boundary,  
6040 for example,  $e_0 \rightarrow_{\Delta}^* \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_3))$   
6041 and the argument reduces to a value, for example,  $\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_3 \rightarrow_{\Delta}^* v_5$   
6042 **Case:**  $(\text{app}\{\tau/\mathcal{U}\} p_0 v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \text{BoundaryErr}(\text{rev}(\mathcal{B}_0(p_0)), v_0); \mathcal{H}_0; \mathcal{B}_1$   
6043 (1)  $e_0 = \text{app}\{\tau/\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim p_0$  and  $v_3 \lesssim v_0$   
6044 By  $\lesssim$  on the redex  
6045 (2)  $v_2$  must be a guarded, typed function  
6046 By (1)  
6047 (3)  $e_0 \rightarrow_{\Delta}^* \text{BoundaryErr}(b, v)$   
6048 By type soundness  
6049 (4)  $\text{BoundaryErr}(b, v) \approx \text{BoundaryErr}(b, v); \mathcal{H}_0; \mathcal{B}_1$   
6050 **Case:**  $(\text{app}\{\tau_0\} p_0 v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} (\text{check}\{\tau_0\} e_0[x_0 \leftarrow v_0] p_0); \mathcal{H}_0; \mathcal{B}_1$   
6051 (1)  $e_0 = \text{app}\{\tau_0\} v_2 v_3$  and  $v_2 \lesssim p_0$  and  $v_3 \lesssim v_0$   
6052 By  $\lesssim$  on the redex  
6053 (2) If  $v_2$  is a function, then  $e_0 \rightarrow_{\Delta}^* \text{check}\{\tau_0\} e_1[x_0 \leftarrow v_3] \bullet$   
6054 and  $\text{check}\{\tau_0\} e_1[x_0 \leftarrow v_3] \bullet \approx (\text{check}\{\tau_0\} e_0[x_0 \leftarrow v_0] p_0); \mathcal{H}_0; \mathcal{B}_1$   
6055 By (1)  
6056 (3) Otherwise  $v_2 \in \mathbb{G} b v_4$  and unfolds to a dyn/stat boundary,  
6057 for example,  $e_0 \rightarrow_{\Delta}^* \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_3))$  and the argu-  
6058 ment reduces to a value,  
6059 for example,  $\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_3 \rightarrow_{\Delta}^* v_5$   
6060 **Case:**  $(\text{app}\{\mathcal{U}\} p_0 v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} (e_0[x_0 \leftarrow v_0]); \mathcal{H}_0; \mathcal{B}_0$   
6061 (1)  $e_0 = \text{app}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim p_0$  and  $v_3 \lesssim v_0$   
6062 By  $\lesssim$  on the redex  
6063 (2) If  $v_2$  is a function, then  $e_0 \rightarrow_{\Delta}^* \text{check}\{\tau_0\} e_1[x_0 \leftarrow v_3] \bullet$   
6064 and  $\text{check}\{\tau_0\} e_1[x_0 \leftarrow v_3] \bullet \approx (\text{check}\{\tau_0\} e_0[x_0 \leftarrow v_0] p_0); \mathcal{H}_0; \mathcal{B}_1$   
6065 By (1)  
6066 (3) Otherwise  $v_2 \in \mathbb{G} b v_4$  and  $e_0$  unfolds to  
6067 a stat boundary  $e_0 \rightarrow_{\Delta}^* \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\tau\} v_4 (\text{dyn}(\ell_1 \blacktriangleleft \tau \blacktriangleleft \ell_0) v_3))$  and the argument  
6068 reduces to a value  $\text{stat}(\ell_1 \blacktriangleleft \tau \blacktriangleleft \ell_0) v_3 \rightarrow_{\Delta}^* v_5$   
6069 and  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\tau\} v_4 v_5) \approx (e_0[x_0 \leftarrow v_0]); \mathcal{H}_0; \mathcal{B}_0$   
6070 **Case:**  $(\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0); \mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} v_0; \mathcal{H}_0; \mathcal{B}_1$   
6071 (1)  $e_0 = \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $v_1 \lesssim v_0$   
6072 By  $\lesssim$  on the redex  
6073 (2) If  $v_1 \in i$  then  $e_0 \rightarrow_{\Delta}^* v_1$  and  $v_1 \approx v_0; \mathcal{H}_0; \mathcal{B}_1$   
6074  
6075  
6076

- 6077 (3) Otherwise  $e_0 \rightarrow_{\mathbb{A}}^* \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1 \approx v_0$ ;  $\mathcal{H}_0; \mathcal{B}_1$
- 6078 **Case:**  $(\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)$ ;  $\mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \text{BoundaryErr}(\{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}, v_0)$ ;  $\mathcal{H}_0; \mathcal{B}_0$
- 6079 (1)  $e_0 = \text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $v_1 \lesssim v_0$
- 6080 By  $\lesssim$  on the redex
- 6081 (2)  $e_0 \rightarrow_{\mathbb{A}}^* \text{BoundaryErr}(\bar{b}, v)$
- 6082 By (1)
- 6083 (3)  $\text{BoundaryErr}(\bar{b}, v) \approx \text{BoundaryErr}(\{(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1)\}, v_0)$ ;  $\mathcal{H}_0; \mathcal{B}_0$
- 6084 **Case:**  $(\text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)$ ;  $\mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} v_0$ ;  $\mathcal{H}_0; \mathcal{B}_1$
- 6085 (1)  $e_0 = \text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $v_1 \lesssim v_0$
- 6086 By  $\lesssim$  on the redex
- 6087 (2) If  $v_1 \in i$  then  $e_0 \rightarrow_{\mathbb{A}}^* v_1$  and  $v_1 \approx v_0$ ;  $\mathcal{H}_0; \mathcal{B}_1$
- 6088 (3) If  $v_1$  has no guard wrappers, then  $e_0 \rightarrow_{\mathbb{A}}^* \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1 \approx v_0$ ;  $\mathcal{H}_0; \mathcal{B}_1$
- 6089 (4) Otherwise  $v_1 = \mathbb{G} b v_2$  and  $e_0 \rightarrow_{\mathbb{A}}^* \mathbb{T} \bar{b} v_2$  and  $\mathbb{T} \bar{b} v_2 \approx v_0$ ;  $\mathcal{H}_0; \mathcal{B}_1$
- 6090 **Case:**  $(\text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)$ ;  $\mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \text{InvariantErr}$ ;  $\mathcal{H}_0; \mathcal{B}_0$
- 6091 Impossible, by type soundness
- 6092 **Case:**  $(\text{check}\{\mathcal{U}\} v_0 p_0)$ ;  $\mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} v_0$ ;  $\mathcal{H}_0; \mathcal{B}_0$
- 6093 (1) If  $e_0 = \text{stat } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  then  $e_0 \rightarrow_{\mathbb{A}}^* v_2$  and  $v_2 \approx v_0$ ;  $\mathcal{H}_0; \mathcal{B}_0$
- 6094 (2) Otherwise  $e_0 = \text{check}\{\mathcal{U}\} v_1 \bullet$  and  $e_0 \rightarrow_{\mathbb{A}}^* v_1$  and  $v_1 \approx v_0$ ;  $\mathcal{H}_0; \mathcal{B}_0$
- 6095 **Case:**  $(\text{check}\{\tau_0\} v_0 p_0)$ ;  $\mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} v_0$ ;  $\mathcal{H}_0; \mathcal{B}_1$
- 6096 (1) If  $e_0 = \text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  then  $v_1 \lesssim v_0$  and  $e_0 \rightarrow_{\mathbb{A}}^* v_2$  and  $v_2 \approx v_0$ ;  $\mathcal{H}_0; \mathcal{B}_1$
- 6097 Same as the dyn case
- 6098 (2) Otherwise  $e_0 = \text{check}\{\tau_0\} v_1 \bullet$  and  $e_0 \rightarrow_{\mathbb{A}}^* v_1$  and  $v_1 \approx v_0$ ;  $\mathcal{H}_0; \mathcal{B}_1$
- 6099 **Case:**  $(\text{check}\{\tau_0\} v_0 p_0)$ ;  $\mathcal{H}_0; \mathcal{B}_0 \triangleright_{\top} \text{BoundaryErr}(\mathcal{B}_0(v_0) \cup \mathcal{B}_0(p_0), v_0)$ ;  $\mathcal{H}_0; \mathcal{B}_0$
- 6100 (1) If  $e_0 = \text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  then  $v_1 \lesssim v_0$  and  $e_0 \rightarrow_{\mathbb{A}}^* \text{BoundaryErr}(\bar{b}, v)$
- 6101 and  $\text{BoundaryErr}(\bar{b}, v) \approx \text{BoundaryErr}(\mathcal{B}_0(v_0) \cup \mathcal{B}_0(p_0), v_0)$ ;  $\mathcal{H}_0; \mathcal{B}_1$
- 6102 Same as the dyn case
- 6103 (2) Otherwise  $e_0 = \text{check}\{\tau_0\} v_1 \bullet$ , but this is impossible by type soundness.
- 6104
- 6105
- 6106
- 6107
- 6108
- 6109
- 6110
- 6111
- 6112
- 6113
- 6114
- 6115
- 6116
- 6117
- 6118
- 6119
- 6120
- 6121
- 6122
- 6123
- 6124
- 6125

LEMMA A.32.

If  $\text{wfr}_{AT}(e_0, e_1)$  and  $e_0 \lesssim e_1$  and either  $e_0 \rightarrow_{\mathbb{A}} e_2$  or  $e_1; \mathcal{H}_0; \mathcal{B}_0 \rightarrow_{\top} e_3; \mathcal{H}_2; \mathcal{B}_2$  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  $\text{wfr}_{AT}(E_0[e_0], e_1)$  and  $E_0[e_0] \lesssim e_1$  and  $e_0(\triangleright_{\mathbb{A}} \cup \blacktriangleright_{\mathbb{A}}) e_2$  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  $E_0[e_0]$ .

