

A Spectrum of Soundness and Performance

Supplementary Material

Anonymous Author(s)

CONTENTS

A	Models	2
A.1	Preliminaries	2
A.2	(H) Higher-Order Embedding	3
A.2.1	Higher-Order Definitions	3
A.2.2	Higher-Order Theorems	5
A.2.3	Higher-Order Lemmas	6
A.3	(E) Erasure Embedding	28
A.3.1	Erasure Definitions	28
A.3.2	Erasure Theorems	30
A.3.3	Erasure Lemmas	31
A.4	(1) First-Order Embedding	41
A.4.1	First-Order Definitions	41
A.4.2	First-Order Theorems	44
A.4.3	First-Order Lemmas	45
A.5	(HC) Co-Natural Embedding	76
A.5.1	Co-Natural Definitions	76
A.5.2	Co-Natural Theorems	78
A.5.3	Co-Natural Lemmas	79
A.6	(HF) Forgetful Embedding	86
A.6.1	Forgetful Definitions	86
A.6.2	Forgetful Theorems	89
A.6.3	Forgetful Lemmas	90
A.7	Embeddings Summary	110
A.8	Simulation Lemmas	111
A.8.1	Definitions	111
A.8.2	Theorems	111
A.8.3	Lemmas	111

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

Conference'17, July 2017, Washington, DC, USA

© 2018 Association for Computing Machinery.

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...\$15.00

<https://doi.org/10.1145/nnnnnnnn.nnnnnnnn>

A Models

This section contains full definitions of the languages and full proofs of our claims about each language.

Aside from the common notions in section 1.1, the definition and proofs of each model are independent and self-contained.

A.1 Preliminaries

Definition 1.0 : \rightarrow^* divergence

Given a reduction relation \rightarrow^* , an expression e diverges if for all e' such that $e \rightarrow^* e'$ there exists an e'' such that $e' \rightarrow e''$.

Convention 1.1 : variable convention

All λ -bound variables in an expression are distinct from one another, and from any free variables in the expression.

Assumption 1.2 : \vdash permutation

For all typing judgments and properties \vdash :

- If $x, x', \Gamma \vdash e$ then $x', x, \Gamma \vdash e$
- If $(x:\tau), (x':\tau'), \Gamma \vdash e$ then $(x':\tau'), (x:\tau), \Gamma \vdash e$

Definition 1.3 : \vdash boundary-free

An expression e is *boundary free* if e does not contain a subterm of the form $(\text{dyn } \tau' e')$, nor a subterm of the form $(\text{stat } \tau' e')$.

Notes:

- The upcoming models use a common surface syntax and typing system, but to keep each model self-contained we reprint this system in each definition.
- The proofs are written in a structured style, typically as a list of basic steps where each step is justified by an assumption, a lemma, or a previous step. Lemma names are *italicized* and hyperlinked to the actual lemma.

A.2 (H) Higher-Order Embedding

A.2.1 Higher-Order Definitions

Language H

$e = x \mid v \mid \langle e, e \rangle \mid e e \mid op^1 e \mid op^2 e e \mid$
 $\text{dyn } \tau e \mid \text{stat } \tau e \mid \text{Err}$
 $v = i \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x:\tau). e \mid$
 $\text{mon}(\tau \Rightarrow \tau) v$
 $\tau = \text{Nat} \mid \text{Int} \mid \tau \times \tau \mid \tau \Rightarrow \tau$
 $\Gamma = \cdot \mid x, \Gamma \mid (x:\tau), \Gamma$
 $\text{Err} = \text{BndryErr} \mid \text{TagErr}$
 $r = v \mid \text{Err}$
 $E^\bullet = [] \mid E^\bullet e \mid v E^\bullet \mid \langle E^\bullet, e \rangle \mid \langle v, E^\bullet \rangle \mid$
 $op^1 E^\bullet \mid op^2 E^\bullet e \mid op^2 v E^\bullet$
 $E = E^\bullet \mid E e \mid v E \mid \langle E, e \rangle \mid \langle v, E \rangle \mid op^1 E \mid$
 $op^2 E e \mid op^2 v E \mid \text{dyn } \tau E \mid \text{stat } \tau E$

$\Delta : op^1 \times \tau \longrightarrow \tau$

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

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

$\Delta : op^2 \times \tau \times \tau \longrightarrow \tau$

$\Delta(op^2, \text{Nat}, \text{Nat}) = \text{Nat}$

$\Delta(op^2, \text{Int}, \text{Int}) = \text{Int}$

$\tau \leqslant \tau$

$\text{Nat} \leqslant \text{Int} \quad \frac{\tau'_d \leqslant \tau_d \quad \tau_c \leqslant \tau'_c}{\tau_d \Rightarrow \tau_c \leqslant \tau'_d \Rightarrow \tau'_c} \quad \frac{\tau_0 \leqslant \tau'_0 \quad \tau_1 \leqslant \tau'_1}{\tau_0 \times \tau_1 \leqslant \tau'_0 \times \tau'_1}$

$\frac{\tau \leqslant \tau'}{\tau \leqslant \tau} \quad \frac{\tau \leqslant \tau' \quad \tau' \leqslant \tau''}{\tau \leqslant \tau''}$

$\Gamma \vdash e$

$\frac{x \in \Gamma}{\Gamma \vdash x} \quad \frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e} \quad \frac{}{\Gamma \vdash i} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle}$

$\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1} \quad \frac{\Gamma \vdash e}{\Gamma \vdash op^1 e} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash \text{Err}}$

$\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e}$

$\Gamma \vdash e : \tau$

$\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau} \quad \frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} \quad \frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}}$

$\frac{}{\Gamma \vdash i : \text{Int}} \quad \frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c}$

$\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash op^1 e_0 : \tau} \quad \frac{\Gamma \vdash e_1 : \tau_1 \quad \Delta(op^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash op^2 e_0 e_1 : \tau} \quad \frac{\Gamma \vdash e : \tau' \quad \tau' \leqslant \tau}{\Gamma \vdash e : \tau} \quad \frac{}{\Gamma \vdash \text{Err} : \tau}$

$\frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau}$

$\Gamma \vdash_H e$

$\frac{x \in \Gamma}{\Gamma \vdash_H x} \quad \frac{x, \Gamma \vdash_H e}{\Gamma \vdash_H \lambda x. e} \quad \frac{}{\Gamma \vdash_H i} \quad \frac{\Gamma \vdash_H e_0 \quad \Gamma \vdash_H e_1}{\Gamma \vdash_H \langle e_0, e_1 \rangle}$

$\frac{\Gamma \vdash_H e_0 \quad \Gamma \vdash_H e_1}{\Gamma \vdash_H e_0 e_1} \quad \frac{\Gamma \vdash_H e}{\Gamma \vdash_H op^1 e} \quad \frac{\Gamma \vdash_H e_0 \quad \Gamma \vdash_H e_1}{\Gamma \vdash_H op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash_H \text{Err}}$

$\frac{\Gamma \vdash_H e : \tau}{\Gamma \vdash_H \text{stat } \tau e} \quad \frac{\Gamma \vdash_H v : \tau_d \Rightarrow \tau_c}{\Gamma \vdash_H \text{mon}(\tau_d \Rightarrow \tau_c) v}$

$\Gamma \vdash_H e : \tau$

$\frac{(x:\tau) \in \Gamma}{\Gamma \vdash_H x : \tau} \quad \frac{(x:\tau_d), \Gamma \vdash_H e : \tau_c}{\Gamma \vdash_H \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} \quad \frac{i \in \mathbb{N}}{\Gamma \vdash_H i : \text{Nat}}$

$\frac{}{\Gamma \vdash_H i : \text{Int}} \quad \frac{\Gamma \vdash_H e_0 : \tau_0 \quad \Gamma \vdash_H e_1 : \tau_1}{\Gamma \vdash_H \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma \vdash_H e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash_H e_1 : \tau_d}{\Gamma \vdash_H e_0 e_1 : \tau_c}$

$\frac{\Gamma \vdash_H e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash_H op^1 e_0 : \tau} \quad \frac{\Gamma \vdash_H e_1 : \tau_1 \quad \Delta(op^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash_H op^2 e_0 e_1 : \tau} \quad \frac{\Gamma \vdash_H e : \tau' \quad \tau' \leqslant \tau}{\Gamma \vdash_H e : \tau}$

$\frac{}{\Gamma \vdash_H \text{Err} : \tau} \quad \frac{\Gamma \vdash_H e}{\Gamma \vdash_H \text{dyn } \tau e : \tau}$

$\frac{\Gamma \vdash_H v}{\Gamma \vdash_H \text{mon}(\tau_d \Rightarrow \tau_c) v : (\tau_d \Rightarrow \tau_c)}$

$\delta(op^1, v) = e$

$\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$

$\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$

$\delta(op^2, v, v) = e$
 $\delta(\text{sum}, i_0, i_1) = i_0 + i_1$
 $\delta(\text{quotient}, i_0, 0) = \text{BndryErr}$
 $\delta(\text{quotient}, i_0, i_1) = \lfloor i_0 / i_1 \rfloor$
 if $i_1 \neq 0$
 $\mathcal{D}_H : \tau \times v \longrightarrow e$
 $\mathcal{D}_H(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v$
 if $v = \lambda x. e$ or $v = \text{mon } \tau' v'$
 $\mathcal{D}_H(\tau_0 \times \tau_1, \langle v_0, v_1 \rangle) = \langle \text{dyn } \tau_0 v_0, \text{dyn } \tau_1 v_1 \rangle$
 $\mathcal{D}_H(\text{Int}, i) = i$
 $\mathcal{D}_H(\text{Nat}, i) = i$
 if $i \in \mathbb{N}$
 $\mathcal{D}_H(\tau, v) = \text{BndryErr}$
 otherwise
 $\mathcal{S}_H : \tau \times v \longrightarrow e$
 $\mathcal{S}_H(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v$
 $\mathcal{S}_H(\tau_0 \times \tau_1, \langle v_0, v_1 \rangle) = \langle \text{stat } \tau_0 v_0, \text{stat } \tau_1 v_1 \rangle$
 $\mathcal{S}_H(\text{Int}, v) = v$
 $\mathcal{S}_H(\text{Nat}, v) = v$
 $e \triangleright_{H-S} e$
 $\text{dyn } \tau v \triangleright_{H-S} \mathcal{D}_H(\tau, v)$
 $(\text{mon}(\tau_d \Rightarrow \tau_c) v_f) v \triangleright_{H-S} \text{dyn } \tau_c (v_f (\text{stat } \tau_d v))$
 $(\lambda(x:\tau). e) v \triangleright_{H-S} e[x \leftarrow v]$
 $op^1 v \triangleright_{H-S} \delta(op^1, v)$
 $op^2 v_0 v_1 \triangleright_{H-S} \delta(op^2, v_0, v_1)$
 $e \triangleright_{H-D} e$
 $\text{stat } \tau v \triangleright_{H-D} \mathcal{S}_H(\tau, v)$
 $v_0 v_1 \triangleright_{H-D} \text{TagErr}$
 if $v_0 \in \mathbb{Z}$ or $v_0 = \langle v, v' \rangle$
 $(\text{mon } \tau_d \Rightarrow \tau_c v_f) v \triangleright_{H-D} \text{stat } \tau_c (v_f (\text{dyn } \tau_d v))$
 $(\lambda x. e) v \triangleright_{H-D} e[x \leftarrow v]$
 $op^1 v \triangleright_{H-D} \text{TagErr}$
 if $\delta(op^1, v)$ is undefined
 $op^1 v \triangleright_{H-D} \delta(op^1, v)$
 $op^2 v_0 v_1 \triangleright_{H-D} \text{TagErr}$
 if $\delta(op^2, v_0, v_1)$ is undefined
 $op^2 v_0 v_1 \triangleright_{H-D} \delta(op^2, v_0, v_1)$
 $e \rightarrow_{H-S} e$
 $E^\bullet[e] \rightarrow_{H-S} E^\bullet[e']$
 if $e \triangleright_{H-S} e'$
 $E[\text{stat } \tau E^\bullet[e]] \rightarrow_{H-S} E[\text{stat } \tau E^\bullet[e']]$
 if $e \triangleright_{H-S} e'$
 $E[\text{dyn } \tau E^\bullet[e]] \rightarrow_{H-S} E[\text{dyn } \tau E^\bullet[e']]$
 if $e \triangleright_{H-D} e'$
 $E[\text{Err}] \rightarrow_{H-S} \text{Err}$

$e \rightarrow_{H-D} e$
 $E^\bullet[e] \rightarrow_{H-D} E^\bullet[e']$
 if $e \triangleright_{H-D} e'$
 $E[\text{stat } \tau E^\bullet[e]] \rightarrow_{H-D} E[\text{stat } \tau E^\bullet[e']]$
 if $e \triangleright_{H-S} e'$
 $E[\text{dyn } \tau E^\bullet[e]] \rightarrow_{H-D} E[\text{dyn } \tau E^\bullet[e']]$
 if $e \triangleright_{H-D} e'$
 $E[\text{Err}] \rightarrow_{H-D} \text{Err}$
 $e \rightarrow_{H-S}^* e$ reflexive, transitive closure of \rightarrow_{H-S}
 $e \rightarrow_{H-D}^* e$ reflexive, transitive closure of \rightarrow_{H-D}

A.2.2 Higher-Order Theorems

Theorem 2.0 : static H-soundness

If $\vdash e : \tau$ then $\vdash_H e : \tau$ and one of the following holds:

- $e \rightarrow_{H-S}^* v$ and $\vdash_H v : \tau$
- $e \rightarrow_{H-S}^* E[\text{dyn } \tau' E^*[e']]$ and $e' \triangleright_{H-D} \text{TagErr}$
- $e \rightarrow_{H-S}^* \text{BndryErr}$
- e diverges

Proof:

1. $\vdash_H e : \tau$
by *static subset*
2. QED by *static progress* and *static preservation*.

□

Theorem 2.1 : dynamic H-soundness

If $\vdash e$ then $\vdash_H e$ and one of the following holds:

- $e \rightarrow_{H-D}^* v$ and $\vdash_H v$
- $e \rightarrow_{H-D}^* E[e']$ and $e' \triangleright_{H-D} \text{TagErr}$
- $e \rightarrow_{H-D}^* \text{BndryErr}$
- e diverges

Proof:

1. $\vdash_H e$
by *dynamic subset*
2. QED by *dynamic progress* and *dynamic preservation*.

□

Corollary 2.2 : H static soundness

If $\vdash e : \tau$ and e is boundary-free, then one of the following holds:

- $e \rightarrow_H^* v$ and $\vdash_H v : \tau$
- $e \rightarrow_H^* \text{BndryErr}$
- e diverges

Proof:

Consequence of the proof for *static H-soundness*

□

Corollary 2.3 : H compilation

If $\vdash e : \tau$
and \mathcal{D}'_H extends \mathcal{D}_H with a rule to monitor a typed function:

$\mathcal{D}'_H(\tau_d \Rightarrow \tau_c, \lambda(x:\tau). e) = \text{mon}(\tau_d \Rightarrow \tau_c)(\lambda(x:\tau). e)$

and $\triangleright_{H-D'}$ extends \triangleright_{H-D} with a rule to apply a typed function:

$(\lambda(x:\tau). e) v \triangleright_{H-D'} e[x \leftarrow v]$

and $e \rightarrow_{H-D'} e$ is defined as:

$E[e] \rightarrow_{H-D'} E[e']$

if $e \triangleright_{H-D'} e'$

$E[\text{stat } \tau v] \rightarrow_{H-D'} E[\mathcal{D}'_H(\tau, v)]$

$E[\text{dyn } \tau v] \rightarrow_{H-D'} E[\mathcal{D}'_H(\tau, v)]$

$E[\text{Err}] \rightarrow_{H-D'} \text{Err}$

and $\rightarrow_{H-D'}^*$ is the reflexive transitive closure of $\rightarrow_{H-D'}$

then one of the following holds:

- $e \rightarrow_{H-D'}^* v$ and $\vdash_H v : \tau$
- $e \rightarrow_{H-D'}^* \text{TagErr}$
- $e \rightarrow_{H-D'}^* \text{BndryErr}$
- e diverges

Proof:

By *static H-soundness* and the fact that \mathcal{S}_H and \triangleright_{H-S} are subsets of \mathcal{D}'_H and $\triangleright_{H-D'}$, respectively.

□

A.2.3 Higher-Order Lemmas

Lemma 2.4 : \mathcal{D}_H soundness

If $\vdash_H v$ then $\vdash_H \mathcal{D}_H(\tau, v) : \tau$

Proof:

CASE $\mathcal{D}_H(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v :$

1. $\vdash_H \text{mon}(\tau_d \Rightarrow \tau_c) v : \tau_d \Rightarrow \tau_c$
by $\vdash_H v$

2. QED

CASE $v = \langle v_0, v_1 \rangle$

$\wedge \mathcal{D}_H(\tau_0 \times \tau_1, v) = \langle \text{dyn } \tau_0 v_0, \text{dyn } \tau_1 v_1 \rangle :$

1. $\vdash_H v_0$
 $\wedge \vdash_H v_1$
by *inversion*
2. $\vdash_H \text{dyn } \tau_0 v_0 : \tau_0$
 $\wedge \vdash_H \text{dyn } \tau_1 v_1 : \tau_1$
by (1)
3. QED (2)

CASE $v = i$

$\wedge \mathcal{D}_H(\text{Int}, v) = v :$

1. QED

CASE $v \in \mathbb{N}$

$\wedge \mathcal{D}_H(\text{Nat}, v) = v :$

1. QED

CASE $\mathcal{D}_H(\tau, v) = \text{BndryErr} :$

1. QED

□

Lemma 2.5 : \mathcal{S}_H soundness

If $\vdash_H v : \tau$ then $\vdash_H \mathcal{S}_H(\tau, v)$

Proof:

CASE $\vdash_H v : \tau_d \Rightarrow \tau_c$

$\wedge \mathcal{S}_H(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v :$

1. QED

CASE $\vdash_H v : \tau_0 \times \tau_1$

$\wedge \mathcal{S}_H(\tau_0 \times \tau_1, v) = \langle \text{stat } \tau_0 v_0, \text{stat } \tau_1 v_1 \rangle :$

1. $v = \langle v_0, v_1 \rangle$
by *canonical forms*
2. $\vdash_H v_0 : \tau_0$
 $\wedge \vdash_H v_1 : \tau_1$
by *inversion* (1)
3. $\vdash_H \text{stat } \tau_0 v_0 : \tau_0$
by the induction hypothesis (2)
4. $\vdash_H \text{stat } \tau_1 v_1 : \tau_1$
by the induction hypothesis (2)
5. QED

CASE $\vdash_H v : \text{Int}$

$\wedge \mathcal{S}_H(\text{Int}, v) = v :$

1. QED

CASE $\vdash_H v : \text{Nat}$

$\wedge \mathcal{S}_H(\text{Nat}, v) = v :$

1. QED

□

Lemma 2.6 : \mathcal{H} static subset

If $\Gamma \vdash e : \tau$ then $\Gamma \vdash_H e : \tau$.

Proof:

By structural induction on the derivation of $\Gamma \vdash e : \tau$.

CASE $\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau} :$

1. $\Gamma \vdash_H x : \tau$
by $(x:\tau) \in \Gamma$
2. QED

CASE $\frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} :$

1. $(x:\tau_d), \Gamma \vdash_H e : \tau_c$
by the induction hypothesis
2. $\Gamma \vdash_H \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c$
3. QED

CASE $\frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}} :$

1. QED

CASE $\frac{}{\Gamma \vdash i : \text{Int}} :$

1. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} :$

1. $\Gamma \vdash_H e_0 : \tau_0$
 $\wedge \Gamma \vdash_H e_1 : \tau_1$
by the induction hypothesis
2. $\Gamma \vdash_H \langle e_0, e_1 \rangle : \tau_0 \times \tau_1$
3. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c} :$

1. $\Gamma \vdash_H e_0 : \tau_d \Rightarrow \tau_c$
 $\wedge \Gamma \vdash_H e_1 : \tau_d$
by the induction hypothesis
2. $\Gamma \vdash_H e_0 e_1 : \tau_c$
3. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(\text{op}^1, \tau_0) = \tau}{\Gamma \vdash \text{op}^1 e_0 : \tau} :$

1. $\Gamma \vdash_H e_0 : \tau_0$
by the induction hypothesis
2. $\Gamma \vdash_H \text{op}^1 e_0 : \tau$
3. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1 \quad \Delta(\text{op}^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash \text{op}^2 e_0 e_1 : \tau} :$

1. $\Gamma \vdash_H e_0 : \tau_0$
 $\wedge \Gamma \vdash_H e_1 : \tau_1$
by the induction hypothesis
2. $\Gamma \vdash_H \text{op}^2 e_0 e_1 : \tau$
3. QED

$$\text{CASE } \frac{\Gamma \vdash e : \tau' \quad \tau' <: \tau}{\Gamma \vdash e : \tau} :$$

1. $\Gamma \vdash_H e : \tau'$
by the induction hypothesis
2. $\Gamma \vdash_H e : \tau$
3. QED

$$\text{CASE } \frac{}{\Gamma \vdash \text{Err} : \tau} :$$

1. QED

$$\text{CASE } \frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau} :$$

1. $\Gamma \vdash_H e$
by *dynamic subset*
2. $\Gamma \vdash_H \text{dyn } \tau e : \tau$
by (1)
3. QED

□

Lemma 2.7 : *H dynamic subset*If $\Gamma \vdash e$ then $\Gamma \vdash_H e$.*Proof:*By structural induction on the derivation of $\Gamma \vdash e$.

$$\text{CASE } \frac{x \in \Gamma}{\Gamma \vdash x} :$$

1. $\Gamma \vdash_H x$
by $x \in \Gamma$
2. QED

$$\text{CASE } \frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e} :$$

1. $x, \Gamma \vdash_H e$
by the induction hypothesis
2. $\Gamma \vdash_H \lambda x. e$
by (1)
3. QED

$$\text{CASE } \frac{}{\Gamma \vdash i} :$$

1. QED

$$\text{CASE } \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle} :$$

1. $\Gamma \vdash_H e_0$
 $\wedge \Gamma \vdash_H e_1$
by the induction hypothesis
2. $\Gamma \vdash_H \langle e_0, e_1 \rangle$
by (1)
3. QED

$$\text{CASE } \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1} :$$

1. $\Gamma \vdash_H e_0$
 $\wedge \Gamma \vdash_H e_1$
by the induction hypothesis
2. $\Gamma \vdash_H e_0 e_1$
by (1)
3. QED

$$\text{CASE } \frac{\Gamma \vdash e}{\Gamma \vdash \text{op}^1 e} :$$

1. $\Gamma \vdash_H e$
by the induction hypothesis
2. $\Gamma \vdash_H \text{op}^1 e$
by (1)
3. QED

$$\text{CASE } \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \text{op}^2 e_0 e_1} :$$

1. $\Gamma \vdash_H e_0$
 $\wedge \Gamma \vdash_H e_1$
by the induction hypothesis
2. $\Gamma \vdash_H \text{op}^2 e_0 e_1$
by (1)
3. QED

$$\text{CASE } \frac{}{\Gamma \vdash \text{Err}} :$$

1. QED

$$\text{CASE } \frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e} :$$

1. $\Gamma \vdash_H e : \tau$
by *static subset*
2. $\Gamma \vdash_H \text{stat } \tau e$
by (1)
3. QED

□

Lemma 2.8 : *H static progress*If $\Gamma \vdash_H e : \tau$ then one of the following holds:

- e is a value
- $e \in \text{Err}$
- $e \rightarrow_{H-S} e'$
- $e \rightarrow_{H-S} \text{BndryErr}$
- $e = E[\text{dyn } \tau' E^\bullet[e']]$ and $e' \triangleright_{H-D} \text{TagErr}$

*Proof:*By the *boundary factoring* lemma, there are seven possible cases.**CASE** e is a value :

1. QED

CASE $e = E^\bullet[v_0 v_1] :$

1. $\vdash_H v_0 v_1 : \tau'$
by *static hole typing*
2. $\vdash_H v_0 : \tau_d \Rightarrow \tau_c$
 $\wedge \vdash_H v_1 : \tau_d$
by *inversion*

771	3. $v_0 = \lambda(x:\tau'_d). e'$	826	IF $e' \rightarrow_{H-D} \text{BndryErr}$:	826
772	$\vee v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) v_f$	827	a. $\text{QED } e \rightarrow_{H-S} E[\text{dyn } \tau' \text{ BndryErr}]$	827
773	by <i>canonical forms</i>	828	ELSE $e' = E'[e'']$ and $e'' \triangleright_{H-D} \text{TagErr}$:	828
774	4. IF $v_0 = \lambda(x:\tau'_d). e' :$	829	a. $E' \in E^\bullet$	829
775	a. $e \rightarrow_{H-S} E^\bullet[e'[x \leftarrow v_1]]$	830	by e' is boundary-free	830
776	by $v_0 v_1 \triangleright_{H-S} e'[x \leftarrow v_1]$	831	b. QED	831
777	b. QED	832	CASE $e = E[\text{stat } \tau' e']$ and e' is boundary-free :	832
778	ELSE $v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) v_f :$	833	1. e' is a value	833
779	a. $e \rightarrow_{H-S} E^\bullet[\text{dyn } \tau'_c (v_f (\text{stat } \tau'_d v_1))]$	834	$\vee e' \in \text{Err}$	834
780	by $v_0 v_1 \triangleright_{H-S} \text{dyn } \tau'_c (v_f (\text{stat } \tau'_d v_1))$	835	$\vee e' \rightarrow_{H-S} e''$	835
781	b. QED	836	$\vee e' \rightarrow_{H-S} \text{BndryErr}$	836
782	CASE $e = E^\bullet[\text{op}^1 v] :$	837	$\vee e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{H-D} \text{TagErr}$	837
783	1. $\vdash_H \text{op}^1 v : \tau'$	838	by <i>static progress</i>	838
784	by <i>static hole typing</i>	839	2. IF e' is a value :	839
785	2. $\vdash_H v : \tau_0 \times \tau_1$	840	a. $\text{QED } e \rightarrow_{H-S} E[\mathcal{S}_H(\tau', e')]$	840
786	by <i>inversion</i>	841	IF $e' \in \text{Err}$:	841
787	3. $v = \langle v_0, v_1 \rangle$	842	a. $\text{QED } e \rightarrow_{H-S} e'$	842
788	by <i>canonical forms</i>	843	IF $e' \rightarrow_{H-S} e'' :$	843
789	4. IF $\text{op}^1 = \text{fst} :$	844	a. $\text{QED } e \rightarrow_{H-S} E[\text{stat } \tau' e'']$	844
790	a. $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$	845	IF $e' \rightarrow_{H-S} \text{BndryErr}$:	845
791	b. $e \rightarrow_{H-S} E^\bullet[v_0]$	846	a. $\text{QED } e \rightarrow_{H-S} E[\text{stat } \tau' \text{ BndryErr}]$	846
792	by $\text{op}^1 v \triangleright_{H-S} v_0$	847	ELSE $e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{H-D} \text{TagErr}$	847
793	c. QED	848	:	848
794	ELSE $\text{op}^1 = \text{snd} :$	849	a. Contradiction by e' is boundary-free	849
795	a. $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$	850	CASE $e = E[\text{Err}] :$	850
796	b. $e \rightarrow_{H-S} E^\bullet[v_1]$	851	1. $\text{QED } e \rightarrow_{H-S} \text{Err}$	851
797	by $\text{op}^1 v \triangleright_{H-S} v_1$	852	\square	852
798	c. QED	853	Lemma 2.9 : H <i>dynamic progress</i>	853
799	CASE $e = E^\bullet[\text{op}^2 v_0 v_1] :$	854	If $\vdash_H e$ then one of the following holds:	854
800	1. $\vdash_H \text{op}^2 v_0 v_1 : \tau'$	855	• e is a value	855
801	by <i>static hole typing</i>	856	• $e \in \text{Err}$	856
802	2. $\vdash_H v_0 : \tau_0$	857	• $e \rightarrow_{H-D} e'$	857
803	$\wedge \vdash_H v_1 : \tau_1$	858	• $e \rightarrow_{H-D} \text{BndryErr}$	858
804	$\wedge \Delta(\text{op}^2, \tau_0, \tau_1) = \tau''$	859	• $e = E[e']$ and $e' \triangleright_{H-D} \text{TagErr}$	859
805	by <i>inversion</i>	860	<i>Proof</i> :	860
806	3. $\delta(\text{op}^2, v_0, v_1) = e'$	861	By the <i>boundary factoring</i> lemma, there are seven cases.	861
807	by Δ <i>type soundness</i> (2)	862	CASE e is a value :	862
808	4. $\text{op}^2 v_0 v_1 \triangleright_{H-S} e'$	863	1. QED	863
809	by (3)	864	CASE $e = E^\bullet[v_0 v_1] :$	864
810	5. QED by $e \rightarrow_{H-S} E^\bullet[e']$	865	IF $v_0 = \lambda x. e' :$	865
811	CASE $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :	866	1. $e \rightarrow_{H-D} E^\bullet[e'[x \leftarrow v_1]]$	866
812	1. e' is a value	867	by $v_0 v_1 \triangleright_{H-D} e'[x \leftarrow v_1]$	867
813	$\vee e' \in \text{Err}$	868	2. QED	868
814	$\vee e' \rightarrow_{H-D} e''$	869	IF $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) v_f :$	869
815	$\vee e' \rightarrow_{H-D} \text{BndryErr}$	870	1. $e \rightarrow_{H-D} E^\bullet[\text{stat } \tau_c (v_f (\text{dyn } \tau_d v_1))]$	870
816	$\vee e' = E'[e'']$ and $e'' \triangleright_{H-D} \text{TagErr}$	871	by $v_0 v_1 \triangleright_{H-D} \text{stat } \tau_c (v_f (\text{dyn } \tau_d v_1))$	871
817	by <i>dynamic progress</i>	872	2. QED	872
818	2. IF e' is a value :	873	ELSE $v_0 = i$	873
819	a. $\text{QED } e \rightarrow_{H-S} E[\mathcal{D}_H(\tau', e')]$	874	$\vee v_0 = \langle v, v' \rangle :$	874
820	IF $e' \in \text{Err}$:	875	1. $e \rightarrow_{H-D} \text{TagErr}$	875
821	a. $\text{QED } e \rightarrow_{H-S} e'$	876	by $(v_0 v_1) \triangleright_{H-D} \text{TagErr}$	876
822	IF $e' \rightarrow_{H-D} e'' :$	877	2. QED	877
823	a. $\text{QED } e \rightarrow_{H-S} E[\text{dyn } \tau' e'']$	878	CASE $e = E^\bullet[\text{op}^1 v] :$	878
824		879	IF $\delta(\text{op}^1, v) = e' :$	879
825		880		880

881 1. $(op^1 v) \triangleright_{H-D} e'$
882 2. QED
883 **ELSE** $\delta(op^1, v)$ is undefined :
884 1. $e \rightarrow_{H-D} \text{TagErr}$
885 by $(op^1 v) \triangleright_{H-D} \text{TagErr}$
886 2. QED
887 **CASE** $e = E^\bullet[op^2 v_0 v_1]$:
888 **IF** $\delta(op^2, v_0, v_1) = e''$:
889 1. $op^2 v_0 v_1 \triangleright_{H-D} e''$
890 2. QED
891 **ELSE** $\delta(op^2, v_0, v_1)$ is undefined :
892 1. $e \rightarrow_{H-D} \text{TagErr}$
893 by $op^2 v_0 v_1 \triangleright_{H-D} \text{TagErr}$
894 2. QED
895 **CASE** $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :
896 1. e' is a value
897 $\vee e' \in \text{Err}$
898 $\vee e' \rightarrow_{H-D} e''$
899 $\vee e' \rightarrow_{H-D} \text{BndryErr}$
900 $\vee e' = E[e'']$ and $e'' \triangleright_{H-D} \text{TagErr}$
901 by *dynamic progress*
902 2. **IF** e' is a value :
903 a. QED $e \rightarrow_{H-D} E[\mathcal{D}_H(\tau', e')]$
904 **IF** $e' \in \text{Err}$:
905 a. QED $e \rightarrow_{H-D} e'$
906 **IF** $e' \rightarrow_{H-D} e''$:
907 a. QED $e \rightarrow_{H-S} E[\text{dyn } \tau' e'']$
908 **IF** $e' \rightarrow_{H-D} \text{BndryErr}$:
909 a. QED $e \rightarrow_{H-D} E[\text{dyn } \tau' \text{BndryErr}]$
910 **ELSE** $e' = E[e'']$ and $e'' \triangleright_{H-D} \text{TagErr}$:
911 a. $E \in E^\bullet$
912 by e' is boundary-free
913 b. QED
914 **CASE** $e = E[\text{stat } \tau' e']$ and e' is boundary-free :
915 1. e' is a value
916 $\vee e' \in \text{Err}$
917 $\vee e' \rightarrow_{H-S} e''$
918 $\vee e' \rightarrow_{H-S} \text{BndryErr}$
919 $\vee e' = E''[\text{dyn } \tau'' E^\bullet[e'']]$ and $e'' \triangleright_{H-D} \text{TagErr}$
920 by *static progress*
921 2. **IF** e' is a value :
922 a. QED $e \rightarrow_{H-S} E[S_H(\tau', e')]$
923 **IF** $e' \in \text{Err}$:
924 a. QED $e \rightarrow_{H-S} e'$
925 **IF** $e' \rightarrow_{H-S} e''$:
926 a. QED $e \rightarrow_{H-S} E[\text{stat } \tau' e'']$
927 **IF** $e' \rightarrow_{H-S} \text{BndryErr}$:
928 a. QED $e \rightarrow_{H-S} E[\text{stat } \tau' \text{BndryErr}]$
929 **ELSE** $e' = E''[\text{dyn } \tau'' E^\bullet[e'']]$ and $e'' \triangleright_{H-D} \text{TagErr}$
930 :
931 a. Contradiction by e' is boundary-free
932 **CASE** $e = E[\text{Err}]$:
933 1. QED $e \rightarrow_{H-D} \text{Err}$
934 \square

Lemma 2.10 : H static preservationIf $\vdash_H e : \tau$ and $e \rightarrow_{H-S} e'$ then $\vdash_H e' : \tau$

Proof:

By the *boundary factoring* lemma there are seven cases.**CASE** e is a value :1. Contradiction by $e \rightarrow_{H-S} e'$ **CASE** $e = E^\bullet[v_0 v_1]$:**IF** $v_0 = \lambda(x:\tau_x). e'$ $\wedge e \rightarrow_{H-S} E^\bullet[e'[x \leftarrow v_1]]$:1. $\vdash_H v_0 v_1 : \tau'$ by *static hole typing*2. $\vdash_H v_0 : \tau_d \Rightarrow \tau_c$ $\wedge \vdash_H v_1 : \tau_d$ $\wedge \tau_c \leq \tau'$ by *inversion*3. $\tau_d \leq \tau_x$ by *canonical forms* (2)4. $(x:\tau_x) \vdash_H e' : \tau_c$ by *inversion* (2)5. $\vdash_H v_1 : \tau_x$

by (2, 3)

6. $\vdash_H e'[x \leftarrow v_1] : \tau_c$ by *substitution* (4, 5)7. $\vdash_H e'[x \leftarrow v_1] : \tau'$

by (2, 6)

8. QED by *hole substitution* (7)**ELSE** $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) v_f$ $\wedge e \rightarrow_{H-S} E^\bullet[\text{dyn } \tau_c (v_f (\text{stat } \tau_d v_1))]$:1. $\vdash_H v_0 v_1 : \tau'$ by *static hole typing*2. $\vdash_H v_0 : \tau'_d \Rightarrow \tau'_c$ $\wedge \vdash_H v_1 : \tau'_d$ $\wedge \tau'_c \leq \tau'$ by *inversion*3. $\vdash_H v_f$ by *inversion* (2)4. $\tau_d \Rightarrow \tau_c \leq \tau'_d \Rightarrow \tau'_c$ by *canonical forms* (2)5. $\tau'_d \leq \tau_d$ $\wedge \tau_c \leq \tau'_c$

by (4)

6. $\vdash_H v_1 : \tau_d$

by (2, 5)

7. $\vdash_H \text{stat } \tau_d v_1$

by (6)

8. $\vdash_H v_f (\text{stat } \tau_d v_1)$

by (3, 7)

9. $\vdash_H \text{dyn } \tau_c v_f (\text{stat } \tau_d v_1) : \tau_c$

by (8)

10. $\vdash_H \text{dyn } \tau_c v_f (\text{stat } \tau_d v_1) : \tau'$

by (2, 5, 9)