6126 LEMMA A.34.

6127 *If  $\text{wfr}_{AT}(e_0, E_1[e_1])$  and  $e_0 \lesssim E_1[e_1]$  and  $e_1; \mathcal{H}_1; \mathcal{B}_1 \triangleright_{\top} e_3; \mathcal{H}_3; \mathcal{B}_3$  then the following results hold:*

- 6128 •  $e_0 = E_0[e_2]$
- 6129 •  $E_0 \lesssim E_1$
- 6130 •  $e_1 \lesssim e_2$ .

6131 PROOF. By induction on  $e_0 \lesssim E_1[e_1]$ , proceeding by case analysis of  $E_1[e_1]$ . □

6133 LEMMA A.35.

6134 *If  $E_0 \lesssim E_1$  and  $e_2 \lesssim e_3$  then  $E_0[e_2] \lesssim E_1[e_3]$ .*

6135 PROOF. By induction on  $E_0 \lesssim E_1$ . □

6137

6138

6139

6140

6141

6142

6143

6144

6145

6146

6147

6148

6149

6150

6151

6152

6153

6154

6155

6156

6157

6158

6159

6160

6161

6162

6163

6164

6165

6166

6167

6168

6169

6170

6171

6172

6173

6174

6175 LEMMA A.36 ( $F \lesssim A$ ).  $F \lesssim A$

6176

6177

PROOF. By lemma A.37 and lemma A.38, the relation  $e \lesssim e$  is a lock-step bisimulation.  $\square$

6178

6179

6180

$\text{wfr}_{FT}(e_0, e_1)$  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  $e_2 \rightarrow_F^* e_0$  and  $e_2 \rightarrow_A^* e_1$

6181

6182

LEMMA A.37. If  $\text{wfr}_{FT}(e_0, e_1)$  and  $e_0 \lesssim e_1$  and  $e_0 \rightarrow_F e_2$  then  $e_1 \rightarrow_A e_3$

6183

PROOF. By lemma A.39, lemma A.42, and case analysis of  $\triangleright_F \cup \blacktriangleright_F$ .

6184

**Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_F \text{InvariantErr}$

6185

Impossible, by type soundness

6186

**Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_F \delta(\text{unop}, v_0)$

6187

(1)  $e_1 = \text{unop}\{\tau_0\} v_1$  and  $v_0 \lesssim v_1$

6188

By  $\lesssim$  on the redex

6189

(2)  $\delta(\text{unop}, v_1)$  is defined

6190

By (1)

6191

(3)  $\delta(\text{unop}, v_0) \lesssim \delta(\text{unop}, v_1)$

6192

By  $\delta$

6193

**Case:**  $\text{fst}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_0) \triangleright_F \text{dyn}(\ell_0 \blacktriangleright \text{fst}(\tau_1) \blacktriangleright \ell_1) (\text{fst}\{\mathcal{U}\} v_0)$

6194

(1)  $e_1 = \text{unop}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_2 \blacktriangleright \ell_1) v_1)$  and  $v_0 \lesssim v_1$  and  $\tau_1 \leq \tau_2$

6195

By  $\lesssim$  on the redex

6196

(2)  $e_1 \triangleright_A \text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) (\text{fst}\{\mathcal{U}\} v_1)$

6197

By (1)

6198

(3)  $\text{dyn}(\ell_0 \blacktriangleright \text{fst}(\tau_1) \blacktriangleright \ell_1) (\text{fst}\{\mathcal{U}\} v_0) \lesssim \text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) (\text{fst}\{\mathcal{U}\} v_1)$

6199

By  $\text{fst}(\tau_1) \leq \tau_0$

6200

**Case:**  $\text{snd}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_0) \triangleright_F \text{dyn}(\ell_0 \blacktriangleright \text{snd}(\tau_1) \blacktriangleright \ell_1) (\text{snd}\{\mathcal{U}\} v_0)$

6201

(1)  $e_1 = \text{unop}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_2 \blacktriangleright \ell_1) v_1)$  and  $v_0 \lesssim v_1$  and  $\tau_1 \leq \tau_2$

6202

By  $\lesssim$  on the redex

6203

(2)  $e_1 \triangleright_A \text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) (\text{snd}\{\mathcal{U}\} v_1)$

6204

By (1)

6205

(3)  $\text{dyn}(\ell_0 \blacktriangleright \text{snd}(\tau_1) \blacktriangleright \ell_1) (\text{snd}\{\mathcal{U}\} v_0) \lesssim \text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) (\text{snd}\{\mathcal{U}\} v_1)$

6206

By  $\text{snd}(\tau_1) \leq \tau_0$

6207

**Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_F \text{InvariantErr}$

6208

Impossible, by type soundness

6209

**Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_F \delta(\text{binop}, v_0, v_1)$

6210

(1)  $e_1 = \text{binop}\{\tau_0\} v_2 v_3$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$

6211

By  $\lesssim$  on the redex

6212

(2)  $\delta(\text{binop}, v_2, v_3)$  is defined

6213

By (1)

6214

(3)  $\delta(\text{binop}, v_0, v_1) \lesssim \delta(\text{binop}, v_2, v_3)$

6215

By  $\delta$

6216

**Case:**  $\text{app}\{\tau_0\} v_0 v_1 \triangleright_F \text{InvariantErr}$

6217

Impossible, by type soundness

6218

**Case:**  $\text{app}\{\tau_0\} (\lambda(x_0 : \tau_1). e_4) v_0 \triangleright_F e_4[x_0 \leftarrow v_0]$

6219

(1)  $e_1 = \text{app}\{\tau_0\} v_1 v_2$  and  $(\lambda(x_0 : \tau_1). e_4) \lesssim v_1$  and  $v_0 \lesssim v_2$

6220

By  $\lesssim$  on the redex

6221

(2)  $v_1 = \lambda(x_0 : \tau_1). e_5$

6222

By (1)

6223

- 6224 (3)  $e_4[x_0 \leftarrow v_0] \lesssim e_5[x_0 \leftarrow v_2]$
- 6225 **Case:**  $\text{app}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) v_1 \triangleright_{\mathbb{F}}$
- 6226  $\text{dyn}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_1))$
- 6227 (1)  $e_1 = \text{app}\{\tau_0\} v_2 v_3$  and  $(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \lesssim v_2$  and  $v_1 \lesssim v_3$
- 6228 By  $\lesssim$  on the redex
- 6229 (2)  $v_2 = \mathbb{G}(\ell_0 \blacktriangleleft \tau_2 \blacktriangleleft \ell_1) v_4$  and  $\tau_1 \leqslant \tau_2$
- 6230 By (1)
- 6231 (3)  $e_1 \triangleright_{\mathbb{A}} \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_3))$
- 6232 By (2)
- 6233 (4)  $\text{dyn}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_1)) \lesssim$
- 6234  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_3))$
- 6235 By  $\text{cod}(\tau_1) \leqslant \tau_0$
- 6236 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_{\mathbb{F}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$
- 6237 (1)  $e_1 = \text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1$  and  $v_0 \lesssim v_1$  and  $\tau_0 \leqslant \tau_1$
- 6238 By  $\lesssim$
- 6239 (2)  $e_1 \triangleright_{\mathbb{A}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1$
- 6240 By  $\triangleright_{\mathbb{A}}$
- 6241 (3)  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \lesssim \mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1$
- 6242 By (1)
- 6243 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\mathbb{T}_? \bar{b}_0 i_0) \triangleright_{\mathbb{F}} i_0$
- 6244 (1)  $e_1 = \text{dyn}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) i_1$  and  $i_0 \lesssim i_1$  and  $\tau_0 \leqslant \tau_1$
- 6245 By  $\lesssim$
- 6246 (2)  $e_1 \triangleright_{\mathbb{A}} i_1$
- 6247 By  $\triangleright_{\mathbb{A}}$  and  $\tau_0 \leqslant \tau_1$
- 6248 (3)  $i_0 \lesssim i_1$
- 6249 By (1)
- 6250 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_{\mathbb{F}} \text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \bar{b}_0, v_0)$
- 6251 Immediate, by  $\text{BoundaryErr}(\bar{b}, v) \lesssim e$
- 6252 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_{\mathbb{F}} \text{TagErr}$
- 6253 (1)  $e_1 = \text{unop}\{\mathcal{U}\} v_1$  and  $v_0 \lesssim v_1$
- 6254 By  $\lesssim$  on the redex
- 6255 (2)  $\delta(\text{unop}, v_1)$  is undefined
- 6256 By (1)
- 6257 (3)  $\text{TagErr} \lesssim \text{TagErr}$
- 6258 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_{\mathbb{F}} \text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, \text{rem-trace}(v_0)))$
- 6259 (1)  $e_1 = \text{unop}\{\mathcal{U}\} v_1$  and  $v_0 \lesssim v_1$
- 6260 By  $\lesssim$  on the redex
- 6261 (2)  $\delta(\text{unop}, \text{rem-trace}(v_1))$  is defined
- 6262 By (1)
- 6263 (3)  $\delta(\text{unop}, \text{rem-trace}(v_0)) \lesssim \delta(\text{unop}, \text{rem-trace}(v_1))$
- 6264 By  $\delta$
- 6265 **Case:**  $\text{fst}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) \blacktriangleright_{\mathbb{F}} \text{trace } \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_0))$
- 6266 (1)  $e_1 = \text{unop}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1))$  and  $v_0 \lesssim v_1$  and  $\tau_0 \leqslant \tau_1$
- 6267 By  $\lesssim$  on the redex
- 6268 (2)  $e_1 \blacktriangleright_{\mathbb{A}} \text{trace } \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_1) \blacktriangleleft \ell_1) (\text{fst}\{\text{fst}(\tau_1)\} v_1))$
- 6269 By (1)
- 6270
- 6271
- 6272



- 6273 (3)  $\text{trace } \bar{b}_0(\text{stat } (\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) (\text{fst}\{\text{fst}(\tau_0)\} v_0)) \lesssim$   
6274  $\text{trace } \bar{b}_0(\text{stat } (\ell_0 \blacktriangleleft \text{fst}(\tau_1) \blacktriangleleft \ell_1) (\text{fst}\{\text{fst}(\tau_1)\} v_1))$   
6275  $\text{By } \text{fst}(\tau_0) \leqslant \text{fst}(\tau_1)$
- 6276 **Case:**  $\text{snd}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) \blacktriangleright_{\mathbb{F}} \text{trace } \bar{b}_0(\text{stat } (\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_0))$
- 6277 (1)  $e_1 = \text{unop}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G} (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1))$  and  $v_0 \lesssim v_1$  and  $\tau_0 \leqslant \tau_1$   
6278  $\text{By } \lesssim$  on the redex
- 6279 (2)  $e_1 \blacktriangleright_{\mathbb{A}} \text{trace } \bar{b}_0(\text{stat } (\ell_0 \blacktriangleleft \text{snd}(\tau_1) \blacktriangleleft \ell_1) (\text{snd}\{\text{snd}(\tau_1)\} v_1))$   
6280  $\text{By (1)}$
- 6281 (3)  $\text{trace } \bar{b}_0(\text{stat } (\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) (\text{snd}\{\text{snd}(\tau_0)\} v_0)) \lesssim$   
6282  $\text{trace } \bar{b}_0(\text{stat } (\ell_0 \blacktriangleleft \text{snd}(\tau_1) \blacktriangleleft \ell_1) (\text{snd}\{\text{snd}(\tau_1)\} v_1))$   
6283  $\text{By } \text{snd}(\tau_0) \leqslant \text{snd}(\tau_1)$
- 6284 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{F}} \text{TagErr}$
- 6285 (1)  $e_1 = \text{binop}\{\mathcal{U}\} v_2 v_3$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$   
6286  $\text{By } \lesssim$  on the redex
- 6287 (2)  $\delta(\text{binop}, v_2, v_3)$  is undefined  
6288  $\text{By (1)}$
- 6289 (3)  $\text{TagErr} \lesssim \text{TagErr}$
- 6290 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{F}} \delta(\text{binop}, \text{rem-trace}(v_0), \text{rem-trace}(v_1))$
- 6291 (1)  $e_1 = \text{binop}\{\mathcal{U}\} v_2 v_3$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$   
6292  $\text{By } \lesssim$  on the redex
- 6293 (2)  $\delta(\text{binop}, \text{rem-trace}(v_2), \text{rem-trace}(v_3))$  is defined  
6294  $\text{By (1)}$
- 6295 (3)  $\delta(\text{binop}, \text{rem-trace}(v_0), \text{rem-trace}(v_1)) \lesssim \delta(\text{binop}, \text{rem-trace}(v_2), \text{rem-trace}(v_3))$   
6296  $\text{By } \delta$
- 6297 **Case:**  $\text{app}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{F}} \text{TagErr}$
- 6298 (1)  $e_1 = \text{app}\{\mathcal{U}\} v_2 v_3$  and  $v_0 \lesssim v_2$  and  $v_1 \lesssim v_3$   
6299  $\text{By } \lesssim$  on the redex
- 6300 (2)  $\text{rem-trace}(v_2) \notin \lambda x. e \cup \mathbb{G} b v$   
6301  $\text{By (1)}$
- 6302 (3)  $\text{TagErr} \lesssim \text{TagErr}$
- 6303 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\lambda x_0. e_4)) v_0 \blacktriangleright_{\mathbb{F}} \text{trace } \bar{b}_0(e_4[x_0 \leftarrow v_1])$
- 6304 (1)  $e_1 = \text{app}\{\mathcal{U}\} v_1 v_2$  and  $(\mathbb{T}_? \bar{b}_0 (\lambda x_0. e_4)) \lesssim v_1$  and  $v_0 \lesssim v_2$   
6305  $\text{By } \lesssim$  on the redex
- 6306 (2)  $v_1 = (\mathbb{T}_? \bar{b}_0 (\lambda x_0. e_5))$   
6307  $\text{By (1)}$
- 6308 (3)  $\text{trace } \bar{b}_0(e_4[x_0 \leftarrow v_1]) \lesssim \text{trace } \bar{b}_0(e_5[x_0 \leftarrow v_2])$
- 6309 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) v_1 \blacktriangleright_{\mathbb{F}}$   
6310  $\text{trace } \bar{b}_0(\text{stat } (\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\tau_1\} v_0 (\text{dyn } (\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_2)))$
- 6311 (1)  $e_1 = \text{app}\{\mathcal{U}\} v_2 v_3$  and  $(\mathbb{T}_? \bar{b}_0 (\mathbb{G} (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) \lesssim v_2$  and  $v_1 \lesssim v_3$   
6312  $\text{By } \lesssim$  on the redex
- 6313 (2)  $v_2 = \mathbb{T}_? \bar{b}_0 (\mathbb{G} (\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_4)$  and  $\tau_0 \leqslant \tau_1$   
6314  $\text{By (1)}$
- 6315 (3)  $e_1 \blacktriangleright_{\mathbb{A}} \text{trace } \bar{b}_0(\text{stat } (\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat } (\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_3)))$   
6316  $\text{By (2)}$
- 6317 (4)  $\text{trace } \bar{b}_0(\text{stat } (\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\tau_1\} v_0 (\text{dyn } (\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_2))) \lesssim$   
6318  $\text{trace } \bar{b}_0(\text{stat } (\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat } (\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_3)))$   
6319  $\text{By } \tau_0 \leqslant \tau_1$
- 6320
- 6321

- 6322 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{F}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
6323 (1)  $e_1 = \text{stat}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1$  and  $v_0 \lesssim v_1$  and  $\tau_0 \leq \tau_1$   
6324 By  $\lesssim$   
6325 (2)  $e_1 \blacktriangleright_{\mathbb{A}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1$   
6326 By  $\blacktriangleright_{\mathbb{A}}$   
6327 (3)  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \lesssim \mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1$   
6328 By (1)  
6329 **Case:**  $\text{stat} b_0 (\mathbb{G} b_1 (\mathbb{T} \bar{b}_0 v_0)) \blacktriangleright_{\mathbb{F}} \text{trace}(b_0 b_1 \bar{b}_0) v_0$   
6330 (1)  $e_1 = \text{stat} b_2 (\mathbb{G} b_3 (\mathbb{T} \bar{b}_1 v_1))$  and  $v_0 \lesssim v_1$  and  $\tau_0 \leq \tau_1$  and  $b_0 \lesssim b_2$  and  $b_1 \lesssim b_3$   
6331 By  $\lesssim$   
6332 (2)  $e_1 \blacktriangleright_{\mathbb{A}} \text{trace}(b_2 b_3 \bar{b}_1) v_1$   
6333 By  $\blacktriangleright_{\mathbb{A}}$   
6334 (3)  $\text{trace}(b_0 b_1 \bar{b}_0) v_0 \lesssim \text{trace}(b_2 b_3 \bar{b}_1) v_1$   
6335 By (1)  
6336 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0 \blacktriangleright_{\mathbb{F}} i_0$   
6337 (1)  $e_1 = \text{stat}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) i_1$  and  $i_0 \lesssim i_1$  and  $\tau_0 \leq \tau_1$   
6338 By  $\lesssim$   
6339 (2)  $e_1 \blacktriangleright_{\mathbb{A}} i_1$   
6340 By  $\blacktriangleright_{\mathbb{A}}$  and  $\tau_0 \leq \tau_1$   
6341 (3)  $i_0 \lesssim i_1$   
6342 By (1)  
6343 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{F}} \text{InvariantErr}$   
6344 Impossible, by type soundness  
6345 **Case:**  $\text{trace} \bar{b}_0 v_0 \blacktriangleright_{\mathbb{F}} \text{add-trace}(\bar{b}_0, v_0)$   
6346 (1)  $e_1 = \text{trace} \bar{b}_1 v_1$   
6347 By  $\lesssim$   
6348 (2)  $e_1 \blacktriangleright_{\mathbb{A}} \text{add-trace}(\bar{b}_1, v_1)$   
6349 By  $\blacktriangleright_{\mathbb{A}}$   
6350 (3)  $\text{add-trace}(\bar{b}_0, v_0) \lesssim \text{add-trace}(\bar{b}_1, v_1)$   
6351 By (1)  
6352  
6353  
6354  
6355  
6356  
6357  
6358  
6359  
6360  
6361  
6362  
6363  
6364  
6365  
6366  
6367  
6368  
6369  
6370

□

6371 LEMMA A.38. *If  $wfr_{FT}(e_0, e_1)$  and  $e_0 \lesssim e_1$  and  $e_1 \rightarrow_A e_3$  then  $e_0 \rightarrow_F e_2$*

6372

6373 PROOF. By lemma A.39, lemma A.42, and case analysis of  $\triangleright_A \cup \blacktriangleright_A$ .

6374

6375 **Case:**  $unop\{\tau_0\} v_0 \triangleright_A \text{InvariantErr}$

Impossible, by type soundness

6376

6377 **Case:**  $unop\{\tau_0\} v_0 \triangleright_A \delta(unop, v_0)$

6378

(1)  $e_0 = unop\{\tau_0\} v_1$  and  $v_1 \lesssim v_0$

6379

By  $\lesssim$  on the redex

6380

(2)  $\delta(unop, v_1)$  is defined

6381

By (1)