11. QED by *hole substitution* (10)**CASE** $e = E^\bullet[op^1 v]$:

991	IF $v = \langle v_0, v_1 \rangle$	2. $\vdash_H \text{dyn } \tau' e' : \tau'$	1046
992	$\wedge op^1 = \text{fst}$	by <i>boundary hole typing</i>	1047
993	$\wedge e \rightarrow_{H-S} E^\bullet[v_0] :$	3. $\vdash_H e'$	1048
994	1. $\vdash_H \text{fst } \langle v_0, v_1 \rangle : \tau'$	by <i>inversion</i> (2)	1049
995	by <i>static hole typing</i>	4. $\vdash_H e''$	1050
996	2. $\vdash_H \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$	by <i>dynamic preservation</i> (3)	1051
997	$\wedge \tau_0 \leq \tau'$	5. $\vdash_H \text{dyn } \tau' e'' : \tau'$	1052
998	by <i>inversion</i> (1)	by (4)	1053
999	3. $\vdash_H v_0 : \tau_0$	6. QED by <i>hole substitution</i> (5)	1054
1000	by <i>inversion</i> (2)	CASE $e = E[\text{stat } \tau' e']$ and e' is boundary-free :	1055
1001	4. $\vdash_H v_0 : \tau'$	IF e' is a value :	1056
1002	by (2, 3)	1. $e \rightarrow_{H-S} E[\mathcal{S}_H(\tau', e')]$	1057
1003	5. QED by <i>hole substitution</i> (4)	2. $\vdash_H \text{stat } \tau' e'$	1058
1004	ELSE $v = \langle v_0, v_1 \rangle$	by <i>boundary hole typing</i>	1059
1005	$\wedge op^1 = \text{snd}$	3. $\vdash_H e' : \tau'$	1060
1006	$\wedge e \rightarrow_{H-S} E^\bullet[v_1] :$	by <i>inversion</i> (2)	1061
1007	1. $\vdash_H \text{snd } \langle v_0, v_1 \rangle : \tau'$	4. $\vdash_H \mathcal{S}_H(\tau', e')$	1062
1008	by <i>static hole typing</i>	by \mathcal{S}_H <i>soundness</i> (3)	1063
1009	2. $\vdash_H \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$	5. QED by <i>hole substitution</i> (4)	1064
1010	$\wedge \tau_1 \leq \tau'$	ELSE $e' \rightarrow_{H-S} e'' :$	1065
1011	by <i>inversion</i> (1)	1. $e \rightarrow_{H-S} E[\text{stat } \tau' e'']$	1066
1012	3. $\vdash_H v_1 : \tau_1$	2. $\vdash_H \text{stat } \tau' e'$	1067
1013	by <i>inversion</i> (2)	by <i>boundary hole typing</i>	1068
1014	4. $\vdash_H v_1 : \tau'$	3. $\vdash_H e' : \tau'$	1069
1015	by (2, 3)	by <i>inversion</i> (2)	1070
1016	5. QED by <i>hole substitution</i> (4)	4. $\vdash_H e'' : \tau'$	1071
1017	CASE $e = E^\bullet[op^2 v_0 v_1] :$	by <i>static preservation</i> (3)	1072
1018	1. $e \rightarrow_{H-S} E^\bullet[\delta(op^2, v_0, v_1)]$	5. $\vdash_H \text{stat } \tau' e''$	1073
1019	by $e \rightarrow_{H-S} e'$	by (4)	1074
1020	2. $\vdash_H op^2 v_0 v_1 : \tau'$	6. QED by <i>hole substitution</i> (5)	1075
1021	by <i>static hole typing</i>	CASE $e = E[\text{Err}] :$	1076
1022	3. $\vdash_H v_0 : \tau_0$	1. $e \rightarrow_{H-S} \text{Err}$	1077
1023	$\wedge \vdash_H v_1 : \tau_1$	2. QED by $\vdash_H \text{Err} : \tau$	1078
1024	$\wedge \Delta(op^2, \tau_0, \tau_1) = \tau''$	\square	1079
1025	$\wedge \tau'' \leq \tau'$	Lemma 2.11 : H <i>dynamic preservation</i>	1080
1026	by <i>inversion</i> (1)	If $\vdash_H e$ and $e \rightarrow_{H-D} e'$ then $\vdash_H e'$	1081
1027	4. $\vdash_H \delta(op^2, v_0, v_1) : \tau''$	<i>Proof</i> :	1082
1028	by Δ <i>type soundness</i> (2)	By the <i>boundary factoring</i> lemma, there are seven cases.	1083
1029	5. $\vdash_H \delta(op^2, v_0, v_1) : \tau'$	CASE e is a value :	1084
1030	by (2, 3)	1. Contradiction by $e \rightarrow_{H-D} e'$	1085
1031	6. QED by <i>hole substitution</i> (4)	CASE $e = E^\bullet[v_0 v_1] :$	1086
1032	CASE $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :	IF $v_0 = \lambda x. e'$	1087
1033	IF e' is a value :	$\wedge e \rightarrow_{H-D} E^\bullet[e'[x \leftarrow v_1]] :$	1088
1034	1. $e \rightarrow_{H-S} E[\mathcal{D}_H(\tau', e')]$	1. $\vdash_H v_0 v_1$	1089
1035	2. $\vdash_H \text{dyn } \tau' e' : \tau'$	by <i>dynamic hole typing</i>	1090
1036	by <i>boundary hole typing</i>	2. $\vdash_H v_0$	1091
1037	3. $\vdash_H e'$	$\wedge \vdash_H v_1$	1092
1038	by <i>inversion</i> (2)	by <i>inversion</i> (1)	1093
1039	4. $\vdash_H \mathcal{D}_H(\tau', e') : \tau'$	3. $x \vdash_H e'$	1094
1040	by \mathcal{D}_H <i>soundness</i> (3)	by <i>inversion</i> (2)	1095
1041	5. QED by <i>hole substitution</i> (4)	4. $\vdash_H e'[x \leftarrow v_1]$	1096
1042	ELSE $e' \rightarrow_{H-D} e'' :$	by <i>substitution</i> (2, 3)	1097
1043	1. $e \rightarrow_{H-S} E[\text{dyn } \tau' e'']$	5. QED <i>hole substitution</i> (4)	1098
1044			1099
1045			1100

1101 **ELSE** $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) v_f$
 1102 $\wedge e \rightarrow_{H-D} E^\bullet[\text{stat } \tau_c (v_f (\text{dyn } \tau_d v_1))]$:
 1103 1. $\vdash_H v_0 v_1$
 1104 by *dynamic hole typing*
 1105 2. $\vdash_H v_0$
 1106 $\wedge \vdash_H v_1$
 1107 by *inversion* (1)
 1108 3. $\vdash_H v_f : \tau_d \Rightarrow \tau_c$
 1109 by *inversion* (2)
 1110 4. $\vdash_H \text{dyn } \tau_d v_1 : \tau_d$
 1111 by (2)
 1112 5. $\vdash_H v_f (\text{dyn } \tau_d v_1) : \tau_c$
 1113 by (3, 4)
 1114 6. $\vdash_H \text{stat } \tau_c v_f (\text{dyn } \tau_d v_1)$
 1115 by (5)
 1116 7. QED by *hole substitution*
 1117 **CASE** $e = E^\bullet[op^1 v]$:
 1118 **IF** $v = \langle v_0, v_1 \rangle$
 1119 $\wedge op^1 = \text{fst}$
 1120 $\wedge e \rightarrow_{H-D} E^\bullet[v_0]$:
 1121 1. $\vdash_H op^1 v$
 1122 by *dynamic hole typing*
 1123 2. $\vdash_H v$
 1124 by *inversion* (1)
 1125 3. $\vdash_H v_0$
 1126 by *inversion* (2)
 1127 4. QED by *hole substitution*
 1128 **ELSE** $v = \langle v_0, v_1 \rangle$
 1129 $\wedge op^1 = \text{snd}$
 1130 $\wedge e \rightarrow_{H-D} E^\bullet[v_1]$:
 1131 1. $\vdash_H op^1 v$
 1132 by *dynamic hole typing*
 1133 2. $\vdash_H v$
 1134 by *inversion* (1)
 1135 3. $\vdash_H v_1$
 1136 by *inversion* (2)
 1137 4. QED by *hole substitution*
 1138 **CASE** $e = E^\bullet[op^2 v_0 v_1]$:
 1139 1. $e \rightarrow_{H-D} E^\bullet[\delta(op^2, v_0, v_1)]$
 1140 2. $\vdash_H op^2 v_0 v_1$
 1141 by *dynamic hole typing*
 1142 3. $\vdash_H v_0$
 1143 $\wedge \vdash_H v_1$
 1144 by *inversion* (1)
 1145 4. $\vdash_H \delta(op^2, v_0, v_1)$
 1146 by δ *preservation* (2)
 1147 5. QED by *hole substitution* (3)
 1148 **CASE** $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :
 1149 **IF** e' is a value :
 1150 1. $e \rightarrow_{H-D} E[\mathcal{D}_H(\tau', e')]$
 1151 2. $\vdash_H \text{dyn } \tau' e' : \tau'$
 1152 by *boundary hole typing*
 1153 3. $\vdash_H e'$
 1154 by *inversion* (2)

4. $\vdash_H \mathcal{D}_H(\tau', e') : \tau'$
 by \mathcal{D}_H *soundness* (3)
 5. QED by *hole substitution* (4)
ELSE $e' \rightarrow_{H-D} e''$:
 1. $e \rightarrow_{H-D} E[\text{dyn } \tau' e'']$
 2. $\vdash_H \text{dyn } \tau' e' : \tau'$
 by *boundary hole typing*
 3. $\vdash_H e'$
 $\wedge \tau' \leq \tau''$
 by *inversion* (2)
 4. $\vdash_H e''$
 by *dynamic preservation* (3)
 5. $\vdash_H \text{dyn } \tau' e'' : \tau'$
 by (4)
 6. QED by *hole substitution* (5)
CASE $e = E[\text{stat } \tau' e']$ and e' is boundary-free :
IF $e' \in v$:
 1. $e \rightarrow_{H-D} E[\mathcal{S}_H(\tau', e')]$
 2. $\vdash_H \text{stat } \tau' e'$
 by *boundary hole typing*
 3. $\vdash_H e' : \tau'$
 by *inversion* (2)
 4. $\vdash_H \mathcal{S}_H(\tau', e')$
 by \mathcal{S}_H *soundness* (3)
 5. QED by *hole substitution* (5)
ELSE $e' \rightarrow_{H-S} e''$:
 1. $e \rightarrow_{H-D} E[\text{stat } \tau' e'']$
 2. $\vdash_H \text{stat } \tau' e'$
 by *boundary hole typing*
 3. $\vdash_H e' : \tau'$
 by *inversion* (2)
 4. $\vdash_H e'' : \tau'$
 by *static preservation* (3)
 5. $\vdash_H \text{stat } \tau' e''$
 by (4)
 6. QED by *hole substitution* (5)
CASE $e = E[\text{Err}]$:
 1. $e \rightarrow_{H-D} \text{Err}$
 2. QED $\vdash_H \text{Err}$

□

Lemma 2.12 : H *static boundary factoring*If $\vdash_H e : \tau$ then one of the following holds:

- e is a value
- $e = E^\bullet[v_0 v_1]$
- $e = E^\bullet[op^1 v]$
- $e = E^\bullet[op^2 v_0 v_1]$
- $e = E[\text{dyn } \tau e']$ where e' is boundary-free
- $e = E[\text{stat } \tau e']$ where e' is boundary-free
- $e = E[\text{Err}]$

Proof:By the *unique static evaluation contexts* lemma, there are seven cases.**CASE** e is a value :

1. QED

1211 **CASE** $e = E[v_0 v_1]$:
 1212 1. $E = E^\bullet$
 1213 $\vee E = E'[\text{dyn } \tau E^\bullet]$
 1214 $\vee E = E'[\text{stat } \tau E^\bullet]$
 1215 by *inner boundary*
 1216 2. **IF** $E = E^\bullet$:
 1217 a. $\text{QED } e = E^\bullet[v_0 v_1]$
 1218 **IF** $E = E'[\text{dyn } \tau E^\bullet]$:
 1219 a. $\text{QED } e = E'[\text{dyn } \tau E^\bullet[v_0 v_1]]$
 1220 **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:
 1221 a. $\text{QED } e = E'[\text{stat } \tau E^\bullet[v_0 v_1]]$
 1222 **CASE** $e = E[\text{op}^1 v]$:
 1223 1. $E = E^\bullet$
 1224 $\vee E = E'[\text{dyn } \tau E^\bullet]$
 1225 $\vee E = E'[\text{stat } \tau E^\bullet]$
 1226 by *inner boundary*
 1227 2. **IF** $E = E^\bullet$:
 1228 a. $\text{QED } e = E^\bullet[\text{op}^1 v]$
 1229 **IF** $E = E'[\text{dyn } \tau E^\bullet]$:
 1230 a. $\text{QED } e = E'[\text{dyn } \tau E^\bullet[\text{op}^1 v]]$
 1231 **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:
 1232 a. $\text{QED } e = E'[\text{stat } \tau E^\bullet[\text{op}^1 v]]$
 1233 **CASE** $e = E[\text{op}^2 v_0 v_1]$:
 1234 1. $E = E^\bullet$
 1235 $\vee E = E'[\text{dyn } \tau E^\bullet]$
 1236 $\vee E = E'[\text{stat } \tau E^\bullet]$
 1237 by *inner boundary*
 1238 2. **IF** $E = E^\bullet$:
 1239 a. $\text{QED } e = E^\bullet[\text{op}^2 v_0 v_1]$
 1240 **IF** $E = E'[\text{dyn } \tau E^\bullet]$:
 1241 a. $\text{QED } e = E'[\text{dyn } \tau E^\bullet[\text{op}^2 v_0 v_1]]$
 1242 **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:
 1243 a. $\text{QED } e = E'[\text{stat } \tau E^\bullet[\text{op}^2 v_0 v_1]]$
 1244 **CASE** $e = E[\text{dyn } \tau v]$:
 1245 1. $\text{QED } v$ is boundary-free
 1246 **CASE** $e = E[\text{stat } \tau v]$:
 1247 1. $\text{QED } v$ is boundary-free
 1248 **CASE** $e = E[\text{Err}]$:
 1249 1. QED

□

Lemma 2.13 : H unique static evaluation contextsIf $\vdash_H e : \tau$ then one of the following holds:

- e is a value
- $e = E[v_0 v_1]$
- $e = E[\text{op}^1 v]$
- $e = E[\text{op}^2 v_0 v_1]$
- $e = E[\text{dyn } \tau v]$
- $e = E[\text{stat } \tau v]$
- $e = E[\text{Err}]$

Proof:By induction on the structure of e .

CASE $e = x$
 $\vee e = \lambda x. e'$
 $\vee e = \text{stat } \tau e'$

1. Contradiction by $\vdash_H e : \tau$
CASE $e = i$
 $\vee e = \lambda(x : \tau_d). e'$
 $\vee e = \text{mon}(\tau_d \Rightarrow \tau_c) v$
 1. $\text{QED } e$ is a value
CASE $e = \langle e_0, e_1 \rangle$:
IF $e_0 \notin v$:
 1. $\vdash_H e_0 : \tau_0$
 by *inversion*
 2. $e_0 = E_0[e'_0]$
 by the induction hypothesis (1)
 3. $E = \langle E_0, e_1 \rangle$
 4. $\text{QED } e = E[e'_0]$
IF $e_0 \in v$
 $\wedge e_1 \notin v$:
 1. $\vdash_H e_1 : \tau_1$
 by *inversion*
 2. $e_1 = E_1[e'_1]$
 by the induction hypothesis (1)
 3. $E = \langle e_0, E_1 \rangle$
 4. $\text{QED } e = E[e'_1]$
ELSE $e_0 \in v$
 $\wedge e_1 \in v$:
 1. $E = []$
 2. $\text{QED } e$ is a value
CASE $e = e_0 e_1$:
IF $e_0 \notin v$:
 1. $\vdash_H e_0 : \tau_0$
 by *inversion*
 2. $e_0 = E_0[e'_0]$
 by the induction hypothesis (1)
 3. $E = E_0 e_1$
 4. $\text{QED } e = E[e'_0]$
IF $e_0 \in v$
 $\wedge e_1 \notin v$:
 1. $\vdash_H e_1 : \tau_1$
 by *inversion*
 2. $e_1 = E_1[e'_1]$
 by the induction hypothesis (1)
 3. $E = e_0 E_1$
 4. $\text{QED } e = E[e'_1]$
ELSE $e_0 \in v$
 $\wedge e_1 \in v$:
 1. $E = []$
 2. $\text{QED } e = E[e_0 e_1]$
CASE $e = \text{op}^1 e_0$:
IF $e_0 \notin v$:
 1. $\vdash_H e_0 : \tau_0$
 by *inversion*
 2. $e_0 = E_0[e'_0]$
 by the induction hypothesis (1)
 3. $E = \text{op}^1 E_0$
 4. $\text{QED } e = E[e'_0]$
ELSE $e_0 \in v$:

1321 1. $E = []$
 1322 2. $\text{QED } e = E[\text{op}^1 e_0]$
 1323 **CASE** $e = \text{op}^2 e_0 e_1$:
 1324 **IF** $e_0 \notin v$:
 1325 1. $\vdash_H e_0 : \tau_0$
 1326 by *inversion*
 1327 2. $e_0 = E_0[e'_0]$
 1328 by the induction hypothesis (1)
 1329 3. $E = \text{op}^2 E_0 e_1$
 1330 4. $\text{QED } e = E[e'_0]$
 1331 **IF** $e_0 \in v$
 1332 $\wedge e_1 \notin v$:
 1333 1. $\vdash_H e_1 : \tau_1$
 1334 by *inversion*
 1335 2. $e_1 = E_1[e'_1]$
 1336 by the induction hypothesis (1)
 1337 3. $E = \text{op}^2 e_0 E_1$
 1338 4. $\text{QED } e = E[e'_1]$
 1339 **ELSE** $e_0 \in v$
 1340 $\wedge e_1 \in v$:
 1341 1. $E = []$
 1342 2. $\text{QED } e = E[\text{op}^2 e_0 e_1]$
 1343 **CASE** $e = \text{dyn } \tau e_0$:
 1344 **IF** $e_0 \notin v$:
 1345 1. $\vdash_H e_0$
 1346 by *inversion*
 1347 2. $e_0 = E_0[e'_0]$
 1348 by *unique dynamic evaluation contexts* (1)
 1349 3. $E = \text{dyn } \tau E_0$
 1350 4. $\text{QED } e = E[e'_0]$
 1351 **ELSE** $e_0 \in v$:
 1352 1. $E = []$
 1353 2. $\text{QED } e = E[\text{dyn } \tau e_0]$
 1354 **CASE** $e = \text{stat } \tau e_0$:
 1355 Contradiction by $\vdash_H e : \tau$
 1356 **CASE** $e = \text{Err}$:
 1357 1. $E = []$
 1358 2. $\text{QED } e = E[\text{Err}]$
 1359 \square

Lemma 2.14 : *H inner boundary*

For all contexts E , one of the following holds:

- $E = E^\bullet$
- $E = E'[\text{dyn } \tau E^\bullet]$
- $E = E'[\text{stat } \tau E^\bullet]$

Proof:

By induction on the structure of E .

1366 **CASE** $E = E^\bullet$:
 1367 1. QED
 1368 **CASE** $E = E_0 e_1$:
 1369 1. $E_0 = E^\bullet$
 1370 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
 1371 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
 1372 by the induction hypothesis
 1373 2. **IF** $E_0 = E^\bullet$:

a. $\text{QED } E$ is boundary-free
IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:
 a. $E' = E'_0 e_1$
 b. $\text{QED } E = E'[\text{dyn } \tau E^\bullet]$
ELSE $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
 a. $E' = E'_0 e_1$
 b. $\text{QED } E = E'[\text{stat } \tau E^\bullet]$
CASE $E = v_0 E_1$:
 1. $E_1 = E^\bullet$
 $\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$
 $\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$
 by the induction hypothesis
 2. **IF** $E_1 = E^\bullet$:
 a. $\text{QED } E$ is boundary-free
IF $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:
 a. $E' = v_0 E'_1$
 b. $\text{QED } E = E'[\text{dyn } \tau E^\bullet]$
ELSE $E_1 = E'_1[\text{stat } \tau E^\bullet]$:
 a. $E' = v_0 E'_1$
 b. $\text{QED } E = E'[\text{stat } \tau E^\bullet]$
CASE $E = \langle E_0, e_1 \rangle$:
 1. $E_0 = E^\bullet$
 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
 by the induction hypothesis
 2. **IF** $E_0 = E^\bullet$:
 a. $\text{QED } E$ is boundary-free
IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:
 a. $E' = \langle E'_0, e_1 \rangle$
 b. $\text{QED } E = E'[\text{dyn } \tau E^\bullet]$
ELSE $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
 a. $E' = \langle E'_0, e_1 \rangle$
 b. $\text{QED } E = E'[\text{stat } \tau E^\bullet]$
CASE $E = \langle v_0, E_1 \rangle$:
 1. $E_1 = E^\bullet$
 $\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$
 $\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$
 by the induction hypothesis
 2. **IF** $E_1 = E^\bullet$:
 a. $\text{QED } E$ is boundary-free
IF $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:
 a. $E' = \langle v_0, E'_1 \rangle$
 b. $\text{QED } E = E'[\text{dyn } \tau E^\bullet]$
ELSE $E_1 = E'_1[\text{stat } \tau E^\bullet]$:
 a. $E' = \langle v_0, E'_1 \rangle$
 b. $\text{QED } E = E'[\text{stat } \tau E^\bullet]$
CASE $E = \text{op}^1 E_0$:
 1. $E_0 = E^\bullet$
 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
 by the induction hypothesis
 2. **IF** $E_0 = E^\bullet$:
 a. $\text{QED } E$ is boundary-free
IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:

1431 a. $E' = op^1 E'_0$
 1432 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 1433 **ELSE** $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
 1434 a. $E' = op^1 E'_0$
 1435 b. QED $E = E'[\text{stat } \tau E^\bullet]$
 1436 **CASE** $E = op^2 E_0 e_1$:
 1437 1. $E_0 = E^\bullet$
 1438 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
 1439 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
 1440 by the induction hypothesis
 1441 2. **IF** $E_0 = E^\bullet$:
 1442 a. QED E is boundary-free
 1443 **IF** $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:
 1444 a. $E' = op^2 E'_0 e_1$
 1445 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 1446 **ELSE** $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
 1447 a. $E' = op^2 E'_0 e_1$
 1448 b. QED $E = E'[\text{stat } \tau E^\bullet]$
 1449 **CASE** $E = op^2 v_0 E_1$:
 1450 1. $E_1 = E^\bullet$
 1451 $\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$
 1452 $\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$
 1453 by the induction hypothesis
 1454 2. **IF** $E_1 = E^\bullet$:
 1455 a. QED E is boundary-free
 1456 **IF** $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:
 1457 a. $E' = op^2 v_0 E'_1$
 1458 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 1459 **ELSE** $E_1 = E'_1[\text{stat } \tau E^\bullet]$:
 1460 a. $E' = op^2 v_0 E'_1$
 1461 b. QED $E = E'[\text{stat } \tau E^\bullet]$
 1462 **CASE** $E = \text{dyn } \tau E_0$:
 1463 1. $E_0 = E^\bullet$
 1464 $\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$
 1465 $\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$
 1466 by the induction hypothesis
 1467 2. **IF** $E_0 = E^\bullet$:
 1468 a. QED
 1469 **IF** $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:
 1470 a. $E' = \text{dyn } \tau E'_0$
 1471 b. QED $E = E'[\text{dyn } \tau' E^\bullet]$
 1472 **ELSE** $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:
 1473 a. $E' = \text{dyn } \tau E'_0$
 1474 b. QED $E = E'[\text{stat } \tau' E^\bullet]$
 1475 **CASE** $E = \text{stat } \tau E_0$:
 1476 1. $E_0 = E^\bullet$
 1477 $\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$
 1478 $\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$
 1479 by the induction hypothesis
 1480 2. **IF** $E_0 = E^\bullet$:
 1481 a. QED
 1482 **IF** $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:
 1483 a. $E' = \text{stat } \tau E'_0$
 1484
 1485

b. QED $E = E'[\text{dyn } \tau' E^\bullet]$
ELSE $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:
 a. $E' = \text{stat } \tau E'_0$
 b. QED $E = E'[\text{stat } \tau' E^\bullet]$

□

Lemma 2.15 : H *dynamic boundary factoring*

If $\vdash_H e$ then one of the following holds:

- e is a value
- $e = E^\bullet[v_0 v_1]$
- $e = E^\bullet[op^1 v]$
- $e = E^\bullet[op^2 v_0 v_1]$
- $e = E[\text{dyn } \tau e']$ where e' is boundary-free
- $e = E[\text{stat } \tau e']$ where e' is boundary-free
- $e = E[\text{Err}]$

Proof:

By the *unique dynamic evaluation contexts* lemma, there are seven cases.

CASE e is a value :

1. QED

CASE $e = E[v_0 v_1]$:

1. $E = E^\bullet$

$\vee E = E'[\text{dyn } \tau E^\bullet]$

$\vee E = E'[\text{stat } \tau E^\bullet]$

by *inner boundary*

2. **IF** $E = E^\bullet$:

a. QED $e = E^\bullet[v_0 v_1]$

IF $E = E'[\text{dyn } \tau E^\bullet]$:

a. QED $e = E'[\text{dyn } \tau E^\bullet[v_0 v_1]]$

ELSE $E = E'[\text{stat } \tau E^\bullet]$:

a. QED $e = E'[\text{stat } \tau E^\bullet[v_0 v_1]]$

CASE $e = E[op^1 v]$:

1. $E = E^\bullet$

$\vee E = E'[\text{dyn } \tau E^\bullet]$

$\vee E = E'[\text{stat } \tau E^\bullet]$

by *inner boundary*

2. **IF** $E = E^\bullet$:

a. QED $e = E^\bullet[op^1 v]$

IF $E = E'[\text{dyn } \tau E^\bullet]$:

a. QED $e = E'[\text{dyn } \tau E^\bullet[op^1 v]]$

ELSE $E = E'[\text{stat } \tau E^\bullet]$:

a. QED $e = E'[\text{stat } \tau E^\bullet[op^1 v]]$

CASE $e = E[op^2 v_0 v_1]$:

1. $E = E^\bullet$

$\vee E = E'[\text{dyn } \tau E^\bullet]$

$\vee E = E'[\text{stat } \tau E^\bullet]$

by *inner boundary*

2. **IF** $E = E^\bullet$:

a. QED $e = E^\bullet[op^2 v_0 v_1]$

IF $E = E'[\text{dyn } \tau E^\bullet]$:

a. QED $e = E'[\text{dyn } \tau E^\bullet[op^2 v_0 v_1]]$

ELSE $E = E'[\text{stat } \tau E^\bullet]$:

a. QED $e = E'[\text{stat } \tau E^\bullet[op^2 v_0 v_1]]$

CASE $e = E[\text{dyn } \tau v]$:

1. QED v is boundary-free

1541 **CASE** $e = E[\text{stat } \tau \ v] :$
 1542 1. QED v is boundary-free
 1543 **CASE** $e = E[\text{Err}] :$
 1544 1. QED
 1545 \square
 1546 **Lemma 2.16** : H unique dynamic evaluation contexts
 1547 If $\vdash_H e$ then one of the following holds:
 1548 • e is a value
 1549 • $e = E[v_0 \ v_1]$
 1550 • $e = E[op^1 \ v]$
 1551 • $e = E[op^2 \ v_0 \ v_1]$
 1552 • $e = E[\text{dyn } \tau \ v]$
 1553 • $e = E[\text{stat } \tau \ v]$
 1554 • $e = E[\text{Err}]$
 1555 *Proof*:
 1556 By induction on the structure of e .
 1557 **CASE** $e = x$
 1558 $\vee e = \lambda(x:\tau). e'$
 1559 $\vee e = \text{dyn } \tau \ e' :$
 1560 1. Contradiction by $\vdash_H e$
 1561 **CASE** $e = i$
 1562 $\vee e = \lambda x. e'$
 1563 $\vee e = \text{mon}(\tau_d \Rightarrow \tau_c) \ v :$
 1564 1. QED e is a value
 1565 **CASE** $e = \text{Err} :$
 1566 1. $E = []$
 1567 2. QED $e = E[\text{Err}]$
 1568 **CASE** $e = \langle e_0, e_1 \rangle :$
 1569 **IF** $e_0 \notin v :$
 1570 1. $\vdash_H e_0$
 1571 by *inversion*
 1572 2. $e_0 = E_0[e'_0]$
 1573 by the induction hypothesis (1)
 1574 3. $E = \langle E_0, e_1 \rangle$
 1575 4. QED $e = E[e'_0]$
 1576 **IF** $e_0 \in v$
 1577 $\wedge e_1 \notin v :$
 1578 1. $\vdash_H e_1$
 1579 by *inversion*
 1580 2. $e_1 = E_1[e'_1]$
 1581 by the induction hypothesis (1)
 1582 3. $E = \langle e_0, E_1 \rangle$
 1583 4. QED $e = E[e'_1]$
 1584 **ELSE** $e_0 \in v$
 1585 $\wedge e_1 \in v :$
 1586 1. $E = []$
 1587 2. QED e is a value
 1588 **CASE** $e = e_0 \ e_1 :$
 1589 **IF** $e_0 \notin v :$
 1590 1. $\vdash_H e_0$
 1591 by *inversion*
 1592 2. $e_0 = E_0[e'_0]$
 1593 by the induction hypothesis (1)
 1594 3. $E = E_0 \ e_1$

4. QED $e = E[e'_0]$
IF $e_0 \in v$
 $\wedge e_1 \notin v :$
 1. $\vdash_H e_1$
 by *inversion*
 2. $e_1 = E_1[e'_1]$
 by the induction hypothesis (1)
 3. $E = e_0 \ E_1$
 4. QED $e = E[e'_1]$
ELSE $e_0 \in v$
 $\wedge e_1 \in v :$
 1. $E = []$
 2. QED $e = E[e_0 \ e_1]$
CASE $e = op^1 \ e_0 :$
IF $e_0 \notin v :$
 1. $\vdash_H e_0$
 by *inversion*
 2. $e_0 = E_0[e'_0]$
 by the induction hypothesis (1)
 3. $E = op^1 \ E_0$
 4. QED $e = E[e'_0]$
ELSE $e_0 \in v :$
 1. $E = []$
 2. QED $e = E[op^1 \ e_0]$
CASE $e = op^2 \ e_0 \ e_1 :$
IF $e_0 \notin v :$
 1. $\vdash_H e_0$
 by *inversion*
 2. $e_0 = E_0[e'_0]$
 by the induction hypothesis (1)
 3. $E = op^2 \ E_0 \ e_1$
 4. QED $e = E[e'_0]$
IF $e_0 \in v$
 $\wedge e_1 \notin v :$
 1. $\vdash_H e_1$
 by *inversion*
 2. $e_1 = E_1[e'_1]$
 by the induction hypothesis (1)
 3. $E = op^2 \ e_0 \ E_1$
 4. QED $e = E[e'_1]$
ELSE $e_0 \in v$
 $\wedge e_1 \in v :$
 1. $E = []$
 2. QED $e = E[op^2 \ e_0 \ e_1]$
CASE $e = \text{stat } \tau \ e_0 :$
IF $e_0 \notin v :$
 1. $\vdash_H e_0$
 by *inversion*
 2. $e_0 = E_0[e'_0]$
 by *unique static evaluation contexts* (1)
 3. $E = \text{stat } \tau \ E_0$
 4. QED $e = E[e'_0]$
ELSE $e_0 \in v :$
 1. $E = []$

2. QED $e = E[\text{stat } \tau \ e_0]$

□

Lemma 2.17 : H static hole typing

If $\vdash_H E^\bullet[e] : \tau$ then the derivation contains a sub-term $\vdash_H e : \tau'$

Proof:

By induction on the structure of E^\bullet .

CASE $E^\bullet = [] :$

1. QED $E^\bullet[e] = e$

CASE $E^\bullet = E^\bullet_0 \ e_1 :$

1. $E^\bullet[e] = E^\bullet_0[e] \ e_1$

2. $\vdash_H E^\bullet_0[e] : \tau_d \Rightarrow \tau_c$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = v_0 \ E^\bullet_1 :$

1. $E^\bullet[e] = v_0 \ E^\bullet_1[e]$

2. $\vdash_H E^\bullet_1[e] : \tau_d$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = \langle E^\bullet_0, e_1 \rangle :$

1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$

2. $\vdash_H E^\bullet_0[e] : \tau_0$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = \langle v_0, E^\bullet_1 \rangle :$

1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$

2. $\vdash_H E^\bullet_1[e] : \tau_1$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = op^1 \ E^\bullet_0 :$

1. $E^\bullet[e] = op^1 \ E^\bullet_0[e]$

2. $\vdash_H E^\bullet_0[e] : \tau_0$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = op^2 \ E^\bullet_0 \ e_1 :$

1. $E^\bullet[e] = op^2 \ E^\bullet_0[e] \ e_1$

2. $\vdash_H E^\bullet_0[e] : \tau_0$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = op^2 \ v_0 \ E^\bullet_1 :$

1. $E^\bullet[e] = op^2 \ v_0 \ E^\bullet_1[e]$

2. $\vdash_H E^\bullet_1[e] : \tau_1$

by *inversion*

3. QED by the induction hypothesis (2)

□

Lemma 2.18 : H dynamic hole typing

If $\vdash_H E^\bullet[e]$ then the derivation contains a sub-term $\vdash_H e$

Proof:

By induction on the structure of E^\bullet .

CASE $E^\bullet = [] :$

1. QED $E^\bullet[e] = e$

CASE $E^\bullet = E^\bullet_0 \ e_1 :$

1. $E^\bullet[e] = E^\bullet_0[e] \ e_1$

2. $\vdash_H E^\bullet_0[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = v_0 \ E^\bullet_1 :$

1. $E^\bullet[e] = v_0 \ E^\bullet_1[e]$

2. $\vdash_H E^\bullet_1[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = \langle E^\bullet_0, e_1 \rangle :$

1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$

2. $\vdash_H E^\bullet_0[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = \langle v_0, E^\bullet_1 \rangle :$

1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$

2. $\vdash_H E^\bullet_1[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = op^1 \ E^\bullet_0 :$

1. $E^\bullet[e] = op^1 \ E^\bullet_0[e]$

2. $\vdash_H E^\bullet_0[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = op^2 \ E^\bullet_0 \ e_1 :$

1. $E^\bullet[e] = op^2 \ E^\bullet_0[e] \ e_1$

2. $\vdash_H E^\bullet_0[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = op^2 \ v_0 \ E^\bullet_1 :$

1. $E^\bullet[e] = op^2 \ v_0 \ E^\bullet_1[e]$

2. $\vdash_H E^\bullet_1[e]$

by *inversion*

3. QED by the induction hypothesis (2)

□

Lemma 2.19 : H boundary hole typing

• If $\vdash_H E[\text{dyn } \tau \ e] : \tau'$ then the derivation contains a sub-term

$\vdash_H \text{dyn } \tau \ e : \tau$

• If $\vdash_H E[\text{dyn } \tau \ e]$ then the derivation contains a sub-term

$\vdash_H \text{dyn } \tau \ e : \tau$

• If $\vdash_H E[\text{stat } \tau \ e] : \tau'$ then the derivation contains a sub-term

$\vdash_H \text{stat } \tau \ e$

• If $\vdash_H E[\text{stat } \tau \ e]$ then the derivation contains a sub-term

$\vdash_H \text{stat } \tau \ e$

Proof:

By the following four lemmas: *static dyn hole typing*, *dynamic dyn hole typing*, *static stat hole typing*, and *dynamic stat hole typing*.

□

Lemma 2.20 : H static dyn hole typing

If $\vdash_H E[\text{dyn } \tau \ e] : \tau'$ then the derivation contains a sub-term

$\vdash_H \text{dyn } \tau \ e : \tau$.

Proof:

By induction on the structure of E .

1761 **CASE** $E \in E^\bullet$:
 1762 1. $\vdash_H \text{dyn } \tau \ e : \tau''$
 1763 by *static hole typing*
 1764 2. $\vdash_H \text{dyn } \tau \ e : \tau$
 1765 by *inversion* (1)
 1766 3. QED
 1767 **CASE** $E = E_0 \ e_1$:
 1768 1. $E[\text{dyn } \tau \ e] = E_0[\text{dyn } \tau \ e] \ e_1$
 1769 2. $\vdash_H E_0[\text{dyn } \tau \ e] : \tau_0$
 1770 by *inversion*
 1771 3. QED by the induction hypothesis (2)
 1772 **CASE** $E = v_0 \ E_1$:
 1773 1. $E[\text{dyn } \tau \ e] = v_0 \ E_1[\text{dyn } \tau \ e]$
 1774 2. $\vdash_H E_1[\text{dyn } \tau \ e] : \tau_1$
 1775 by *inversion*
 1776 3. QED by the induction hypothesis (2)
 1777 **CASE** $E = \langle E_0, e_1 \rangle$:
 1778 1. $E[\text{dyn } \tau \ e] = \langle E_0[\text{dyn } \tau \ e], e_1 \rangle$
 1779 2. $\vdash_H E_0[\text{dyn } \tau \ e] : \tau_0$
 1780 by *inversion*
 1781 3. QED by the induction hypothesis (2)
 1782 **CASE** $E = \langle v_0, E_1 \rangle$:
 1783 1. $E[\text{dyn } \tau \ e] = \langle v_0, E_1[\text{dyn } \tau \ e] \rangle$
 1784 2. $\vdash_H E_1[\text{dyn } \tau \ e] : \tau_1$
 1785 by *inversion*
 1786 3. QED by the induction hypothesis (2)
 1787 **CASE** $E = \text{op}^1 \ E_0$:
 1788 1. $E[\text{dyn } \tau \ e] = \text{op}^1 \ E_0[\text{dyn } \tau \ e]$
 1789 2. $\vdash_H E_0[\text{dyn } \tau \ e] : \tau_0$
 1790 by *inversion*
 1791 3. QED by the induction hypothesis (2)
 1792 **CASE** $E = \text{op}^2 \ E_0 \ e_1$:
 1793 1. $E[\text{dyn } \tau \ e] = \text{op}^2 \ E_0[\text{dyn } \tau \ e] \ e_1$
 1794 2. $\vdash_H E_0[\text{dyn } \tau \ e] : \tau_0$
 1795 by *inversion*
 1796 3. QED by the induction hypothesis (2)
 1797 **CASE** $E = \text{op}^2 \ v_0 \ E_1$:
 1798 1. $E[\text{dyn } \tau \ e] = \text{op}^2 \ v_0 \ E_1[\text{dyn } \tau \ e]$
 1799 2. $\vdash_H E_1[\text{dyn } \tau \ e] : \tau_1$
 1800 by *inversion*
 1801 3. QED by the induction hypothesis (2)
 1802 **CASE** $E = \text{dyn } \tau_0 \ E_0$:
 1803 1. $E[\text{dyn } \tau \ e] = \text{dyn } \tau_0 \ E_0[\text{dyn } \tau \ e]$
 1804 2. $\vdash_H E_0[\text{dyn } \tau \ e] :$
 1805 by *inversion*
 1806 3. QED by *dynamic dyn hole typing* (2)
 1807 **CASE** $E = \text{stat } \tau_0 \ E_0$:
 1808 1. Contradiction by $\vdash_H E[\text{dyn } \tau \ e] : \tau'$
 1809 \square
 1810 **Lemma 2.21** : H *dynamic dyn hole typing*
 1811 If $\vdash_H E[\text{dyn } \tau \ e]$ then the derivation contains a sub-term
 1812 $\vdash_H \text{dyn } \tau \ e : \tau$.
 1813 *Proof*:
 1814
 1815

By induction on the structure of E .