6382

(3)  $\delta(unop, v_1) \lesssim \delta(unop, v_0)$

6383

By  $\delta$

6384

6385 **Case:**  $\text{fst}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_0) \triangleright_A \text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) (\text{fst}\{\mathcal{U}\} v_0)$

6386

(1)  $e_0 = unop\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_2 \blacktriangleright \ell_1) v_1)$  and  $v_1 \lesssim v_0$  and  $\text{fst}(\tau_2) \leq \tau_0$

6387

By  $\lesssim$  on the redex

6388

(2)  $e_0 \triangleright_F \text{dyn}(\ell_0 \blacktriangleright \text{fst}(\tau_2) \blacktriangleright \ell_1) (\text{fst}\{\mathcal{U}\} v_1)$

6389

By (1)

6390

(3)  $\text{dyn}(\ell_0 \blacktriangleright \text{fst}(\tau_2) \blacktriangleright \ell_1) (\text{fst}\{\mathcal{U}\} v_1) \lesssim \text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) (\text{fst}\{\mathcal{U}\} v_0)$

6391

By (1)

6392

6393 **Case:**  $\text{snd}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_0) \triangleright_A \text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) (\text{snd}\{\mathcal{U}\} v_0)$

6394

(1)  $e_1 = unop\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_2 \blacktriangleright \ell_1) v_1)$  and  $v_1 \lesssim v_0$  and  $\text{snd}(\tau_2) \leq \tau_0$

6395

By  $\lesssim$  on the redex

6396

(2)  $e_0 \triangleright_F \text{dyn}(\ell_0 \blacktriangleright \text{snd}(\tau_2) \blacktriangleright \ell_1) (\text{snd}\{\mathcal{U}\} v_1)$

6397

By (1)

6398

(3)  $\text{dyn}(\ell_0 \blacktriangleright \text{snd}(\tau_2) \blacktriangleright \ell_1) (\text{snd}\{\mathcal{U}\} v_1) \lesssim \text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) (\text{snd}\{\mathcal{U}\} v_0)$

6399

By (1)

6400

6401 **Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_A \text{InvariantErr}$

6402

Impossible, by type soundness

6403

6404 **Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_A \delta(\text{binop}, v_0, v_1)$

6405

(1)  $e_0 = \text{binop}\{\tau_0\} v_2 v_3$  and  $v_2 \lesssim v_0$  and  $v_3 \lesssim v_1$

6406

By  $\lesssim$  on the redex

6407

(2)  $\delta(\text{binop}, v_2, v_3)$  is defined

6408

By (1)

6409

(3)  $\delta(\text{binop}, v_2, v_3) \lesssim \delta(\text{binop}, v_0, v_1)$

6410

By  $\delta$

6411

6412 **Case:**  $\text{app}\{\tau_0\} v_0 v_1 \triangleright_A \text{InvariantErr}$

6413

Impossible, by type soundness

6414

6415 **Case:**  $\text{app}\{\tau_0\} (\lambda(x_0 : \tau_1). e_0) v_0 \triangleright_A e_0[x_0 \leftarrow v_0]$

6416

(1)  $e_0 = \text{app}\{\tau_0\} v_1 v_2$  and  $v_1 \lesssim (\lambda(x_0 : \tau_1). e_4)$  and  $v_2 \lesssim v_0$

6417

By  $\lesssim$  on the redex

6418

(2)  $v_1 = \lambda(x_0 : \tau_1). e_5$

6419

By (1)

(3)  $e_5[x_0 \leftarrow v_2] \lesssim e_4[x_0 \leftarrow v_0]$

6420

6421 **Case:**  $\text{app}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_0) v_1 \triangleright_A$

6422

$\text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_1))$

6423

(1)  $e_1 = \text{app}\{\tau_0\} v_2 v_3$  and  $v_2 \lesssim (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_0)$  and  $v_3 \lesssim v_1$

6424

By  $\lesssim$  on the redex

6425

- 6420 (2)  $v_2 = \mathbb{G}(\ell_0 \blacktriangleright \tau_2 \blacktriangleright \ell_1) v_4$  and  $\text{cod}(\tau_2) \leq \tau_0$
- 6421 By (1)
- 6422 (3)  $e_1 \triangleright_{\mathbb{F}} \text{dyn}(\ell_0 \blacktriangleright \text{cod}(\tau_2) \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_3))$
- 6423 By (2)
- 6424 (4)  $\text{dyn}(\ell_0 \blacktriangleright \text{cod}(\tau_2) \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_3)) \lesssim$
- 6425  $\text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) (\text{app}\{\mathcal{U}\} v_0 (\text{stat}(\ell_1 \blacktriangleright \text{dom}(\tau_1) \blacktriangleright \ell_0) v_1))$
- 6426 By  $\text{cod}(\tau_0) \leq \tau_0$
- 6427 **Case:**  $\text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0 \triangleright_{\mathbb{A}} \mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0$
- 6428 (1)  $e_1 = \text{dyn}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_1$  and  $v_1 \lesssim v_0$  and  $\tau_1 \leq \tau_0$
- 6429 By  $\lesssim$
- 6430 (2) Either  $e_1 \triangleright_{\mathbb{F}} \mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_1$  or  $e_1 \triangleright_{\mathbb{F}} \text{BoundaryErr}(\bar{b}, v)$
- 6431 By  $\triangleright_{\mathbb{F}}$
- 6432 (3)  $\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_1 \lesssim \mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0$
- 6433 By (1)
- 6434 **Case:**  $\text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) (\mathbb{T}_? \bar{b}_0 i_0) \triangleright_{\mathbb{A}} i_0$
- 6435 (1)  $e_1 = \text{dyn}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) i_1$  and  $i_1 \lesssim i_0$  and  $\tau_1 \leq \tau_0$
- 6436 By  $\lesssim$
- 6437 (2) Either  $e_1 \triangleright_{\mathbb{F}} i_1$  or  $e_1 \triangleright_{\mathbb{F}} \text{BoundaryErr}(\bar{b}, i)$
- 6438 By  $\triangleright_{\mathbb{F}}$  and  $\tau_0 \leq \tau_1$
- 6439 (3)  $i_1 \lesssim i_0$
- 6440 By (1)
- 6441 **Case:**  $\text{dyn}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0 \triangleright_{\mathbb{A}} \text{BoundaryErr}((\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) \bar{b}_0, v_0)$
- 6442 (1)  $e_1 = \text{dyn}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_1$  and  $v_1 \lesssim v_0$  and  $\tau_1 \leq \tau_0$
- 6443 By  $\lesssim$
- 6444 (2)  $\text{BoundaryErr}(\bar{b}_1, v_1) \lesssim \text{BoundaryErr}(\bar{b}_0, v_0)$
- 6445 By (1) and  $\triangleright_{\mathbb{F}}$
- 6446 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_{\mathbb{A}} \text{TagErr}$
- 6447 (1)  $e_1 = \text{unop}\{\mathcal{U}\} v_1$  and  $v_1 \lesssim v_0$
- 6448 By  $\lesssim$  on the redex
- 6449 (2)  $\delta(\text{unop}, \text{rem-trace}(v_1))$  is defined
- 6450 By (1)
- 6451 (3)  $\delta(\text{unop}, \text{rem-trace}(v_1)) \lesssim \delta(\text{unop}, \text{rem-trace}(v_0))$
- 6452 By  $\delta$
- 6453 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_{\mathbb{A}} \text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, v_1))$
- 6454 (1)  $e_1 = \text{unop}\{\mathcal{U}\} v_1$  and  $v_1 \lesssim v_0$
- 6455 By  $\lesssim$  on the redex
- 6456 (2)  $\delta(\text{unop}, \text{rem-trace}(v_1))$  is defined
- 6457 By (1)
- 6458 (3)  $\delta(\text{unop}, \text{rem-trace}(v_1)) \lesssim \delta(\text{unop}, \text{rem-trace}(v_0))$
- 6459 By  $\delta$
- 6460 **Case:**  $\text{fst}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleright \tau_0 \blacktriangleright \ell_1) v_0)) \blacktriangleright_{\mathbb{A}} \text{trace } \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleright \text{fst}(\tau_0) \blacktriangleright \ell_1) (\text{fst}\{\tau_1\} v_0))$
- 6461 (1)  $e_1 = \text{unop}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleright \tau_1 \blacktriangleright \ell_1) v_1))$  and  $v_1 \lesssim v_0$  and  $\tau_1 \leq \tau_0$
- 6462 By  $\lesssim$  on the redex
- 6463 (2)  $e_1 \blacktriangleright_{\mathbb{F}} \text{trace } \bar{b}_0 (\text{stat}(\ell_0 \blacktriangleright \text{fst}(\tau_1) \blacktriangleright \ell_1) (\text{fst}\{\text{fst}(\tau_1)\} v_1))$
- 6464 By (1)
- 6465
- 6466
- 6467
- 6468