CASE $E \in E^\bullet$:

1. Contradiction by $\vdash_H E[\text{dyn } \tau \ e]$

CASE $E = E_0 \ e_1$:

1. $E[\text{dyn } \tau \ e] = E_0[\text{dyn } \tau \ e] \ e_1$

2. $\vdash_H E_0[\text{dyn } \tau \ e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = v_0 \ E_1$:

1. $E[\text{dyn } \tau \ e] = v_0 \ E_1[\text{dyn } \tau \ e]$

2. $\vdash_H E_1[\text{dyn } \tau \ e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \langle E_0, e_1 \rangle$:

1. $E[\text{dyn } \tau \ e] = \langle E_0[\text{dyn } \tau \ e], e_1 \rangle$

2. $\vdash_H E_0[\text{dyn } \tau \ e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \langle v_0, E_1 \rangle$:

1. $E[\text{dyn } \tau \ e] = \langle v_0, E_1[\text{dyn } \tau \ e] \rangle$

2. $\vdash_H E_1[\text{dyn } \tau \ e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \text{op}^1 \ E_0$:

1. $E[\text{dyn } \tau \ e] = \text{op}^1 \ E_0[\text{dyn } \tau \ e]$

2. $\vdash_H E_0[\text{dyn } \tau \ e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \text{op}^2 \ E_0 \ e_1$:

1. $E[\text{dyn } \tau \ e] = \text{op}^2 \ E_0[\text{dyn } \tau \ e] \ e_1$

2. $\vdash_H E_0[\text{dyn } \tau \ e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \text{op}^2 \ v_0 \ E_1$:

1. $E[\text{dyn } \tau \ e] = \text{op}^2 \ v_0 \ E_1[\text{dyn } \tau \ e]$

2. $\vdash_H E_1[\text{dyn } \tau \ e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \text{dyn } \tau \ E_0$:

1. Contradiction by $\vdash_H E[\text{dyn } \tau \ e]$

CASE $E = \text{stat } \tau_0 \ E_0$:

1. $E[\text{dyn } \tau \ e] = \text{stat } \tau_0 \ E_0[\text{dyn } \tau \ e]$

2. $\vdash_H E_0[\text{dyn } \tau \ e] : \tau_0$

by *inversion*

3. QED by *static dyn hole typing* (2)

\square

Lemma 2.22 : H *static stat hole typing*

If $\vdash_H E[\text{stat } \tau \ e] : \tau'$ then the derivation contains a sub-term
 $\vdash_H \text{stat } \tau \ e$.

Proof:

By induction on the structure of E .

CASE $E \in E^\bullet$:

1. Contradiction by $\vdash_H E[\text{stat } \tau \ e] : \tau'$

1871 **CASE** $E = E_0 e_1$:
 1872 1. $E[\text{stat } \tau e] = E_0[\text{stat } \tau e] e_1$
 1873 2. $\vdash_H E_0[\text{stat } \tau e] : \tau_0$
 1874 by *inversion*
 1875 3. QED by the induction hypothesis (2)
 1876 **CASE** $E = v_0 E_1$:
 1877 1. $E[\text{stat } \tau e] = v_0 E_1[\text{stat } \tau e]$
 1878 2. $\vdash_H E_1[\text{stat } \tau e] : \tau_1$
 1879 by *inversion*
 1880 3. QED by the induction hypothesis (2)
 1881 **CASE** $E = \langle E_0, e_1 \rangle$:
 1882 1. $E[\text{stat } \tau e] = \langle E_0[\text{stat } \tau e], e_1 \rangle$
 1883 2. $\vdash_H E_0[\text{stat } \tau e] : \tau_0$
 1884 by *inversion*
 1885 3. QED by the induction hypothesis (2)
 1886 **CASE** $E = \langle v_0, E_1 \rangle$:
 1887 1. $E[\text{stat } \tau e] = \langle v_0, E_1[\text{stat } \tau e] \rangle$
 1888 2. $\vdash_H E_1[\text{stat } \tau e] : \tau_1$
 1889 by *inversion*
 1890 3. QED by the induction hypothesis (2)
 1891 **CASE** $E = \text{op}^1 E_0$:
 1892 1. $E[\text{stat } \tau e] = \text{op}^1 E_0[\text{stat } \tau e]$
 1893 2. $\vdash_H E_0[\text{stat } \tau e] : \tau_0$
 1894 by *inversion*
 1895 3. QED by the induction hypothesis (2)
 1896 **CASE** $E = \text{op}^2 E_0 e_1$:
 1897 1. $E[\text{stat } \tau e] = \text{op}^2 E_0[\text{stat } \tau e] e_1$
 1898 2. $\vdash_H E_0[\text{stat } \tau e] : \tau_0$
 1899 by *inversion*
 1900 3. QED by the induction hypothesis (2)
 1901 **CASE** $E = \text{op}^2 v_0 E_1$:
 1902 1. $E[\text{stat } \tau e] = \text{op}^2 v_0 E_1[\text{stat } \tau e]$
 1903 2. $\vdash_H E_1[\text{stat } \tau e] : \tau_1$
 1904 by *inversion*
 1905 3. QED by the induction hypothesis (2)
 1906 **CASE** $E = \text{dyn } \tau_0 E_0$:
 1907 1. $E[\text{stat } \tau e] = \text{dyn } \tau_0 E_0[\text{stat } \tau e]$
 1908 2. $\vdash_H E_0[\text{stat } \tau e]$
 1909 by *inversion*
 1910 3. QED by *dynamic stat hole typing* (2)
 1911 **CASE** $E = \text{stat } \tau_0 E_0$:
 1912 1. Contradiction by $\vdash_H E[\text{stat } \tau e] : \tau'$
 1913 \square

Lemma 2.23 : H *dynamic stat hole typing*

If $\vdash_H E[\text{stat } \tau e]$ then the derivation contains a sub-term $\vdash_H \text{stat } \tau e$.

Proof:

By induction on the structure of E .

CASE $E \in E^*$:

1. QED by *dynamic hole typing*

CASE $E = E_0 e_1$:

1. $E[\text{stat } \tau e] = E_0[\text{stat } \tau e] e_1$

2. $\vdash_H E_0[\text{stat } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)

CASE $E = v_0 E_1$:

1. $E[\text{stat } \tau e] = v_0 E_1[\text{stat } \tau e]$

2. $\vdash_H E_1[\text{stat } \tau e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \langle E_0, e_1 \rangle$:

1. $E[\text{stat } \tau e] = \langle E_0[\text{stat } \tau e], e_1 \rangle$

2. $\vdash_H E_0[\text{stat } \tau e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \langle v_0, E_1 \rangle$:

1. $E[\text{stat } \tau e] = \langle v_0, E_1[\text{stat } \tau e] \rangle$

2. $\vdash_H E_1[\text{stat } \tau e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \text{op}^1 E_0$:

1. $E[\text{stat } \tau e] = \text{op}^1 E_0[\text{stat } \tau e]$

2. $\vdash_H E_0[\text{stat } \tau e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \text{op}^2 E_0 e_1$:

1. $E[\text{stat } \tau e] = \text{op}^2 E_0[\text{stat } \tau e] e_1$

2. $\vdash_H E_0[\text{stat } \tau e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \text{op}^2 v_0 E_1$:

1. $E[\text{stat } \tau e] = \text{op}^2 v_0 E_1[\text{stat } \tau e]$

2. $\vdash_H E_1[\text{stat } \tau e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \text{dyn } \tau_0 E_0$:

1. Contradiction by $\vdash_H E[\text{stat } \tau e]$

CASE $E = \text{stat } \tau_0 E_0$:

1. $E[\text{stat } \tau e] = \text{stat } \tau_0 E_0[\text{stat } \tau e]$

2. $\vdash_H E_0[\text{stat } \tau e] : \tau_0$

by *inversion*

3. QED by *static stat hole typing* (2)

\square

Lemma 2.24 : H *static boundary-free hole substitution*

If $\vdash_H E^*[e] : \tau$ and the derivation contains a sub-term $\vdash_H e : \tau'$ and $\vdash_H e' : \tau'$ then $\vdash_H E^*[e'] : \tau$.

Proof:

By induction on the structure of E^*

CASE $E^* = []$:

1. $E^*[e] = e$

$\wedge E^*[e'] = e'$

2. $\vdash_H e : \tau$

by (1)

3. $\tau' = \tau$

4. $\vdash_H e' : \tau$

1981	5. QED by (1, 4)	2036
1982	CASE $E^\bullet = E^\bullet_0 e_1 :$	2037
1983	1. $E^\bullet[e] = E^\bullet_0[e] e_1$	2038
1984	$\wedge E^\bullet[e'] = E^\bullet_0[e'] e_1$	2039
1985	2. $\vdash_H E^\bullet_0[e] e_1 : \tau$	2040
1986	3. $\vdash_H E^\bullet_0[e] : \tau_0$	2041
1987	$\wedge \vdash_H e_1 : \tau_1$	2042
1988	by <i>inversion</i>	2043
1989	4. $\vdash_H E^\bullet_0[e'] : \tau_0$	2044
1990	by the induction hypothesis (3)	2045
1991	5. $\vdash_H E^\bullet_0[e'] e_1 : \tau$	2046
1992	by (2, 3, 4)	2047
1993	6. QED by (1, 5)	2048
1994	CASE $E^\bullet = v_0 E^\bullet_1 :$	2049
1995	1. $E^\bullet[e] = v_0 E^\bullet_1[e]$	2050
1996	$\wedge E^\bullet[e'] = v_0 E^\bullet_1[e']$	2051
1997	2. $\vdash_H v_0 E^\bullet_1[e] : \tau$	2052
1998	3. $\vdash_H v_0 : \tau_0$	2053
1999	$\wedge \vdash_H E^\bullet_1[e] : \tau_1$	2054
2000	by <i>inversion</i>	2055
2001	4. $\vdash_H E^\bullet_1[e'] : \tau_1$	2056
2002	by the induction hypothesis (3)	2057
2003	5. $\vdash_H v_0 E^\bullet_1[e'] : \tau$	2058
2004	by (2, 3, 4)	2059
2005	6. QED by (1, 5)	2060
2006	CASE $E^\bullet = op^1 E^\bullet_0 :$	2061
2007	1. $E^\bullet[e] = op^1 E^\bullet_0[e]$	2062
2008	$\wedge E^\bullet[e'] = op^1 E^\bullet_0[e']$	2063
2009	2. $\vdash_H op^1 E^\bullet_0[e] : \tau$	2064
2010	3. $\vdash_H E^\bullet_0[e] : \tau_0$	2065
2011	by <i>inversion</i>	2066
2012	4. $\vdash_H E^\bullet_0[e'] : \tau_0$	2067
2013	by the induction hypothesis (3)	2068
2014	5. $\vdash_H op^1 E^\bullet_0[e'] : \tau$	2069
2015	by (2, 3, 4)	2070
2016	6. QED by (1, 5)	2071
2017	CASE $E^\bullet = \langle E^\bullet_0, e_1 \rangle :$	2072
2018	1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$	2073
2019	$\wedge E^\bullet[e'] = \langle E^\bullet_0[e'], e_1 \rangle$	2074
2020	2. $\vdash_H \langle E^\bullet_0[e], e_1 \rangle : \tau$	2075
2021	3. $\vdash_H E^\bullet_0[e] : \tau_0$	2076
2022	$\wedge \vdash_H e_1 : \tau_1$	2077
2023	by <i>inversion</i>	2078
2024	4. $\vdash_H E^\bullet_0[e'] : \tau_0$	2079
2025	by the induction hypothesis (3)	2080
2026	5. $\vdash_H \langle E^\bullet_0[e'], e_1 \rangle : \tau$	2081
2027	by (2, 3, 4)	2082
2028	6. QED by (1, 5)	2083
2029	CASE $E^\bullet = \langle v_0, E^\bullet_1 \rangle :$	2084
2030	1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$	2085
2031	$\wedge E^\bullet[e'] = \langle v_0, E^\bullet_1[e'] \rangle$	2086
2032	2. $\vdash_H \langle v_0, E^\bullet_1[e] \rangle : \tau$	2087
2033		2088
2034		2089
2035		2090
	3. $\vdash_H v_0 : \tau_0$	2036
	$\wedge \vdash_H E^\bullet_1[e] : \tau_1$	2037
	by <i>inversion</i>	2038
	4. $\vdash_H E^\bullet_1[e'] : \tau_1$	2039
	by the induction hypothesis (3)	2040
	5. $\vdash_H \langle v_0, E^\bullet_1[e'] \rangle : \tau$	2041
	by (2, 3, 4)	2042
	6. QED by (1, 5)	2043
	CASE $E^\bullet = op^2 E^\bullet_0 e_1 :$	2044
	1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$	2045
	$\wedge E^\bullet[e'] = op^2 E^\bullet_0[e'] e_1$	2046
	2. $\vdash_H op^2 E^\bullet_0[e] e_1 : \tau$	2047
	3. $\vdash_H E^\bullet_0[e] : \tau_0$	2048
	$\wedge \vdash_H e_1 : \tau_1$	2049
	by <i>inversion</i>	2050
	4. $\vdash_H E^\bullet_0[e'] : \tau_0$	2051
	by the induction hypothesis (3)	2052
	5. $\vdash_H op^2 E^\bullet_0[e'] e_1 : \tau$	2053
	by (2, 3, 4)	2054
	6. QED by (1, 5)	2055
	CASE $E^\bullet = op^2 v_0 E^\bullet_1 :$	2056
	1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$	2057
	$\wedge E^\bullet[e'] = op^2 v_0 E^\bullet_1[e']$	2058
	2. $\vdash_H op^2 v_0 E^\bullet_1[e] : \tau$	2059
	3. $\vdash_H v_0 : \tau_0$	2060
	$\wedge \vdash_H E^\bullet_1[e] : \tau_1$	2061
	by <i>inversion</i>	2062
	4. $\vdash_H E^\bullet_1[e'] : \tau_1$	2063
	by the induction hypothesis (3)	2064
	5. $\vdash_H op^2 v_0 E^\bullet_1[e'] : \tau$	2065
	by (2, 3, 4)	2066
	6. QED by (1, 5)	2067
	□	2068
	Lemma 2.25 : H dynamic hole substitution	2069
	■ If $\vdash_H E^\bullet[e]$ and $\vdash_H e'$ then $\vdash_H E^\bullet[e']$	2070
	<i>Proof</i> :	2071
	By induction on the structure of E^\bullet	2072
	CASE $E^\bullet = [] :$	2073
	1. QED $E^\bullet[e'] = e'$	2074
	CASE $E^\bullet = \langle E^\bullet_0, e_1 \rangle :$	2075
	1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$	2076
	$\wedge E^\bullet[e'] = \langle E^\bullet_0[e'], e_1 \rangle$	2077
	2. $\vdash_H \langle E^\bullet_0[e], e_1 \rangle$	2078
	3. $\vdash_H E^\bullet_0[e]$	2079
	$\wedge \vdash_H e_1$	2080
	by <i>inversion</i>	2081
	4. $\vdash_H E^\bullet_0[e']$	2082
	by the induction hypothesis (3)	2083
	5. $\vdash_H \langle E^\bullet_0[e'], e_1 \rangle$	2084
	by (3, 4)	2085
	6. QED by (1, 5)	2086
	CASE $E^\bullet = \langle v_0, E^\bullet_1 \rangle :$	2087
		2088
		2089
		2090

1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$
 $\wedge E^\bullet[e'] = \langle v_0, E^\bullet_1[e'] \rangle$
 2. $\vdash_H \langle v_0, E^\bullet_1[e] \rangle$
 3. $\vdash_H v_0$
 $\wedge \vdash_H E^\bullet_1[e]$
 by *inversion*
 4. $\vdash_H E^\bullet_1[e']$
 by the induction hypothesis (3)
 5. $\vdash_H \langle v_0, E^\bullet_1[e'] \rangle$
 by (3, 4)
 6. QED by (1, 5)
CASE $E^\bullet = E^\bullet_0 e_1$:
 1. $E^\bullet[e] = E^\bullet_0[e] e_1$
 $\wedge E^\bullet[e'] = E^\bullet_0[e'] e_1$
 2. $\vdash_H E^\bullet_0[e] e_1$
 3. $\vdash_H E^\bullet_0[e]$
 $\wedge \vdash_H e_1$
 by *inversion*
 4. $\vdash_H E^\bullet_0[e']$
 by the induction hypothesis (3)
 5. $\vdash_H E^\bullet_0[e'] e_1$
 by (3, 4)
 6. QED by (1, 5)
CASE $E^\bullet = v_0 E^\bullet_1$:
 1. $E^\bullet[e] = v_0 E^\bullet_1[e]$
 $\wedge E^\bullet[e'] = v_0 E^\bullet_1[e']$
 2. $\vdash_H v_0 E^\bullet_1[e]$
 3. $\vdash_H v_0$
 $\wedge \vdash_H E^\bullet_1[e]$
 by *inversion*
 4. $\vdash_H E^\bullet_1[e']$
 by the induction hypothesis (3)
 5. $\vdash_H v_0 E^\bullet_1[e']$
 by (3, 4)
 6. QED by (1, 5)
CASE $E^\bullet = op^1 E^\bullet_0$:
 1. $E^\bullet[e] = op^1 E^\bullet_0[e]$
 $\wedge E^\bullet[e'] = op^1 E^\bullet_0[e']$
 2. $\vdash_H op^1 E^\bullet_0[e]$
 3. $\vdash_H E^\bullet_0[e]$
 by *inversion*
 4. $\vdash_H E^\bullet_0[e']$
 by the induction hypothesis (3)
 5. $\vdash_H op^1 E^\bullet_0[e']$
 by (4)
 6. QED by (1, 5)
CASE $E^\bullet = op^2 E^\bullet_0 e_1$:
 1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$
 $\wedge E^\bullet[e'] = op^2 E^\bullet_0[e'] e_1$
 2. $\vdash_H op^2 E^\bullet_0[e] e_1$
 3. $\vdash_H E^\bullet_0[e]$
 $\wedge \vdash_H e_1$
 by *inversion*

4. $\vdash_H E^\bullet_0[e']$
 by the induction hypothesis (3)
 5. $\vdash_H op^2 E^\bullet_0[e'] e_1$
 by (3, 4)
 6. QED by (1, 5)
CASE $E^\bullet = op^2 v_0 E^\bullet_1$:
 1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$
 $\wedge E^\bullet[e'] = op^2 v_0 E^\bullet_1[e']$
 2. $\vdash_H op^2 v_0 E^\bullet_1[e]$
 3. $\vdash_H v_0$
 $\wedge \vdash_H E^\bullet_1[e]$
 by *inversion*
 4. $\vdash_H E^\bullet_1[e']$
 by the induction hypothesis (3)
 5. $\vdash_H op^2 v_0 E^\bullet_1[e']$
 by (3, 4)
 6. QED by (1, 5)

□

Lemma 2.26 : H *hole substitution*

- If $\vdash_H E[e]$ and the derivation contains a sub-term $\vdash_H e : \tau'$ and $\vdash_H e' : \tau'$ then $\vdash_H E[e']$.
- If $\vdash_H E[e]$ and the derivation contains a sub-term $\vdash_H e$ and $\vdash_H e'$ then $\vdash_H E[e']$.
- If $\vdash_H E[e] : \tau$ and the derivation contains a sub-term $\vdash_H e : \tau'$ and $\vdash_H e' : \tau'$ then $\vdash_H E[e'] : \tau$.
- If $\vdash_H E[e] : \tau$ and the derivation contains a sub-term $\vdash_H e$ and $\vdash_H e'$ then $\vdash_H E[e'] : \tau$.

Proof:

By the following four lemmas: *dynamic context static hole substitution*, *dynamic context dynamic hole substitution*, *static context static hole substitution*, and *static context dynamic hole substitution*.

□

Lemma 2.27 : H *dynamic context static hole substitution*

- If $\vdash_H E[e]$ and contains $\vdash_H e : \tau'$, and furthermore $\vdash_H e' : \tau'$, then $\vdash_H E[e']$

Proof:

By induction on the structure of E .

CASE $E \in E^\bullet$:

1. Contradiction by $\vdash_H E[e]$

CASE $E = E_0 e_1$:

1. $E[e] = E_0[e] e_1$

2. $\vdash_H E_0[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = v_0 E_1$:

1. $E[e] = v_0 E_1[e]$

2. $\vdash_H E_1[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \langle E_0, e_1 \rangle$:

1. $E[e] = \langle E_0[e], e_1 \rangle$

2201 2. $\vdash_H E_0[e]$
 2202 by *inversion*
 2203 3. QED by the induction hypothesis (2)
 2204 **CASE** $E = \langle v_0, E_1 \rangle :$
 2205 1. $E[e] = \langle v_0, E_1[e] \rangle$
 2206 2. $\vdash_H E_1[e]$
 2207 by *inversion*
 2208 3. QED by the induction hypothesis (2)
 2209 **CASE** $E = op^1 E_0 :$
 2210 1. $E[e] = op^1 E_0[e]$
 2211 2. $\vdash_H E_0[e]$
 2212 by *inversion*
 2213 3. QED by the induction hypothesis (2)
 2214 **CASE** $E = op^2 E_0 e_1 :$
 2215 1. $E[e] = op^2 E_0[e] e_1$
 2216 2. $\vdash_H E_0[e]$
 2217 by *inversion*
 2218 3. QED by the induction hypothesis (2)
 2219 **CASE** $E = op^2 v_0 E_1 :$
 2220 1. $E[e] = op^2 v_0 E_1[e]$
 2221 2. $\vdash_H E_1[e]$
 2222 by *inversion*
 2223 3. QED by the induction hypothesis (2)
 2224 **CASE** $E = \text{dyn } \tau'' E_0 :$
 2225 1. Contradiction by $\vdash_H E[e]$
 2226 **CASE** $E = \text{stat } \tau_0 E_0 :$
 2227 1. $E[e] = \text{stat } \tau_0 E_0[e]$
 2228 2. $\vdash_H E_0[e] : \tau_0$
 2229 by *inversion*
 2230 3. QED by *static context static hole substitution* (2)
 2231 \square
 2232 **Lemma 2.28** : H *dynamic context dynamic hole substitution*
 2233 If $\vdash_H E[e]$ and contains $\vdash_H e$, and furthermore $\vdash_H e' : \tau'$, then
 2234 $\vdash_H E[e']$
 2235 *Proof*:
 2236 By induction on the structure of E .
 2237 **CASE** $E \in E^* :$
 2238 1. QED by *dynamic boundary-free hole substitution*
 2239 **CASE** $E = E_0 e_1 :$
 2240 1. $E[e] = E_0[e] e_1$
 2241 2. $\vdash_H E_0[e]$
 2242 by *inversion*
 2243 3. QED by the induction hypothesis (2)
 2244 **CASE** $E = v_0 E_1 :$
 2245 1. $E[e] = v_0 E_1[e]$
 2246 2. $\vdash_H E_1[e]$
 2247 by *inversion*
 2248 3. QED by the induction hypothesis (2)
 2249 **CASE** $E = \langle E_0, e_1 \rangle :$
 2250 1. $E[e] = \langle E_0[e], e_1 \rangle$
 2251 2. $\vdash_H E_0[e]$
 2252 by *inversion*
 2253 3. QED by the induction hypothesis (2)
 2254
 2255

CASE $E = \langle v_0, E_1 \rangle :$
 1. $E[e] = \langle v_0, E_1[e] \rangle$
 2. $\vdash_H E_1[e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^1 E_0 :$
 1. $E[e] = op^1 E_0[e]$
 2. $\vdash_H E_0[e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^2 E_0 e_1 :$
 1. $E[e] = op^2 E_0[e] e_1$
 2. $\vdash_H E_0[e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^2 v_0 E_1 :$
 1. $E[e] = op^2 v_0 E_1[e]$
 2. $\vdash_H E_1[e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{dyn } \tau'' E_0 :$
 1. Contradiction by $\vdash_H E[e]$
CASE $E = \text{stat } \tau_0 E_0 :$
 1. $E[e] = \text{stat } \tau_0 E_0[e]$
 2. $\vdash_H E_0[e] : \tau_0$
 by *inversion*
 3. QED by *static context dynamic hole substitution* (2)
 \square
Lemma 2.29 : H *static context static hole substitution*
 If $\vdash_H E[e] : \tau$ and contains $\vdash_H e : \tau'$, and furthermore $\vdash_H e' : \tau'$,
 then $\vdash_H E[e'] : \tau$
Proof:
 By induction on the structure of E .
CASE $E \in E^* :$
 1. QED by *static boundary-free hole substitution*
CASE $E = E_0 e_1 :$
 1. $E[e] = E_0[e] e_1$
 2. $\vdash_H E_0[e] : \tau_0$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = v_0 E_1 :$
 1. $E[e] = v_0 E_1[e]$
 2. $\vdash_H E_1[e] : \tau_1$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \langle E_0, e_1 \rangle :$
 1. $E[e] = \langle E_0[e], e_1 \rangle$
 2. $\vdash_H E_0[e] : \tau_0$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \langle v_0, E_1 \rangle :$
 1. $E[e] = \langle v_0, E_1[e] \rangle$

2311 2. $\vdash_H E_1[e] : \tau_1$
 2312 by *inversion*
 2313 3. QED by the induction hypothesis (2)
 2314 **CASE** $E = op^1 E_0 :$
 2315 1. $E[e] = op^1 E_0[e]$
 2316 2. $\vdash_H E_0[e] : \tau_0$
 2317 by *inversion*
 2318 3. QED by the induction hypothesis (2)
 2319 **CASE** $E = op^2 E_0 e_1 :$
 2320 1. $E[e] = op^2 E_0[e] e_1$
 2321 2. $\vdash_H E_0[e] : \tau_0$
 2322 by *inversion*
 2323 3. QED by the induction hypothesis (2)
 2324 **CASE** $E = op^2 v_0 E_1 :$
 2325 1. $E[e] = op^2 v_0 E_1[e]$
 2326 2. $\vdash_H E_1[e] : \tau_1$
 2327 by *inversion*
 2328 3. QED by the induction hypothesis (2)
 2329 **CASE** $E = \text{dyn } \tau_0 E_0 :$
 2330 1. $E[e] = \text{dyn } \tau_0 E_0[e]$
 2331 2. $\vdash_H E_0[e]$
 2332 by *inversion*
 2333 3. QED by *static dyn hole typing* (2)
 2334 **CASE** $E = \text{stat } \tau_0 E_0 :$
 2335 1. Contradiction by $\vdash_H E[e] : \tau$
 2336 \square

Lemma 2.30 : H *static context dynamic hole substitution*

2338 If $\vdash_H E[e] : \tau$ and contains $\vdash_H e$, and furthermore $\vdash_H e'$, then
 2339 $\vdash_H E[e'] : \tau$

2340 *Proof*:

2341 By induction on the structure of E .

2342 **CASE** $E \in E^\bullet :$
 2343 1. Contradiction by $\vdash_H E[e] : \tau$
 2344 **CASE** $E = E_0 e_1 :$
 2345 1. $E[e] = E_0[e] e_1$
 2346 2. $\vdash_H E_0[e] : \tau_0$
 2347 by *inversion*
 2348 3. QED by the induction hypothesis (2)
 2349 **CASE** $E = v_0 E_1 :$
 2350 1. $E[e] = v_0 E_1[e]$
 2351 2. $\vdash_H E_1[e] : \tau_1$
 2352 by *inversion*
 2353 3. QED by the induction hypothesis (2)
 2354 **CASE** $E = \langle E_0, e_1 \rangle :$
 2355 1. $E[e] = \langle E_0[e], e_1 \rangle$
 2356 2. $\vdash_H E_0[e] : \tau_0$
 2357 by *inversion*
 2358 3. QED by the induction hypothesis (2)
 2359 **CASE** $E = \langle v_0, E_1 \rangle :$
 2360 1. $E[e] = \langle v_0, E_1[e] \rangle$
 2361 2. $\vdash_H E_1[e] : \tau_1$
 2362 by *inversion*
 2363 3. QED by the induction hypothesis (2)
 2364
 2365

CASE $E = op^1 E_0 :$
 2366 1. $E[e] = op^1 E_0[e]$
 2367 2. $\vdash_H E_0[e] : \tau_0$
 2368 by *inversion*
 2369 3. QED by the induction hypothesis (2)
 2370 **CASE** $E = op^2 E_0 e_1 :$
 2371 1. $E[e] = op^2 E_0[e] e_1$
 2372 2. $\vdash_H E_0[e] : \tau_0$
 2373 by *inversion*
 2374 3. QED by the induction hypothesis (2)
 2375 **CASE** $E = op^2 v_0 E_1 :$
 2376 1. $E[e] = op^2 v_0 E_1[e]$
 2377 2. $\vdash_H E_1[e] : \tau_1$
 2378 by *inversion*
 2379 3. QED by the induction hypothesis (2)
 2380 **CASE** $E = \text{dyn } \tau_0 E_0 :$
 2381 1. $E[e] = \text{dyn } \tau_0 E_0[e]$
 2382 2. $\vdash_H E_0[e]$
 2383 by *inversion*
 2384 3. QED by *dynamic stat hole typing* (2)
 2385 **CASE** $E = \text{stat } \tau_0 E_0 :$
 2386 1. Contradiction by $\vdash_H E[e] : \tau$
 2387 \square

Lemma 2.31 : \vdash_H *static inversion*

- If $\Gamma \vdash_H x : \tau$ then $(x : \tau') \in \Gamma$ and $\tau' \leq \tau$ 2390
- If $\Gamma \vdash_H \lambda(x : \tau'_d). e' : \tau$ then $(x : \tau'_d), \Gamma \vdash_H e' : \tau'_c$ and $\tau'_d \Rightarrow \tau'_c \leq \tau$ 2391
- If $\Gamma \vdash_H \langle e_0, e_1 \rangle : \tau$ then $\Gamma \vdash_H e_0 : \tau_0$ and $\Gamma \vdash_H e_1 : \tau_1$ and $\tau_0 \times \tau_1 \leq \tau$ 2392
- If $\Gamma \vdash_H e_0 e_1 : \tau_c$ then $\Gamma \vdash_H e_0 : \tau'_d \Rightarrow \tau'_c$ and $\Gamma \vdash_H e_1 : \tau'_d$ and $\tau'_c \leq \tau_c$ 2393
- If $\Gamma \vdash_H \text{fst } e : \tau$ then $\Gamma \vdash_H e : \tau_0 \times \tau_1$ and $\Delta(\text{fst}, \tau_0 \times \tau_1) = \tau_0$ and $\tau_0 \leq \tau$ 2394
- If $\Gamma \vdash_H \text{snd } e : \tau$ then $\Gamma \vdash_H e : \tau_0 \times \tau_1$ and $\Delta(\text{snd}, \tau_0 \times \tau_1) = \tau_1$ and $\tau_1 \leq \tau$ 2395
- If $\Gamma \vdash_H op^2 e_0 e_1 : \tau$ then $\Gamma \vdash_H e_0 : \tau_0$ and $\Gamma \vdash_H e_1 : \tau_1$ and $\Delta(op^2, \tau_0, \tau_1) = \tau'$ and $\tau' \leq \tau$ 2396
- If $\Gamma \vdash_H \text{mon } \tau_d \Rightarrow \tau_c v' : \tau$ then $\Gamma \vdash_H v' : \tau_d \Rightarrow \tau_c$ and $\tau' \leq \tau$ 2397
- If $\Gamma \vdash_H \text{dyn } \tau' e' : \tau$ then $\Gamma \vdash_H e' : \tau'$ and $\tau' \leq \tau$ 2398

2399 *Proof*:

2400 QED by the definition of $\Gamma \vdash_H e : \tau$

2401 \square

Lemma 2.32 : \vdash_H *dynamic inversion*

- If $\Gamma \vdash_H x$ then $x \in \Gamma$ 2402
- If $\Gamma \vdash_H \lambda x. e'$ then $x, \Gamma \vdash_H e'$ 2403
- If $\Gamma \vdash_H \langle e_0, e_1 \rangle$ then $\Gamma \vdash_H e_0$ and $\Gamma \vdash_H e_1$ 2404
- If $\Gamma \vdash_H e_0 e_1$ then $\Gamma \vdash_H e_0$ and $\Gamma \vdash_H e_1$ 2405
- If $\Gamma \vdash_H op^1 e_0$ then $\Gamma \vdash_H e_0$ 2406
- If $\Gamma \vdash_H op^2 e_0 e_1$ then $\Gamma \vdash_H e_0$ and $\Gamma \vdash_H e_1$ 2407
- If $\Gamma \vdash_H \text{mon } \tau_d \Rightarrow \tau_c v' : \tau$ then $\Gamma \vdash_H v' : \tau_d \Rightarrow \tau_c$ 2408
- If $\Gamma \vdash_H \text{stat } \tau' e' : \tau$ then $\Gamma \vdash_H e' : \tau'$ 2409

2410 *Proof*:

2411 QED by the definition of $\Gamma \vdash_H e$

□

Lemma 2.33 : H canonical forms

- If $\vdash_H v : \tau_0 \times \tau_1$ then $v = \langle v_0, v_1 \rangle$
- If $\vdash_H v : \tau_d \Rightarrow \tau_c$ then either:
 - $v = \lambda(x:\tau_x). e'$
 - $\wedge \tau_d \leq \tau_x$
 - or $v = \text{mon}(\tau'_d \Rightarrow \tau'_c) v'$
 - $\wedge \tau'_d \Rightarrow \tau'_c \leq \tau_d \Rightarrow \tau_c$
- If $\vdash_H v : \text{Int}$ then $v \in i$
- If $\vdash_H v : \text{Nat}$ then $v \in \mathbb{N}$

*Proof:*QED by definition of $\vdash_H e : \tau$

□

Lemma 2.34 : Δ type soundness

If $\vdash_H v_0 : \tau_0$ and $\vdash_H v_1 : \tau_1$ and $\Delta(\text{op}^2, \tau_0, \tau_1) = \tau$ then $\vdash_H \delta(\text{op}^2, v_0, v_1) : \tau$.

*Proof:*By case analysis on the definition of Δ .**CASE** $\Delta(\text{sum}, \text{Nat}, \text{Nat}) = \text{Nat}$:

1. $v_0 = i_0, i_0 \in \mathbb{N}$
 $\wedge v_1 = i_1, i_1 \in \mathbb{N}$
 by *canonical forms*
2. $\delta(\text{sum}, i_0, i_1) = i_0 + i_1 \in \mathbb{N}$
3. QED

CASE $\Delta(\text{sum}, \text{Int}, \text{Int}) = \text{Int}$:

1. $v_0 = i_0$
 $\wedge v_1 = i_1$
 by *canonical forms*
2. $\delta(\text{sum}, i_0, i_1) = i_0 + i_1 \in i$
3. QED

CASE $\Delta(\text{quotient}, \text{Nat}, \text{Nat}) = \text{Nat}$:

1. $v_0 = i_0, i_0 \in \mathbb{N}$
 $\wedge v_1 = i_1, i_1 \in \mathbb{N}$
 by *canonical forms*
2. **IF** $i_1 = 0$:
 - a. $\delta(\text{quotient}, i_0, i_1) = \text{BndryErr}$
 - b. QED by $\vdash_H \text{BndryErr} : \tau$
- ELSE** $i_1 \neq 0$:
 - a. $\delta(\text{quotient}, i_0, i_1) = \lfloor i_0/i_1 \rfloor \in \mathbb{N}$
 - b. QED

CASE $\Delta(\text{quotient}, \text{Int}, \text{Int}) = \text{Int}$:

1. $v_0 = i_0$
 $\wedge v_1 = i_1$
 by *canonical forms*
2. **IF** $i_1 = 0$:
 - a. $\delta(\text{quotient}, i_0, i_1) = \text{BndryErr}$
 - b. QED by $\vdash_H \text{BndryErr} : \tau$
- ELSE** $i_1 \neq 0$:
 - a. $\delta(\text{quotient}, i_0, i_1) = \lfloor i_0/i_1 \rfloor \in i$
 - b. QED

□

Lemma 2.35 : δ preservation

- If $\vdash_H v$ and $\delta(\text{op}^1, v) = e$ then $\vdash_H e$
- If $\vdash_H v_0$ and $\vdash_H v_1$ and $\delta(\text{op}^2, v_0, v_1) = e$ then $\vdash_H e$

*Proof:***CASE** $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$:

1. $\vdash_H v_0$
 by *inversion*

2. QED

CASE $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$:

1. $\vdash_H v_1$
 by *inversion*

2. QED

CASE $\delta(\text{sum}, v_0, v_1) = v_0 + v_1$:

1. QED

CASE $\delta(\text{quotient}, v_0, v_1) = \lfloor v_0/v_1 \rfloor$:

1. QED

CASE $\delta(\text{op}^2, v_0, v_1) = \text{BndryErr}$:

1. QED

□

Lemma 2.36 : H substitution

- If $(x:\tau_x), \Gamma \vdash_H e$ and $\vdash_H v : \tau_x$ then $\Gamma \vdash_H e[x \leftarrow v]$
- If $x, \Gamma \vdash_H e$ and $\vdash_H v$ then $\Gamma \vdash_H e[x \leftarrow v]$
- If $(x:\tau_x), \Gamma \vdash_H e : \tau$ and $\vdash_H v : \tau_x$ then $\Gamma \vdash_H e[x \leftarrow v] : \tau$
- If $x, \Gamma \vdash_H e : \tau$ and $\vdash_H v$ then $\Gamma \vdash_H e[x \leftarrow v] : \tau$

Proof:

By the following four lemmas: *dynamic context static value substitution*, *dynamic context dynamic value substitution*, *static context static value substitution*, and *static context dynamic value substitution*.