- 6469 (3)  $\text{trace } \bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_1) \blacktriangleleft \ell_1) (\text{fst}\{\text{fst}(\tau_1)\} v_1)) \lesssim$   
6470  $\text{trace } \bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \text{fst}(\tau_0) \blacktriangleleft \ell_1) (\text{fst}\{\tau_1\} v_0))$   
6471  $\text{By } \text{fst}(\tau_1) \leqslant \text{fst}(\tau_0)$
- 6472 **Case:**  $\text{snd}\{\mathcal{U}\}(\mathbb{T} \bar{b}_0(\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) \blacktriangleright_{\mathbb{A}} \text{trace } \bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) (\text{snd}\{\tau_1\} v_0))$
- 6473 (1)  $e_1 = \text{unop}\{\mathcal{U}\}(\mathbb{T} \bar{b}_0(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1))$  and  $v_1 \lesssim v_0$  and  $\tau_1 \leqslant \tau_0$   
6474  $\text{By } \lesssim \text{ on the redex}$
- 6475 (2)  $e_1 \blacktriangleright_{\mathbb{F}} \text{trace } \bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_1) \blacktriangleleft \ell_1) (\text{snd}\{\text{snd}(\tau_1)\} v_1))$   
6476  $\text{By (1)}$
- 6477 (3)  $\text{trace } \bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_1) \blacktriangleleft \ell_1) (\text{snd}\{\text{snd}(\tau_1)\} v_1)) \lesssim$   
6478  $\text{trace } \bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \text{snd}(\tau_0) \blacktriangleleft \ell_1) (\text{snd}\{\tau_1\} v_0))$   
6479  $\text{By } \text{snd}(\tau_1) \leqslant \text{snd}(\tau_0)$
- 6480 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{A}} \text{TagErr}$
- 6481 (1)  $e_1 = \text{binop}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim v_0$  and  $v_3 \lesssim v_1$   
6482  $\text{By } \lesssim \text{ on the redex}$
- 6483 (2)  $\delta(\text{binop}, v_2, v_3)$  is undefined  
6484  $\text{By (1)}$
- 6485 (3)  $\text{TagErr} \lesssim \text{TagErr}$
- 6486 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{A}} \delta(\text{binop}, v_2, v_3)$
- 6487 (1)  $e_1 = \text{binop}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim v_0$  and  $v_3 \lesssim v_1$   
6488  $\text{By } \lesssim \text{ on the redex}$
- 6489 (2)  $\delta(\text{binop}, \text{rem-trace}(v_2), \text{rem-trace}(v_3))$  is defined  
6490  $\text{By (1)}$
- 6491 (3)  $\delta(\text{binop}, \text{rem-trace}(v_2), \text{rem-trace}(v_3)) \lesssim \delta(\text{binop}, \text{rem-trace}(v_0), \text{rem-trace}(v_1))$   
6492  $\text{By } \delta$
- 6493 **Case:**  $\text{app}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_{\mathbb{A}} \text{TagErr}$
- 6494 (1)  $e_1 = \text{app}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim v_0$  and  $v_3 \lesssim v_1$   
6495  $\text{By } \lesssim \text{ on the redex}$
- 6496 (2)  $\text{rem-trace}(v_2) \notin \lambda x. e \cup \mathbb{G} b v$   
6497  $\text{By (1)}$
- 6498 (3)  $\text{TagErr} \lesssim \text{TagErr}$
- 6499 **Case:**  $\text{app}\{\mathcal{U}\}(\mathbb{T} \bar{b}_0(\lambda x_0. e_0)) v_0 \blacktriangleright_{\mathbb{A}} \text{trace } \bar{b}_0(e_0[x_0 \leftarrow v_1])$
- 6500 (1)  $e_1 = \text{app}\{\mathcal{U}\} v_1 v_2$  and  $v_1 \lesssim (\mathbb{T} \bar{b}_0(\lambda x_0. e_4))$  and  $v_2 \lesssim v_0$   
6501  $\text{By } \lesssim \text{ on the redex}$
- 6502 (2)  $v_1 = (\mathbb{T} \bar{b}_0(\lambda x_0. e_5))$   
6503  $\text{By (1)}$
- 6504 (3)  $\text{trace } \bar{b}_0(e_5[x_0 \leftarrow v_2]) \lesssim \text{trace } \bar{b}_0(e_4[x_0 \leftarrow v_1])$
- 6505 **Case:**  $\text{app}\{\mathcal{U}\}(\mathbb{T} \bar{b}_0(\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) v_1 \blacktriangleright_{\mathbb{A}}$   
6506  $\text{trace } \bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\tau_2\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_2)))$
- 6507 (1)  $e_1 = \text{app}\{\mathcal{U}\} v_2 v_3$  and  $v_2 \lesssim (\mathbb{T} \bar{b}_0(\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0))$  and  $v_3 \lesssim v_1$   
6508  $\text{By } \lesssim \text{ on the redex}$
- 6509 (2)  $v_2 = \mathbb{T} \bar{b}_0(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_4)$  and  $\tau_1 \leqslant \tau_0$   
6510  $\text{By (1)}$
- 6511 (3)  $e_1 \blacktriangleright_{\mathbb{F}} \text{trace } \bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_3)))$   
6512  $\text{By (2)}$
- 6513 (4)  $\text{trace } \bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_1) \blacktriangleleft \ell_1) (\text{app}\{\mathcal{U}\} v_4 (\text{stat}(\ell_1 \blacktriangleleft \text{dom}(\tau_1) \blacktriangleleft \ell_0) v_3))) \lesssim$   
6514  $\text{trace } \bar{b}_0(\text{stat}(\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\tau_2\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) v_2)))$   
6515  $\text{By } \tau_1 \leqslant \tau_0$
- 6516
- 6517

6518 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{A}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
6519 (1)  $e_1 = \text{stat}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1$  and  $v_1 \lesssim v_0$  and  $\tau_1 \leq \tau_0$   
6520 By  $\lesssim$   
6521 (2) Either  $e_1 \blacktriangleright_{\mathbb{F}} \mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1$  or  $e_1 \blacktriangleright_{\mathbb{F}} \text{BoundaryErr}(\bar{b}, v)$   
6522 By  $\blacktriangleright_{\mathbb{F}}$   
6523 (3)  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_1 \lesssim \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
6524 By (1)  
6525 **Case:**  $\text{stat } b_0 (\mathbb{G} b_1 (\mathbb{T} \bar{b}_0 v_0)) \blacktriangleright_{\mathbb{A}} \text{trace}(b_0 b_1 \bar{b}_0) v_0$   
6526 (1)  $e_1 = \text{stat } b_2 (\mathbb{G} b_3 (\mathbb{T} \bar{b}_1 v_1))$  and  $v_1 \lesssim v_0$  and  $\tau_1 \leq \tau_0$  and  $b_2 \lesssim b_0$  and  $b_3 \lesssim b_1$   
6527 By  $\lesssim$   
6528 (2) Either  $e_1 \blacktriangleright_{\mathbb{F}} \text{trace}(b_2 b_3 \bar{b}_1) v_1$  or  $e_1 \blacktriangleright_{\mathbb{F}} \text{BoundaryErr}(\bar{b}, v)$   
6529 By  $\blacktriangleright_{\mathbb{F}}$   
6530 (3)  $\text{trace}(b_2 b_3 \bar{b}_1) v_1 \lesssim \text{trace}(b_0 b_1 \bar{b}_0) v_0$   
6531 By (1)  
6532 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0 \blacktriangleright_{\mathbb{A}} i_0$   
6533 (1)  $e_1 = \text{stat}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) i_1$  and  $i_1 \lesssim i_0$  and  $\tau_1 \leq \tau_0$   
6534 By  $\lesssim$   
6535 (2) Either  $e_1 \blacktriangleright_{\mathbb{F}} i_1$  or  $e_1 \blacktriangleright_{\mathbb{F}} \text{BoundaryErr}(\bar{b}, i)$   
6536 By  $\blacktriangleright_{\mathbb{F}}$  and  $\tau_1 \leq \tau_0$   
6537 (3)  $i_1 \lesssim i_0$   
6538 By (1)  
6539 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_{\mathbb{A}} \text{InvariantErr}$   
6540 Impossible, by type soundness  
6541 **Case:**  $\text{trace } \bar{b}_0 v_0 \blacktriangleright_{\mathbb{A}} v_1$   
6542 (1)  $e_1 = \text{trace } \bar{b}_1 v_1$   
6543 By  $\lesssim$   
6544 (2)  $e_1 \blacktriangleright_{\mathbb{A}} \text{add-trace}(\bar{b}_1, v_1)$   
6545 By  $\blacktriangleright_{\mathbb{A}}$   
6546 (3)  $\text{add-trace}(\bar{b}_1, v_1) \lesssim \text{add-trace}(\bar{b}_0, v_0)$   
6547 By (1)  
6548  
6549  
6550

□

LEMMA A.39.

6551 If  $\text{wfr}_{FT}(e_0, e_1)$  and  $e_0 \lesssim e_1$  and either  $e_0 \rightarrow_{\mathbb{F}} e_2$  or  $e_1 \rightarrow_{\mathbb{A}} e_3$  then the following results hold:

- 6553 •  $e_0 = E_0[e_4]$
- 6554 •  $e_1 = E_1[e_5]$
- 6555 •  $E_0 \lesssim E_1$
- 6556 •  $e_4 \lesssim e_5$ .

6557 PROOF. By lemma A.40 and lemma A.41.  
6558

□

LEMMA A.40.

6560 If  $\text{wfr}_{FT}(E_0[e_0], e_1)$  and  $E_0[e_0] \lesssim e_1$  and  $e_0 (\blacktriangleright_{\mathbb{F}} \cup \blacktriangleright_{\mathbb{F}}) e_2$  then the following results hold:

- 6561 •  $e_1 = E_1[e_3]$
- 6562 •  $E_0 \lesssim E_1$
- 6563 •  $e_0 \lesssim e_3$ .