□

Lemma 2.37 : H dynamic-static substitution

If $(x:\tau_x), \Gamma \vdash_H e$ and $\vdash_H v : \tau_x$ then $\Gamma \vdash_H e[x \leftarrow v]$

*Proof:*By induction on the structure of e .**CASE** $e = x$:

1. Contradiction by $(x:\tau_x), \Gamma \vdash_H x$

CASE $e = x'$:

1. QED by $(x'[x \leftarrow v]) = x'$

CASE $e = i$:

1. QED by $i[x \leftarrow v] = i$

CASE $e = \lambda x'. e'$:

1. $e[x \leftarrow v] = \lambda x'. (e'[x \leftarrow v])$

2. $x', (x:\tau_x), \Gamma \vdash_H e'$

by *inversion*

3. $x', \Gamma \vdash_H e'[x \leftarrow v]$

by the induction hypothesis (2)

4. $\Gamma \vdash_H \lambda x'. (e'[x \leftarrow v])$

by (3)

5. QED

CASE $e = \lambda(x':\tau'). e'$:

1. Contradiction by $(x:\tau_x), \Gamma \vdash_H e$

CASE $e = \text{mon}(\tau_d \Rightarrow \tau_c) v'$:

1. $e[x \leftarrow v] = \text{mon}(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v]$

2531 2. $(x:\tau_x), \Gamma \vdash_H v' : \tau_d \Rightarrow \tau_c$
 2532 by *inversion*
 2533 3. $\Gamma \vdash_H v'[x \leftarrow v] : \tau_d \Rightarrow \tau_c$
 2534 by *static context static value substitution* (2)
 2535 4. $\Gamma \vdash_H \text{mon}(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v]$
 2536 by (3)
 2537 5. QED
 2538 **CASE** $e = \langle e_0, e_1 \rangle :$
 2539 1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
 2540 2. $(x:\tau_x), \Gamma \vdash_H e_0$
 2541 $\wedge (x:\tau_x), \Gamma \vdash_H e_1$
 2542 by *inversion*
 2543 3. $\Gamma \vdash_H e_0[x \leftarrow v]$
 2544 $\wedge \Gamma \vdash_H e_1[x \leftarrow v]$
 2545 by the induction hypothesis (2)
 2546 4. $\Gamma \vdash_H \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
 2547 by (3)
 2548 5. QED
 2549 **CASE** $e = e_0 e_1 :$
 2550 1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$
 2551 2. $(x:\tau_x), \Gamma \vdash_H e_0$
 2552 $\wedge (x:\tau_x), \Gamma \vdash_H e_1$
 2553 by *inversion*
 2554 3. $\Gamma \vdash_H e_0[x \leftarrow v]$
 2555 $\wedge \Gamma \vdash_H e_1[x \leftarrow v]$
 2556 by the induction hypothesis (2)
 2557 4. $\Gamma \vdash_H e_0[x \leftarrow v] e_1[x \leftarrow v]$
 2558 by (3)
 2559 5. QED
 2560 **CASE** $e = \text{op}^1 e_0 :$
 2561 1. $e[x \leftarrow v] = \text{op}^1 e_0[x \leftarrow v]$
 2562 2. $(x:\tau_x), \Gamma \vdash_H e_0$
 2563 by *inversion*
 2564 3. $\Gamma \vdash_H e_0[x \leftarrow v]$
 2565 by the induction hypothesis (2)
 2566 4. $\Gamma \vdash_H \text{op}^1 e_0[x \leftarrow v]$
 2567 by (3)
 2568 5. QED
 2569 **CASE** $e = \text{op}^2 e_0 e_1 :$
 2570 1. $e[x \leftarrow v] = \text{op}^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 2571 2. $(x:\tau_x), \Gamma \vdash_H e_0$
 2572 $\wedge (x:\tau_x), \Gamma \vdash_H e_1$
 2573 by *inversion*
 2574 3. $\Gamma \vdash_H e_0[x \leftarrow v]$
 2575 $\wedge \Gamma \vdash_H e_1[x \leftarrow v]$
 2576 by the induction hypothesis (2)
 2577 4. $\Gamma \vdash_H \text{op}^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 2578 by (3)
 2579 5. QED
 2580 **CASE** $e = \text{stat } \tau' e' :$
 2581 1. $e[x \leftarrow v] = \text{stat } \tau' e'[x \leftarrow v]$
 2582 2. $(x:\tau_x), \Gamma \vdash_H e' : \tau'$
 2583 by *inversion*

3. $\Gamma \vdash_H e'[x \leftarrow v] : \tau'$
 by *static context static value substitution* (2)
 4. $\Gamma \vdash_H \text{stat } \tau' e'[x \leftarrow v]$
 by (3)
 5. QED
CASE $e = \text{Err} :$
 1. QED $\text{Err} = \text{Err}[x \leftarrow v]$

□

Lemma 2.38 : H dynamic-dynamic substitutionIf $x, \Gamma \vdash_H e$ and $\vdash_H v$ then $\Gamma \vdash_H e[x \leftarrow v]$ *Proof*:By induction on the structure of e **CASE** $e = x :$ 1. $e[x \leftarrow v] = v$ 2. $\Gamma \vdash_H v$ by *weakening*

3. QED

CASE $e = x' :$ 1. QED by $(x'[x \leftarrow v]) = x'$ **CASE** $e = i :$ 1. QED by $i[x \leftarrow v] = i$ **CASE** $e = \lambda x'. e' :$ 1. $e[x \leftarrow v] = \lambda x'. (e'[x \leftarrow v])$ 2. $x', x, \Gamma \vdash_H e'$ by *inversion*3. $x', \Gamma \vdash_H e'[x \leftarrow v]$

by the induction hypothesis (2)

4. $\Gamma \vdash_H \lambda x'. (e'[x \leftarrow v])$

by (3)

5. QED

CASE $e = \lambda(x':\tau'). e' :$ 1. Contradiction by $x, \Gamma \vdash_H e$ **CASE** $e = \text{mon}(\tau_d \Rightarrow \tau_c) v' :$ 1. $e[x \leftarrow v] = \text{mon}(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v]$ 2. $x, \Gamma \vdash_H v' : \tau_d \Rightarrow \tau_c$ by *inversion*3. $\Gamma \vdash_H v'[x \leftarrow v] : \tau_d \Rightarrow \tau_c$ by *static context dynamic value substitution* (2)4. $\Gamma \vdash_H \text{mon}(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v]$

by (3)

5. QED

CASE $e = \langle e_0, e_1 \rangle :$ 1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$ 2. $x, \Gamma \vdash_H e_0$ $\wedge x, \Gamma \vdash_H e_1$ by *inversion*3. $\Gamma \vdash_H e_0[x \leftarrow v]$ $\wedge \Gamma \vdash_H e_1[x \leftarrow v]$

by the induction hypothesis (2)

4. $\Gamma \vdash_H \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$

by (3)

5. QED

CASE $e = e_0 e_1 :$

2641	1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$	5. $\Gamma \vdash_H v : \tau$	2696
2642	2. $x, \Gamma \vdash_H e_0$	by <i>weakening</i>	2697
2643	$\wedge x, \Gamma \vdash_H e_1$	6. QED	2698
2644	by <i>inversion</i>	CASE $e = x' :$	2699
2645	3. $\Gamma \vdash_H e_0[x \leftarrow v]$	1. QED by $(x'[x \leftarrow v]) = x'$	2700
2646	$\wedge \Gamma \vdash_H e_1[x \leftarrow v]$	CASE $e = i :$	2701
2647	by the induction hypothesis (2)	1. QED by $i[x \leftarrow v] = i$	2702
2648	4. $\Gamma \vdash_H e_0[x \leftarrow v] e_1[x \leftarrow v]$	CASE $e = \lambda x'. e' :$	2703
2649	by (3)	1. Contradiction by $(x : \tau_x), \Gamma \vdash_H e : \tau$	2704
2650	5. QED	CASE $e = \lambda(x' : \tau'). e' :$	2705
2651	CASE $e = op^1 e_0 :$	1. $e[x \leftarrow v] = \lambda(x' : \tau'). (e'[x \leftarrow v])$	2706
2652	1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$	2. $(x' : \tau'), (x : \tau_x), \Gamma \vdash_H e' : \tau'_c$	2707
2653	2. $x, \Gamma \vdash_H e_0$	$\wedge \tau' \Rightarrow \tau'_c \leq \tau$	2708
2654	by <i>inversion</i>	3. $(x' : \tau'), \Gamma \vdash_H e'[x \leftarrow v] : \tau'_c$	2709
2655	3. $\Gamma \vdash_H e_0[x \leftarrow v]$	by the induction hypothesis (2)	2710
2656	by the induction hypothesis (2)	4. $\Gamma \vdash_H \lambda(x' : \tau'). e' : \tau$	2711
2657	4. $\Gamma \vdash_H op^1 e_0[x \leftarrow v]$	5. QED	2712
2658	by (3)	CASE $e = \text{mon}(\tau_d \Rightarrow \tau_c) v' :$	2713
2659	5. QED	1. $e[x \leftarrow v] = \text{mon}(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v]$	2714
2660	CASE $e = op^2 e_0 e_1 :$	2. $(x : \tau_x), \Gamma \vdash_H v'$	2715
2661	1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$	by <i>inversion</i>	2716
2662	2. $x, \Gamma \vdash_H e_0$	3. $\Gamma \vdash_H v'[x \leftarrow v]$	2717
2663	$\wedge x, \Gamma \vdash_H e_1$	by <i>dynamic context static value substitution</i> (2)	2718
2664	by <i>inversion</i>	4. $\Gamma \vdash_H \text{mon}(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v] : \tau$	2719
2665	3. $\Gamma \vdash_H e_0[x \leftarrow v]$	by (3)	2720
2666	$\wedge \Gamma \vdash_H e_1[x \leftarrow v]$	5. QED	2721
2667	by the induction hypothesis (2)	CASE $e = \langle e_0, e_1 \rangle :$	2722
2668	4. $\Gamma \vdash_H op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$	1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$	2723
2669	by (3)	2. $(x : \tau_x), \Gamma \vdash_H e_0 : \tau_0$	2724
2670	5. QED	$\wedge (x : \tau_x), \Gamma \vdash_H e_1 : \tau_1$	2725
2671	CASE $e = \text{stat } \tau' e' :$	by <i>inversion</i>	2726
2672	1. $e[x \leftarrow v] = \text{stat } \tau' e'[x \leftarrow v]$	3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$	2727
2673	2. $x, \Gamma \vdash_H e' : \tau'$	$\wedge \Gamma \vdash_H e_1[x \leftarrow v] : \tau_1$	2728
2674	by <i>inversion</i>	by the induction hypothesis (2)	2729
2675	3. $\Gamma \vdash_H e'[x \leftarrow v] : \tau'$	4. $\Gamma \vdash_H \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle : \tau$	2730
2676	by <i>static context static value substitution</i> (2)	by (3)	2731
2677	4. $\Gamma \vdash_H \text{stat } \tau' e'[x \leftarrow v]$	5. QED	2732
2678	by (3)	CASE $e = e_0 e_1 :$	2733
2679	5. QED	1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$	2734
2680	CASE $e = \text{Err} :$	2. $(x : \tau_x), \Gamma \vdash_H e_0 : \tau_0$	2735
2681	1. QED $\text{Err} = \text{Err}[x \leftarrow v]$	$\wedge (x : \tau_x), \Gamma \vdash_H e_1 : \tau_1$	2736
2682	□	by <i>inversion</i>	2737
2683	Lemma 2.39 : H <i>static-static substitution</i>	3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$	2738
2684	■ If $(x : \tau_x), \Gamma \vdash_H e : \tau$ and $\vdash_H v : \tau_x$ then $\Gamma \vdash_H e[x \leftarrow v] : \tau$	$\wedge \Gamma \vdash_H e_1[x \leftarrow v] : \tau_1$	2739
2685	<i>Proof</i> :	by the induction hypothesis (2)	2740
2686	By induction on the structure of e .	4. $\Gamma \vdash_H e_0[x \leftarrow v] e_1[x \leftarrow v] : \tau$	2741
2687	CASE $e = x :$	by (3)	2742
2688	1. $e[x \leftarrow v] = v$	5. QED	2743
2689	2. $(x : \tau_x), \Gamma \vdash_H x : \tau$	CASE $e = op^1 e_0 :$	2744
2690	3. $\tau_x \leq \tau$	1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$	2745
2691	by <i>inversion</i>	2. $(x : \tau_x), \Gamma \vdash_H e_0 : \tau_0$	2746
2692	4. $\vdash_H v : \tau$	by <i>inversion</i>	2747
2693	by (3)	3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$	2748
2694		by the induction hypothesis (2)	2749
2695			2750

2751 4. $\Gamma \vdash_H op^1 e_0[x \leftarrow v] : \tau$
 2752 by (3)
 2753 5. QED
 2754 **CASE** $e = op^2 e_0 e_1 :$
 2755 1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 2756 2. $(x : \tau_x), \Gamma \vdash_H e_0 : \tau_0$
 2757 $\wedge (x : \tau_x), \Gamma \vdash_H e_1 : \tau_1$
 2758 by *inversion*
 2759 3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$
 2760 $\wedge \Gamma \vdash_H e_1[x \leftarrow v] : \tau_1$
 2761 by the induction hypothesis (2)
 2762 4. $\Gamma \vdash_H op^2 e_0[x \leftarrow v] e_1[x \leftarrow v] : \tau$
 2763 by (3)
 2764 5. QED
 2765 **CASE** $e = \text{dyn } \tau' e' :$
 2766 1. $e[x \leftarrow v] = \text{dyn } \tau' e'[x \leftarrow v]$
 2767 2. $(x : \tau_x), \Gamma \vdash_H e' :$
 2768 by *inversion*
 2769 3. $\Gamma \vdash_H e'[x \leftarrow v]$
 2770 by *dynamic context static value substitution* (2)
 2771 4. $\Gamma \vdash_H \text{dyn } \tau' e'[x \leftarrow v] : \tau$
 2772 by (3)
 2773 5. QED
 2774 **CASE** $e = \text{Err} :$
 2775 1. QED by $\text{Err} = \text{Err}[x \leftarrow v]$
 2776 \square
 2777 **Lemma 2.40** : H *static-dynamic substitution*
 2778 If $x, \Gamma \vdash_H e : \tau$ and $\vdash_H v$ then $\Gamma \vdash_H e[x \leftarrow v] : \tau$
 2779 *Proof*:
 2780 By induction on the structure of e .
 2781 **CASE** $e = x :$
 2782 1. Contradiction by $x, \Gamma \vdash_H x : \tau$
 2783 **CASE** $e = x' :$
 2784 1. QED by $(x'[x \leftarrow v]) = x'$
 2785 **CASE** $e = i :$
 2786 1. QED by $i[x \leftarrow v] = i$
 2787 **CASE** $e = \lambda x'. e' :$
 2788 1. Contradiction by $(x : \tau_x), \Gamma \vdash_H e : \tau$
 2789 **CASE** $e = \lambda(x' : \tau'). e' :$
 2790 1. $e[x \leftarrow v] = \lambda(x' : \tau'). (e'[x \leftarrow v])$
 2791 2. $(x' : \tau'), x, \Gamma \vdash_H e' : \tau'_c$
 2792 $\wedge \tau' \Rightarrow \tau'_c \leq \tau$
 2793 3. $(x' : \tau'), \Gamma \vdash_H e'[x \leftarrow v] : \tau'_c$
 2794 by the induction hypothesis (2)
 2795 4. $\Gamma \vdash_H \lambda(x' : \tau'). e' : \tau$
 2796 5. QED
 2797 **CASE** $e = \text{mon}(\tau_d \Rightarrow \tau_c) v' :$
 2798 1. $e[x \leftarrow v] = \text{mon}(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v]$
 2799 2. $x, \Gamma \vdash_H v' :$
 2800 by *inversion*
 2801 3. $\Gamma \vdash_H v'[x \leftarrow v]$
 2802 by *dynamic context dynamic value substitution* (2)
 2803
 2804
 2805

2806 4. $\Gamma \vdash_H \text{mon}(\tau_d \Rightarrow \tau_c) v'[x \leftarrow v] : \tau$
 2807 by (3)
 2808 5. QED
 2809 **CASE** $e = \langle e_0, e_1 \rangle :$
 2810 1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
 2811 2. $x, \Gamma \vdash_H e_0 : \tau_0$
 2812 $\wedge x, \Gamma \vdash_H e_1 : \tau_1$
 2813 by *inversion*
 2814 3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$
 2815 $\wedge \Gamma \vdash_H e_1[x \leftarrow v] : \tau_1$
 2816 by the induction hypothesis (2)
 2817 4. $\Gamma \vdash_H \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle : \tau$
 2818 by (3)
 2819 5. QED
 2820 **CASE** $e = e_0 e_1 :$
 2821 1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$
 2822 2. $x, \Gamma \vdash_H e_0 : \tau_0$
 2823 $\wedge x, \Gamma \vdash_H e_1 : \tau_1$
 2824 by *inversion*
 2825 3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$
 2826 $\wedge \Gamma \vdash_H e_1[x \leftarrow v] : \tau_1$
 2827 by the induction hypothesis (2)
 2828 4. $\Gamma \vdash_H e_0[x \leftarrow v] e_1[x \leftarrow v] : \tau$
 2829 by (3)
 2830 5. QED
 2831 **CASE** $e = op^1 e_0 :$
 2832 1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$
 2833 2. $x, \Gamma \vdash_H e_0 : \tau_0$
 2834 by *inversion*
 2835 3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$
 2836 by the induction hypothesis (2)
 2837 4. $\Gamma \vdash_H op^1 e_0[x \leftarrow v] : \tau$
 2838 by (3)
 2839 5. QED
 2840 **CASE** $e = op^2 e_0 e_1 :$
 2841 1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 2842 2. $x, \Gamma \vdash_H e_0 : \tau_0$
 2843 $\wedge x, \Gamma \vdash_H e_1 : \tau_1$
 2844 by *inversion*
 2845 3. $\Gamma \vdash_H e_0[x \leftarrow v] : \tau_0$
 2846 $\wedge \Gamma \vdash_H e_1[x \leftarrow v] : \tau_1$
 2847 by the induction hypothesis (2)
 2848 4. $\Gamma \vdash_H op^2 e_0[x \leftarrow v] e_1[x \leftarrow v] : \tau$
 2849 by (3)
 2850 5. QED
 2851 **CASE** $e = \text{dyn } \tau' e' :$
 2852 1. $e[x \leftarrow v] = \text{dyn } \tau' e'[x \leftarrow v]$
 2853 2. $x, \Gamma \vdash_H e' :$
 2854 by *inversion*
 2855 3. $\Gamma \vdash_H e'[x \leftarrow v]$
 2856 by *dynamic context dynamic value substitution* (2)
 2857 4. $\Gamma \vdash_H \text{dyn } \tau' e'[x \leftarrow v] : \tau$
 2858 by (3)
 2859 5. QED
 2860

2861	CASE $e = \text{Err}$:	2916
2862	1. QED by $\text{Err} = \text{Err}[x \leftarrow v]$	2917
2863	\square	2918
2864	Lemma 2.41 : <i>weakening</i>	2919
2865	• If $\Gamma \vdash_H e$ then $x, \Gamma \vdash_H e$	2920
2866	• If $\Gamma \vdash_H e : \tau$ then $(x : \tau'), \Gamma \vdash_H e : \tau$	2921
2867	<i>Proof</i> :	2922
2868	• e is closed under Γ	2923
2869	by $\Gamma \vdash_H e$	2924
2870	$\vee \Gamma \vdash_H e : \tau$	2925
2871	• QED x is unused in the derivation	2926
2872	\square	2927
2873		2928
2874		2929
2875		2930
2876		2931
2877		2932
2878		2933
2879		2934
2880		2935
2881		2936
2882		2937
2883		2938
2884		2939
2885		2940
2886		2941
2887		2942
2888		2943
2889		2944
2890		2945
2891		2946
2892		2947
2893		2948
2894		2949
2895		2950
2896		2951
2897		2952
2898		2953
2899		2954
2900		2955
2901		2956
2902		2957
2903		2958
2904		2959
2905		2960
2906		2961
2907		2962
2908		2963
2909		2964
2910		2965
2911		2966
2912		2967
2913		2968
2914		2969
2915		2970

A.3 (E) Erasure Embedding

A.3.1 Erasure Definitions

Language E

$e = x \mid v \mid \langle e, e \rangle \mid e e \mid op^1 e \mid op^2 e e \mid$
 $\text{dyn } \tau e \mid \text{stat } \tau e \mid \text{Err}$
 $v = i \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x:\tau). e$
 $\tau = \text{Nat} \mid \text{Int} \mid \tau \times \tau \mid \tau \Rightarrow \tau$
 $\Gamma = \cdot \mid x, \Gamma \mid (x:\tau), \Gamma$
 $\text{Err} = \text{BndryErr} \mid \text{TagErr}$
 $r = v \mid \text{Err}$
 $E^\bullet = [] \mid E^\bullet e \mid v E^\bullet \mid \langle E^\bullet, e \rangle \mid \langle v, E^\bullet \rangle \mid$
 $op^1 E^\bullet \mid op^2 E^\bullet e \mid op^2 v E^\bullet$
 $E = E^\bullet \mid E e \mid v E \mid \langle E, e \rangle \mid \langle v, E \rangle \mid op^1 E \mid$
 $op^2 E e \mid op^2 v E \mid \text{dyn } \tau E \mid \text{stat } \tau E$

$\Delta : op^1 \times \tau \longrightarrow \tau$

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

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

$\Delta : op^2 \times \tau \times \tau \longrightarrow \tau$

$\Delta(op^2, \text{Nat}, \text{Nat}) = \text{Nat}$

$\Delta(op^2, \text{Int}, \text{Int}) = \text{Int}$

$\tau \leqslant: \tau$

$\text{Nat} \leqslant: \text{Int} \quad \frac{\tau'_d \leqslant: \tau_d \quad \tau_c \leqslant: \tau'_c}{\tau_d \Rightarrow \tau_c \leqslant: \tau'_d \Rightarrow \tau'_c} \quad \frac{\tau_0 \leqslant: \tau'_0 \quad \tau_1 \leqslant: \tau'_1}{\tau_0 \times \tau_1 \leqslant: \tau'_0 \times \tau'_1}$

$\frac{\tau \leqslant: \tau' \quad \tau' \leqslant: \tau''}{\tau \leqslant: \tau''}$

$\Gamma \vdash e$

$\frac{x \in \Gamma}{\Gamma \vdash x} \quad \frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e} \quad \frac{}{\Gamma \vdash i} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle}$

$\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1} \quad \frac{\Gamma \vdash e}{\Gamma \vdash op^1 e} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash \text{Err}}$

$\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e}$

$\Gamma \vdash e : \tau$

$\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau} \quad \frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} \quad \frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}}$

$\frac{}{\Gamma \vdash i : \text{Int}} \quad \frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c}$

$\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash op^1 e_0 : \tau} \quad \frac{\Gamma \vdash e_1 : \tau_1 \quad \Delta(op^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash op^2 e_0 e_1 : \tau} \quad \frac{\Gamma \vdash e : \tau' \quad \tau' \leqslant: \tau}{\Gamma \vdash e : \tau} \quad \frac{}{\Gamma \vdash \text{Err} : \tau}$

$\frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau}$

$\Gamma \Vdash e$

$\frac{x \in \Gamma}{\Gamma \Vdash x} \quad \frac{(x:\tau) \in \Gamma}{\Gamma \Vdash x} \quad \frac{x, \Gamma \Vdash e}{\Gamma \Vdash \lambda x. e} \quad \frac{(x:\tau), \Gamma \Vdash e}{\Gamma \Vdash \lambda(x:\tau). e} \quad \frac{}{\Gamma \Vdash i}$

$\frac{\Gamma \Vdash e_0 \quad \Gamma \Vdash e_1}{\Gamma \Vdash \langle e_0, e_1 \rangle} \quad \frac{\Gamma \Vdash e_0 \quad \Gamma \Vdash e_1}{\Gamma \Vdash e_0 e_1} \quad \frac{\Gamma \Vdash e}{\Gamma \Vdash op^1 e}$

$\frac{\Gamma \Vdash e_0 \quad \Gamma \Vdash e_1}{\Gamma \Vdash op^2 e_0 e_1} \quad \frac{}{\Gamma \Vdash \text{Err}} \quad \frac{\Gamma \Vdash e}{\Gamma \Vdash \text{dyn } \tau e} \quad \frac{\Gamma \Vdash e}{\Gamma \Vdash \text{stat } \tau e}$

$\delta(op^1, v) = e$

$\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$

$\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$

$\delta(op^2, v, v) = e$

$\delta(\text{sum}, i_0, i_1) = i_0 + i_1$

$\delta(\text{quotient}, i_0, 0) = \text{BndryErr}$

$\delta(\text{quotient}, i_0, i_1) = \lfloor i_0 / i_1 \rfloor$
if $i_1 \neq 0$

$\mathcal{D}_E : \tau \times v \longrightarrow e$

$\mathcal{D}_E(\tau, v) = v$

$\mathcal{S}_E : \tau \times v \longrightarrow e$

$\mathcal{S}_E(\tau, v) = v$

3081	$e \triangleright_{E-S} e$	3136
3082	$\text{dyn } \tau \ v \quad \triangleright_{E-S} \mathcal{D}_E(\tau, v)$	3137
3083	$\text{stat } \tau \ v \quad \triangleright_{E-S} \mathcal{S}_E(\tau, v)$	3138
3084	$v_0 \ v_1 \quad \triangleright_{E-S} \text{TagErr}$	3139
3085	if $v_0 \in \mathbb{Z}$ or $v_0 = \langle v, v' \rangle$	3140
3086	$(\lambda(x:\tau). e) \ v \quad \triangleright_{E-S} e[x \leftarrow v]$	3141
3087	$(\lambda x. e) \ v \quad \triangleright_{E-S} e[x \leftarrow v]$	3142
3088	$op^1 \ v \quad \triangleright_{E-S} \text{TagErr}$	3143
3089	if $\delta(op^1, v)$ is undefined	3144
3090	$op^1 \ v \quad \triangleright_{E-S} \delta(op^1, v)$	3145
3091	$op^2 \ v_0 \ v_1 \quad \triangleright_{E-S} \text{TagErr}$	3146
3092	if $\delta(op^2, v_0, v_1)$ is undefined	3147
3093	$op^2 \ v_0 \ v_1 \quad \triangleright_{E-S} \delta(op^2, v_0, v_1)$	3148
3094	$e \triangleright_{E-D} e$	3149
3095	$\text{stat } \tau \ v \quad \triangleright_{E-D} \mathcal{S}_E(\tau, v)$	3150
3096	$\text{dyn } \tau \ v \quad \triangleright_{E-D} \mathcal{D}_E(\tau, v)$	3151
3097	$v_0 \ v_1 \quad \triangleright_{E-D} \text{TagErr}$	3152
3098	if $v_0 \in \mathbb{Z}$ or $v_0 = \langle v, v' \rangle$	3153
3099	$(\lambda(x:\tau). e) \ v \quad \triangleright_{E-D} e[x \leftarrow v]$	3154
3100	$(\lambda x. e) \ v \quad \triangleright_{E-D} e[x \leftarrow v]$	3155
3101	$op^1 \ v \quad \triangleright_{E-D} \text{TagErr}$	3156
3102	if $\delta(op^1, v)$ is undefined	3157
3103	$op^1 \ v \quad \triangleright_{E-D} \delta(op^1, v)$	3158
3104	$op^2 \ v_0 \ v_1 \quad \triangleright_{E-D} \text{TagErr}$	3159
3105	if $\delta(op^2, v_0, v_1)$ is undefined	3160
3106	$op^2 \ v_0 \ v_1 \quad \triangleright_{E-D} \delta(op^2, v_0, v_1)$	3161
3107	$e \rightarrow_{E-S} e$	3162
3108	$E[e] \rightarrow_{E-S} E[e']$	3163
3109	if $e \triangleright_{E-S} e'$	3164
3110	$E[\text{Err}] \rightarrow_{E-S} \text{Err}$	3165
3111	$e \rightarrow_{E-D} e$	3166
3112	$E[e] \rightarrow_{E-D} E[e']$	3167
3113	if $e \triangleright_{E-D} e'$	3168
3114	$E[\text{Err}] \rightarrow_{E-D} \text{Err}$	3169
3115	$e \rightarrow_{E-S}^* e$ reflexive, transitive closure of \rightarrow_{E-S}	3170
3116	$e \rightarrow_{E-D}^* e$ reflexive, transitive closure of \rightarrow_{E-D}	3171
3117		3172
3118		3173
3119		3174
3120		3175
3121		3176
3122		3177
3123		3178
3124		3179
3125		3180
3126		3181
3127		3182
3128		3183
3129		3184
3130		3185
3131		3186
3132		3187
3133		3188
3134		3189
3135		3190

A.3.2 Erasure Theorems

Theorem 3.0 : static E-soundness

If $\vdash e : \tau$ then $\vdash_E e$ and one of the following holds:

- $e \rightarrow_{E-S}^* v$ and $\vdash_E v$
- $e \rightarrow_{E-S}^* \text{TagErr}$
- $e \rightarrow_{E-S}^* \text{BndryErr}$
- e diverges

Proof:

1. $\vdash_E e$
by *static subset*
2. QED by *progress* and *preservation*

□

Theorem 3.1 : dynamic E-soundness

If $\vdash e$ then $\vdash_E e$ and one of the following holds:

- $e \rightarrow_{E-D}^* v$ and $\vdash_E v$
- $e \rightarrow_{E-D}^* \text{TagErr}$
- $e \rightarrow_{E-D}^* \text{BndryErr}$
- e diverges

Proof:

1. $\rightarrow_{E-D}^* \Rightarrow \rightarrow_{E-S}^*$
by *definition*
2. QED by *static E soundness*

□

Remark 3.2 : E-compilation

The \rightarrow_{E-S}^* and \rightarrow_{E-D}^* relations are identical. In practice, uses of \rightarrow_{E-S}^* may be replaced with \rightarrow_{E-D}^* .

Theorem 3.3 : boundary-free E-soundness

If $\vdash e : \tau$ and e is boundary-free then one of the following holds:

- $e \rightarrow_{E-S}^* v$ and $\vdash v : \tau$
- $e \rightarrow_{E-S}^* \text{BndryErr}$
- e diverges

Proof:

QED by *boundary-free progress* and *boundary-free preservation*.

□

A.3.3 Erasure Lemmas

Lemma 3.4 : \mathcal{D}_E soundness

If $\vdash_E v$ then $\vdash_E \mathcal{D}_E(\tau, v)$.

Proof:

CASE $\mathcal{D}_E(\tau, v) = v$:

1. QED

□

Lemma 3.5 : \mathcal{S}_E soundness

If $\vdash_E v$ then $\vdash_E \mathcal{S}_E(\tau, v)$.

Proof:

CASE $\mathcal{S}_E(\tau, v) = v$:

1. QED

□

Lemma 3.6 : static subset

If $\Gamma \vdash e : \tau$ then $\Gamma \vdash_E e$.

Proof:

By structural induction on the typing relation.

CASE $\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau}$:

1. $(x:\tau) \in \Gamma$

2. $\Gamma \vdash_E x$

by (1)

3. QED

CASE $\frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c}$:

1. $(x:\tau_d), \Gamma \vdash_E e$

by the induction hypothesis

2. $\Gamma \vdash_E \lambda(x:\tau_d). e$

by (1)

3. QED

CASE $\frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}}$:

1. QED

CASE $\frac{}{\Gamma \vdash_E i : \text{Int}}$:

1. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1}$:

1. $\Gamma \vdash_E e_0$

$\wedge \Gamma \vdash_E e_1$

by the induction hypothesis

2. $\Gamma \vdash_E \langle e_0, e_1 \rangle$

by (1)

3. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c}$:

1. $\Gamma \vdash_E e_0$

$\wedge \Gamma \vdash_E e_1$

by the induction hypothesis

2. $\Gamma \vdash_E e_0 e_1$

by (1)

3. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash op^1 e_0 : \tau}$:

1. $\Gamma \vdash_E e_0$

by the induction hypothesis

2. $\Gamma \vdash_E op^1 e_0$

by (1)

3. QED

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1 \quad \Delta(op^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash op^2 e_0 e_1 : \tau}$:

1. $\Gamma \vdash_E e_0$

$\wedge \Gamma \vdash_E e_1$

by the induction hypothesis

2. $\Gamma \vdash_E op^2 e_0 e_1$

by (1)

3. QED

CASE $\frac{\Gamma \vdash e : \tau' \quad \tau' <: \tau}{\Gamma \vdash e : \tau}$:

1. $\Gamma \vdash_E e$

by the induction hypothesis

2. QED

CASE $\frac{}{\Gamma \vdash \text{Err} : \tau}$:

1. QED

CASE $\frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau}$:

1. $\Gamma \vdash_E e$

by *dynamic subset*

2. $\Gamma \vdash_E \text{dyn } \tau e$

by (1)

3. QED

□

Lemma 3.7 : dynamic subset

If $\Gamma \vdash e$ then $\Gamma \vdash_E e$.

Proof:

By structural induction on the \vdash relation.

CASE $\frac{x \in \Gamma}{\Gamma \vdash x}$:

1. $x \in \Gamma$

2. $\Gamma \vdash_E x$

by (1)

3. QED

CASE $\frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e}$:

1. $x, \Gamma \vdash_E e$

by the induction hypothesis

3411 2. $\Gamma \vdash_{\mathbb{E}} \lambda x. e$
 3412 by (1)
 3413 3. QED
 3414 **CASE** $\frac{}{\Gamma \vdash i}$:
 3415 $\Gamma \vdash i$
 3416 1. QED
 3417 **CASE** $\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle}$:
 3418 $\Gamma \vdash e_0 \quad \Gamma \vdash e_1$
 3419 by the induction hypothesis
 3420 2. $\Gamma \vdash_{\mathbb{E}} \langle e_0, e_1 \rangle$
 3421 by (1)
 3422 3. QED
 3423 **CASE** $\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1}$:
 3424 $\Gamma \vdash e_0 \quad \Gamma \vdash e_1$
 3425 by the induction hypothesis
 3426 2. $\Gamma \vdash_{\mathbb{E}} e_0 e_1$
 3427 by (1)
 3428 3. QED
 3429 **CASE** $\frac{\Gamma \vdash e}{\Gamma \vdash op^1 e}$:
 3430 $\Gamma \vdash e$
 3431 by the induction hypothesis
 3432 2. $\Gamma \vdash_{\mathbb{E}} op^1 e$
 3433 by (1)
 3434 3. QED
 3435 **CASE** $\frac{\Gamma \vdash e}{\Gamma \vdash op^2 e}$:
 3436 $\Gamma \vdash e$
 3437 by the induction hypothesis
 3438 2. $\Gamma \vdash_{\mathbb{E}} op^2 e$
 3439 by (1)
 3440 3. QED
 3441 **CASE** $\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash op^2 e_0 e_1}$:
 3442 $\Gamma \vdash e_0 \quad \Gamma \vdash e_1$
 3443 by the induction hypothesis
 3444 2. $\Gamma \vdash_{\mathbb{E}} op^2 e_0 e_1$
 3445 by (1)
 3446 3. QED
 3447 **CASE** $\frac{}{\Gamma \vdash \text{Err}}$:
 3448 $\Gamma \vdash \text{Err}$
 3449 1. QED
 3450 **CASE** $\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e}$:
 3451 $\Gamma \vdash e : \tau$
 3452 by static subset
 3453 2. $\Gamma \vdash_{\mathbb{E}} \text{stat } \tau e$
 3454 by (1)
 3455 3. QED
 3456 \square

Lemma 3.8 : \mathbb{E} progress

If $\vdash_{\mathbb{E}} e$ then one of the following holds:

- e is a value
- $e \in \text{Err}$
- $e \rightarrow_{\mathbb{E}-S} e'$
- $e \rightarrow_{\mathbb{E}-S} \text{TagErr}$
- $e \rightarrow_{\mathbb{E}-S} \text{BndryErr}$

Proof:

By the *unique evaluation contexts* lemma, there are seven possible cases.

CASE e is a value :

1. QED

CASE $e = E[v_0 v_1]$:

IF $v_0 = \lambda x. e'$:

1. $e \rightarrow_{\mathbb{E}-S} E[e'[x \leftarrow v_1]]$
by $v_0 v_1 \triangleright_{\mathbb{E}-S} e'[x \leftarrow v_1]$
2. QED

IF $v_0 = \lambda(x:\tau). e'$:

1. $e \rightarrow_{\mathbb{E}-S} E[e'[x \leftarrow v_1]]$
by $v_0 v_1 \triangleright_{\mathbb{E}-S} e'[x \leftarrow v_1]$
2. QED

ELSE $v_0 = i$

$\vee v_0 = \langle v, v' \rangle$:

1. $e \rightarrow_{\mathbb{E}-S} \text{TagErr}$
by $v_0 v_1 \triangleright_{\mathbb{E}-S} \text{TagErr}$
2. QED

CASE $e = E[op^1 v]$:

IF $\delta(op^1, v) = e''$:

1. $e \rightarrow_{\mathbb{E}-S} E[e'']$
by $(op^1 v) \triangleright_{\mathbb{E}-S} e''$
2. QED

ELSE $\delta(op^1, v)$ is undefined :

1. $e \rightarrow_{\mathbb{E}-S} \text{TagErr}$
by $(op^1 v) \triangleright_{\mathbb{E}-S} \text{TagErr}$
2. QED

CASE $e = E[op^2 v_0 v_1]$:

IF $\delta(op^2, v_0, v_1) = e''$:

1. $e \rightarrow_{\mathbb{E}-S} E[e'']$
by $(op^2 v_0 v_1) \triangleright_{\mathbb{E}-S} e''$
2. QED

IF $\delta(op^2, v_0, v_1) = \text{BndryErr}$:

1. $e \rightarrow_{\mathbb{E}-S} \text{BndryErr}$
by $(op^2 v_0 v_1) \triangleright_{\mathbb{E}-S} \text{BndryErr}$
2. QED

ELSE $\delta(op^2, v_0, v_1)$ is undefined :

1. $e \rightarrow_{\mathbb{E}-S} \text{TagErr}$
by $(op^2 v_0 v_1) \triangleright_{\mathbb{E}-S} \text{TagErr}$
2. QED

CASE $e = E[\text{dyn } \tau v]$:

1. $e \rightarrow_{\mathbb{E}-S} E[\mathcal{D}_{\mathbb{E}}(\tau, v)]$
2. QED

CASE $e = E[\text{stat } \tau v]$:

1. $e \rightarrow_{\mathbb{E}-S} E[\mathcal{S}_{\mathbb{E}}(\tau, v)]$
2. QED

CASE $e \in \text{Err}$:

3521 1. $e \rightarrow_{E-S} \text{Err}$
 3522 2. QED
 3523 \square
 3524 **Lemma 3.9** : *E preservation*
 3525 If $\vdash_E e$ and $e \rightarrow_{E-S} e'$ then $\vdash_E e'$.
 3526 *Proof*:
 3527 By *unique evaluation contexts* there are seven cases.
 3528 **CASE** e is a value :
 3529 1. Contradiction by $e \rightarrow_{E-S} e'$
 3530 **CASE** $e = E[v_0 v_1]$:
 3531 1. $v_0 = \lambda x. e'$ or $v_0 = \lambda(x:\tau). e'$
 3532 $\wedge E[v_0 v_1] \rightarrow_{E-S} E[e'[x \leftarrow v_1]]$
 3533 2. $\vdash_E v_0 v_1$
 3534 by *hole typing*
 3535 3. $\vdash_E v_0$
 3536 $\wedge \vdash_E v_1$
 3537 by *inversion* (2)
 3538 4. $x \vdash_E e'$
 3539 by *inversion* (3)
 3540 5. $\vdash_E e'[x \leftarrow v_1]$
 3541 by *substitution* (3, 4)
 3542 6. QED by *hole substitution* (5)
 3543 **CASE** $e = E[op^1 v]$:
 3544 1. $E[op^1 v] \rightarrow_{E-S} E[v']$
 3545 $\wedge \delta(op^1, v) = e''$
 3546 2. $\vdash_E op^1 v$
 3547 by *hole typing*
 3548 3. $\vdash_E v$
 3549 by *inversion* (2)
 3550 4. $\vdash_E e''$
 3551 by δ *preservation* (1,3)
 3552 5. QED by *hole substitution* (4)
 3553 **CASE** $e = E[op^2 v_0 v_1]$:
 3554 1. $E[op^2 v_0 v_1] \rightarrow_{E-S} E[v']$
 3555 $\wedge \delta(op^2, v_0, v_1) = e''$
 3556 2. $\vdash_E op^2 v_0 v_1$
 3557 by *hole typing*
 3558 3. $\vdash_E v_0$
 3559 $\wedge \vdash_E v_1$
 3560 by *inversion* (2)
 3561 4. $\vdash_E e''$
 3562 by δ *preservation* (3)
 3563 5. QED by *hole substitution* (4)
 3564 **CASE** $e = E[\text{dyn } \tau v]$:
 3565 1. $E[\text{dyn } \tau v] \rightarrow_{E-S} E[\mathcal{D}_E(\tau, v)]$
 3566 2. $\vdash_E \text{dyn } \tau v$
 3567 by *hole typing*
 3568 3. $\vdash_E v$
 3569 by *inversion* (2)
 3570 4. $\vdash_E \mathcal{D}_E(\tau, v)$
 3571 by \mathcal{D}_E *soundness* (3)
 3572 5. QED by *hole substitution* (4)
 3573 **CASE** $e = E[\text{stat } \tau v]$:

3574 1. $E[\text{stat } \tau v] \rightarrow_{E-S} S_E(\tau, v)$
 3575 2. $\vdash_E \text{stat } \tau v$
 3576 by *hole typing*
 3577 3. $\vdash_E v$
 3578 by *inversion* (2)
 3579 4. $\vdash_E S_E(\tau, v)$
 3580 by S_E *soundness* (3)
 3581 5. QED by *hole substitution* (4)
 3582 **CASE** $e = E[\text{Err}]$:
 3583 1. $E[\text{Err}] \rightarrow_{E-S} \text{Err}$
 3584 2. QED
 3585 \square
 3586 **Lemma 3.10** : *E boundary-free progress*
 3587 If $\vdash e : \tau$ and e is boundary-free, then one of the following
 3588 holds:
 3589 • e is a value
 3590 • $e \in \text{Err}$
 3591 • $e \rightarrow_{E-S} e'$
 3592 • $e \rightarrow_{E-S} \text{BndryErr}$
 3593 *Proof*:
 3594 By the *unique static evaluation contexts* lemma, there are
 3595 five cases:
 3596 **CASE** $e = v$:
 3597 1. QED
 3598 **CASE** $e = E[v_0 v_1]$:
 3599 **IF** $v_0 = \lambda(x:\tau'). e'$:
 3600 1. $e \rightarrow_{E-S} E[e'[x \leftarrow v_1]]$
 3601 by $v_0 v_1 \triangleright_{E-S} e'[x \leftarrow v_1]$
 3602 2. QED
 3603 **ELSE** $v_0 = \lambda x. e'$
 3604 $\vee v_0 = i$
 3605 $\vee v_0 = \langle v, v' \rangle$:
 3606 1. Contradiction by $\vdash e : \tau$
 3607 **CASE** $e = E[op^1 v]$:
 3608 **IF** $\delta(op^1, v) = e''$:
 3609 1. $e \rightarrow_{E-S} E[e'']$
 3610 by $(op^1 v) \triangleright_{E-S} e''$
 3611 2. QED
 3612 **ELSE** $\delta(op^1, v)$ is undefined :
 3613 1. Contradiction by $\vdash e : \tau$
 3614 **CASE** $e = E[op^2 v_0 v_1]$:
 3615 **IF** $\delta(op^2, v_0, v_1) = e''$:
 3616 1. $e \rightarrow_{E-S} E[e'']$
 3617 by $(op^2 v_0 v_1) \triangleright_{E-S} e''$
 3618 2. QED
 3619 **ELSE** $\delta(op^2, v_0, v_1)$ is undefined :
 3620 1. Contradiction by $\vdash e : \tau$
 3621 **CASE** $e = E[\text{dyn } \tau v]$:
 3622 1. $e \rightarrow_{E-S} \text{BndryErr}$
 3623 by $(\text{dyn } \tau v) \triangleright_{E-S} \text{BndryErr}$
 3624 2. QED
 3625 **ELSE** $\delta(\text{dyn } \tau, v)$ is undefined :
 3626 1. Contradiction by $\vdash e : \tau$
 3627 **CASE** $e = E[\text{Err}]$:
 3628 1. $E[\text{Err}] \rightarrow_{E-S} \text{Err}$
 3629 2. QED

□

Lemma 3.11 : E boundary-free preservation

If $\vdash e : \tau$ and e is boundary-free and $e \rightarrow_{E-S} e'$ then $\vdash e' : \tau$ and e' is boundary-free.

Proof:

By the *unique static evaluation contexts* lemma, there are five cases.

CASE e is a value :

1. Contradiction by $e \rightarrow_{E-S} e'$

CASE $e = E[v_0 v_1]$:**IF** $v_0 = \lambda(x:\tau_d). e'$:

1. $E[v_0 v_1] \rightarrow_{E-S} E[e'[x \leftarrow v_1]]$
2. $\vdash v_0 v_1 : \tau_c$
3. $\vdash v_0 : \tau_d \Rightarrow \tau_c$
 $\wedge \vdash v_1 : \tau_d$
 by (2)
4. $(x:\tau_d) \vdash e' : \tau_c$
 by (3)
5. $\vdash e'[x \leftarrow v_1] : \tau_c$
 by *substitution* (3, 4)
6. $e'[x \leftarrow v_1]$ is boundary-free
 by e' and v_1 are boundary-free

7. QED

ELSE :

1. Contradiction by $\vdash e : \tau$

CASE $e = E[op^1 v]$:

1. $E[op^1 v] \rightarrow_{E-S} E[v']$
 $\wedge \delta(op^1, v) = e''$
2. $\vdash op^1 v : \tau'$
3. $\vdash v : \tau_0$
4. $\vdash e'' : \tau'$
 by δ *preservation* (3)

5. QED

CASE $e = E[op^2 v_0 v_1]$:

1. $E[op^2 v_0 v_1] \rightarrow_{E-S} E[v']$
 $\wedge \delta(op^2, v_0, v_1) = e''$
2. $\vdash op^2 v_0 v_1 : \tau'$
3. $\vdash v_0 : \tau_0$
 $\wedge \vdash v_1 : \tau_1$
4. $\vdash e'' : \tau'$
 by δ *preservation* (3)

5. QED

CASE $e = E[Err]$:

1. $E[Err] \rightarrow_{E-S} Err$
2. QED by $\vdash Err : \tau$

□

Lemma 3.12 : E unique evaluation contextsIf $\vdash_E e$ then one of the following holds:

- e is a value
- $e = E[v_0 v_1]$
- $e = E[op^1 v]$
- $e = E[op^2 v_0 v_1]$
- $e = E[\text{dyn } \tau v]$
- $e = E[\text{stat } \tau v]$
- $e = E[Err]$

Proof:By induction on the structure of e .**CASE** $e = x$:

1. Contradiction by $\vdash_E e$

CASE $e = i$

- $\vee e = \lambda x. e'$
- $\vee e = \lambda(x:\tau_d). e' :$

1. QED

CASE $e = \langle e_0, e_1 \rangle$:**IF** $e_0 \notin v$:

1. $\vdash_E e_0$
 by *inversion*
2. $e_0 = E_0[e'_0]$
 by the induction hypothesis
3. $E = \langle E_0, e_1 \rangle$
4. QED $e = E[e'_0]$

IF $e_0 \in v$ $\wedge e_1 \notin v$:

1. $\vdash_E e_1$
 by *inversion*
2. $e_1 = E_1[e'_1]$
 by the induction hypothesis
3. $E = \langle e_0, E_1 \rangle$
4. QED $e = E[e'_1]$

ELSE $e_0 \in v$ $\wedge e_1 \in v$:

1. QED

CASE $e = e_0 e_1$:**IF** $e_0 \notin v$:

1. $\vdash_E e_0$
 by *inversion*
2. $e_0 = E_0[e'_0]$
 by the induction hypothesis
3. $E = E_0 e_1$
4. QED $e = E[e'_0]$

IF $e_0 \in v$ $\wedge e_1 \notin v$:

1. $\vdash_E e_1$
 by *inversion*
2. $e_1 = E_1[e'_1]$
 by the induction hypothesis
3. $E = e_0 E_1$
4. QED $e = E[e'_1]$

ELSE $e_0 \in v$ $\wedge e_1 \in v$:

1. $E = []$

3741 2. QED
 3742 **CASE** $e = op^1 e_0$:
 3743 **IF** $e_0 \notin v$:
 3744 1. $\vdash_E e_0$
 3745 by *inversion*
 3746 2. $e_0 = E_0[e'_0]$
 3747 by the induction hypothesis
 3748 3. $E = op^1 E_0$
 3749 4. QED $e = E[e'_0]$
 3750 **ELSE** $e_0 \in v$:
 3751 1. $E = []$
 3752 2. QED
 3753 **CASE** $e = op^2 e_0 e_1$:
 3754 **IF** $e_0 \notin v$:
 3755 1. $\vdash_E e_0$
 3756 by *inversion*
 3757 2. $e_0 = E_0[e'_0]$
 3758 by the induction hypothesis
 3759 3. $E = op^2 E_0 e_1$
 3760 4. QED $e = E[e'_0]$
 3761 **IF** $e_0 \in v$
 3762 $\wedge e_1 \notin v$:
 3763 1. $\vdash_E e_1$
 3764 by *inversion*
 3765 2. $e_1 = E_1[e'_1]$
 3766 by the induction hypothesis
 3767 3. $E = op^2 e_0 E_1$
 3768 4. QED $e = E[e'_1]$
 3769 **ELSE** $e_0 \in v$
 3770 $\wedge e_1 \in v$:
 3771 1. $E = []$
 3772 2. QED
 3773 **CASE** $e = \text{dyn } \tau e_0$:
 3774 **IF** $e_0 \notin v$:
 3775 1. $\vdash_E e_0$
 3776 by *inversion*
 3777 2. $e_0 = E_0[e'_0]$
 3778 by the induction hypothesis
 3779 3. $E = \text{dyn } \tau E_0$
 3780 4. QED $e = E[e'_0]$
 3781 **ELSE** $e_0 \in v$:
 3782 1. $E = []$
 3783 2. QED
 3784 **CASE** $e = \text{stat } \tau e_0$:
 3785 **IF** $e_0 \notin v$:
 3786 1. $\vdash_E e_0$
 3787 by *inversion*
 3788 2. $e_0 = E_0[e'_0]$
 3789 by the induction hypothesis
 3790 3. $E = \text{stat } \tau E_0$
 3791 4. QED $e = E[e'_0]$
 3792 **ELSE** $e_0 \in v$:
 3793 1. $E = []$
 3794 2. QED
 3795

CASE $e = \text{Err}$: 3796
 1. $E = []$ 3797
 2. QED 3798
 □ 3799
Lemma 3.13 : *E hole typing* 3800
 If $\vdash_E E[e]$ then the derivation contains a sub-term $\vdash_E e$ 3801
Proof: 3802
 By induction on the structure of E . 3803
CASE $E = []$: 3804
 1. QED $E[e] = e$ 3805
CASE $E = E_0 e_1$: 3806
 1. $E[e] = E_0[e] e_1$ 3807
 2. $\vdash_E E_0[e]$ 3808
 by *inversion* 3809
 3. QED by the induction hypothesis (2) 3810
CASE $E = v_0 E_1$: 3811
 1. $E[e] = v_0 E_1[e]$ 3812
 2. $\vdash_E E_1[e]$ 3813
 by *inversion* 3814
 3. QED by the induction hypothesis (2) 3815
CASE $E = \langle E_0, e_1 \rangle$: 3816
 1. $E[e] = \langle E_0[e], e_1 \rangle$ 3817
 2. $\vdash_E E_0[e]$ 3818
 by *inversion* 3819
 3. QED by the induction hypothesis (2) 3820
CASE $E = \langle v_0, E_1 \rangle$: 3821
 1. $E[e] = \langle v_0, E_1[e] \rangle$ 3822
 2. $\vdash_E E_1[e]$ 3823
 by *inversion* 3824
 3. QED by the induction hypothesis (2) 3825
CASE $E = op^1 E_0$: 3826
 1. $E[e] = op^1 E_0[e]$ 3827
 2. $\vdash_E E_0[e]$ 3828
 by *inversion* 3829
 3. QED by the induction hypothesis (2) 3830
CASE $E = op^2 E_0 e_1$: 3831
 1. $E[e] = op^2 E_0[e] e_1$ 3832
 2. $\vdash_E E_0[e]$ 3833
 by *inversion* 3834
 3. QED by the induction hypothesis (2) 3835
CASE $E = op^2 v_0 E_1$: 3836
 1. $E[e] = op^2 v_0 E_1[e]$ 3837
 2. $\vdash_E E_1[e]$ 3838
 by *inversion* 3839
 3. QED by the induction hypothesis (2) 3840
CASE $E = \text{dyn } \tau E_0$: 3841
 1. $E[e] = \text{dyn } \tau E_0[e]$ 3842
 2. $\vdash_E E_0[e]$ 3843
 by *inversion* 3844
 3. QED by the induction hypothesis (2) 3845
CASE $E = \text{stat } \tau E_0$: 3846
 1. $E[e] = \text{stat } \tau E_0[e]$ 3847
 3848
 3849
 3850

- 3851 2. $\vdash_E E_0[e]$
 3852 by *inversion*
 3853 3. QED by the induction hypothesis (2)
 3854 \square

3855 **Lemma 3.14** : *E hole substitution*

3856 If $\vdash_E E[e]$ and $\vdash_E e'$ then $\vdash_E E[e']$

3857 *Proof*:

3858 By induction on the structure of E .

3859 **CASE** $E = []$:

- 3860 1. QED $E[e'] = e'$

3861 **CASE** $E = \langle E_0, e_1 \rangle$:

- 3862 1. $E[e] = \langle E_0[e], e_1 \rangle$
 3863 $\wedge E[e'] = \langle E_0[e'], e_1 \rangle$

- 3864 2. $\vdash_E \langle E_0[e], e_1 \rangle$

- 3865 3. $\vdash_E E_0[e]$

3866 $\wedge \vdash_E e_1$

3867 by *inversion*

- 3868 4. $\vdash_E E_0[e']$

3869 by the induction hypothesis (3)

- 3870 5. $\vdash_E \langle E_0[e'], e_1 \rangle$

3871 by (3, 4)

- 3872 6. QED by (1, 5)

3873 **CASE** $E = \langle v_0, E_1 \rangle$:

- 3874 1. $E[e] = \langle v_0, E_1[e] \rangle$
 3875 $\wedge E[e'] = \langle v_0, E_1[e'] \rangle$

- 3876 2. $\vdash_E \langle v_0, E_1[e] \rangle$

- 3877 3. $\vdash_E v_0$

3878 $\wedge \vdash_E E_1[e]$

3879 by *inversion*

- 3880 4. $\vdash_E E_1[e']$

3881 by the induction hypothesis (3)

- 3882 5. $\vdash_E \langle v_0, E_1[e'] \rangle$

3883 by (3, 4)

- 3884 6. QED by (1, 5)

3885 **CASE** $E = E_0 e_1$:

- 3886 1. $E[e] = E_0[e] e_1$

3887 $\wedge E[e'] = E_0[e'] e_1$

- 3888 2. $\vdash_E E_0[e] e_1$

- 3889 3. $\vdash_E E_0[e]$

3890 $\wedge \vdash_E e_1$

3891 by *inversion*

- 3892 4. $\vdash_E E_0[e']$

3893 by the induction hypothesis (3)

- 3894 5. $\vdash_E E_0[e'] e_1$

3895 by (3, 4)

- 3896 6. QED by (1, 5)

3897 **CASE** $E = v_0 E_1$:

- 3898 1. $E[e] = v_0 E_1[e]$

3899 $\wedge E[e'] = v_0 E_1[e']$

- 3900 2. $\vdash_E v_0 E_1[e]$

- 3901 3. $\vdash_E v_0$

3902 $\wedge \vdash_E E_1[e]$

3903 by *inversion*

4. $\vdash_E E_1[e']$
 by the induction hypothesis (3)

5. $\vdash_E v_0 E_1[e']$

by (3, 4)

6. QED by (1, 5)

CASE $E = op^1 E_0$:

1. $E[e] = op^1 E_0[e]$

$\wedge E[e'] = op^1 E_0[e']$

2. $\vdash_E op^1 E_0[e]$

3. $\vdash_E E_0[e]$

by *inversion*

4. $\vdash_E E_0[e']$

by the induction hypothesis (3)

5. $\vdash_E op^1 E_0[e']$

by (3, 4)

6. QED by (1, 5)

CASE $E = op^2 E_0 e_1$:

1. $E[e] = op^2 E_0[e] e_1$

$\wedge E[e'] = op^2 E_0[e'] e_1$

2. $\vdash_E op^2 E_0[e] e_1$

3. $\vdash_E E_0[e]$

$\wedge \vdash_E e_1$

by *inversion*

4. $\vdash_E E_0[e']$

by the induction hypothesis (3)

5. $\vdash_E op^2 E_0[e'] e_1$

by (3, 4)

6. QED by (1, 5)

CASE $E = op^2 v_0 E_1$:

1. $E[e] = op^2 v_0 E_1[e]$

$\wedge E[e'] = op^2 v_0 E_1[e']$

2. $\vdash_E op^2 v_0 E_1[e]$

3. $\vdash_E v_0$

$\wedge \vdash_E E_1[e]$

by *inversion*

4. $\vdash_E E_1[e']$

by the induction hypothesis (3)

5. $\vdash_E op^2 v_0 E_1[e']$

by (3, 4)

6. QED by (1, 5)

CASE $E = \text{dyn } \tau E_0$:

1. $E[e] = \text{dyn } \tau E_0[e]$

$\wedge E[e'] = \text{dyn } \tau E_0[e']$

2. $\vdash_E \text{dyn } \tau E_0[e]$

3. $\vdash_E E_0[e]$

by *inversion*

4. $\vdash_E E_0[e']$

by the induction hypothesis (3)

5. $\vdash_E \text{dyn } \tau E_0[e']$

by (3, 4)

6. QED by (1, 5)

CASE $E = \text{stat } \tau E_0$:

1. $E[e] = \text{stat } \tau E_0[e]$

$\wedge E[e'] = \text{stat } \tau E_0[e']$

2. $\vdash_E \text{stat } \tau E_0[e]$
3. $\vdash_E E_0[e]$
by *inversion*
4. $\vdash_E E_0[e']$
by the induction hypothesis (3)
5. $\vdash_E \text{stat } \tau E_0[e']$
by (3, 4)
6. QED by (1, 5)

□

Lemma 3.15 : \vdash_E *inversion*

- If $\Gamma \vdash_E e_0 e_1$ then $\Gamma \vdash_E e_0$ and $\Gamma \vdash_E e_1$
- If $\Gamma \vdash_E \lambda x. e$ then $x, \Gamma \vdash_E e$
- If $\Gamma \vdash_E \lambda(x:\tau). e$ then $(x:\tau), \Gamma \vdash_E e$
- If $\Gamma \vdash_E \text{op}^1 e$ then $\Gamma \vdash_E e$
- If $\Gamma \vdash_E \text{op}^2 e_0 e_1$ then $\Gamma \vdash_E e_0$ and $\Gamma \vdash_E e_1$
- If $\Gamma \vdash_E \text{dyn } \tau e$ then $\Gamma \vdash_E e$
- If $\Gamma \vdash_E \text{stat } \tau e$ then $\Gamma \vdash_E e$

*Proof:*QED by the definition of \vdash_E .

□

Lemma 3.16 : \vdash_E *substitution*If $\Gamma, \Gamma \vdash_E e$ or $(x:\tau), \Gamma \vdash_E e$, and $\vdash_E v$ then $\Gamma \vdash_E e[x \leftarrow v]$ *Proof:*By induction on the structure of e .**CASE** $e = x$:

1. $e[x \leftarrow v] = v$
2. $\Gamma \vdash_E v$
by *weakening*
3. QED

CASE $e = x'$:

1. QED by $x'[x \leftarrow v] = x'$

CASE $e = i$:

1. QED by $i[x \leftarrow v] = i$

CASE $e = \lambda x. e'$:

1. QED by $(\lambda x. e')[x \leftarrow v] = \lambda x. e'$

CASE $e = \lambda(x:\tau'). e'$:

1. QED by $(\lambda(x:\tau'). e')[x \leftarrow v] = \lambda(x:\tau'). e'$

CASE $e = \lambda x'. e'$:

1. $e[x \leftarrow v] = \lambda x'. (e'[x \leftarrow v])$
2. $x', x, \Gamma \vdash_E e'$
by *inversion*
3. $x', \Gamma \vdash_E e'[x \leftarrow v]$
by the induction hypothesis (2)
4. $\Gamma \vdash_E \lambda x'. e'[x \leftarrow v]$
by (3)
5. QED

CASE $e = \lambda(x':\tau'). e'$:

1. $e[x \leftarrow v] = \lambda(x':\tau'). (e'[x \leftarrow v])$
2. $(x':\tau'), x, \Gamma \vdash_E e'$
by *inversion*
3. $(x':\tau'), \Gamma \vdash_E e'[x \leftarrow v]$
by the induction hypothesis (2)

4. $\Gamma \vdash_E \lambda(x':\tau'). (e'[x \leftarrow v])$
by (3)

5. QED

CASE $e = \langle e_0, e_1 \rangle$:

1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
2. $x, \Gamma \vdash_E e_0$
 $\wedge x, \Gamma \vdash_E e_1$
by *inversion*
3. $\Gamma \vdash_E e_0[x \leftarrow v]$
 $\wedge \Gamma \vdash_E e_1[x \leftarrow v]$
by the induction hypothesis (2)
4. $\Gamma \vdash_E \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
by (3)
5. QED

CASE $e = e_0 e_1$:

1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$
2. $x, \Gamma \vdash_E e_0$
 $\wedge x, \Gamma \vdash_E e_1$
by *inversion*
3. $\Gamma \vdash_E e_0[x \leftarrow v]$
 $\wedge \Gamma \vdash_E e_1[x \leftarrow v]$
by the induction hypothesis (2)
4. $\Gamma \vdash_E e_0[x \leftarrow v] e_1[x \leftarrow v]$
by (3)
5. QED

CASE $e = \text{op}^1 e_0$:

1. $e[x \leftarrow v] = \text{op}^1 e_0[x \leftarrow v]$
2. $x, \Gamma \vdash_E e_0$
by *inversion*
3. $\Gamma \vdash_E e_0[x \leftarrow v]$
by the induction hypothesis (2)
4. $\Gamma \vdash_E \text{op}^1 e_0[x \leftarrow v]$
by (3)
5. QED

CASE $e = \text{op}^2 e_0 e_1$:

1. $e[x \leftarrow v] = \text{op}^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
2. $x, \Gamma \vdash_E e_0$
 $\wedge x, \Gamma \vdash_E e_1$
by *inversion*
3. $\Gamma \vdash_E e_0[x \leftarrow v]$
 $\wedge \Gamma \vdash_E e_1[x \leftarrow v]$
by the induction hypothesis (2)
4. $\Gamma \vdash_E \text{op}^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
by (3)
5. QED

CASE $e = \text{dyn } \tau' e'$:

1. $e[x \leftarrow v] = \text{dyn } \tau' e'[x \leftarrow v]$
2. $x, \Gamma \vdash_E e'$
by *inversion*
3. $\Gamma \vdash_E e'[x \leftarrow v]$
by the induction hypothesis (2)
4. $\Gamma \vdash_E \text{dyn } \tau' (e'[x \leftarrow v])$
by (3)
5. QED

4071 **CASE** $e = \text{stat } \tau' e' :$
 4072 1. $e[x \leftarrow v] = \text{stat } \tau' e'[x \leftarrow v]$
 4073 2. $x, \Gamma \vdash_E e'$
 4074 by *inversion*
 4075 3. $\Gamma \vdash_E e'[x \leftarrow v]$
 4076 by the induction hypothesis (2)
 4077 4. $\Gamma \vdash_E \text{stat } \tau' (e'[x \leftarrow v])$
 4078 by (3)
 4079 5. QED
 4080 **CASE** $e = \text{Err} :$
 4081 1. QED by $\text{Err}[x \leftarrow v] = \text{Err}$
 4082 \square

4083 **Lemma 3.17** : δ preservation

- 4084 • If $\vdash_E v$ and $\delta(\text{op}^1, v) = e'$ then $\vdash_E e'$
- 4085 • If $\vdash_E v_0$ and $\vdash_E v_1$ and $\delta(\text{op}^2, v_0, v_1) = e'$ then $\vdash_E v'$

4086 *Proof*:

4087 **CASE** $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0 :$
 4088 1. $\vdash_E v_0$
 4089 by *inversion*
 4090 2. QED
 4091 **CASE** $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1 :$
 4092 1. $\vdash_E v_1$
 4093 by *inversion*
 4094 2. QED
 4095 **CASE** $\delta(\text{sum}, v_0, v_1) = v_0 + v_1 :$
 4096 1. QED
 4097 **CASE** $\delta(\text{quotient}, v_0, v_1) = \lfloor v_0/v_1 \rfloor :$
 4098 1. QED
 4099 **CASE** $\delta(\text{quotient}, v_0, v_1) = \text{BndryErr} :$
 4100 1. QED
 4101 \square

4102 **Lemma 3.18** : *weakening*

- 4103 • If $\Gamma \vdash_E e$ then $x, \Gamma \vdash_E e$
- 4104 • If $\Gamma \vdash_E e$ then $(x : \tau), \Gamma \vdash_E e$

4105 *Proof*:

4106 QED because e is closed under Γ
 4107 \square

4108 **Lemma 3.19** : *unique static evaluation contexts*

4109 If $\vdash e : \tau$ then one of the following holds:

- 4110 • e is a value
- 4111 • $e = E[v_0 v_1]$
- 4112 • $e = E[\text{op}^1 v]$
- 4113 • $e = E[\text{op}^2 v_0 v_1]$
- 4114 • $e = E[\text{Err}]$

4115 *Proof*:

4116 By induction on the structure of e .

4117 **CASE** $e = x :$
 4118 1. Contradiction by $\vdash e : \tau$
 4119 **CASE** $e = i$
 4120 $\vee e = \lambda(x : \tau_d). e' :$
 4121 1. QED e is a value
 4122 **CASE** $e = \text{stat } \tau e' :$
 4123 1. Contradiction by $\vdash_1 e : K$
 4124
 4125

CASE $e = \langle e_0, e_1 \rangle :$
 4126 **IF** $e_0 \notin v :$
 4127 1. $e_0 = E_0[e'_0]$
 4128 by the induction hypothesis
 4129 2. $E = \langle E_0, e_1 \rangle$
 4130 3. QED by $e = E[e'_0]$
 4131 **IF** $e_0 \in v$
 4132 $\wedge e_1 \notin v :$
 4133 1. $e_1 = E_1[e'_1]$
 4134 by the induction hypothesis
 4135 2. $E = \langle e_0, E_1 \rangle$
 4136 3. QED by $e = E[e'_1]$
 4137 **ELSE** $e_0 \in v$
 4138 $\wedge e_1 \in v :$
 4139 1. $E = []$
 4140 2. QED $e = E[\langle e_0, e_1 \rangle]$
 4141 **CASE** $e = e_0 e_1 :$
 4142 **IF** $e_0 \notin v :$
 4143 1. $e_0 = E_0[e'_0]$
 4144 by the induction hypothesis
 4145 2. $E = E_0 e_1$
 4146 3. QED by $e = E[e'_0]$
 4147 **IF** $e_0 \in v$
 4148 $\wedge e_1 \notin v :$
 4149 1. $e_1 = E_1[e'_1]$
 4150 by the induction hypothesis
 4151 2. $E = e_0 E_1$
 4152 3. QED by $e = E[e'_1]$
 4153 **ELSE** $e_0 \in v$
 4154 $\wedge e_1 \in v :$
 4155 1. $E = []$
 4156 2. QED $e = E[e_0 e_1]$
 4157 **CASE** $e = \text{op}^1 e_0 :$
 4158 **IF** $e_0 \notin v :$
 4159 1. $e_0 = E_0[e'_0]$
 4160 by the induction hypothesis
 4161 2. $E = \text{op}^1 E_0$
 4162 3. QED $e = E[e'_0]$
 4163 **ELSE** $e_0 \in v :$
 4164 1. $E = []$
 4165 2. QED $e = E[\text{op}^1 e_0]$
 4166 **CASE** $e = \text{op}^2 e_0 e_1 :$
 4167 **IF** $e_0 \notin v :$
 4168 1. $e_0 = E_0[e'_0]$
 4169 by the induction hypothesis
 4170 2. $E = \text{op}^2 E_0 e_1$
 4171 3. QED $e = E[e'_0]$
 4172 **IF** $e_0 \in v$
 4173 $\wedge e_1 \notin v :$
 4174 1. $e_1 = E_1[e'_1]$
 4175 by the induction hypothesis
 4176 2. $E = \text{op}^2 e_0 E_1$
 4177 3. QED $e = E[e'_1]$
 4178
 4179
 4180

4181 **ELSE** $e_0 \in v$
 4182 $\wedge e_1 \in v :$
 4183 1. $E = []$
 4184 2. QED $e = E[op^2 e_0 e_1]$
 4185 **CASE** $e = \text{dyn } \tau e_0 :$
 4186 1. Contradiction by e is boundary-free
 4187 **CASE** $e = \text{stat } \tau e_0 :$
 4188 1. Contradiction by $\vdash e : \tau$
 4189 **CASE** $e = \text{Err} :$
 4190 1. $E = []$
 4191 2. QED $e = E[\text{Err}]$
 4192 \square

Lemma 3.20 : \vdash static inversion

- If $\Gamma \vdash x : \tau$ then $(x : \tau') \in \Gamma$ and $\tau' \leq \tau$
- If $\Gamma \vdash \lambda(x : \tau'_d). e' : \tau$ then $(x : \tau'_d), \Gamma \vdash e' : \tau'_c$ and $\tau'_d \Rightarrow \tau'_c \leq \tau$
- If $\Gamma \vdash \langle e_0, e_1 \rangle : \tau$ then $\Gamma \vdash e_0 : \tau_0$ and $\Gamma \vdash e_1 : \tau_1$ and $\tau_0 \times \tau_1 \leq \tau$
- If $\Gamma \vdash e_0 e_1 : \tau_c$ then $\Gamma \vdash e_0 : \tau'_d \Rightarrow \tau'_c$ and $\Gamma \vdash e_1 : \tau'_d$ and $\tau'_c \leq \tau_c$
- If $\Gamma \vdash \text{fst } e : \tau$ then $\Gamma \vdash e : \tau_0 \times \tau_1$ and $\Delta(\text{fst}, \tau_0 \times \tau_1) = \tau_0$ and $\tau_0 \leq \tau$
- If $\Gamma \vdash \text{snd } e : \tau$ then $\Gamma \vdash e : \tau_0 \times \tau_1$ and $\Delta(\text{snd}, \tau_0 \times \tau_1) = \tau_1$ and $\tau_1 \leq \tau$
- If $\Gamma \vdash op^2 e_0 e_1 : \tau$ then $\Gamma \vdash e_0 : \tau_0$ and $\Gamma \vdash e_1 : \tau_1$ and $\Delta(op^2, \tau_0, \tau_1) = \tau'$ and $\tau' \leq \tau$
- If $\Gamma \vdash \text{dyn } \tau' e' : \tau$ then $\Gamma \vdash e'$ and $\tau' \leq \tau$

Proof:

4209 QED by the definition of $\Gamma \vdash e : \tau$
 4210 \square

Lemma 3.21 : canonical forms

- If $\vdash v : \tau_0 \times \tau_1$ then $v = \langle v_0, v_1 \rangle$
- If $\vdash v : \tau_d \Rightarrow \tau_c$ then $v = \lambda(x : \tau_x). e'$
 $\wedge \tau_d \leq \tau_x$
- If $\vdash v : \text{Int}$ then $v = i$
- If $\vdash v : \text{Nat}$ then $v = i$ and $v \in \mathbb{N}$

Proof:

4218 QED by definition of $\vdash e : \tau$
 4219 \square

Lemma 3.22 : substitution

4221 If $(x : \tau_x), \Gamma \vdash e : \tau$, and e is boundary-free and $\vdash v : \tau_x$ then
 4222 $\Gamma \vdash e[x \leftarrow v] : \tau$

Proof:

4224 By induction on the structure of e .

- CASE** $e = x :$
 4225 1. $e[x \leftarrow v] = v$
 4226 2. $\tau_x = \tau$
 4227 3. $\Gamma \vdash v : \tau$
 4228 by *weakening*
 4229 4. QED
- CASE** $e = x' :$
 4231 1. QED by $x'[x \leftarrow v] = x'$
- CASE** $e = i :$
 4233 1. QED by $i[x \leftarrow v] = i$

4236 **CASE** $e = \lambda x. e' :$
 4237 1. Contradiction by $(x : \tau_x), \Gamma \vdash e : \tau$
 4238 **CASE** $e = \lambda(x : \tau'). e' :$
 4239 1. QED by $(\lambda(x : \tau'). e')[x \leftarrow v] = \lambda(x : \tau'). e'$
 4240 **CASE** $e = \lambda(x' : \tau'). e' :$
 4241 1. $e[x \leftarrow v] = \lambda(x' : \tau'). (e'[x \leftarrow v])$
 4242 2. $(x' : \tau'), x, \Gamma \vdash e'$
 4243 by *static inversion forms*
 4244 3. $(x' : \tau'), \Gamma \vdash e'[x \leftarrow v]$
 4245 by the induction hypothesis (2)
 4246 4. $\Gamma \vdash \lambda(x' : \tau'). (e'[x \leftarrow v])$
 4247 by (3)
 4248 5. QED
- CASE** $e = \langle e_0, e_1 \rangle :$
 4249 1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
 4250 2. $x, \Gamma \vdash e_0$
 4251 $\wedge x, \Gamma \vdash e_1$
 4252 by *static inversion forms*
 4253 3. $\Gamma \vdash e_0[x \leftarrow v]$
 4254 $\wedge \Gamma \vdash e_1[x \leftarrow v]$
 4255 by the induction hypothesis (2)
 4256 4. $\Gamma \vdash \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
 4257 by (3)
 4258 5. QED
- CASE** $e = e_0 e_1 :$
 4259 1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$
 4260 2. $x, \Gamma \vdash e_0$
 4261 $\wedge x, \Gamma \vdash e_1$
 4262 by *static inversion forms*
 4263 3. $\Gamma \vdash e_0[x \leftarrow v]$
 4264 $\wedge \Gamma \vdash e_1[x \leftarrow v]$
 4265 by the induction hypothesis (2)
 4266 4. $\Gamma \vdash e_0[x \leftarrow v] e_1[x \leftarrow v]$
 4267 by (3)
 4268 5. QED
- CASE** $e = op^1 e_0 :$
 4269 1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$
 4270 2. $x, \Gamma \vdash e_0$
 4271 by *static inversion forms*
 4272 3. $\Gamma \vdash e_0[x \leftarrow v]$
 4273 by the induction hypothesis (2)
 4274 4. $\Gamma \vdash op^1 e_0[x \leftarrow v]$
 4275 by (3)
 4276 5. QED
- CASE** $e = op^2 e_0 e_1 :$
 4277 1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 4278 2. $x, \Gamma \vdash e_0$
 4279 $\wedge x, \Gamma \vdash e_1$
 4280 by *static inversion forms*
 4281 3. $\Gamma \vdash e_0[x \leftarrow v]$
 4282 $\wedge \Gamma \vdash e_1[x \leftarrow v]$
 4283 by the induction hypothesis (2)
 4284 4. $\Gamma \vdash op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 4285 by (3)
 4286 5. QED

4291	5. QED	4346
4292	CASE $e = \text{dyn } \tau' e' :$	4347
4293	1. Contradiction by e is boundary-free	4348
4294	CASE $e = \text{stat } \tau' e' :$	4349
4295	1. Contradiction by e is boundary-free	4350
4296	CASE $e = \text{Err} :$	4351
4297	1. QED $\text{Err}[x \leftarrow v] = \text{Err}$	4352
4298	□	4353
4299	Lemma 3.23 : δ preservation	4354
4300	• If $\vdash v$ and $\delta(\text{op}^1, v) = v'$ then $\vdash e'$	4355
4301	• If $\vdash v_0$ and $\vdash v_1$ and $\delta(\text{op}^2, v_0, v_1) = e'$ then $\vdash v'$	4356
4302	<i>Proof</i> :	4357
4303	CASE $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0 :$	4358
4304	1. $\vdash v_0$	4359
4305	by <i>static inversion forms</i>	4360
4306	2. QED	4361
4307	CASE $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1 :$	4362
4308	1. $\vdash v_1$	4363
4309	by <i>static inversion forms</i>	4364
4310	2. QED	4365
4311	CASE $\delta(\text{sum}, v_0, v_1) = v_0 + v_1 :$	4366
4312	1. QED	4367
4313	CASE $\delta(\text{quotient}, v_0, v_1) = \lfloor v_0/v_1 \rfloor :$	4368
4314	1. QED	4369
4315	CASE $\delta(\text{quotient}, v_0, v_1) = \text{BndryErr} :$	4370
4316	1. QED	4371
4317	□	4372
4318	Lemma 3.24 : <i>weakening</i>	4373
4319	• If $\Gamma \vdash e$ then $x, \Gamma \vdash e$	4374
4320	• If $\Gamma \vdash e$ then $(x:\tau), \Gamma \vdash e$	4375
4321	<i>Proof</i> :	4376
4322	QED because e is closed under Γ	4377
4323	□	4378
4324		4379
4325		4380
4326		4381
4327		4382
4328		4383
4329		4384
4330		4385
4331		4386
4332		4387
4333		4388
4334		4389
4335		4390
4336		4391
4337		4392
4338		4393
4339		4394
4340		4395
4341		4396
4342		4397
4343		4398
4344		4399
4345		4400

A.4 (1) First-Order Embedding

A.4.1 First-Order Definitions

Language 1

$e = x \mid v \mid e e \mid \langle e, e \rangle \mid op^1 e \mid op^2 e e \mid$
 $\text{dyn } \tau e \mid \text{stat } \tau e \mid \text{Err} \mid \text{chk } K e \mid \text{dyn } e \mid \text{stat } e$
 $v = i \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x:\tau). e$
 $\tau = \text{Nat} \mid \text{Int} \mid \tau \times \tau \mid \tau \Rightarrow \tau$
 $K = \text{Nat} \mid \text{Int} \mid \text{Pair} \mid \text{Fun} \mid \text{Any}$
 $\Gamma = \cdot \mid x, \Gamma \mid (x:\tau), \Gamma$
 $\text{Err} = \text{BndryErr} \mid \text{TagErr}$
 $r = v \mid \text{Err}$
 $E^\bullet = [] \mid E^\bullet e \mid v E^\bullet \mid \langle E^\bullet, e \rangle \mid \langle v, E^\bullet \rangle \mid$
 $op^1 E^\bullet \mid op^2 E^\bullet e \mid op^2 v E^\bullet \mid \text{chk } K E^\bullet$
 $E = E^\bullet \mid E e \mid v E \mid \langle E, e \rangle \mid \langle v, E \rangle \mid op^1 E \mid$
 $op^2 E e \mid op^2 v E \mid \text{dyn } \tau E \mid \text{stat } \tau E \mid$
 $\text{chk } K E \mid \text{dyn } E \mid \text{stat } E$