6565 PROOF. By induction on  $E_0[e_0] \lesssim e_1$ , proceeding by case analysis of  $E_0[e_0]$ .  
6566

□

6567 LEMMA A.41.

6568 *If  $\text{wfr}_{FT}(e_0, E_1[e_1])$  and  $e_0 \lesssim E_1[e_1]$  and  $e_1 (\triangleright_A \cup \blacktriangleright_A) e_3$  then the following results hold:*

- 6569 •  $e_0 = E_0[e_2]$
- 6570 •  $E_0 \lesssim E_1$
- 6571 •  $e_2 \lesssim e_1$ .

6572 PROOF. By induction on  $e_0 \lesssim E_1[e_1]$ , proceeding by case analysis of  $E_1[e_1]$ . □

6574 LEMMA A.42.

6575 *If  $E_0 \lesssim E_1$  and  $e_2 \lesssim e_3$  then  $E_0[e_2] \lesssim E_1[e_3]$ .*

6576 PROOF. By induction on  $E_0 \lesssim E_1$ . □

6578

6579

6580

6581

6582

6583

6584

6585

6586

6587

6588

6589

6590

6591

6592

6593

6594

6595

6596

6597

6598

6599

6600

6601

6602

6603

6604

6605

6606

6607

6608

6609

6610

6611

6612

6613

6614

6615

6616 **A.6 Erasure**6617 LEMMA A.43 (ERASURE TYPE PROGRESS). *If  $\cdot \vdash_0 E_0[e_0] : \mathcal{U}$  then one of the following holds:*

- 6618 •  $e_0 \in v \cup \text{Err}$
- 6619 •  $\exists e_1. e_0 \triangleright_E e_1$

6620 PROOF. By unique decomposition (lemma 6.1) and case analysis:

6621 **Case:**  $\cdot \vdash_1 i : \mathcal{U}$ 

6622 Immediate.

6623 **Case:**  $\cdot \vdash_1 \lambda(x_0 : \tau_0). e_0 : \mathcal{U}$ 

6624 Immediate.

6625 **Case:**  $\cdot \vdash_1 \lambda x_0. e_0 : \mathcal{U}$ 

6626 Immediate.

6627 **Case:**  $\cdot \vdash_1 \langle v_0, v_1 \rangle : \mathcal{U}$ 

6628 Immediate.

6629 **Case:**  $\cdot \vdash_1 \text{unop}\{\mathcal{U}\} v_0 : \mathcal{U}$ 6630 -  $\triangleright_E \delta(\text{unop}, v_0)$  if defined6631 -  $\triangleright_E \text{Err}$  otherwise6632 **Case:**  $\cdot \vdash_1 \text{binop}\{\mathcal{U}\} v_0 v_1 : \mathcal{U}$ 6633 -  $\triangleright_E \delta(\text{binop}, v_0, v_1)$  if defined6634 -  $\triangleright_E \text{Err}$  otherwise6635 **Case:**  $\cdot \vdash_1 \text{app}\{\mathcal{U}\} v_0 v_1 : \mathcal{U}$ 6636 -  $\triangleright_E e_1[x_0 \leftarrow v_1]$ 6637 if  $v_0 = \lambda(x_0 : \tau_0). e_1$ 6638 -  $\triangleright_E e_1[x_0 \leftarrow v_1]$ 6639 if  $v_0 = \lambda x_0. e_1$ 6640 -  $\triangleright_E \text{Err}$  otherwise6641 **Case:**  $\cdot \vdash_1 \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 : \mathcal{U}$ 6642 -  $\triangleright_E v_0$ 6643 **Case:**  $\cdot \vdash_1 \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 : \mathcal{U}$ 6644 -  $\triangleright_E v_0$ 6645 **Case:**  $\cdot \vdash_1 \text{Err} : \mathcal{U}$ 

6646 Immediate.

6647

6648

6649

6650

6651

6652

6653

6654

6655

6656

6657

6658

6659

6660

6661

6662

6663

6664

□



6665 LEMMA A.44 (ERASURE TYPE PRESERVATION).

6666 *If  $\cdot \vdash_0 e_0 : \mathcal{U}$  and  $e_0 \triangleright_E e_1$  then  $\cdot \vdash_0 e_1 : \mathcal{U}$ .*

6667 PROOF. By case analysis of the reduction relation.

6668 **Case:**  $unop\{\tau_0\} v_0 \triangleright_E \text{BoundaryErr}(\emptyset, v_0)$   
 6669 Immediate.

6670 **Case:**  $unop\{\mathcal{U}\} v_0 \triangleright_E \text{TagErr}$   
 6671 Immediate.

6672 **Case:**  $unop\{\tau/\mathcal{U}\} v_0 \triangleright_E \delta(unop, v_0)$   
 6673 Immediate.

6674 **Case:**  $binop\{\tau_0\} v_0 v_1 \triangleright_E \text{BoundaryErr}(\emptyset, v_0)$   
 6675 Immediate.

6676 **Case:**  $binop\{\tau_0\} v_0 v_1 \triangleright_E \text{BoundaryErr}(\emptyset, v_1)$   
 6677 Immediate.

6678 **Case:**  $binop\{\mathcal{U}\} v_0 v_1 \triangleright_E \text{TagErr}$   
 6679 Immediate.

6680 **Case:**  $binop\{\tau/\mathcal{U}\} v_0 v_1 \triangleright_E \delta(binop, v_0, v_1)$   
 6681 Immediate.

6682 **Case:**  $app\{\tau_0\} v_0 v_1 \triangleright_E \text{BoundaryErr}(\emptyset, v_0)$   
 6683 Immediate.

6684 **Case:**  $app\{\mathcal{U}\} v_0 v_1 \triangleright_E \text{TagErr}$   
 6685 Immediate.

6686 **Case:**  $app\{\tau/\mathcal{U}\} (\lambda(x_0 : \tau_0). e_0) v_0 \triangleright_E e_0[x_0 \leftarrow v_0]$   
 6687 By a substitution lemma for the erased syntax.

6688 **Case:**  $app\{\tau/\mathcal{U}\} (\lambda x_0. e_0) v_0 \triangleright_E e_0[x_0 \leftarrow v_0]$   
 6689 By a substitution lemma for the erased syntax.

6690 **Case:**  $dyn(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_E v_0$   
 6691 Immediate.

6692 **Case:**  $stat(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_E v_0$   
 6693 Immediate.

6694 □

6695

6696

6697

6698

6699

6700

6701

6702

6703

6704

6705

6706

6707

6708

6709

6710

6711

6712

6713

6714 LEMMA A.45 ( $A \lesssim E$ ).

6715 *There is a stuttering simulation between Amnesic and Erasure. More precisely, the following two results*  
 6716 *hold:*

- 6717 • If  $e_0 \lesssim e_2$  and  $e_0 \rightarrow_A e_1$  then  $\exists e_3, e_4$  such that  $e_1 \rightarrow_A^* e_3$  and  $e_2 \rightarrow_E e_4$  and  $e_3 \lesssim e_4$ .
- 6718 • If  $e_0 \lesssim e_2$  and  $e_2 \rightarrow_E e_3$  then  $\exists e_1$  and  $e_0 \rightarrow_A^* e_1$  and  $e_1 \lesssim e_4$

6720 PROOF. By lemma A.46 and lemma A.47. □

6721  $\boxed{\text{wfr}_{AE}(e_0, e_1)}$  holds for well-formed residuals of a common term; that is, pairs such that there  
 6722 exists an  $e_2$  where  $e_2 : \tau/\mathcal{U}$  wf and  $e_2 \rightarrow_A^* e_0$  and  $e_2 \rightarrow_E^* e_1$   
 6723

6724 LEMMA A.46.

6725 *If  $\text{wfr}_{AE}(e_0, e_2)$  and  $e_0 \lesssim e_2$  and  $e_0 \rightarrow_A e_1$  then  $\exists e_3, e_4$  such that  $e_1 \rightarrow_A^* e_3$  and  $e_2 \rightarrow_E^* e_4$  and  $e_3 \lesssim e_4$ .*

6727 PROOF. By lemma A.48, lemma A.51, and case analysis of  $\triangleright_A \cup \blacktriangleright_A$ .

6728 **Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_A \text{InvariantErr}$

6729 Impossible, by type soundness

6730 **Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_A \delta(\text{unop}, v_0)$

6731 (1)  $e_2 \rightarrow_E \delta(\text{unop}, v_1)$

6732 By  $\lesssim$  on the redex

6733 (2)  $\delta(\text{unop}, v_0) \lesssim \delta(\text{unop}, v_1)$

6734 By (1)

6735 **Case:**  $\text{fst}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \triangleright_A \text{dyn } b_0 (\text{fst}\{\mathcal{U}\} v_0)$

6736 Immediate,  $\text{dyn } b_0 (\text{fst}\{\mathcal{U}\} v_0) \lesssim e_2$

6737 **Case:**  $\text{snd}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \triangleright_A \text{dyn } b_0 (\text{snd}\{\mathcal{U}\} v_0)$

6738 Immediate,  $\text{dyn } b_0 (\text{snd}\{\mathcal{U}\} v_0) \lesssim e_2$

6739 **Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_A \text{InvariantErr}$

6740 Impossible, by type soundness

6741 **Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_A \delta(\text{binop}, v_0, v_1)$

6742 (1)  $e_2 \rightarrow_E \delta(\text{binop}, v_2, v_3)$

6743 By  $\lesssim$  on the redex

6744 (2)  $\delta(\text{binop}, v_0, v_1) \lesssim \delta(\text{binop}, v_2, v_3)$

6745 By (1)

6746 **Case:**  $\text{app}\{\tau_0\} v_0 v_1 \triangleright_A \text{InvariantErr}$