 $\Delta : op^1 \times \tau \longrightarrow \tau$ $\Delta(\text{fst}, \tau_0 \times \tau_1) = \tau_0$ $\Delta(\text{snd}, \tau_0 \times \tau_1) = \tau_1$ $\Delta : op^2 \times \tau \times \tau \longrightarrow \tau$ $\Delta(op^2, \text{Nat}, \text{Nat}) = \text{Nat}$ $\Delta(op^2, \text{Int}, \text{Int}) = \text{Int}$ $\tau \leqslant: \tau$

$$\text{Nat} \leqslant: \text{Int} \quad \frac{\tau'_d \leqslant: \tau_d \quad \tau_c \leqslant: \tau'_c}{\tau_d \Rightarrow \tau_c \leqslant: \tau'_d \Rightarrow \tau'_c} \quad \frac{\tau_0 \leqslant: \tau'_0 \quad \tau_1 \leqslant: \tau'_1}{\tau_0 \times \tau_1 \leqslant: \tau'_0 \times \tau'_1}$$

$$\frac{\tau \leqslant: \tau' \quad \tau' \leqslant: \tau''}{\tau \leqslant: \tau''}$$
 $\Gamma \vdash e$

$$\frac{x \in \Gamma}{\Gamma \vdash x} \quad \frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e} \quad \frac{}{\Gamma \vdash i} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle}$$

$$\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1} \quad \frac{\Gamma \vdash e}{\Gamma \vdash op^1 e} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash \text{Err}}$$

$$\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e}$$
 $\Gamma \vdash e : \tau$

$$\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau} \quad \frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} \quad \frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}}$$

$$\frac{}{\Gamma \vdash i : \text{Int}} \quad \frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c}$$

$$\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash op^1 e_0 : \tau} \quad \frac{\Gamma \vdash e_1 : \tau_1 \quad \Delta(op^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash op^2 e_0 e_1 : \tau} \quad \frac{\Gamma \vdash e : \tau' \quad \tau' \leqslant: \tau}{\Gamma \vdash e : \tau} \quad \frac{}{\Gamma \vdash \text{Err} : \tau}$$

$$\frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau}$$
 $K \leqslant: K$

$$\frac{}{K \leqslant: \text{Any}} \quad \frac{}{\text{Nat} \leqslant: \text{Int}} \quad \frac{}{K \leqslant: K} \quad \frac{K \leqslant: K' \quad K' \leqslant: K''}{K \leqslant: K''}$$
 $\lfloor \tau \rfloor = K$

$$\begin{aligned} \lfloor \text{Nat} \rfloor &= \text{Nat} \\ \lfloor \text{Int} \rfloor &= \text{Int} \\ \lfloor \tau_0 \times \tau_1 \rfloor &= \text{Pair} \\ \lfloor \tau_d \Rightarrow \tau_c \rfloor &= \text{Fun} \end{aligned}$$
 $\Gamma \vdash e \rightsquigarrow e$

$$\frac{}{\Gamma \vdash i \rightsquigarrow i} \quad \frac{\Gamma \vdash e_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 \rightsquigarrow e'_1}{\Gamma \vdash \langle e_0, e_1 \rangle \rightsquigarrow \langle e'_0, e'_1 \rangle} \quad \frac{x, \Gamma \vdash e \rightsquigarrow e'}{\Gamma \vdash \lambda x. e \rightsquigarrow \lambda x. e'}$$

$$\frac{}{\Gamma \vdash x \rightsquigarrow x} \quad \frac{\Gamma \vdash e_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 \rightsquigarrow e'_1}{\Gamma \vdash e_0 e_1 \rightsquigarrow e'_0 e'_1} \quad \frac{\Gamma \vdash e \rightsquigarrow e'}{\Gamma \vdash op^1 e \rightsquigarrow op^1 e'}$$

$$\frac{\Gamma \vdash e_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 \rightsquigarrow e'_1}{\Gamma \vdash op^2 e_0 e_1 \rightsquigarrow op^2 e'_0 e'_1} \quad \frac{}{\Gamma \vdash \text{Err} \rightsquigarrow \text{Err}}$$

$$\frac{\Gamma \vdash e : \tau \rightsquigarrow e'}{\Gamma \vdash \text{stat } \tau e \rightsquigarrow \text{stat } \tau e'}$$

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

$$\overline{\Gamma \vdash i : \text{Nat} \rightsquigarrow i} \quad \overline{\Gamma \vdash i : \text{Int} \rightsquigarrow i}$$

$$\frac{\Gamma \vdash e_0 : \tau_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 : \tau_1 \rightsquigarrow e'_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1 \rightsquigarrow \langle e'_0, e'_1 \rangle}$$

$$\frac{(x : \tau_d), \Gamma \vdash e : \tau_c \rightsquigarrow e'}{\Gamma \vdash \lambda(x : \tau_d). e : \tau_d \Rightarrow \tau_c \rightsquigarrow \lambda(x : \tau_d). e'} \quad \overline{\Gamma \vdash x : \tau \rightsquigarrow x}$$

$$\frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \rightsquigarrow e'_0 \quad \Gamma \vdash e_1 : \tau_d \rightsquigarrow e'_1 \quad [\tau_c] = K}{\Gamma \vdash e_0 e_1 : \tau_c \rightsquigarrow \text{chk } K (e'_0 e'_1)}$$

$$\frac{\Gamma \vdash e : \tau_0 \times \tau_1 \rightsquigarrow e' \quad [\tau_0] = K}{\Gamma \vdash \text{fst } e : \tau_0 \rightsquigarrow \text{chk } K (\text{fst } e')}$$

$$\frac{\Gamma \vdash e : \tau_0 \times \tau_1 \rightsquigarrow e' \quad [\tau_1] = K}{\Gamma \vdash \text{snd } e : \tau_1 \rightsquigarrow \text{chk } K (\text{snd } e')}$$

$$\frac{\Gamma \vdash e_0 : \tau_0 \rightsquigarrow e'_0 \quad \Gamma \vdash e : \tau' \rightsquigarrow e' \quad \tau' \leq \tau}{\Gamma \vdash \text{op}^2 e_0 e_1 : \tau \rightsquigarrow \text{op}^2 e'_0 e'_1} \quad \frac{\Gamma \vdash e : \tau' \rightsquigarrow e' \quad \tau' \leq \tau}{\Gamma \vdash e : \tau \rightsquigarrow e'}$$

$$\overline{\Gamma \vdash \text{Err} : \tau \rightsquigarrow \text{Err}} \quad \overline{\Gamma \vdash \text{dyn } \tau e : \tau \rightsquigarrow \text{dyn } \tau e'}$$

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

$$\overline{\Gamma \vdash i} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle} \quad \frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e} \quad \frac{(x : \tau), \Gamma \vdash e : \text{Any}}{\Gamma \vdash \lambda(x : \tau). e}$$

$$\frac{x \in \Gamma}{\Gamma \vdash x} \quad \frac{(x : \tau) \in \Gamma}{\Gamma \vdash x} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1} \quad \frac{\Gamma \vdash e}{\Gamma \vdash \text{op}^1 e}$$

$$\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \text{op}^2 e_0 e_1} \quad \overline{\Gamma \vdash \text{Err}} \quad \frac{\Gamma \vdash e : [\tau]}{\Gamma \vdash \text{stat } \tau e} \quad \frac{\Gamma \vdash e : \text{Any}}{\Gamma \vdash \text{stat } e}$$

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

$$\frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}} \quad \overline{\Gamma \vdash i : \text{Int}} \quad \frac{\Gamma \vdash e_0 : \text{Any} \quad \Gamma \vdash e_1 : \text{Any}}{\Gamma \vdash \langle e_0, e_1 \rangle : \text{Pair}}$$

$$\frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e : \text{Fun}} \quad \frac{(x : \tau), \Gamma \vdash e : \text{Any}}{\Gamma \vdash \lambda(x : \tau). e : \text{Fun}} \quad \frac{x \in \Gamma}{\Gamma \vdash x : \text{Any}}$$

$$\frac{(x : \tau) \in \Gamma \quad [\tau] = K}{\Gamma \vdash x : K} \quad \frac{\Gamma \vdash e_0 : \text{Fun}}{\Gamma \vdash e_0 e_1 : \text{Any}} \quad \frac{\Gamma \vdash e_1 : \text{Any} \quad \Gamma \vdash e : \text{Pair}}{\Gamma \vdash \text{fst } e : \text{Any}}$$

$$\frac{\Gamma \vdash e : \text{Pair}}{\Gamma \vdash \text{snd } e : \text{Any}} \quad \frac{\Gamma \vdash e_0 : K_0 \quad \Gamma \vdash e_1 : K_1 \quad \Delta(\text{op}^2, K_0, K_1) = K}{\Gamma \vdash \text{op}^2 e_0 e_1 : K}$$

$$\frac{\Gamma \vdash e : K' \quad K' \leq K}{\Gamma \vdash e : K} \quad \overline{\Gamma \vdash \text{Err} : K} \quad \frac{\Gamma \vdash e \quad [\tau] = K}{\Gamma \vdash \text{dyn } \tau e : K}$$

$$\frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } e : \text{Any}} \quad \frac{\Gamma \vdash e : \text{Any}}{\Gamma \vdash \text{chk } K e : K}$$

$$\boxed{\delta(\text{op}^1, v) = e}$$

$$\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$$

$$\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$$

$$\boxed{\delta(\text{op}^2, v, v) = e}$$

$$\delta(\text{sum}, i_0, i_1) = i_0 + i_1$$

$$\delta(\text{quotient}, i_0, 0) = \text{BndryErr}$$

$$\delta(\text{quotient}, i_0, i_1) = \lfloor i_0 / i_1 \rfloor$$

$$\text{if } i_1 \neq 0$$

$$\boxed{\mathcal{D}_1 : \tau \times v \longrightarrow v}$$

$$\mathcal{D}_1(\tau, v) = \mathcal{X}(\lfloor \tau \rfloor, v)$$

$$\boxed{\mathcal{S}_1 : \tau \times v \longrightarrow v}$$

$$\mathcal{S}_1(\tau, v) = v$$

$$\boxed{\mathcal{X} : K \times v \longrightarrow v}$$

$$\mathcal{X}(\text{Fun}, \lambda x. e) = \lambda x. e$$

$$\mathcal{X}(\text{Fun}, \lambda(x : \tau). e) = \lambda(x : \tau). e$$

$$\mathcal{X}(\text{Pair}, \langle v_0, v_1 \rangle) = \langle v_0, v_1 \rangle$$

$$\mathcal{X}(\text{Int}, i) = i$$

$$\mathcal{X}(\text{Nat}, i) = i$$

$$\text{if } i \in \mathbb{N}$$

$$\mathcal{X}(K, v) = \text{BndryErr}$$

$$\text{otherwise}$$

4621	$e \triangleright_{1-S} e$	
4622	$\text{dyn } v$	$\triangleright_{1-S} v$
4623	$\text{dyn } \tau v$	$\triangleright_{1-S} \mathcal{D}(\tau, v)$
4624	$\text{chk } K v$	$\triangleright_{1-S} \mathcal{X}(K, v)$
4625	$(\lambda(x:\tau). e) v$	$\triangleright_{1-S} \text{BndryErr}$
4626	if $\mathcal{X}(\lfloor \tau \rfloor, v) = \text{BndryErr}$	
4627	$(\lambda(x:\tau). e) v$	$\triangleright_{1-S} e[x \leftarrow \mathcal{X}(\lfloor \tau \rfloor, v)]$
4628	$(\lambda x. e) v$	$\triangleright_{1-S} \text{dyn } (e[x \leftarrow v])$
4629	$op^1 v$	$\triangleright_{1-S} \delta(op^1, v)$
4630	$op^2 v_0 v_1$	$\triangleright_{1-S} \delta(op^2, v_0, v_1)$
4631	$e \triangleright_{1-D} e$	
4632	$\text{stat } v$	$\triangleright_{1-D} v$
4633	$\text{stat } \tau v$	$\triangleright_{1-D} \mathcal{S}(\tau, v)$
4634	$v_0 v_1$	$\triangleright_{1-D} \text{TagErr}$
4635	if $v_0 \in \mathbb{Z}$ or $v_0 = \langle v, v' \rangle$	
4636	$(\lambda(x:\tau). e) v$	$\triangleright_{1-D} \text{BndryErr}$
4637	if $\mathcal{X}(\lfloor \tau \rfloor, v) = \text{BndryErr}$	
4638	$(\lambda(x:\tau). e) v$	$\triangleright_{1-D} \text{stat } (e[x \leftarrow \mathcal{X}(\lfloor \tau \rfloor, v)])$
4639	$(\lambda x. e) v$	$\triangleright_{1-D} e[x \leftarrow v]$
4640	$op^1 v$	$\triangleright_{1-D} \text{TagErr}$
4641	if $\delta(op^1, v)$ is undefined	
4642	$op^1 v$	$\triangleright_{1-D} \delta(op^1, v)$
4643	$op^2 v_0 v_1$	$\triangleright_{1-D} \text{TagErr}$
4644	if $\delta(op^2, v_0, v_1)$ is undefined	
4645	$op^2 v_0 v_1$	$\triangleright_{1-D} \delta(op^2, v_0, v_1)$
4646	$e \rightarrow_{1-S} e$	
4647	$E^\bullet[e]$	$\rightarrow_{1-S} E^\bullet[e']$
4648	if $e \triangleright_{1-S} e'$	
4649	$E[\text{stat } \tau E^\bullet[e]]$	$\rightarrow_{1-S} E[\text{stat } \tau E^\bullet[e']]$
4650	if $e \triangleright_{1-S} e'$	
4651	$E[\text{dyn } \tau E^\bullet[e]]$	$\rightarrow_{1-S} E[\text{dyn } \tau E^\bullet[e']]$
4652	if $e \triangleright_{1-D} e'$	
4653	$E[\text{Err}]$	$\rightarrow_{1-S} \text{Err}$
4654	$e \rightarrow_{1-D} e$	
4655	$E^\bullet[e]$	$\rightarrow_{1-D} E^\bullet[e']$
4656	if $e \triangleright_{1-D} e'$	
4657	$E[\text{stat } \tau E^\bullet[e]]$	$\rightarrow_{1-D} E[\text{stat } \tau E^\bullet[e']]$
4658	if $e \triangleright_{1-S} e'$	
4659	$E[\text{dyn } \tau E^\bullet[e]]$	$\rightarrow_{1-D} E[\text{dyn } \tau E^\bullet[e']]$
4660	if $e \triangleright_{1-D} e'$	
4661	$E[\text{Err}]$	$\rightarrow_{1-D} \text{Err}$
4662	$e \rightarrow_{1-S}^* e$	reflexive, transitive closure of \rightarrow_{1-S}
4663	$e \rightarrow_{1-D}^* e$	reflexive, transitive closure of \rightarrow_{1-D}

Definition 4.0 : 1 boundary-free

An expression e is *boundary free* if e does not contain a subterm of the form:

- $(\text{dyn } \tau' e')$,
- $(\text{stat } \tau' e')$,
- $(\text{dyn } e')$, or
- $(\text{stat } e')$.

A.4.2 First-Order Theorems

Theorem 4.1 : static 1-soundness

If $\vdash e : \tau$ then $\vdash e : \tau \rightsquigarrow e''$ and $\vdash_1 e'' : \lfloor \tau \rfloor$ and one of the following holds:

- $e'' \rightarrow_{1-S}^* v$ and $\vdash_1 v : \lfloor \tau \rfloor$
- $e'' \rightarrow_{1-S}^* E[\text{dyn } \tau' E^*[e']]$ and $e' \triangleright_{1-D} \text{TagErr}$
- $e'' \rightarrow_{1-S}^* E[\text{dyn } E^*[e']]$ and $e' \triangleright_{1-D} \text{TagErr}$
- $e'' \rightarrow_{1-S}^* \text{BndryErr}$
- e'' diverges

Proof:

1. $\vdash_1 e : \tau \rightsquigarrow e''$
 $\wedge \vdash_1 e'' : \lfloor \tau \rfloor$
 by \rightsquigarrow static soundness
2. QED by static progress and static preservation

□

Theorem 4.2 : dynamic 1-soundness

If $\vdash e$ then $\vdash e \rightsquigarrow e''$ and $\vdash_1 e''$ and one of the following holds:

- $e'' \rightarrow_{1-D}^* v$ and $\vdash_1 v$
- $e'' \rightarrow_{1-D}^* E[e']$ and $e' \triangleright_{1-D} \text{TagErr}$
- $e'' \rightarrow_{1-D}^* \text{BndryErr}$
- e'' diverges

Proof:

1. $\vdash_1 e \rightsquigarrow e''$
 $\wedge \vdash_1 e''$
 by \rightsquigarrow dynamic soundness
2. QED by dynamic progress and dynamic preservation

□

Theorem 4.3 : boundary-free 1-soundness

If $\vdash e : \tau$ and e is boundary-free then one of the following holds:

- $e \rightarrow_{1-S}^* v$ and $\vdash v : \tau$
- $e \rightarrow_{1-S}^* \text{BndryErr}$
- e diverges

Proof:

QED by progress and preservation

□

Theorem 4.4 : H/1 base type equivalence

If $\vdash e : \tau$ and all boundary terms in e are of the following four forms:

- $\text{dyn Int } e'$
- $\text{stat Int } e'$
- $\text{stat Nat } e'$
- $\text{dyn Nat } e'$

and $\vdash e : \tau \rightsquigarrow e''$, then $e \rightarrow_{H-S}^* v$ if and only if $e'' \rightarrow_{1-S}^* v$.

Proof:

1. $\mathcal{D}_H(\text{Int}, v) = \mathcal{D}_1(\text{Int}, v)$
 by definition
2. $\mathcal{D}_H(\text{Nat}, v) = \mathcal{D}_1(\text{Nat}, v)$
 by definition
3. $\mathcal{S}_H(\text{Int}, v) = \mathcal{S}_1(\text{Int}, v)$
 by definition
4. $\mathcal{S}_H(\text{Nat}, v) = \mathcal{S}_1(\text{Nat}, v)$
 by definition

5. QED

□

Corollary 4.5 : 1 compilation

If $\vdash e : \tau$

and $\vdash e : \tau \rightsquigarrow e''$

and $\vdash_1 e'' : \lfloor \tau \rfloor$

and $\triangleright_{1-D'}$ is similar to \triangleright_{1-D} but without the no-op boundaries, as follows:

$\text{chk } K v \triangleright_{1-D'} X(K, v)$
 $v_0 v_1 \triangleright_{1-D'} \text{TagErr}$
 if $v_0 \in \mathbb{Z}$ or $v_0 = \langle v, v' \rangle$
 $(\lambda(x:\tau). e) v \triangleright_{1-D'} \text{BndryErr}$
 if $X(\lfloor \tau \rfloor, v) = \text{BndryErr}$
 $(\lambda(x:\tau). e) v \triangleright_{1-D'} e[x \leftarrow X(\lfloor \tau \rfloor, v)]$
 $(\lambda x. e) v \triangleright_{1-D'} e[x \leftarrow v]$
 $op^1 v \triangleright_{1-D'} \text{TagErr}$
 if $\delta(op^1, v)$ is undefined
 $op^1 v \triangleright_{1-D'} \delta(op^1, v)$
 $op^2 v_0 v_1 \triangleright_{1-D'} \text{TagErr}$
 if $\delta(op^2, v_0, v_1)$ is undefined
 $op^2 v_0 v_1 \triangleright_{1-D'} \delta(op^2, v_0, v_1)$

and $e \rightarrow_{1-D'} e$ is defined as:

$E[e] \rightarrow_{1-D'} E[e']$
 if $e \triangleright_{1-D'} e'$
 $E[\text{stat } \tau v] \rightarrow_{1-D'} E[\mathcal{D}_1(\tau, v)]$
 $E[\text{dyn } \tau v] \rightarrow_{1-D'} E[\mathcal{D}_1(\tau, v)]$
 $E[\text{Err}] \rightarrow_{1-D'} \text{Err}$

and $\rightarrow_{1-D'}^*$ is the reflexive transitive closure of $\rightarrow_{1-D'}$

then one of the following holds:

- $e'' \rightarrow_{1-D'}^* v$ and $\vdash_1 v : \lfloor \tau \rfloor$
- $e'' \rightarrow_{1-D'}^* \text{TagErr}$
- $e'' \rightarrow_{1-D'}^* \text{BndryErr}$
- e diverges

Proof (sketch): By static 1-soundness and the fact that \triangleright_{1-S} is a subset of $\triangleright_{1-D'}$ (modulo the dyn e and stat e boundaries). □

A.4.3 First-Order Lemmas

Lemma 4.6 : \mathcal{D}_1 soundness

If $\vdash_1 v$ then $\vdash_1 \mathcal{D}_1(\tau, v) : \lfloor \tau \rfloor$.

Proof:

- $\mathcal{D}_1(\tau, v) = X(\lfloor \tau \rfloor, v)$
- QED by *check soundness*

□

Lemma 4.7 : \mathcal{S}_1 soundness

If $\vdash_1 v : \tau$ then $\vdash_1 \mathcal{S}_1(\tau, v)$.

Proof:

- $\mathcal{S}_1(\tau, v) = X(\lfloor \tau \rfloor, v)$
- QED *check soundness*

□

Lemma 4.8 : \rightsquigarrow static soundness

If $\Gamma \vdash e : \tau$ then $\Gamma \vdash e : \tau \rightsquigarrow e'$ and $\Gamma \vdash_1 e' : \lfloor \tau \rfloor$.

Proof:

By induction on the structure of $\Gamma \vdash e : \tau$.

CASE $\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau}$:

1. $\Gamma \vdash x \rightsquigarrow x$
2. $\Gamma \vdash_1 x : \lfloor \tau \rfloor$
by $(x:\tau) \in \Gamma$
3. QED

CASE $\frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c}$:

1. $\Gamma \vdash e : \tau_c \rightsquigarrow e'$
 $\wedge (x:\tau_d), \Gamma \vdash e' : \lfloor \tau_c \rfloor$
by the induction hypothesis
2. $(x:\tau_d), \Gamma \vdash e' : \text{Any}$
by $\lfloor \tau_c \rfloor <: \text{Any}$
3. $\lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c \rightsquigarrow \lambda(x:\tau_d). e'$
4. $\Gamma \vdash_1 \lambda(x:\tau_d). e' : \text{Fun}$
by (2)
5. QED (3, 4)

CASE $\frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}}$:

1. $\Gamma \vdash i : \text{Nat} \rightsquigarrow i$
2. QED by $\Gamma \vdash_1 i : \text{Nat}$

CASE $\frac{}{\Gamma \vdash i : \text{Int}}$:

1. $\Gamma \vdash i : \text{Int} \rightsquigarrow i$
2. QED by $\Gamma \vdash_1 i : \text{Int}$

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1}$:

1. $\Gamma \vdash e_0 : \tau_0 \rightsquigarrow e'_0$
 $\wedge \Gamma \vdash e'_0 : \lfloor \tau_0 \rfloor$
by the induction hypothesis

2. $\Gamma \vdash e_1 : \tau_1 \rightsquigarrow e'_1$
 $\wedge \Gamma \vdash e'_1 : \lfloor \tau_1 \rfloor$
by the induction hypothesis
3. $\Gamma \vdash_1 e_0 : \text{Any}$
by $\lfloor \tau_0 \rfloor <: \text{Any}$
4. $\Gamma \vdash_1 e_1 : \text{Any}$
by $\lfloor \tau_1 \rfloor <: \text{Any}$
5. $\Gamma \vdash \langle e_0, e_1 \rangle : \tau \rightsquigarrow \langle e'_0, e'_1 \rangle$
by (1, 2)
6. $\Gamma \vdash_1 \langle e'_0, e'_1 \rangle : \text{Pair}$
by (3, 4)
7. QED by (5, 6)

CASE $\frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c}$:

1. $\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \rightsquigarrow e'_0$
 $\wedge \Gamma \vdash_1 e'_0 : \lfloor \tau_d \Rightarrow \tau_c \rfloor$
by the induction hypothesis
2. $\Gamma \vdash e_1 : \tau_d \rightsquigarrow e'_1$
 $\wedge \Gamma \vdash_1 e'_1 : \lfloor \tau_c \rfloor$
by the induction hypothesis
3. $\Gamma \vdash_1 e'_0 : \text{Fun}$
by $\lfloor \tau_d \Rightarrow \tau_c \rfloor = \text{Fun}$
4. $\Gamma \vdash_1 e'_1 : \text{Any}$
by $\lfloor \tau_c \rfloor <: \text{Any}$
5. $\Gamma \vdash e_0 e_1 : \tau_c \rightsquigarrow \text{chk } \lfloor \tau_c \rfloor (e'_0 e'_1)$
by (1, 2)
6. $\Gamma \vdash_1 \text{chk } \lfloor \tau_c \rfloor (e'_0 e'_1) : \lfloor \tau_c \rfloor$
by (3, 4)
7. QED by (5, 6)

CASE $\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(\text{op}^1, \tau_0) = \tau}{\Gamma \vdash \text{op}^1 e_0 : \tau}$:

IF $\text{op}^1 = \text{fst}$:

1. $\Delta(\text{fst}, \tau_0) = \tau$
2. $\tau_0 = \tau \times \tau'$
by Δ inversion
3. $\Gamma \vdash e_0 : \tau \times \tau' \rightsquigarrow e'_0$
 $\wedge \Gamma \vdash_1 e'_0 : \lfloor \tau \times \tau' \rfloor$
by the induction hypothesis
4. $\Gamma \vdash_1 e'_0 : \text{Pair}$
by $\lfloor \tau \times \tau' \rfloor = \text{Pair}$
5. $\Gamma \vdash \text{fst } e_0 : \tau \rightsquigarrow \text{chk } \lfloor \tau \rfloor (\text{fst } e'_0)$
by (2)
6. $\Gamma \vdash_1 \text{chk } \lfloor \tau \rfloor (\text{fst } e'_0) : \lfloor \tau \rfloor$
by (3)
7. QED by 4,5

ELSE $\text{op}^1 = \text{snd}$:

1. $\Delta(\text{snd}, \tau_0) = \tau$
2. $\tau_0 = \tau' \times \tau$
by Δ inversion
3. $\Gamma \vdash e_0 : \tau' \times \tau \rightsquigarrow e'_0$
 $\wedge \Gamma \vdash_1 e'_0 : \lfloor \tau' \times \tau \rfloor$
by the induction hypothesis

4. $\Gamma \vdash_1 e'_0 : \text{Pair}$
by $\lfloor \tau' \times \tau \rfloor = \text{Pair}$
5. $\Gamma \vdash \text{snd } e_0 : \tau \rightsquigarrow \text{chk } \lfloor \tau \rfloor (\text{snd } e'_0)$
by (2)
6. $\Gamma \vdash_1 \text{chk } \lfloor \tau \rfloor (\text{snd } e'_0) : \lfloor \tau \rfloor$
by (3)
7. QED by 4,5

$$\text{CASE } \frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1 \quad \Delta(\text{op}^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash \text{op}^2 e_0 e_1 : \tau} :$$

1. $\Gamma \vdash e_0 : \tau_0 \rightsquigarrow e'_0$
 $\wedge \Gamma \vdash_1 e'_0 : \lfloor \tau_0 \rfloor$
by the induction hypothesis
2. $\Gamma \vdash e_1 : \tau_1 \rightsquigarrow e'_1$
 $\wedge \Gamma \vdash_1 e'_1 : \lfloor \tau_1 \rfloor$
by the induction hypothesis
3. $\Delta(\text{op}^2, \lfloor \tau_0 \rfloor, \lfloor \tau_1 \rfloor) = \lfloor \tau \rfloor$
by Δ tag preservation
4. $\Gamma \vdash \text{op}^2 e_0 e_1 : \tau \rightsquigarrow \text{op}^2 e'_0 e'_1$
by (1, 2)
5. $\Gamma \vdash_1 \text{op}^2 e'_0 e'_1 : \lfloor \tau \rfloor$
by (1, 2, 3)
6. QED by (5, 6)

$$\text{CASE } \frac{\Gamma \vdash e : \tau' \quad \tau' <: \tau}{\Gamma \vdash e : \tau} :$$

1. $\Gamma \vdash e : \tau' \rightsquigarrow e'$
 $\wedge \Gamma \vdash_1 e' : \lfloor \tau' \rfloor$
by the induction hypothesis
2. $\lfloor \tau' \rfloor \leqslant \lfloor \tau \rfloor$
by *subtyping preservation*
3. $\Gamma \vdash_1 e' : \lfloor \tau \rfloor$
by (2)
4. QED by (1, 3)

$$\text{CASE } \frac{}{\Gamma \vdash \text{Err} : \tau} :$$

1. $\Gamma \vdash \text{Err} : \tau \rightsquigarrow \text{Err}$
2. $\Gamma \vdash_1 \text{Err} : \tau$
3. QED

$$\text{CASE } \frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau} :$$

1. $\Gamma \vdash e \rightsquigarrow e'$
 $\wedge \Gamma \vdash_1 e'$
by \rightsquigarrow *dynamic soundness*
2. $\Gamma \vdash \text{dyn } \tau e : \tau \rightsquigarrow \text{dyn } \tau e'$
by (1)
3. $\Gamma \vdash_1 \text{dyn } \tau e' : \lfloor \tau \rfloor$
by (1)
4. QED by (2, 3)

□

Lemma 4.9 : \rightsquigarrow *dynamic soundness*If $\Gamma \vdash e$ then $\Gamma \vdash e \rightsquigarrow e'$ and $\Gamma \vdash_1 e'$ *Proof:*By induction on the structure of $\Gamma \vdash e$.

$$\text{CASE } \frac{x \in \Gamma}{\Gamma \vdash x} :$$

1. $\Gamma \vdash x \rightsquigarrow x$
2. $\Gamma \vdash_1 x$
by $x \in \Gamma$
3. QED

$$\text{CASE } \frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e} :$$

1. $x, \Gamma \vdash e \rightsquigarrow e'$
 $\wedge x, \Gamma \vdash_1 e'$
by the induction hypothesis
2. $\Gamma \vdash \lambda x. e \rightsquigarrow \lambda x. e'$
by (1)
3. $\Gamma \vdash_1 \lambda x. e'$
by (1)
4. QED by (2, 3)

$$\text{CASE } \frac{}{\Gamma \vdash i} :$$

1. $\Gamma \vdash i \rightsquigarrow i$
2. $\Gamma \vdash_1 i$
3. QED

$$\text{CASE } \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle} :$$

1. $\Gamma \vdash e_0 \rightsquigarrow e'_0$
 $\wedge \Gamma \vdash_1 e'_0$
by the induction hypothesis
2. $\Gamma \vdash e_1 \rightsquigarrow e'_1$
 $\wedge \Gamma \vdash_1 e'_1$
by the induction hypothesis
3. $\Gamma \vdash \langle e_0, e_1 \rangle \rightsquigarrow \langle e'_0, e'_1 \rangle$
by (1, 2)
4. $\Gamma \vdash_1 \langle e'_0, e'_1 \rangle$
by (1, 2)
5. QED by (3, 4)

$$\text{CASE } \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1} :$$

1. $\Gamma \vdash e_0 \rightsquigarrow e'_0$
 $\wedge \Gamma \vdash_1 e'_0$
by the induction hypothesis
2. $\Gamma \vdash e_1 \rightsquigarrow e'_1$
 $\wedge \Gamma \vdash_1 e'_1$
by the induction hypothesis
3. $\Gamma \vdash e_0 e_1 \rightsquigarrow e'_0 e'_1$
by (1, 2)
4. $\Gamma \vdash_1 e'_0 e'_1$
by (1, 2)
5. QED by (3, 4)

5061 **CASE** $\frac{\Gamma \vdash e}{\Gamma \vdash op^1 e}$:
 5062
 5063
 5064 1. $\Gamma \vdash e \rightsquigarrow e'$
 5065 $\wedge \Gamma \vdash_1 e'$
 5066 by the induction hypothesis
 5067 2. $\Gamma \vdash op^1 e \rightsquigarrow op^1 e'$
 5068 by (1)
 5069 3. $\Gamma \vdash_1 op^1 e'$
 5070 by (1)
 5071 4. QED by (2, 3)
 5072 **CASE** $\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash op^2 e_0 e_1}$:
 5073
 5074 1. $\Gamma \vdash e_0 \rightsquigarrow e'_0$
 5075 $\wedge \Gamma \vdash_1 e'_0$
 5076 by the induction hypothesis
 5077 2. $\Gamma \vdash e_1 \rightsquigarrow e'_1$
 5078 $\wedge \Gamma \vdash_1 e'_1$
 5079 by the induction hypothesis
 5080 3. $\Gamma \vdash op^2 e_0 e_1 \rightsquigarrow op^2 e'_0 e'_1$
 5081 by (1, 2)
 5082 4. $\Gamma \vdash_1 op^2 e'_0 e'_1$
 5083 by (1, 2)
 5084 5. QED by 3,4
 5085 **CASE** $\frac{}{\Gamma \vdash \text{Err}}$:
 5086
 5087 1. $\Gamma \vdash \text{Err} \rightsquigarrow \text{Err}$
 5088 2. $\Gamma \vdash_1 \text{Err}$
 5089 3. QED
 5090 **CASE** $\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e}$:
 5091
 5092 1. $\Gamma \vdash e : \tau \rightsquigarrow e'$
 5093 $\wedge \Gamma \vdash_1 e' : \lfloor \tau \rfloor$
 5094 by \rightsquigarrow static soundness
 5095 2. $\Gamma \vdash \text{stat } \tau e \rightsquigarrow \text{stat } \tau e'$
 5096 by (1)
 5097 3. $\Gamma \vdash_1 \text{stat } \tau e$
 5098 by (1)
 5099 4. QED by (2,3)
 5100
 5101 \square

Lemma 4.10 : 1 static progress

5102 If $\vdash_1 e : K$ then one of the following holds:

- 5103 • e is a value
- 5104 • $e \in \text{Err}$
- 5105 • $e \rightarrow_{1-S} e'$
- 5106 • $e \rightarrow_{1-S} \text{BndryErr}$
- 5107 • $e = E[\text{dyn } \tau' E^*[e']]$ and $e' \rightarrow_{1-D} \text{TagErr}$
- 5108 • $e = E[\text{dyn } E^*[e']]$ and $e' \rightarrow_{1-D} \text{TagErr}$

5109 *Proof:*

5110 By the *boundary factoring* lemma, there are ten cases.

5111 **CASE** e is a value :

- 5112 1. QED

5116 **CASE** $e = E^*[v_0 v_1]$:
 5117 1. $\vdash_1 v_0 v_1 : K'$
 5118 by *static hole typing*
 5119 2. $\vdash_1 v_0 : \text{Fun}$
 5120 by *inversion* (1)
 5121 3. $v_0 = \lambda x. e'$
 5122 $\vee v_0 = \lambda(x : \tau_d). e'$
 5123 by *canonical forms* (2)
 5124 4. **IF** $v_0 = \lambda x. e'$:
 5125 a. $e \rightarrow_{1-S} E^*[\text{dyn } (e'[x \leftarrow v_1])]$
 5126 by $(\lambda x. e') v_1 \triangleright_{1-S} (\text{dyn } (e'[x \leftarrow v_1]))$
 5127 b. QED
 5128 **IF** $v_0 = \lambda(x : \tau_d). e'$
 5129 $\wedge X(\lfloor \tau_d \rfloor, v_1) = v_1$:
 5130 a. $e \rightarrow_{1-S} E^*[e'[x \leftarrow v_1]]$
 5131 by $(\lambda(x : \tau_d). e') v_1 \triangleright_{1-S} e'[x \leftarrow v_1]$
 5132 b. QED
 5133 **ELSE** $v_0 = \lambda(x : \tau_d). e'$
 5134 $\wedge X(\lfloor \tau_d \rfloor, v_1) = \text{BndryErr}$:
 5135 a. $e \rightarrow_{1-S} E^*[\text{BndryErr}]$
 5136 by $(\lambda(x : \tau_d). e') v_1 \triangleright_{1-S} \text{BndryErr}$
 5137 b. QED
 5138 **CASE** $e = E^*[op^1 v]$:
 5139 1. $op^1 = \text{fst}$
 5140 $\vee op^1 = \text{snd}$
 5141 2. $\vdash_1 op^1 v : K'$
 5142 by *static hole typing*
 5143 3. $\vdash_1 v : \text{Pair}$
 5144 by *inversion* (2)
 5145 4. $v = \langle v_0, v_1 \rangle$
 5146 by *canonical forms* (3)
 5147 5. $\delta(op^1, v) = v_i$ where $i \in \{0, 1\}$
 5148 by (1, 3)
 5149 6. $e \rightarrow_{1-S} E^*[v_i]$
 5150 by $(op^1 v) \triangleright_{1-S} v_i$
 5151 7. QED
 5152 **CASE** $e = E^*[op^2 v_0 v_1]$:
 5153 1. $\vdash_1 op^2 v_0 v_1 : K'$
 5154 by *static hole typing*
 5155 2. $\vdash_1 v_0 : K_0$
 5156 $\wedge \vdash_1 v_1 : K_1$
 5157 $\wedge \Delta(op^2, K_0, K_1) = K_2$
 5158 by *inversion* (1)
 5159 3. $\delta(op^2, v_0, v_1) = e''$
 5160 by Δ tag soundness
 5161 4. QED by $e \rightarrow_{1-S} E^*[e'']$
 5162 **CASE** $e = E^*[\text{chk } K v_0]$:
 5163 1. $e \rightarrow_{1-S} E^*[\chi(K, v)]$
 5164 2. QED
 5165 **CASE** $e = E[\text{dyn } e']$ where e' is boundary-free :
 5166 1. e' is a value
 5167 $\vee e' \in \text{Err}$
 5168 $\vee e' \rightarrow_{1-D} e''$