6747 Impossible, by type soundness

6748 **Case:**  $\text{app}\{\tau_0\} (\lambda(x_0 : \tau_1). e_5) v_0 \triangleright_A e_5[x_0 \leftarrow v_0]$

6749 (1)  $e_2 = \text{app}\{\tau_0\} (\lambda(x_0 : \tau_1). e_6) v_1$

6750 By  $\lesssim$  on the redex

6751 (2)  $e_5[x_0 \leftarrow v_0] \lesssim e_6[x_0 \leftarrow v_1]$

6752 **Case:**  $\text{app}\{\tau_0\} (\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) v_1 \triangleright_A \text{dyn } b_0 (\text{app}\{\mathcal{U}\} v_0 (\text{stat } b_1 v_1))$

6753 (1)  $e_1 = \text{app}\{\tau_0\} v_2 v_3$  where  $(\mathbb{G}(\ell_0 \blacktriangleleft \tau_1 \blacktriangleleft \ell_1) v_0) \lesssim v_2$  and  $v_1 \lesssim v_3$

6754 By  $\lesssim$  on the redex

6755 (2)  $\text{stat } b_1 v_1 \blacktriangleright_A v_4$  and  $v_4 \lesssim v_3$

6756 By type soundness

6757 (3)  $\text{dyn } b_0 (\text{app}\{\mathcal{U}\} v_0 v_4) \lesssim \text{app}\{\tau_0\} v_2 v_3$

6758 By (1) and (2)

6759 **Case:**  $\text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_A \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$

6760 (1) Either  $e_2 = v_1$  or  $e_2 = \text{dyn } (\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $e_2 \triangleright_E v_1$

6761 By  $\lesssim$  on the redex

6762

6763 (2)  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \lesssim v_1$   
6764 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) (\mathbb{T}_? \bar{b}_0 i_0) \triangleright_A i_0$   
6765 (1) Either  $e_2 = v_1$  or  $e_2 = \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $e_2 \triangleright_E v_1$   
6766 By  $\lesssim$  on the redex  
6767 (2)  $i_0 \lesssim v_1$   
6768 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_A \text{BoundaryErr}((\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) \bar{b}_0, v_0)$   
6769 Immediate.  
6770 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_A \text{TagErr}$   
6771 (1)  $e_2 \rightarrow_E \text{BoundaryErr}(\bar{b}, v)$   
6772 By  $\lesssim$  on the redex  
6773 (2)  $\text{TagErr} \lesssim \text{BoundaryErr}(\bar{b}, v)$   
6774 **Case:**  $\text{unop}\{\mathcal{U}\} v_0 \blacktriangleright_A \text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, \text{rem-trace}(v_0)))$   
6775 (1)  $e_2 \rightarrow_E \delta(\text{unop}, v_1)$   
6776 By  $\lesssim$  on the redex  
6777 (2)  $\text{add-trace}(\text{get-trace}(v_0), \delta(\text{unop}, \text{rem-trace}(v_0))) \lesssim \delta(\text{unop}, v_1)$   
6778 By (1)  
6779 **Case:**  $\text{fst}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) \blacktriangleright_A \text{trace } \bar{b}_0 (\text{stat } b_0 (\text{fst}\{\tau_1\} v_0))$   
6780 Immediate,  $\text{trace } \bar{b}_0 (\text{stat } b_0 (\text{fst}\{\tau_1\} v_0)) \lesssim e_2$   
6781 **Case:**  $\text{snd}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) \blacktriangleright_A \text{trace } \bar{b}_0 (\text{stat } b_0 (\text{snd}\{\tau_1\} v_0))$   
6782 Immediate,  $\text{trace } \bar{b}_0 (\text{stat } b_0 (\text{snd}\{\tau_1\} v_0)) \lesssim e_2$   
6783 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_A \text{TagErr}$   
6784 (1)  $e_2 \rightarrow_E \text{BoundaryErr}(\bar{b}, v)$   
6785 By  $\lesssim$  on the redex  
6786 (2)  $\text{TagErr} \lesssim \text{BoundaryErr}(\bar{b}, v)$   
6787 **Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_A \delta(\text{binop}, \text{rem-trace}(v_0), \text{rem-trace}(v_1))$   
6788 (1)  $e_2 \rightarrow_E \delta(\text{binop}, v_2, v_3)$   
6789 By  $\lesssim$  on the redex  
6790 (2)  $\delta(\text{binop}, \text{rem-trace}(v_0), \text{rem-trace}(v_1)) \lesssim \delta(\text{binop}, v_2, v_3)$   
6791 By (1)  
6792 **Case:**  $\text{app}\{\mathcal{U}\} v_0 v_1 \blacktriangleright_A \text{TagErr}$   
6793 (1)  $e_2 \rightarrow_E \text{BoundaryErr}(\bar{b}, v)$   
6794 By  $\lesssim$  on the redex  
6795 (2)  $\text{TagErr} \lesssim \text{BoundaryErr}(\bar{b}, v)$   
6796 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\lambda x_0. e_5)) v_0 \blacktriangleright_A \text{trace } \bar{b}_0 (e_5[x_0 \leftarrow v_1])$   
6797 (1)  $e_2 = \text{app}\{\text{tdyn}\} (\lambda x_0. e_6) v_1$   
6798 By  $\lesssim$  on the redex  
6799 (2)  $e_5[x_0 \leftarrow v_0] \lesssim e_6[x_0 \leftarrow v_1]$   
6800 **Case:**  $\text{app}\{\mathcal{U}\} (\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) v_1 \blacktriangleright_A$   
6801  $\text{trace } \bar{b}_0 (\text{stat } (\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 (\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) \text{add-trace}(\text{rev}(\bar{b}_0), v_1))))$   
6802 (1)  $e_2 = \text{app}\{\text{tdyn}\} v_2 v_3$  and  $(\mathbb{T}_? \bar{b}_0 (\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0)) \lesssim v_2$  and  $v_1 \lesssim v_3$   
6803 By  $\lesssim$  on the redex  
6804 (2)  $\text{dyn}(\ell_1 \blacktriangleleft \text{dom}(\tau_0) \blacktriangleleft \ell_0) \text{add-trace}(\text{rev}(\bar{b}_0), v_1)$  steps to either a boundary error or to  $v_4$  where  
6805  $v_4 \lesssim v_3$   
6806 By (1)  
6807 (3)  $\text{trace } \bar{b}_0 (\text{stat } (\ell_0 \blacktriangleleft \text{cod}(\tau_0) \blacktriangleleft \ell_1) (\text{app}\{\text{cod}(\tau_0)\} v_0 v_4)) \lesssim \text{app}\{\mathcal{U}\} v_2 v_3$   
6808 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_A \mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0$   
6809  
6810  
6811

6812 (1) Either  $e_1 = v_1$  or  $e_1 = \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $e_1 \triangleright_E v_1$

6813 By  $\lesssim$  on the redex

6814 (2)  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \lesssim v_1$

6815 **Case:**  $\text{stat } b_0 (\mathbb{G} b_1 (\mathbb{T} \bar{b}_0 v_0)) \blacktriangleright_A \text{trace}(b_0 b_1 \bar{b}_0) v_0$

6816 (1) Either  $e_1 = v_1$  or  $e_1 = \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $e_1 \triangleright_E v_1$

6817 By  $\lesssim$  on the redex

6818 (2)  $\mathbb{G}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \lesssim v_1$

6819 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) i_0 \blacktriangleright_A i_0$

6820 (1) Either  $e_1 = v_1$  or  $e_1 = \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  and  $e_1 \triangleright_E v_1$

6821 By  $\lesssim$  on the redex

6822 (2)  $i_0 \lesssim v_1$

6823 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \blacktriangleright_A \text{InvariantErr}$

6824 Impossible, by type soundness

6825 **Case:**  $\text{trace } \bar{b}_0 v_0 \blacktriangleright_A v_1$

6826 Immediate,  $v_1 \lesssim e_2$

6827

6828

6829

6830

6831

6832

6833

6834

6835

6836

6837

6838

6839

6840

6841

6842

6843

6844

6845

6846

6847

6848

6849

6850

6851

6852

6853

6854

6855

6856

6857

6858

6859

6860

□

LEMMA A.47.

If  $\text{wfr}_{AE}(e_0, e_2)$  and  $e_0 \leq e_2$  and  $e_2 \rightarrow_E e_3$  then  $\exists e_1$  and  $e_0 \rightarrow_A^* e_1$  and  $e_1 \leq e_4$

PROOF. By lemma A.48, lemma A.51, and case analysis of  $\triangleright_E$ .

**Case:**  $\text{unop}\{\tau_0\} v_0 \triangleright_E \text{BoundaryErr}(\emptyset, v_0)$

(1) Either  $e_0 \rightarrow_A^* \text{unop}\{\tau_0\} v_1$  or  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$

By  $\leq$  on the redex

(2)  $v_1 \notin \langle v, v \rangle \cup (\mathbb{G}(\ell \blacktriangleleft (\tau \times \tau) \blacktriangleleft \ell) v)$

By  $\leq$  on the redex and (1)

(3) But (2) is impossible by type soundness. Amnesic must raise a boundary error earlier.

**Case:**  $\text{unop}\{\mathcal{U}\} v_0 \triangleright_E \text{TagErr}$

(1) Either  $e_0 \rightarrow_A^* \text{unop}\{\tau_0\} v_1$  or  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$

By  $\leq$  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  $\leq$  on the redex and (1)

(3)  $\text{TagErr} \leq \text{TagErr}$

**Case:**  $\text{unop}\{\tau/\mathcal{U}\} v_0 \triangleright_E \delta(\text{unop}, v_0)$

(1) Either  $e_0 \rightarrow_A^* \text{unop}\{\tau_0\} v_1$  or  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$

By  $\leq$  on the redex ( $e_0$  is either a unop or a trace expression)

(2)  $\text{unop}\{\tau_0\} v_1 \rightarrow_A^* E_2[\text{unop}\{\tau_0\} \langle v_2, v_3 \rangle]$  and  $E_2$  contains only trace expressions and boundaries

By  $\rightarrow_A^*$

(3) Either  $E_2[\text{unop}\{\tau_0\} \langle v_2, v_3 \rangle] \rightarrow_A^* v_4$  where  $v_4 \leq \delta(\text{unop}, v_0)$  or  $E_2[\text{unop}\{\tau_0\} \langle v_2, v_3 \rangle] \rightarrow_A^*$

$\text{BoundaryErr}(\bar{b}, v)$

**Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_E \text{BoundaryErr}(\emptyset, v_0)$

(1)  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$

By type soundness

**Case:**  $\text{binop}\{\tau_0\} v_0 v_1 \triangleright_E \text{BoundaryErr}(\emptyset, v_1)$

(1)  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$

By type soundness

**Case:**  $\text{binop}\{\mathcal{U}\} v_0 v_1 \triangleright_E \text{TagErr}$

(1) Either  $e_0 \rightarrow_A^* \text{binop}\{\mathcal{U}\} v_2 v_3$  or  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$

By  $\leq$  on the redex ( $e_0$  is either a binop or a trace expression)

(2)  $\text{TagErr} \leq \text{BoundaryErr}(\bar{b}, v)$

**Case:**  $\text{binop}\{\tau/\mathcal{U}\} v_0 v_1 \triangleright_E \delta(\text{binop}, v_0, v_1)$

(1) Either  $e_0 \rightarrow_A^* \text{binop}\{\tau/\mathcal{U}\} v_2 v_3$  or  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$

By  $\leq$  on the redex ( $e_0$  is either a binop or a trace expression)

(2)  $\delta(\text{binop}, v_2, v_3) \leq \delta(\text{binop}, v_0, v_1)$

**Case:**  $\text{app}\{\tau_0\} v_0 v_1 \triangleright_E \text{BoundaryErr}(\emptyset, v_0)$

(1)  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$

By type soundness

**Case:**  $\text{app}\{\mathcal{U}\} v_0 v_1 \triangleright_E \text{TagErr}$

(1) Either  $e_0 \rightarrow_A^* \text{TagErr}$  or  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$

By  $\leq$  on the redex

(2)  $\text{TagErr} \leq \text{TagErr}$

**Case:**  $\text{app}\{\tau_0\} (\lambda(x_0 : \tau_0). e_0) v_0 \triangleright_E e_0[x_0 \leftarrow v_0]$

6861

6862

6863

6864

6865

6866

6867

6868

6869

6870

6871

6872

6873

6874

6875

6876

6877

6878

6879

6880

6881

6882

6883

6884

6885

6886

6887

6888

6889

6890

6891

6892

6893

6894

6895

6896

6897

6898

6899

6900

6901

6902

6903

6904

6905

6906

6907

6908

6909

- 6910 (1) Either  $e_0 \rightarrow_A^* \text{app}\{\tau_0\} v_1 v_2$  or  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$   
 6911 By  $\lesssim$  on the redex
- 6912 (2)  $e_0 \rightarrow_A^* E_2[\text{app}\{\tau_0\}(\lambda(x_0 : \tau_0). e_1) E_3[v_2]]$  and both  $E_2$  and  $E_3$  contain only trace expressions  
 6913 and boundaries
- 6914 (3) Either  $E_3[v_2] \rightarrow_A^* v_4$  where  $v_4 \lesssim v_0$  or  $E_3[v_2] \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$   
 6915 (4)  $E_2[e_1[x_0 \leftarrow v_4]] \lesssim e_0[x_0 \leftarrow v_0]$
- 6916 **Case:**  $\text{app}\{\mathcal{U}\}(\lambda(x_0 : \tau_0). e_0) v_0 \triangleright_E e_0[x_0 \leftarrow v_0]$
- 6917 (1) Either  $e_0 \rightarrow_A^* \text{app}\{\tau_0\} v_1 v_2$  or  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$   
 6918 By  $\lesssim$  on the redex
- 6919 (2)  $e_0 \rightarrow_A^* E_2[\text{app}\{\tau_0\}(\lambda(x_0 : \tau_0). e_1) E_3[v_2]]$  and both  $E_2$  and  $E_3$  contain only trace expressions  
 6920 and boundaries
- 6921 (3) Either  $E_3[v_2] \rightarrow_A^* v_4$  where  $v_4 \lesssim v_0$  or  $E_3[v_2] \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$   
 6922 (4)  $E_2[e_1[x_0 \leftarrow v_4]] \lesssim e_0[x_0 \leftarrow v_0]$
- 6923 **Case:**  $\text{app}\{\tau_0\}(\lambda x_0. e_0) v_0 \triangleright_E e_0[x_0 \leftarrow v_0]$
- 6924 (1) Either  $e_0 \rightarrow_A^* \text{app}\{\tau_0\} v_1 v_2$  or  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$   
 6925 By  $\lesssim$  on the redex
- 6926 (2)  $e_0 \rightarrow_A^* E_2[\text{app}\{\tau_0\}(\lambda x_0. e_1) E_3[v_2]]$  and both  $E_2$  and  $E_3$  contain only trace expressions and  
 6927 boundaries
- 6928 (3) Either  $E_3[v_2] \rightarrow_A^* v_4$  where  $v_4 \lesssim v_0$  or  $E_3[v_2] \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$   
 6929 (4)  $E_2[e_1[x_0 \leftarrow v_4]] \lesssim e_0[x_0 \leftarrow v_0]$
- 6930 **Case:**  $\text{app}\{\mathcal{U}\}(\lambda x_0. e_0) v_0 \triangleright_E e_0[x_0 \leftarrow v_0]$
- 6931 (1) Either  $e_0 \rightarrow_A^* \text{app}\{\tau_0\} v_1 v_2$  or  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$   
 6932 By  $\lesssim$  on the redex
- 6933 (2)  $e_0 \rightarrow_A^* E_2[\text{app}\{\tau_0\}(\lambda x_0. e_1) E_3[v_2]]$  and both  $E_2$  and  $E_3$  contain only trace expressions and  
 6934 boundaries
- 6935 (3) Either  $E_3[v_2] \rightarrow_A^* v_4$  where  $v_4 \lesssim v_0$  or  $E_3[v_2] \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$   
 6936 (4)  $E_2[e_1[x_0 \leftarrow v_4]] \lesssim e_0[x_0 \leftarrow v_0]$
- 6937 **Case:**  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_E v_0$
- 6938 (1) Either  $e_0 \rightarrow_A^* \text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  or  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$   
 6939 (2) Either  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1 \rightarrow_A^* v_2$  or  $\text{dyn}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$   
 6940 (3)  $v_2 \lesssim v_0$
- 6941 **Case:**  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_0 \triangleright_E v_0$
- 6942 (1) Either  $e_0 \rightarrow_A^* \text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1$  or  $e_0 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$   
 6943 (2) Either  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1 \rightarrow_A^* v_2$  or  $\text{stat}(\ell_0 \blacktriangleleft \tau_0 \blacktriangleleft \ell_1) v_1 \rightarrow_A^* \text{BoundaryErr}(\bar{b}, v)$   
 6944 (3)  $v_2 \lesssim v_0$

□

LEMMA A.48.

6950 If  $\text{wfr}_{AE}(e_0, e_1)$  and  $e_0 \lesssim e_1$  and either  $e_0 \rightarrow_A e_2$  or  $e_1 \rightarrow_E e_3$  then the following results hold:

- 6951 •  $e_0 = E_0[e_4]$
- 6952 •  $e_1 = E_1[e_5]$
- 6953 •  $E_0 \lesssim E_1$
- 6954 •  $e_4 \lesssim e_5$ .

6956 **PROOF.** By lemma A.49 and lemma A.50. □

6959 LEMMA A.49.

6960 *If  $\text{wfr}_{AE}(E_0[e_0], e_1)$  and  $E_0[e_0] \lesssim e_1$  and  $e_0 (\triangleright_A \cup \blacktriangleright_A) e_2$  then the following results hold:*

- 6961 •  $e_1 = E_1[e_3]$
- 6962 •  $E_0 \lesssim E_1$
- 6963 •  $e_0 \lesssim e_3$ .

6964 PROOF. By induction on  $E_0[e_0] \lesssim e_1$ , proceeding by case analysis of  $E_0[e_0]$ . □

6966 LEMMA A.50.

6967 *If  $\text{wfr}_{AE}(e_0, E_1[e_1])$  and  $e_0 \lesssim E_1[e_1]$  and  $e_1 \triangleright_E e_3$  then the following results hold:*

- 6968 •  $e_0 = E_0[e_2]$
- 6969 •  $E_0 \lesssim E_1$
- 6970 •  $e_2 \lesssim e_1$ .

6972 PROOF. By induction on  $e_0 \lesssim E_1[e_1]$ , proceeding by case analysis of  $E_1[e_1]$ . □

6973 LEMMA A.51.

6974 *If  $E_0 \lesssim E_1$  and  $e_2 \lesssim e_3$  then  $E_0[e_2] \lesssim E_1[e_3]$ .*

6976 PROOF. By induction on  $E_0 \lesssim E_1$ . □

6977  
6978  
6979  
6980  
6981  
6982  
6983  
6984  
6985  
6986  
6987  
6988  
6989  
6990  
6991  
6992  
6993  
6994  
6995  
6996  
6997  
6998  
6999  
7000  
7001  
7002  
7003  
7004  
7005  
7006  
7007