$\forall e' \rightarrow_{1-D} \text{BndryErr}$
 $\forall e' = E'[e'']$ and $e'' \triangleright_{1-D} \text{TagErr}$
 by *dynamic progress*
 2. **IF** e' is a value :
 a. **QED** $e \rightarrow_{1-S} E[v]$
 IF $e' \in \text{Err}$:
 a. **QED** $e \rightarrow_{1-S} e'$
 IF $e' \rightarrow_{1-D} e''$:
 a. **QED** $e \rightarrow_{1-S} E[\text{dyn } e'']$
 IF $e' \rightarrow_{1-D} \text{BndryErr}$:
 a. **QED** $e \rightarrow_{1-S} E[\text{dyn BndryErr}]$
 ELSE $e' = E'[e'']$ and $e'' \triangleright_{1-D} \text{TagErr}$:
 a. $E' \in E^\bullet$
 by e' is boundary-free
 b. **QED**
CASE $e = E[\text{stat } e']$ where e' is boundary-free :
 1. e' is a value
 $\forall e' \in \text{Err}$
 $\forall e' \rightarrow_{1-S} e''$
 $\forall e' \rightarrow_{1-S} \text{BndryErr}$
 $\forall e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
 $\forall e' = E''[\text{dyn } E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
 by *static progress*
 2. **IF** e' is a value :
 a. **QED** $e \rightarrow_{1-S} E[e']$
 IF $e' \in \text{Err}$:
 a. **QED** $e \rightarrow_{1-S} e'$
 IF $e' \rightarrow_{1-S} e''$:
 a. **QED** $e \rightarrow_{1-S} E[\text{stat } e'']$
 IF $e' \rightarrow_{1-S} \text{BndryErr}$:
 a. **QED** $e \rightarrow_{1-S} E[\text{stat BndryErr}]$
 IF $e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$:
 a. Contradiction by e' is boundary-free
 ELSE $e' = E''[\text{dyn } E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$:
 a. Contradiction by e' is boundary-free
CASE $e = E[\text{dyn } \tau e']$ where e' is boundary-free :
 1. e' is a value
 $\forall e' \in \text{Err}$
 $\forall e' \rightarrow_{1-D} e''$
 $\forall e' \rightarrow_{1-D} \text{BndryErr}$
 $\forall e' = E'[e'']$ and $e'' \triangleright_{1-D} \text{TagErr}$
 by *dynamic progress*
 2. **IF** e' is a value :
 a. **QED** $e \rightarrow_{1-S} E[\mathcal{D}_1(\tau', e')]$
 IF $e' \in \text{Err}$:
 a. **QED** $e \rightarrow_{1-S} e'$
 IF $e' \rightarrow_{1-D} e''$:
 a. **QED** $e \rightarrow_{1-S} E[\text{dyn } \tau' e'']$
 IF $e' \rightarrow_{1-D} \text{BndryErr}$:
 a. **QED** $e \rightarrow_{1-S} E[\text{dyn } \tau' \text{BndryErr}]$
 ELSE $e' = E'[e'']$ and $e'' \triangleright_{1-D} \text{TagErr}$:
 a. Contradiction by e' is boundary-free
 b. **QED**

 a. $E' \in E^\bullet$
 by e' is boundary-free
 b. **QED**
CASE $e = E[\text{stat } \tau e']$ where e' is boundary-free :
 1. e' is a value
 $\forall e' \in \text{Err}$
 $\forall e' \rightarrow_{1-S} e''$
 $\forall e' \rightarrow_{1-S} \text{BndryErr}$
 $\forall e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
 $\forall e' = E''[\text{dyn } E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
 by *static progress*
 2. **IF** e' is a value :
 a. **QED** $e \rightarrow_{1-S} E[S_1(\tau', e')]$
 IF $e' \in \text{Err}$:
 a. **QED** $e \rightarrow_{1-S} e'$
 IF $e' \rightarrow_{1-S} e''$:
 a. **QED** $e \rightarrow_{1-S} E[\text{stat } \tau' e'']$
 IF $e' \rightarrow_{1-S} \text{BndryErr}$:
 a. **QED** $e \rightarrow_{1-S} E[\text{stat } \tau' \text{BndryErr}]$
 IF $e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$:
 a. Contradiction by e' is boundary-free
 ELSE $e' = E''[\text{dyn } E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$:
 a. Contradiction by e' is boundary-free
CASE $e = E[\text{Err}]$:
 1. **QED** $e \rightarrow_{1-S} \text{Err}$

□

Lemma 4.11 : 1 *dynamic progress*If $\vdash_1 e : K$ then one of the following holds:

- e is a value
- $e \in \text{Err}$
- $e \rightarrow_{1-D} e'$
- $e \rightarrow_{1-D} \text{BndryErr}$
- $e = E[e']$ and $e' \rightarrow_{1-D} \text{TagErr}$

Proof:By the *boundary factoring* lemma, there are nine cases.**CASE** $e = v$:1. **QED****CASE** $e = E^\bullet[v_0 v_1]$:**IF** $v_0 = \lambda x. e_0$:

1. $e \rightarrow_{1-D} E^\bullet[e_0[x \leftarrow v_1]]$
 by $(\lambda x. e_0) v_1 \triangleright_{1-D} e_0[x \leftarrow v_1]$

2. **QED****IF** $v_0 = \lambda(x : \tau_d). e_0$ $\wedge \mathcal{X}(\lfloor \tau_d \rfloor, v_1) = v_1$:

1. $e \rightarrow_{1-D} E^\bullet[\text{stat } (e_0[x \leftarrow v_1])]$
 by $(\lambda(x : \tau_d). e_0) v_1 \triangleright_{1-D} (\text{stat } e_0[x \leftarrow v_1])$

2. **QED****IF** $v_0 = \lambda(x : \tau_d). e_0$ $\wedge \mathcal{X}(\lfloor \tau_d \rfloor, v_1) = \text{BndryErr}$:

1. $e \rightarrow_{1-D} E^\bullet[\text{BndryErr}]$
 by $(\lambda(x : \tau_d). e_0) v_1 \triangleright_{1-D} \text{BndryErr}$

2. **QED**

5281 **ELSE** $v_0 = i$
5282 $\vee v_0 = \langle v, v' \rangle :$
5283 1. $e \rightarrow_{1-D} E^\bullet[\text{TagErr}]$
5284 by $v_0 v_1 \triangleright_{1-D} \text{TagErr}$
5285 2. QED
5286 **CASE** $e = E^\bullet[op^1 v] :$
5287 **IF** $\delta(op^1, v) = v' :$
5288 1. $e \rightarrow_{1-D} E^\bullet[v']$
5289 by $(op^1 v) \triangleright_{1-D} v'$
5290 2. QED
5291 **ELSE** $\delta(op^1, v)$ is undefined :
5292 1. $e \rightarrow_{1-D} \text{TagErr}$
5293 by $(op^1 v) \triangleright_{1-D} \text{TagErr}$
5294 2. QED
5295 **CASE** $e = E^\bullet[op^2 v_0 v_1] :$
5296 **IF** $\delta(op^2, v_0, v_1) = e'' :$
5297 1. QED by $e \rightarrow_{1-D} E[e'']$
5298 **ELSE** $\delta(op^2, v_0, v_1)$ is undefined :
5299 1. $e \rightarrow_{1-D} E^\bullet[\text{TagErr}]$
5300 by $(op^2 v_0 v_1) \triangleright_{1-D} \text{TagErr}$
5301 2. QED
5302 **CASE** $e = E^\bullet[\text{chk } K v_0] :$
5303 1. Contradiction by $\vdash_1 e$
5304 **CASE** $e = E[\text{dyn } v]$ where e' is boundary-free :
5305 1. e' is a value
5306 $\vee e' \in \text{Err}$
5307 $\vee e' \rightarrow_{1-D} e''$
5308 $\vee e' \rightarrow_{1-D} \text{BndryErr}$
5309 $\vee e' = E'[e'']$ and $e'' \triangleright_{1-D} \text{TagErr}$
5310 by *dynamic progress*
5311 2. **IF** e' is a value :
5312 a. QED $e \rightarrow_{1-S} E[v]$
5313 **IF** $e' \in \text{Err} :$
5314 a. QED $e \rightarrow_{1-S} e'$
5315 **IF** $e' \rightarrow_{1-D} e'' :$
5316 a. QED $e \rightarrow_{1-S} E[\text{dyn } e'']$
5317 **IF** $e' \rightarrow_{1-D} \text{BndryErr} :$
5318 a. QED $e \rightarrow_{1-S} E[\text{dyn BndryErr}]$
5319 **ELSE** $e' = E'[e'']$ and $e'' \triangleright_{1-D} \text{TagErr} :$
5320 a. $E' \in E^\bullet$
5321 by e' is boundary-free
5322 b. QED
5323 **CASE** $e = E[\text{stat } e']$ where e' is boundary-free :
5324 1. e' is a value
5325 $\vee e' \in \text{Err}$
5326 $\vee e' \rightarrow_{1-S} e''$
5327 $\vee e' \rightarrow_{1-S} \text{BndryErr}$
5328 $\vee e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
5329 $\vee e' = E''[\text{dyn } E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
5330 by *static progress*
5331 2. **IF** e' is a value :
5332 a. QED $e \rightarrow_{1-S} E[e']$
5333 **IF** $e' \in \text{Err} :$
5334 a. QED $e \rightarrow_{1-S} e'$
5335

5336 **IF** $e' \rightarrow_{1-S} e'' :$
5337 a. QED $e \rightarrow_{1-S} E[\text{stat } e'']$
5338 **IF** $e' \rightarrow_{1-S} \text{BndryErr} :$
5339 a. QED $e \rightarrow_{1-S} E[\text{stat BndryErr}]$
5340 **IF** $e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
5341 :
5342 a. Contradiction by e' is boundary-free
5343 **ELSE** $e' = E''[\text{dyn } E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
5344 :
5345 a. Contradiction by e' is boundary-free
5346 **CASE** $e = E[\text{dyn } \tau e']$ where e' is boundary-free :
5347 1. e' is a value
5348 $\vee e' \in \text{Err}$
5349 $\vee e' \rightarrow_{1-D} e''$
5350 $\vee e' \rightarrow_{1-D} \text{BndryErr}$
5351 $\vee e' = E[e'']$ and $e'' \triangleright_{1-D} \text{TagErr}$
5352 by *dynamic progress*
5353 2. **IF** e' is a value :
5354 a. QED $e \rightarrow_{1-D} E[\mathcal{D}_1(\tau', e')]$
5355 **IF** $e' \in \text{Err} :$
5356 a. QED $e \rightarrow_{1-D} e'$
5357 **IF** $e' \rightarrow_{1-D} e'' :$
5358 a. QED $e \rightarrow_{1-S} E[\text{dyn } \tau' e'']$
5359 **IF** $e' \rightarrow_{1-D} \text{BndryErr} :$
5360 a. QED $e \rightarrow_{1-D} E[\text{dyn } \tau' \text{BndryErr}]$
5361 **ELSE** $e' = E[e'']$ and $e'' \triangleright_{1-D} \text{TagErr} :$
5362 a. $E \in E^\bullet$
5363 by e' is boundary-free
5364 b. QED
5365 **CASE** $e = E[\text{stat } \tau e']$ where e' is boundary-free :
5366 1. e' is a value
5367 $\vee e' \in \text{Err}$
5368 $\vee e' \rightarrow_{1-S} e''$
5369 $\vee e' \rightarrow_{1-S} \text{BndryErr}$
5370 $\vee e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
5371 $\vee e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
5372 by *static progress*
5373 2. **IF** e' is a value :
5374 a. QED $e \rightarrow_{1-S} E[\mathcal{S}_1(\tau', e')]$
5375 **IF** $e' \in \text{Err} :$
5376 a. QED $e \rightarrow_{1-S} e'$
5377 **IF** $e' \rightarrow_{1-S} e'' :$
5378 a. QED $e \rightarrow_{1-S} E[\text{stat } \tau' e'']$
5379 **IF** $e' \rightarrow_{1-S} \text{BndryErr} :$
5380 a. QED $e \rightarrow_{1-S} E[\text{stat } \tau' \text{BndryErr}]$
5381 **IF** $e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
5382 :
5383 a. Contradiction by e' is boundary-free
5384 **ELSE** $e' = E''[\text{dyn } E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{1-D} \text{TagErr}$
5385 :
5386 a. Contradiction by e' is boundary-free
5387 **CASE** $e = E[\text{Err}] :$
5388 1. $e \rightarrow_{1-D} \text{Err}$
5389 2. QED
5390

□

Lemma 4.12 : 1 static preservationIf $\vdash_1 e : K$ and $e \rightarrow_{1-S} e'$ then $\vdash_1 e' : K$ *Proof*:By the *boundary factoring* lemma, there are ten cases to consider.**CASE** e is a value :

1. Contradiction by
- $e \rightarrow_{1-S} e'$

CASE $e = E^\bullet[v_0 v_1]$:**IF** $v_0 = \lambda x. e'$ $\wedge e \rightarrow_{1-S} E^\bullet[\text{dyn } e'[x \leftarrow v_1]]$:

1. $\vdash_1 v_0 v_1 : \text{Any}$
by *static hole typing*
2. $\vdash_1 v_0 : \text{Fun}$
 $\wedge \vdash_1 v_1 : \text{Any}$
by *inversion*
3. $x \vdash_1 e'$
by *inversion* (2)
4. $\vdash_1 v_1$
by *static value inversion* (2)
5. $\vdash_1 e'[x \leftarrow v_1]$
by *substitution* (3, 4)
6. $\vdash_1 \text{dyn } (e'[x \leftarrow v_1]) : \text{Any}$
by (5)
7. QED by *hole substitution*

IF $v_0 = \lambda(x:\tau). e'$ $\wedge X(\lfloor \tau \rfloor, v_1) = \text{BndryErr}$ $\wedge e \rightarrow_{1-D} E^\bullet[\text{BndryErr}]$:

1. $\vdash_1 v_0 v_1 : \text{Any}$
by *static hole typing*
2. $\vdash_1 \text{BndryErr} : \text{Any}$
3. QED by *hole substitution* (2)

ELSE $v_0 = \lambda(x:\tau). e'$ $\wedge e \rightarrow_{1-S} E^\bullet[e'[x \leftarrow X(\lfloor \tau \rfloor, v_1)]]$:

1. $\vdash_1 v_0 v_1 : \text{Any}$
by *static hole typing*
2. $\vdash_1 v_0 : \text{Fun}$
 $\wedge \vdash_1 v_1 : \text{Any}$
by *inversion* (1)
3. $(x:\tau) \vdash_1 e' : \text{Any}$
by *inversion* (2)
4. $\vdash_1 X(\lfloor \tau \rfloor, v_1) : \lfloor \tau \rfloor$
by *check soundness* (2)
5. $\vdash_1 e[x \leftarrow X(\lfloor \tau \rfloor, v_1)] : \text{Any}$
by *substitution* (3, 4)
6. QED by *hole substitution*

CASE $e = E^\bullet[op^1 v]$ $\wedge \delta(op^1, v) = v'$ $\wedge e \rightarrow_{1-S} E^\bullet[v']$:

1. $\vdash_1 op^1 v : \text{Any}$
by *static hole typing*
2. $\vdash_1 v : \text{Pair}$
by *inversion*

- 3.
- $v = \langle v_0, v_1 \rangle$

by *canonical forms*

- 4.
- $\vdash_1 v_0 : \text{Any}$

 $\wedge \vdash_1 v_1 : \text{Any}$ by *inversion* (2, 3)

- 5.
- $v' = v_0$

 $\vee v' = v_1$ by $\delta(\text{fst}, v) = v_0$ $\wedge \delta(\text{snd}, v) = v_1$

6. QED by
- hole substitution*
- (5)

CASE $e = E^\bullet[op^2 v_0 v_1]$ $\wedge \delta(op^2, v_0, v_1) = e''$ $\wedge e \rightarrow_{1-S} E^\bullet[e'']$:

- 1.
- $\vdash_1 op^2 v_0 v_1 : K'$

by *static hole typing*

- 2.
- $\vdash_1 v_0 : K_0$

 $\wedge \vdash_1 v_1 : K_1$ $\wedge \Delta(op^2, K_0, K_1) = K''$ $\wedge K'' \leq K'$ by *inversion* (1)

- 3.
- $\vdash_1 e'' : K''$

by Δ *tag soundness* (3)

- 4.
- $\vdash_1 e'' : K'$

by (2, 3)

5. QED by
- hole substitution*
- (4)

CASE $e = E^\bullet[\text{chk } K_0 v_0]$:

- 1.
- $E^\bullet[\text{chk } K_0 v_0] \rightarrow_{1-S} E^\bullet[X(K_0, v_0)]$

- 2.
- $\vdash_1 \text{chk } K_0 v : K''$

by *static hole typing*

- 3.
- $K_0 \leq K''$

by *inversion*

- 4.
- $\vdash_1 X(K_0, v_0) : K_0$

by *check soundness*

5. QED by (3, 4,
- hole substitution*
-)

CASE $e = E[\text{dyn } e']$ where e' is boundary-free :**IF** e' is a value :

- 1.
- $e \rightarrow_{1-S} E[e']$

- 2.
- $\vdash_1 \text{dyn } e' : \text{Any}$

by *boundary hole typing*

- 3.
- $\vdash_1 e'$

by *inversion* (2)

- 4.
- $\vdash_1 e' : \text{Any}$

by *dynamic value inversion* (3)

5. QED by
- hole substitution*
- (4)

ELSE $e' \rightarrow_{1-D} e''$:

- 1.
- $e \rightarrow_{1-S} E[\text{dyn } e'']$

- 2.
- $\vdash_1 \text{dyn } e' : \text{Any}$

by *boundary hole typing*

- 3.
- $\vdash_1 e'$

by *inversion* (2)

- 4.
- $\vdash_1 e''$

by *dynamic preservation* (3)

5501 5. $\vdash_1 \text{dyn } e'' : \text{Any}$
 5502 by (4)
 5503 6. QED by *hole substitution* (5)
 5504 **CASE** $e = E[\text{stat } e']$ where e' is boundary-free :
 5505 **IF** e' is a value :
 5506 1. $e \rightarrow_{1-S} E[e']$
 5507 2. $\vdash_1 \text{stat } e'$
 5508 by *boundary hole typing*
 5509 3. $\vdash_1 e' : \text{Any}$
 5510 by *inversion* (2)
 5511 4. $\vdash_1 e'$
 5512 by *static value inversion* (3)
 5513 5. QED by *hole substitution* (4)
 5514 **ELSE** $e' \rightarrow_{1-S} e''$:
 5515 1. $e \rightarrow_{1-S} E[\text{stat } e'']$
 5516 2. $\vdash_1 \text{stat } e'$
 5517 by *boundary hole typing*
 5518 3. $\vdash_1 e' : \text{Any}$
 5519 by *inversion* (2)
 5520 4. $\vdash_1 e'' : \text{Any}$
 5521 by *static preservation* (3)
 5522 5. $\vdash_1 \text{stat } e''$
 5523 by (4)
 5524 6. QED by *hole substitution* (5)
 5525 **CASE** $e = E[\text{dyn } \tau e']$ where e' is boundary-free :
 5526 **IF** e' is a value :
 5527 1. $e \rightarrow_{1-S} E[\mathcal{D}_1(\tau', e')]$
 5528 2. $\vdash_1 \text{dyn } \tau' e' : \lfloor \tau' \rfloor$
 5529 by *boundary hole typing*
 5530 3. $\vdash_1 e'$
 5531 by *inversion* (2)
 5532 4. $\vdash_1 \mathcal{D}_1(\tau', e') : \lfloor \tau' \rfloor$
 5533 by \mathcal{D}_1 *soundness* (3)
 5534 5. QED by *hole substitution* (4)
 5535 **ELSE** $e' \rightarrow_{1-D} e''$:
 5536 1. $e \rightarrow_{1-S} E[\text{dyn } \tau' e'']$
 5537 2. $\vdash_1 \text{dyn } \tau' e' : \lfloor \tau' \rfloor$
 5538 by *boundary hole typing*
 5539 3. $\vdash_1 e'$
 5540 by *inversion* (2)
 5541 4. $\vdash_1 e''$
 5542 by *dynamic preservation* (3)
 5543 5. $\vdash_1 \text{dyn } \tau' e'' : \lfloor \tau' \rfloor$
 5544 by (4)
 5545 6. QED by *hole substitution* (5)
 5546 **CASE** $e = E[\text{stat } \tau e']$ where e' is boundary-free :
 5547 **IF** e' is a value :
 5548 1. $e \rightarrow_{1-S} E[\mathcal{S}_1(\tau', e')]$
 5549 2. $\vdash_1 \text{stat } \tau' e'$
 5550 by *boundary hole typing*
 5551 3. $\vdash_1 e' : \lfloor \tau' \rfloor$
 5552 by *inversion* (2)
 5553 4. $\vdash_1 \mathcal{S}_1(\tau', e')$
 5554 by \mathcal{S}_1 *soundness* (3)
 5555

5. QED by *hole substitution* (4)
ELSE $e' \rightarrow_{1-S} e''$:
 1. $e \rightarrow_{1-S} E[\text{stat } \tau' e'']$
 2. $\vdash_1 \text{stat } \tau' e'$
 by *boundary hole typing*
 3. $\vdash_1 e' : \lfloor \tau' \rfloor$
 by *inversion* (2)
 4. $\vdash_1 e'' : \lfloor \tau' \rfloor$
 by *static preservation* (3)
 5. $\vdash_1 \text{stat } \tau' e''$
 by (4)
 6. QED by *hole substitution* (5)
CASE $e = E[\text{Err}]$:
 1. $e \rightarrow_{1-S} \text{Err}$
 2. QED $\vdash_1 \text{Err} : K$
 □

Lemma 4.13 : 1 *dynamic preservation*If $\vdash_1 e$ and $e \rightarrow_{1-D} e'$ then $\vdash_1 e'$ *Proof*:By *boundary factoring* there are nine cases.**CASE** e is a value :1. Contradiction by $e \rightarrow_{1-D} e'$ **CASE** $e = E^*[v_0 v_1]$:**IF** $v_0 = \lambda x. e'$ $\wedge e \rightarrow_{1-D} E^*[e'[x \leftarrow v_1]]$:1. $\vdash_1 v_0 v_1$ by *dynamic hole typing*2. $\vdash_1 v_0$ $\wedge \vdash_1 v_1$ by *inversion* (1)3. $x \vdash_1 e'$ by *inversion* (2)4. $\vdash_1 e'[x \leftarrow v_1]$ by *substitution* (2, 3)5. QED by *hole substitution***IF** $v_0 = \lambda(x:\tau). e'$ $\wedge \mathcal{X}(\lfloor \tau \rfloor, v_1) = \text{BndryErr}$ $\wedge e \rightarrow_{1-D} E^*[\text{BndryErr}]$:1. $\vdash_1 v_0 v_1$ by *dynamic hole typing*2. $\vdash_1 \text{BndryErr}$ 3. QED by *hole substitution* (2)**ELSE** $v_0 = \lambda(x:\tau). e'$ $\wedge e \rightarrow_{1-D} E^*[\text{stat } (e'[x \leftarrow \mathcal{X}(\lfloor \tau \rfloor, v_1)])]$:1. $\vdash_1 v_0 v_1$ by *dynamic hole typing*2. $\vdash_1 v_0$ $\wedge \vdash_1 v_1$ by *inversion* (1)3. $(x:\tau) \vdash_1 e : \text{Any}$ by *inversion* (2)4. $\vdash_1 \mathcal{X}(\lfloor \tau \rfloor, v_1) : \lfloor \tau \rfloor$ by *check soundness* (2)

5611	5. $\vdash_1 e[x \leftarrow X(\lfloor \tau \rfloor, v_1)] : \text{Any}$	4. $\vdash_1 e'$	5666
5612	by <i>substitution</i> (3, 4)	by <i>static value inversion</i> (3)	5667
5613	6. $\vdash_1 \text{stat } (e[x \leftarrow X(\lfloor \tau \rfloor, v_1)])$	5. QED by <i>hole substitution</i> (5)	5668
5614	by (5)	ELSE $e' \rightarrow_{1-S} e'' :$	5669
5615	7. QED by <i>hole substitution</i> (6)	1. $e \rightarrow_{1-D} E[\text{stat } e'']$	5670
5616	CASE $e = E^\bullet[op^1 v]$	2. $\vdash_1 \text{stat } e'$	5671
5617	$\wedge \delta(op^1, v) = v'$	by <i>boundary hole typing</i>	5672
5618	$\wedge e \rightarrow_{1-D} E^\bullet[v'] :$	3. $\vdash_1 e' : \text{Any}$	5673
5619	1. $\vdash_1 op^1 v$	by <i>inversion</i> (2)	5674
5620	by <i>dynamic hole typing</i>	4. $\vdash_1 e'' : \text{Any}$	5675
5621	2. $\vdash_1 v$	by <i>static preservation</i> (3)	5676
5622	by <i>inversion</i> (1)	5. $\vdash_1 \text{stat } e''$	5677
5623	3. $\vdash_1 v'$	by (4)	5678
5624	by δ <i>preservation</i> (2)	6. QED by <i>hole substitution</i> (5)	5679
5625	4. QED by <i>hole substitution</i> (3)	CASE $e = E[\text{dyn } \tau e']$ where e' is boundary-free :	5680
5626	CASE $e = E^\bullet[op^2 v_0 v_1]$	IF e' is a value :	5681
5627	$\wedge \delta(op^2, v_0, v_1) = e''$	1. $e \rightarrow_{1-D} E[\mathcal{D}_1(\tau', e')]$	5682
5628	$\wedge e \rightarrow_{1-D} E^\bullet[e''] :$	2. $\vdash_1 \text{dyn } \tau' e' : \lfloor \tau' \rfloor$	5683
5629	1. $\vdash_1 op^2 v_0 v_1$	by <i>boundary hole typing</i>	5684
5630	by <i>dynamic hole typing</i>	3. $\vdash_1 e'$	5685
5631	2. $\vdash_1 v_0$	by <i>inversion</i> (2)	5686
5632	$\wedge \vdash_1 v_1$	4. $\vdash_1 \mathcal{D}_1(\tau', e') : \lfloor \tau' \rfloor$	5687
5633	by <i>inversion</i> (1)	by \mathcal{D}_1 <i>soundness</i> (3)	5688
5634	3. $\vdash_1 e''$	5. QED by <i>hole substitution</i> (4)	5689
5635	by δ <i>preservation</i> (2)	ELSE $e' \rightarrow_{1-D} e'' :$	5690
5636	4. QED by <i>hole substitution</i> (3)	1. $e \rightarrow_{1-D} E[\text{dyn } \tau' e'']$	5691
5637	CASE $e = E[\text{dyn } e']$ where e' is boundary-free :	2. $\vdash_1 \text{dyn } \tau' e' : \lfloor \tau' \rfloor$	5692
5638	IF e' is a value :	by <i>boundary hole typing</i>	5693
5639	1. $e \rightarrow_{1-D} E[e']$	3. $\vdash_1 e'$	5694
5640	2. $\vdash_1 \text{dyn } e' : \text{Any}$	$\wedge \tau' \leq \tau''$	5695
5641	by <i>boundary hole typing</i>	by <i>inversion</i> (2)	5696
5642	3. $\vdash_1 e'$	4. $\vdash_1 e''$	5697
5643	by <i>inversion</i> (2)	by <i>dynamic preservation</i> (3)	5698
5644	4. $\vdash_1 e' : \text{Any}$	5. $\vdash_1 \text{dyn } \tau' e'' : \lfloor \tau' \rfloor$	5699
5645	by \mathcal{D}_1 <i>soundness</i> (3)	by (4)	5700
5646	5. QED by <i>hole substitution</i> (4)	6. QED by <i>hole substitution</i> (5)	5701
5647	ELSE $e' \rightarrow_{1-D} e'' :$	CASE $e = E[\text{stat } \tau e']$ where e' is boundary-free :	5702
5648	1. $e \rightarrow_{1-D} E[\text{dyn } e'']$	IF $e' \in v :$	5703
5649	2. $\vdash_1 \text{dyn } e' : \text{Any}$	1. $e \rightarrow_{1-D} E[\mathcal{S}_1(\tau', e')]$	5704
5650	by <i>boundary hole typing</i>	2. $\vdash_1 \text{stat } \tau' e'$	5705
5651	3. $\vdash_1 e'$	by <i>boundary hole typing</i>	5706
5652	by <i>inversion</i> (2)	3. $\vdash_1 e' : \lfloor \tau' \rfloor$	5707
5653	4. $\vdash_1 e''$	by <i>inversion</i> (2)	5708
5654	by <i>dynamic preservation</i> (3)	4. $\vdash_1 \mathcal{S}_1(\tau', e')$	5709
5655	5. $\vdash_1 \text{dyn } e'' : \text{Any}$	by \mathcal{S}_1 <i>soundness</i> (3)	5710
5656	by (4)	5. QED by <i>hole substitution</i> (5)	5711
5657	6. QED by <i>hole substitution</i> (5)	ELSE $e' \rightarrow_{1-S} e'' :$	5712
5658	CASE $e = E[\text{stat } e']$ where e' is boundary-free :	1. $e \rightarrow_{1-D} E[\text{stat } \tau' e'']$	5713
5659	IF $e' \in v :$	2. $\vdash_1 \text{stat } \tau' e'$	5714
5660	1. $e \rightarrow_{1-D} E[e']$	by <i>boundary hole typing</i>	5715
5661	2. $\vdash_1 \text{stat } e'$	3. $\vdash_1 e' : \lfloor \tau' \rfloor$	5716
5662	by <i>boundary hole typing</i>	by <i>inversion</i> (2)	5717
5663	3. $\vdash_1 e' : \text{Any}$	4. $\vdash_1 e'' : \lfloor \tau' \rfloor$	5718
5664	by <i>inversion</i> (2)	by <i>static preservation</i> (3)	5719
5665			5720

5721 5. $\vdash_1 \text{stat } \tau' e''$
 5722 by (4)
 5723 6. QED by *hole substitution* (5)
 5724 **CASE** $e = E[\text{Err}]$:
 5725 1. $e \rightarrow_{1-D} \text{Err}$
 5726 2. QED $\vdash_1 \text{Err}$

□

Lemma 4.14 : *boundary-free progress*

If $\vdash e : \tau$ and e is boundary-free, then one of the following holds:

- e is a value
- $e \rightarrow_{1-S} e'$
- $e \rightarrow_{1-S} \text{BndryErr}$

Proof:

By the L *unique static evaluation contexts* lemma, there are five cases:

CASE $e = v$:
 1. QED
CASE $e = E^\bullet[v_0 v_1]$:
IF $v_0 = \lambda(x:\tau'). e'$:
 1. $e \rightarrow_{1-S} E^\bullet[e'[x \leftarrow v_1]]$
 by $v_0 v_1 \triangleright_{1-S} e'[x \leftarrow v_1]$
 2. QED
ELSE $v_0 = \lambda x. e'$
 $\vee v_0 = i$
 $\vee v_0 = \langle v, v' \rangle$:

1. Contradiction by $\vdash e : \tau$

CASE $e = E^\bullet[op^1 v]$:

IF $\delta(op^1, v) = e''$:

1. $e \rightarrow_{1-S} E^\bullet[e'']$
 by $(op^1 v) \triangleright_{1-S} e''$

2. QED

ELSE $\delta(op^1, v)$ is undefined :

1. Contradiction by $\vdash e : \tau$

CASE $e = E^\bullet[op^2 v_0 v_1]$:

IF $\delta(op^2, v_0, v_1) = e''$:

1. $e \rightarrow_{1-S} E^\bullet[e'']$
 by $(op^2 v_0 v_1) \triangleright_{1-S} e''$

2. QED

IF $\delta(op^2, v_0, v_1) = \text{BndryErr}$:

1. $e \rightarrow_{1-S} \text{BndryErr}$
 by $(op^2 v_0 v_1) \triangleright_{1-S} \text{BndryErr}$

2. QED

ELSE $\delta(op^2, v_0, v_1)$ is undefined :

1. Contradiction by $\vdash e : \tau$

CASE $e = E^\bullet[\text{Err}]$:

1. $E^\bullet[\text{Err}] \rightarrow_{1-S} \text{Err}$
 2. QED

□

Lemma 4.15 : 1 *boundary-free preservation*

If $\vdash e : \tau$ and e is boundary-free and $e \rightarrow_{1-S} e'$ then $\vdash e' : \tau$ and e' is boundary-free.

Proof:

By the L *unique static evaluation contexts* lemma, there are five cases.

CASE e is a value :

1. Contradiction by $e \rightarrow_{1-S} e'$

CASE $e = E^\bullet[v_0 v_1]$:

IF $v_0 = \lambda(x:\tau_d). e'$:

1. $E^\bullet[v_0 v_1] \rightarrow_{1-S} E^\bullet[e'[x \leftarrow v_1]]$

2. $\vdash v_0 v_1 : \tau_c$

3. $\vdash v_0 : \tau_d \Rightarrow \tau_c$

$\wedge \vdash v_1 : \tau_d$

by (2)

4. $(x:\tau_d) \vdash e' : \tau_c$

by (3)

5. $\vdash e'[x \leftarrow v_1] : \tau_c$

by *substitution* (3, 4)

6. $e'[x \leftarrow v_1]$ is boundary-free

by e' and v_1 are boundary-free

7. QED

ELSE :

1. Contradiction by $\vdash e : \tau$

CASE $e = E^\bullet[op^1 v]$:

1. $E^\bullet[op^1 v] \rightarrow_{1-S} E^\bullet[v']$

$\wedge \delta(op^1, v) = e''$

2. $\vdash op^1 v : \tau'$

3. $\vdash v : \tau_0$

4. $\vdash e'' : \tau'$

by δ *preservation* (3)

5. QED

CASE $e = E^\bullet[op^2 v_0 v_1]$:

1. $E^\bullet[op^2 v_0 v_1] \rightarrow_{1-S} E^\bullet[v']$

$\wedge \delta(op^2, v_0, v_1) = e''$

2. $\vdash op^2 v_0 v_1 : \tau'$

3. $\vdash v_0 : \tau_0$

$\wedge \vdash v_1 : \tau_1$

4. $\vdash e'' : \tau'$

by δ *preservation* (3)

5. QED

CASE $e = E^\bullet[\text{Err}]$:

1. $E^\bullet[\text{Err}] \rightarrow_{1-S} \text{Err}$

2. QED by $\vdash \text{Err} : \tau$

□

Lemma 4.16 : \mathcal{X} *soundness*

For all K and v , $\vdash_1 \mathcal{X}(K, v) : K$.

Proof:

CASE $\vdash_1 v : K$:

1. $\mathcal{X}(K, v) = v$

2. QED

CASE $\nvdash_1 v : K$:

1. $\mathcal{X}(K, v) = \text{BndryErr}$

2. QED

□

Lemma 4.17 : 1 *static boundary factoring*

If $\vdash_1 e : K$ then one of the following holds:

- e is a value
- $e = E^\bullet[v_0 v_1]$
- $e = E^\bullet[op^1 v]$
- $e = E^\bullet[op^2 v_0 v_1]$
- $e = E^\bullet[\text{chk } K v]$
- $e = E[\text{dyn } e']$ where e' is boundary-free
- $e = E[\text{stat } e']$ where e' is boundary-free
- $e = E[\text{dyn } \tau e']$ where e' is boundary-free
- $e = E[\text{stat } \tau e']$ where e' is boundary-free
- $e = E[\text{Err}]$

Proof:

By the *unique evaluation contexts* lemma, there are ten cases.

CASE e is a value :

1. QED

CASE $e = E[v_0 v_1]$:

1. $E = E^\bullet$

$\vee E = E'[\text{dyn } E^\bullet]$

$\vee E = E'[\text{stat } E^\bullet]$

$\vee E = E'[\text{dyn } \tau E^\bullet]$

$\vee E = E'[\text{stat } \tau E^\bullet]$

by *inner boundary*

2. **IF** $E = E^\bullet$:

a. QED $e = E^\bullet[v_0 v_1]$

IF $E = E'[\text{dyn } E^\bullet]$:

a. QED $e = E'[\text{dyn } E^\bullet[v_0 v_1]]$

IF $E = E'[\text{stat } E^\bullet]$:

a. QED $e = E'[\text{stat } E^\bullet[v_0 v_1]]$

IF $E = E'[\text{dyn } \tau E^\bullet]$:

a. QED $e = E'[\text{dyn } \tau E^\bullet[v_0 v_1]]$

ELSE $E = E'[\text{stat } \tau E^\bullet]$:

a. QED $e = E'[\text{stat } \tau E^\bullet[v_0 v_1]]$

CASE $e = E[op^1 v]$:

1. $E = E^\bullet$

$\vee E = E'[\text{dyn } E^\bullet]$

$\vee E = E'[\text{stat } E^\bullet]$

$\vee E = E'[\text{dyn } \tau E^\bullet]$

$\vee E = E'[\text{stat } \tau E^\bullet]$

by *inner boundary*

2. **IF** $E = E^\bullet$:

a. QED $e = E^\bullet[op^1 v]$

IF $E = E'[\text{dyn } E^\bullet]$:

a. QED $e = E'[\text{dyn } E^\bullet[op^1 v]]$

IF $E = E'[\text{stat } E^\bullet]$:

a. QED $e = E'[\text{stat } E^\bullet[op^1 v]]$

IF $E = E'[\text{dyn } \tau E^\bullet]$:

a. QED $e = E'[\text{dyn } \tau E^\bullet[op^1 v]]$

ELSE $E = E'[\text{stat } \tau E^\bullet]$:

a. QED $e = E'[\text{stat } \tau E^\bullet[op^1 v]]$

CASE $e = E[op^2 v_0 v_1]$:

1. $E = E^\bullet$

$\vee E = E'[\text{dyn } E^\bullet]$

$\vee E = E'[\text{stat } E^\bullet]$

$\vee E = E'[\text{dyn } \tau E^\bullet]$

$\vee E = E'[\text{stat } \tau E^\bullet]$

by *inner boundary*

2. **IF** $E = E^\bullet$:

a. QED $e = E^\bullet[op^2 v_0 v_1]$

IF $E = E'[\text{dyn } E^\bullet]$:

a. QED $e = E'[\text{dyn } E^\bullet[op^2 v_0 v_1]]$

IF $E = E'[\text{stat } E^\bullet]$:

a. QED $e = E'[\text{stat } E^\bullet[op^2 v_0 v_1]]$

IF $E = E'[\text{dyn } \tau E^\bullet]$:

a. QED $e = E'[\text{dyn } \tau E^\bullet[op^2 v_0 v_1]]$

ELSE $E = E'[\text{stat } \tau E^\bullet]$:

a. QED $e = E'[\text{stat } \tau E^\bullet[op^2 v_0 v_1]]$

CASE $e = E[\text{dyn } v]$:

1. QED v is boundary-free

CASE $e = E[\text{stat } v]$:

1. QED v is boundary-free

CASE $e = E[\text{dyn } \tau v]$:

1. QED v is boundary-free

CASE $e = E[\text{stat } \tau v]$:

1. QED v is boundary-free

CASE $e = E[\text{Err}]$:

1. QED

□

Lemma 4.18 : 1 *unique static evaluation contexts*

If $\vdash_1 e : K$ then one of the following holds:

- e is a value
- $e = E[v_0 v_1]$
- $e = E[op^1 v]$
- $e = E[op^2 v_0 v_1]$
- $e = E[\text{chk } K v]$
- $e = E[\text{dyn } v]$
- $e = E[\text{stat } v]$
- $e = E[\text{dyn } \tau v]$
- $e = E[\text{stat } \tau v]$
- $e = E[\text{Err}]$

Proof:

By induction on the structure of e .

CASE $e = x$:

1. Contradiction by $\vdash_1 e : K$

CASE $e = i$

$\vee e = \lambda x. e'$

$\vee e = \lambda(x:\tau_d). e'$

1. QED e is a value

CASE $e = \langle e_0, e_1 \rangle$:

IF $e_0 \notin v$:

1. $e_0 = E_0[e'_0]$

by the induction hypothesis

2. $E = \langle E_0, e_1 \rangle$

3. QED by $e = E[e'_0]$

IF $e_0 \in v$

$\wedge e_1 \notin v$:

1. $e_1 = E_1[e'_1]$

by the induction hypothesis

5941 2. $E = \langle e_0, E_1 \rangle$
5942 3. QED by $e = E[e'_1]$
5943 **ELSE** $e_0 \in v$
5944 $\wedge e_1 \in v$:
5945 1. $E = []$
5946 2. QED $e = E[\langle e_0, e_1 \rangle]$
5947 **CASE** $e = e_0 e_1$:
5948 **IF** $e_0 \notin v$:
5949 1. $e_0 = E_0[e'_0]$
5950 by the induction hypothesis
5951 2. $E = E_0 e_1$
5952 3. QED by $e = E[e'_0]$
5953 **IF** $e_0 \in v$
5954 $\wedge e_1 \notin v$:
5955 1. $e_1 = E_1[e'_1]$
5956 by the induction hypothesis
5957 2. $E = e_0 E_1$
5958 3. QED by $e = E[e'_1]$
5959 **ELSE** $e_0 \in v$
5960 $\wedge e_1 \in v$:
5961 1. $E = []$
5962 2. QED $e = E[e_0 e_1]$
5963 **CASE** $e = op^1 e_0$:
5964 1. **IF** $e_0 \notin v$:
5965 a. $e_0 = E_0[e'_0]$
5966 by the induction hypothesis
5967 b. $E = op^1 E_0$
5968 c. QED $e = E[e'_0]$
5969 2. **ELSE** $e_0 \in v$:
5970 a. $E = []$
5971 b. QED $e = E[op^1 e_0]$
5972 **CASE** $e = op^2 e_0 e_1$:
5973 **IF** $e_0 \notin v$:
5974 1. $e_0 = E_0[e'_0]$
5975 by the induction hypothesis
5976 2. $E = op^2 E_0 e_1$
5977 3. QED $e = E[e'_0]$
5978 **IF** $e_0 \in v$
5979 $\wedge e_1 \notin v$:
5980 1. $e_1 = E_1[e'_1]$
5981 by the induction hypothesis
5982 2. $E = op^2 e_0 E_1$
5983 3. QED $e = E[e'_1]$
5984 **ELSE** $e_0 \in v$
5985 $\wedge e_1 \in v$:
5986 1. $E = []$
5987 2. QED $e = E[op^2 e_0 e_1]$
5988 **CASE** $e = chk K e_0$:
5989 **IF** $e_0 \notin v$:
5990 1. $e_0 = E_0[e'_0]$
5991 by the induction hypothesis
5992 2. $E = chk K E_0$
5993 3. QED $e = E[e'_0]$
5994 **ELSE** $e_0 \in v$:
5995

1. $E = []$
2. QED $e = E[chk K e_0]$
CASE $e = dyn e_0$:
IF $e_0 \notin v$:
1. $\vdash_1 e_0$
by inversion
2. $e_0 = E_0[e'_0]$
by unique evaluation contexts (1)
3. $E = dyn E_0$
4. QED $e = E[e'_0]$
ELSE $e_0 \in v$:
1. $E = []$
2. QED $e = E[dyn e_0]$
CASE $e = stat e_0$:
1. Contradiction by $\vdash_1 e : K$
CASE $e = dyn \tau e_0$:
IF $e_0 \notin v$:
1. $\vdash_1 e_0$
by inversion
2. $e_0 = E_0[e'_0]$
by unique evaluation contexts (1)
3. $E = dyn \tau E_0$
4. QED $e = E[e'_0]$
ELSE $e_0 \in v$:
1. $E = []$
2. QED $e = E[dyn \tau e_0]$
CASE $e = stat K' e_0$:
1. Contradiction by $\vdash_1 e : K$
CASE $e = Err$:
1. $E = []$
2. QED $e = E[Err]$

□

Lemma 4.19 : 1 inner boundaryFor all contexts E , one of the following holds:

- $E = E^\bullet$
- $E = E'[\text{dyn } v]$
- $E = E'[\text{stat } v]$
- $E = E'[\text{dyn } \tau E^\bullet]$
- $E = E'[\text{stat } \tau E^\bullet]$

*Proof:*By induction on the structure of E .**CASE** $E = E^\bullet$:

1. QED

CASE $E = E_0 e_1$:1. $E_0 = E^\bullet$ $\vee E_0 = E'_0[\text{dyn } E^\bullet]$ $\vee E_0 = E'_0[\text{stat } E^\bullet]$ $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$ $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$

by the induction hypothesis

2. **IF** $E_0 = E^\bullet$:a. QED E is boundary-free**IF** $E_0 = E'_0[\text{dyn } E^\bullet]$:a. $E' = E'_0 e_1$

6051 b. QED $E = E'[\text{dyn } E^\bullet]$
 6052 **IF** $E_0 = E'_0[\text{stat } E^\bullet]$:
 6053 a. $E' = E'_0 e_1$
 6054 b. QED $E = E'[\text{stat } E^\bullet]$
 6055 **IF** $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:
 6056 a. $E' = E'_0 e_1$
 6057 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 6058 **ELSE** $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
 6059 a. $E' = E'_0 e_1$
 6060 b. QED $E = E'[\text{stat } \tau E^\bullet]$
 6061 **CASE** $E = v_0 E_1$:
 6062 1. $E_1 = E^\bullet$
 6063 $\vee E_1 = E'_1[\text{dyn } E^\bullet]$
 6064 $\vee E_1 = E'_1[\text{stat } E^\bullet]$
 6065 $\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$
 6066 $\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$
 6067 by the induction hypothesis
 6068 2. **IF** $E_1 = E^\bullet$:
 6069 a. QED E is boundary-free
 6070 **IF** $E_1 = E'_1[\text{dyn } E^\bullet]$:
 6071 a. $E' = v_0 E'_1$
 6072 b. QED $E = E'[\text{dyn } E^\bullet]$
 6073 **IF** $E_1 = E'_1[\text{stat } E^\bullet]$:
 6074 a. $E' = v_0 E'_1$
 6075 b. QED $E = E'[\text{stat } E^\bullet]$
 6076 **IF** $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:
 6077 a. $E' = v_0 E'_1$
 6078 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 6079 **ELSE** $E_1 = E'_1[\text{stat } \tau E^\bullet]$:
 6080 a. $E' = v_0 E'_1$
 6081 b. QED $E = E'[\text{stat } \tau E^\bullet]$
 6082 **CASE** $E = \langle E_0, e_1 \rangle$:
 6083 1. $E_0 = E^\bullet$
 6084 $\vee E_0 = E'_0[\text{dyn } E^\bullet]$
 6085 $\vee E_0 = E'_0[\text{stat } E^\bullet]$
 6086 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
 6087 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
 6088 by the induction hypothesis
 6089 2. **IF** $E_0 = E^\bullet$:
 6090 a. QED E is boundary-free
 6091 **IF** $E_0 = E'_0[\text{dyn } E^\bullet]$:
 6092 a. $E' = \langle E'_0, e_1 \rangle$
 6093 b. QED $E = E'[\text{dyn } E^\bullet]$
 6094 **IF** $E_0 = E'_0[\text{stat } E^\bullet]$:
 6095 a. $E' = \langle E'_0, e_1 \rangle$
 6096 b. QED $E = E'[\text{stat } E^\bullet]$
 6097 **IF** $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:
 6098 a. $E' = \langle E'_0, e_1 \rangle$
 6099 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 6100 **ELSE** $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
 6101 a. $E' = \langle E'_0, e_1 \rangle$
 6102 b. QED $E = E'[\text{stat } \tau E^\bullet]$
 6103 **CASE** $E = \langle v_0, E_1 \rangle$:
 6104
 6105

1. $E_1 = E^\bullet$
 $\vee E_0 = E'_0[\text{dyn } E^\bullet]$
 $\vee E_0 = E'_0[\text{stat } E^\bullet]$
 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
 by the induction hypothesis
 2. **IF** $E_1 = E^\bullet$:
 a. QED E is boundary-free
 IF $E_1 = E'_1[\text{dyn } E^\bullet]$:
 a. $E' = \langle v_0, E'_1 \rangle$
 b. QED $E = E'[\text{dyn } E^\bullet]$
 IF $E_1 = E'_1[\text{stat } E^\bullet]$:
 a. $E' = \langle v_0, E'_1 \rangle$
 b. QED $E = E'[\text{stat } E^\bullet]$
 IF $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:
 a. $E' = \langle v_0, E'_1 \rangle$
 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 ELSE $E_1 = E'_1[\text{stat } \tau E^\bullet]$:
 a. $E' = \langle v_0, E'_1 \rangle$
 b. QED $E = E'[\text{stat } \tau E^\bullet]$
CASE $E = op^1 E_0$:
 1. $E_0 = E^\bullet$
 $\vee E_0 = E'_0[\text{dyn } E^\bullet]$
 $\vee E_0 = E'_0[\text{stat } E^\bullet]$
 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
 by the induction hypothesis
 2. **IF** $E_0 = E^\bullet$:
 a. QED E is boundary-free
 IF $E_0 = E'_0[\text{dyn } E^\bullet]$:
 a. $E' = op^1 E'_0$
 b. QED $E = E'[\text{dyn } E^\bullet]$
 IF $E_0 = E'_0[\text{stat } E^\bullet]$:
 a. $E' = op^1 E'_0$
 b. QED $E = E'[\text{stat } E^\bullet]$
 IF $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:
 a. $E' = op^1 E'_0$
 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 ELSE $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
 a. $E' = op^1 E'_0$
 b. QED $E = E'[\text{stat } \tau E^\bullet]$
CASE $E = op^2 E_0 e_1$:
 1. $E_0 = E^\bullet$
 $\vee E_0 = E'_0[\text{dyn } E^\bullet]$
 $\vee E_0 = E'_0[\text{stat } E^\bullet]$
 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
 by the induction hypothesis
 2. **IF** $E_0 = E^\bullet$:
 a. QED E is boundary-free
 IF $E_0 = E'_0[\text{dyn } E^\bullet]$:
 a. $E' = op^2 E'_0 e_1$
 b. QED $E = E'[\text{dyn } E^\bullet]$

6161 **IF** $E_0 = E'_0[\text{stat } E^\bullet]$:
 6162 a. $E' = op^2 E'_0 e_1$
 6163 b. $\text{QED } E = E'[\text{stat } E^\bullet]$
 6164 **IF** $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:
 6165 a. $E' = op^2 E'_0 e_1$
 6166 b. $\text{QED } E = E'[\text{dyn } \tau E^\bullet]$
 6167 **ELSE** $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
 6168 a. $E' = op^2 E'_0 e_1$
 6169 b. $\text{QED } E = E'[\text{stat } \tau E^\bullet]$
 6170 **CASE** $E = op^2 v_0 E_1$:
 6171 1. $E_1 = E^\bullet$
 6172 $\vee E_1 = E'_1[\text{dyn } E^\bullet]$
 6173 $\vee E_1 = E'_1[\text{stat } E^\bullet]$
 6174 $\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$
 6175 $\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$
 6176 by the induction hypothesis
 6177 2. **IF** $E_1 = E^\bullet$:
 6178 a. $\text{QED } E$ is boundary-free
 6179 **IF** $E_1 = E'_1[\text{dyn } E^\bullet]$:
 6180 a. $E' = op^2 v_0 E'_1$
 6181 b. $\text{QED } E = E'[\text{dyn } E^\bullet]$
 6182 **IF** $E_1 = E'_1[\text{stat } E^\bullet]$:
 6183 a. $E' = op^2 v_0 E'_1$
 6184 b. $\text{QED } E = E'[\text{stat } E^\bullet]$
 6185 **IF** $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:
 6186 a. $E' = op^2 v_0 E'_1$
 6187 b. $\text{QED } E = E'[\text{dyn } \tau E^\bullet]$
 6188 **ELSE** $E_1 = E'_1[\text{stat } \tau E^\bullet]$:
 6189 a. $E' = op^2 v_0 E'_1$
 6190 b. $\text{QED } E = E'[\text{stat } \tau E^\bullet]$
 6191 **CASE** $E = \text{dyn } E_0$:
 6192 1. $E_0 = E^\bullet$
 6193 $\vee E_0 = E'_0[\text{dyn } E^\bullet]$
 6194 $\vee E_0 = E'_0[\text{stat } E^\bullet]$
 6195 $\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$
 6196 $\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$
 6197 by the induction hypothesis
 6198 2. **IF** $E_0 = E^\bullet$:
 6199 a. QED
 6200 **IF** $E_0 = E'_0[\text{dyn } E^\bullet]$:
 6201 a. $E' = \text{dyn } E'_0$
 6202 b. $\text{QED } E = E'[\text{dyn } E^\bullet]$
 6203 **IF** $E_0 = E'_0[\text{stat } E^\bullet]$:
 6204 a. $E' = \text{dyn } E'_0$
 6205 b. $\text{QED } E = E'[\text{stat } E^\bullet]$
 6206 **IF** $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:
 6207 a. $E' = \text{dyn } E'_0$
 6208 b. $\text{QED } E = E'[\text{dyn } \tau' E^\bullet]$
 6209 **ELSE** $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:
 6210 a. $E' = \text{dyn } E'_0$
 6211 b. $\text{QED } E = E'[\text{stat } \tau' E^\bullet]$
 6212 **CASE** $E = \text{stat } E_0$:
 6213
 6214
 6215

1. $E_0 = E^\bullet$
 $\vee E_0 = E'_0[\text{dyn } E^\bullet]$
 $\vee E_0 = E'_0[\text{stat } E^\bullet]$
 $\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$
 $\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$
 by the induction hypothesis
 2. **IF** $E_0 = E^\bullet$:
 a. QED
 IF $E_0 = E'_0[\text{dyn } E^\bullet]$:
 a. $E' = \text{stat } E'_0$
 b. $\text{QED } E = E'[\text{dyn } E^\bullet]$
 IF $E_0 = E'_0[\text{stat } E^\bullet]$:
 a. $E' = \text{stat } E'_0$
 b. $\text{QED } E = E'[\text{stat } E^\bullet]$
 IF $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:
 a. $E' = \text{stat } E'_0$
 b. $\text{QED } E = E'[\text{dyn } \tau' E^\bullet]$
 ELSE $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:
 a. $E' = \text{stat } E'_0$
 b. $\text{QED } E = E'[\text{stat } \tau' E^\bullet]$
CASE $E = \text{dyn } \tau E_0$:
 1. $E_0 = E^\bullet$
 $\vee E_0 = E'_0[\text{dyn } E^\bullet]$
 $\vee E_0 = E'_0[\text{stat } E^\bullet]$
 $\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$
 $\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$
 by the induction hypothesis
 2. **IF** $E_0 = E^\bullet$:
 a. QED
 IF $E_0 = E'_0[\text{dyn } E^\bullet]$:
 a. $E' = \text{dyn } \tau E'_0$
 b. $\text{QED } E = E'[\text{dyn } E^\bullet]$
 IF $E_0 = E'_0[\text{stat } E^\bullet]$:
 a. $E' = \text{dyn } \tau E'_0$
 b. $\text{QED } E = E'[\text{stat } E^\bullet]$
 IF $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:
 a. $E' = \text{dyn } \tau E'_0$
 b. $\text{QED } E = E'[\text{dyn } \tau' E^\bullet]$
 ELSE $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:
 a. $E' = \text{dyn } \tau E'_0$
 b. $\text{QED } E = E'[\text{stat } \tau' E^\bullet]$
CASE $E = \text{stat } \tau E_0$:
 1. $E_0 = E^\bullet$
 $\vee E_0 = E'_0[\text{dyn } E^\bullet]$
 $\vee E_0 = E'_0[\text{stat } E^\bullet]$
 $\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$
 $\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$
 by the induction hypothesis
 2. **IF** $E_0 = E^\bullet$:
 a. QED
 IF $E_0 = E'_0[\text{dyn } E^\bullet]$:
 a. $E' = \text{stat } \tau E'_0$
 b. $\text{QED } E = E'[\text{dyn } E^\bullet]$
 IF $E_0 = E'_0[\text{stat } E^\bullet]$:
 a. $E' = \text{stat } \tau E'_0$
 b. $\text{QED } E = E'[\text{stat } E^\bullet]$

6271 a. $E' = \text{stat } \tau E'_0$
 6272 b. $\text{QED } E = E'[\text{stat } E^\bullet]$
 6273 **IF** $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:
 6274 a. $E' = \text{stat } \tau E'_0$
 6275 b. $\text{QED } E = E'[\text{dyn } \tau' E^\bullet]$
 6276 **ELSE** $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:
 6277 a. $E' = \text{stat } \tau E'_0$
 6278 b. $\text{QED } E = E'[\text{stat } \tau' E^\bullet]$
 6279 **CASE** $E = \text{chk } K_0 E_0$:
 6280 1. $E_0 = E^\bullet$
 6281 $\vee E_0 = E'_0[\text{dyn } E^\bullet]$
 6282 $\vee E_0 = E'_0[\text{stat } E^\bullet]$
 6283 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
 6284 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
 6285 by the induction hypothesis
 6286 2. **IF** $E_0 = E^\bullet$:
 6287 a. $\text{QED } E$ is boundary-free
 6288 **IF** $E_0 = E'_0[\text{dyn } E^\bullet]$:
 6289 a. $E' = \text{chk } K_0 E'_0$
 6290 b. $\text{QED } E = E'[\text{dyn } E^\bullet]$
 6291 **IF** $E_0 = E'_0[\text{stat } E^\bullet]$:
 6292 a. $E' = \text{chk } K_0 E'_0$
 6293 b. $\text{QED } E = E'[\text{stat } E^\bullet]$
 6294 **IF** $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:
 6295 a. $E' = \text{chk } K_0 E'_0$
 6296 b. $\text{QED } E = E'[\text{dyn } \tau E^\bullet]$
 6297 **ELSE** $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
 6298 a. $E' = \text{chk } K_0 E'_0$
 6299 b. $\text{QED } E = E'[\text{stat } \tau E^\bullet]$
 6300 \square

Lemma 4.20 : 1 *dynamic boundary factoring*

If $\vdash_1 e$ then one of the following holds:

- e is a value
- $e = E^\bullet[v_0 v_1]$
- $e = E^\bullet[op^1 v]$
- $e = E^\bullet[op^2 v_0 v_1]$
- $e = E[\text{dyn } e']$ where e' is boundary-free
- $e = E[\text{stat } e']$ where e' is boundary-free
- $e = E[\text{dyn } \tau e']$ where e' is boundary-free
- $e = E[\text{stat } \tau e']$ where e' is boundary-free
- $e = E[\text{Err}]$

Proof:

By the *unique evaluation contexts* lemma, there are ten cases.

CASE e is a value :

1. **QED**

CASE $e = E[v_0 v_1]$:

1. $E = E^\bullet$

$\vee E = E'[\text{dyn } E^\bullet]$

$\vee E = E'[\text{stat } E^\bullet]$

$\vee E = E'[\text{dyn } \tau E^\bullet]$

$\vee E = E'[\text{stat } \tau E^\bullet]$

by *inner boundary*

2. **IF** $E = E^\bullet$:

a. $\text{QED } e = E^\bullet[v_0 v_1]$
IF $E = E'[\text{dyn } E^\bullet]$:
 a. $\text{QED } e = E'[\text{dyn } E^\bullet[v_0 v_1]]$
IF $E = E'[\text{stat } E^\bullet]$:
 a. $\text{QED } e = E'[\text{stat } E^\bullet[v_0 v_1]]$
IF $E = E'[\text{dyn } \tau E^\bullet]$:
 a. $\text{QED } e = E'[\text{dyn } \tau E^\bullet[v_0 v_1]]$
ELSE $E = E'[\text{stat } \tau E^\bullet]$:
 a. $\text{QED } e = E'[\text{stat } \tau E^\bullet[v_0 v_1]]$
CASE $e = E[op^1 v]$:

1. $E = E^\bullet$

$\vee E = E'[\text{dyn } E^\bullet]$

$\vee E = E'[\text{stat } E^\bullet]$

$\vee E = E'[\text{dyn } \tau E^\bullet]$

$\vee E = E'[\text{stat } \tau E^\bullet]$

by *inner boundary*

2. **IF** $E = E^\bullet$:

a. $\text{QED } e = E^\bullet[op^1 v]$

IF $E = E'[\text{dyn } E^\bullet]$:

a. $\text{QED } e = E'[\text{dyn } E^\bullet[op^1 v]]$

IF $E = E'[\text{stat } E^\bullet]$:

a. $\text{QED } e = E'[\text{stat } E^\bullet[op^1 v]]$

IF $E = E'[\text{dyn } \tau E^\bullet]$:

a. $\text{QED } e = E'[\text{dyn } \tau E^\bullet[op^1 v]]$

ELSE $E = E'[\text{stat } \tau E^\bullet]$:

a. $\text{QED } e = E'[\text{stat } \tau E^\bullet[op^1 v]]$

CASE $e = E[op^2 v_0 v_1]$:

1. $E = E^\bullet$

$\vee E = E'[\text{dyn } E^\bullet]$

$\vee E = E'[\text{stat } E^\bullet]$

$\vee E = E'[\text{dyn } \tau E^\bullet]$

$\vee E = E'[\text{stat } \tau E^\bullet]$

by *inner boundary*

2. **IF** $E = E^\bullet$:

a. $\text{QED } e = E^\bullet[op^2 v_0 v_1]$

IF $E = E'[\text{dyn } E^\bullet]$:

a. $\text{QED } e = E'[\text{dyn } E^\bullet[op^2 v_0 v_1]]$

IF $E = E'[\text{stat } E^\bullet]$:

a. $\text{QED } e = E'[\text{stat } E^\bullet[op^2 v_0 v_1]]$

IF $E = E'[\text{dyn } \tau E^\bullet]$:

a. $\text{QED } e = E'[\text{dyn } \tau E^\bullet[op^2 v_0 v_1]]$

ELSE $E = E'[\text{stat } \tau E^\bullet]$:

a. $\text{QED } e = E'[\text{stat } \tau E^\bullet[op^2 v_0 v_1]]$

CASE $e = E[\text{chk } K' v]$:

1. $E = E^\bullet$

$\vee E = E'[\text{dyn } E^\bullet]$

$\vee E = E'[\text{stat } E^\bullet]$

$\vee E = E'[\text{dyn } \tau E^\bullet]$

$\vee E = E'[\text{stat } \tau E^\bullet]$

by *inner boundary*

2. **IF** $E = E^\bullet$:

a. $\text{QED } e = E^\bullet[\text{chk } K' v]$

IF $E = E'[\text{dyn } E^\bullet]$:

a. $\text{QED } e = E'[\text{dyn } E^\bullet[\text{chk } K' v]]$

6381 **IF** $E = E'[\text{stat } E^\bullet]$:
 6382 a. $\text{QED } e = E'[\text{stat } E^\bullet[\text{chk } K' \ v]]$
 6383 **IF** $E = E'[\text{dyn } \tau \ E^\bullet]$:
 6384 a. $\text{QED } e = E'[\text{dyn } \tau \ E^\bullet[\text{chk } K' \ v]]$
 6385 **ELSE** $E = E'[\text{stat } \tau \ E^\bullet]$:
 6386 a. $\text{QED } e = E'[\text{stat } \tau \ E^\bullet[\text{chk } K' \ v]]$
 6387 **CASE** $e = E[\text{dyn } v]$:
 6388 1. $\text{QED } v$ is boundary-free
 6389 **CASE** $e = E[\text{stat } v]$:
 6390 1. $\text{QED } v$ is boundary-free
 6391 **CASE** $e = E[\text{dyn } \tau \ v]$:
 6392 1. $\text{QED } v$ is boundary-free
 6393 **CASE** $e = E[\text{stat } \tau \ v]$:
 6394 1. $\text{QED } v$ is boundary-free
 6395 **CASE** $e = E[\text{Err}]$:
 6396 1. QED
 6397 \square

Lemma 4.21 : 1 unique dynamic evaluation contexts

If $\vdash_1 e$ then one of the following holds:

- e is a value
- $e = E[v_0 \ v_1]$
- $e = E[\text{op}^1 \ v]$
- $e = E[\text{op}^2 \ v_0 \ v_1]$
- $e = E[\text{chk } K \ v]$
- $e = E[\text{dyn } v]$
- $e = E[\text{stat } v]$
- $e = E[\text{dyn } \tau \ v]$
- $e = E[\text{stat } \tau \ v]$
- $e = E[\text{Err}]$

Proof:

By induction on the structure of e .

6411 **CASE** $e = x$:
 6412 1. Contradiction by $\vdash_1 e$
 6413 **CASE** $e = i$
 6414 $\vee e = \lambda x. e'$
 6415 $\vee e = \lambda(x:\tau_d). e'$
 6416 1. $\text{QED } e$ is a value
 6417 **CASE** $e = \langle e_0, e_1 \rangle$:
 6418 **IF** $e_0 \notin v$:
 6419 1. $e_0 = E_0[e'_0]$
 6420 by the induction hypothesis
 6421 2. $E = \langle E_0, e_1 \rangle$
 6422 3. $\text{QED } e = E[e'_0]$
 6423 **IF** $e_0 \in v$
 6424 $\wedge e_1 \notin v$:
 6425 1. $e_1 = E_1[e'_1]$
 6426 by the induction hypothesis
 6427 2. $E = \langle e_0, E_1 \rangle$
 6428 3. $\text{QED } e = E[e'_1]$
 6429 **ELSE** $e_0 \in v$
 6430 $\wedge e_1 \in v$:
 6431 1. $E = []$
 6432 2. $\text{QED } e = E[\langle e_0, e_1 \rangle]$
 6433 **CASE** $e = e_0 \ e_1$:
 6434
 6435

6436 **IF** $e_0 \notin v$:
 6437 1. $e_0 = E_0[e'_0]$
 6438 by the induction hypothesis
 6439 2. $E = E_0 \ e_1$
 6440 3. $\text{QED } e = E[e'_0]$
 6441 **IF** $e_0 \in v$
 6442 $\wedge e_1 \notin v$:
 6443 1. $e_1 = E_1[e'_1]$
 6444 by the induction hypothesis
 6445 2. $E = e_0 \ E_1$
 6446 3. $\text{QED } e = E[e'_1]$
 6447 **ELSE** $e_0 \in v$
 6448 $\wedge e_1 \in v$:
 6449 1. $E = []$
 6450 2. $\text{QED } e = E[e_0 \ e_1]$
 6451 **CASE** $e = \text{op}^1 \ e_0$:
 6452 **IF** $e_0 \notin v$:
 6453 1. $e_0 = E_0[e'_0]$
 6454 by the induction hypothesis
 6455 2. $E = \text{op}^1 \ E_0$
 6456 3. $\text{QED } e = E[e'_0]$
 6457 **ELSE** $e_0 \in v$:
 6458 1. $E = []$
 6459 2. $\text{QED } e = E[\text{op}^1 \ e_0]$
 6460 **CASE** $e = \text{op}^2 \ e_0 \ e_1$:
 6461 **IF** $e_0 \notin v$:
 6462 1. $e_0 = E_0[e'_0]$
 6463 by the induction hypothesis
 6464 2. $E = \text{op}^2 \ E_0 \ e_1$
 6465 3. $\text{QED } e = E[e'_0]$
 6466 **IF** $e_0 \in v$
 6467 $\wedge e_1 \notin v$:
 6468 1. $e_1 = E_1[e'_1]$
 6469 by the induction hypothesis
 6470 2. $E = \text{op}^2 \ e_0 \ E_1$
 6471 3. $\text{QED } e = E[e'_1]$
 6472 **ELSE** $e_0 \in v$
 6473 $\wedge e_1 \in v$:
 6474 1. $E = []$
 6475 2. $\text{QED } e = E[\text{op}^2 \ e_0 \ e_1]$
 6476 **CASE** $e = \text{chk } K \ e'$:
 6477 1. Contradiction by $\vdash_1 e$
 6478 **CASE** $e = \text{dyn } e_0$:
 6479 1. Contradiction by $\vdash_1 e$
 6480 **CASE** $e = \text{stat } e_0$:
 6481 **IF** $e_0 \notin v$:
 6482 1. $\vdash_1 e_0$
 6483 by *inversion*
 6484 2. $e_0 = E_0[e'_0]$
 6485 by *unique evaluation contexts* (1)
 6486 3. $E = \text{stat } E_0$
 6487 4. $\text{QED } e = E[e'_0]$
 6488 **ELSE** $e_0 \in v$:
 6489 1. $E = []$
 6490

6491 2. QED $e = E[\text{stat } e_0]$
6492 **CASE** $e = \text{dyn } e_0$:
6493 Contradiction by $\vdash_1 e$
6494 **CASE** $e = \text{stat } K_0 e_0$:
6495 **IF** $e_0 \notin v$:
6496 1. $\vdash_1 e_0$
6497 by *inversion*
6498 2. $e_0 = E_0[e'_0]$
6499 by *unique evaluation contexts* (1)
6500 3. $E = \text{stat } \tau E_0$
6501 4. QED $e = E[e'_0]$
6502 **ELSE** $e_0 \in v$:
6503 1. $E = []$
6504 2. QED $e = E[\text{stat } \tau e_0]$
6505 \square
6506 **Lemma 4.22** : 1 *static hole typing*
6507 If $\vdash_1 E^\bullet[e] : K$ then the typing derivation contains a sub-term
6508 $\vdash_1 e : K'$ for some K' .
6509 *Proof*:
6510 By induction on the structure of E^\bullet .
6511 **CASE** $E^\bullet = []$:
6512 1. QED $E^\bullet[e] = e$
6513 **CASE** $E^\bullet = E^\bullet_0 e_1$:
6514 1. $E^\bullet[e] = E^\bullet_0[e] e_1$
6515 2. $\vdash_1 E^\bullet_0[e] : \text{Fun}$
6516 by *inversion*
6517 3. QED by the induction hypothesis (2)
6518 **CASE** $E^\bullet = v_0 E^\bullet_1$:
6519 1. $E^\bullet[e] = v_0 E^\bullet_1[e]$
6520 2. $\vdash_1 E^\bullet_1[e] : \text{Any}$
6521 by *inversion*
6522 3. QED by the induction hypothesis (2)
6523 **CASE** $E^\bullet = \langle E^\bullet_0, e_1 \rangle$:
6524 1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$
6525 2. $\vdash_1 E^\bullet_0[e] : \text{Any}$
6526 by *inversion*
6527 3. QED by the induction hypothesis (2)
6528 **CASE** $E^\bullet = \langle v_0, E^\bullet_1 \rangle$:
6529 1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$
6530 2. $\vdash_1 E^\bullet_1[e] : \text{Any}$
6531 by *inversion*
6532 3. QED the induction hypothesis (2)
6533 **CASE** $E^\bullet = op^1 E^\bullet_0$:
6534 1. $E^\bullet[e] = op^1 E^\bullet_0[e]$
6535 2. $\vdash_1 E^\bullet_0[e] : \text{Pair}$
6536 by *inversion*
6537 3. QED the induction hypothesis (2)
6538 **CASE** $E^\bullet = op^2 E^\bullet_0 e_1$:
6539 1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$
6540 2. $\vdash_1 E^\bullet_0[e] : K_0$
6541 by *inversion*
6542 3. QED the induction hypothesis (2)
6543 **CASE** $E^\bullet = op^2 v_0 E^\bullet_1$:
6544 1. Contradiction by $\vdash_1 E^\bullet[e]$
6545

1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$ 6546
2. $\vdash_1 E^\bullet_1[e] : K_1$ 6547
by *inversion* 6548
3. QED the induction hypothesis (2) 6549
CASE $E^\bullet = \text{chk } K E^\bullet_0$: 6550
1. $E^\bullet[e] = \text{chk } K E^\bullet_0[e]$ 6551
2. $\vdash_1 E^\bullet_0[e] : \text{Any}$ 6552
by *inversion* 6553
3. QED the induction hypothesis (2) 6554
 \square 6555
Lemma 4.23 : 1 *dynamic hole typing* 6556
If $\vdash_1 E^\bullet[e]$ then the derivation contains a sub-term $\vdash_1 e$ 6557
Proof: 6558
By induction on the structure of E^\bullet . 6559
CASE $E^\bullet = []$: 6560
1. QED $E^\bullet[e] = e$ 6561
CASE $E^\bullet = E^\bullet_0 e_1$: 6562
1. $E^\bullet[e] = E^\bullet_0[e] e_1$ 6563
2. $\vdash_1 E^\bullet_0[e]$ 6564
by *inversion* 6565
3. QED the induction hypothesis (2) 6566
CASE $E^\bullet = v_0 E^\bullet_1$: 6567
1. $E^\bullet[e] = v_0 E^\bullet_1[e]$ 6568
2. $\vdash_1 E^\bullet_1[e]$ 6569
by *inversion* 6570
3. QED the induction hypothesis (2) 6571
CASE $E^\bullet = \langle E^\bullet_0, e_1 \rangle$: 6572
1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$ 6573
2. $\vdash_1 E^\bullet_0[e]$ 6574
by *inversion* 6575
3. QED the induction hypothesis (2) 6576
CASE $E^\bullet = \langle v_0, E^\bullet_1 \rangle$: 6577
1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$ 6578
2. $\vdash_1 E^\bullet_1[e]$ 6579
by *inversion* 6580
3. QED the induction hypothesis (2) 6581
CASE $E^\bullet = op^1 E^\bullet_0$: 6582
1. $E^\bullet[e] = op^1 E^\bullet_0[e]$ 6583
2. $\vdash_1 E^\bullet_0[e]$ 6584
by *inversion* 6585
3. QED the induction hypothesis (2) 6586
CASE $E^\bullet = op^2 E^\bullet_0 e_1$: 6587
1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$ 6588
2. $\vdash_1 E^\bullet_0[e]$ 6589
by *inversion* 6590
3. QED the induction hypothesis (2) 6591
CASE $E^\bullet = op^2 v_0 E^\bullet_1$: 6592
1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$ 6593
2. $\vdash_1 E^\bullet_1[e]$ 6594
by *inversion* 6595
3. QED the induction hypothesis (2) 6596
CASE $E^\bullet = \text{chk } K E^\bullet_0$: 6597
1. Contradiction by $\vdash_1 E^\bullet[e]$ 6598
6599
6600

□

Lemma 4.24 : 1 *boundary hole typing*

- If $\vdash_1 E[\text{dyn } e]$ then the derivation contains a sub-term $\vdash_1 \text{dyn } e : \text{Any}$
- If $\vdash_1 E[\text{dyn } e] : K'$ then the derivation contains a sub-term $\vdash_1 \text{dyn } e : \text{Any}$
- If $\vdash_1 E[\text{stat } e]$ then the derivation contains a sub-term $\vdash_1 \text{stat } e$
- If $\vdash_1 E[\text{stat } e] : K'$ then the derivation contains a sub-term $\vdash_1 \text{stat } e$
- If $\vdash_1 E[\text{dyn } \tau e]$ then the derivation contains a sub-term $\vdash_1 \text{dyn } \tau e : [\tau]$
- If $\vdash_1 E[\text{dyn } \tau e] : K'$ then the derivation contains a sub-term $\vdash_1 \text{dyn } \tau e : [\tau]$
- If $\vdash_1 E[\text{stat } \tau e]$ then the derivation contains a sub-term $\vdash_1 \text{stat } \tau e$
- If $\vdash_1 E[\text{stat } \tau e] : K'$ then the derivation contains a sub-term $\vdash_1 \text{stat } \tau e$

Proof:

By the following four lemmas: *static dyn hole typing*, *dynamic dyn hole typing*, *static stat hole typing*, and *dynamic stat hole typing*.

□

Lemma 4.25 : 1 *static dyn hole typing*

- If $\vdash_1 E[\text{dyn } \tau e] : K'$ then the derivation contains a sub-term $\vdash_1 \text{dyn } \tau e : [\tau]$.

Proof:

By induction on the structure of E .

CASE $E \in E^*$:

1. $\vdash_1 \text{dyn } \tau e : K''$
by *static hole typing*
2. $\vdash_1 \text{dyn } \tau e : [\tau]$
by *inversion* (1)
3. QED

CASE $E = E_0 e_1$:

1. $E[\text{dyn } \tau e] = E_0[\text{dyn } \tau e] e_1$
2. $\vdash_1 E_0[\text{dyn } \tau e] : K_0$
by *inversion*
3. QED by the induction hypothesis (2)

CASE $E = v_0 E_1$:

1. $E[\text{dyn } \tau e] = v_0 E_1[\text{dyn } \tau e]$
2. $\vdash_1 E_1[\text{dyn } \tau e] : K_1$
by *inversion*
3. QED by the induction hypothesis (2)

CASE $E = \langle E_0, e_1 \rangle$:

1. $E[\text{dyn } \tau e] = \langle E_0[\text{dyn } \tau e], e_1 \rangle$
2. $\vdash_1 E_0[\text{dyn } \tau e] : K_0$
by *inversion*
3. QED by the induction hypothesis (2)

CASE $E = \langle v_0, E_1 \rangle$:

1. $E[\text{dyn } \tau e] = \langle v_0, E_1[\text{dyn } \tau e] \rangle$
2. $\vdash_1 E_1[\text{dyn } \tau e] : K_1$
by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \text{op}^1 E_0$:

1. $E[\text{dyn } \tau e] = \text{op}^1 E_0[\text{dyn } \tau e]$
2. $\vdash_1 E_0[\text{dyn } \tau e] : K_0$
by *inversion*
3. QED by the induction hypothesis (2)

CASE $E = \text{op}^2 E_0 e_1$:

1. $E[\text{dyn } \tau e] = \text{op}^2 E_0[\text{dyn } \tau e] e_1$
2. $\vdash_1 E_0[\text{dyn } \tau e] : K_0$
by *inversion*
3. QED by the induction hypothesis (2)

CASE $E = \text{op}^2 v_0 E_1$:

1. $E[\text{dyn } \tau e] = \text{op}^2 v_0 E_1[\text{dyn } \tau e]$
2. $\vdash_1 E_1[\text{dyn } \tau e] : K_1$
by *inversion*
3. QED by the induction hypothesis (2)

CASE $E = \text{dyn } E_0$:

1. $E[\text{dyn } \tau e] = \text{dyn } E_0[\text{dyn } \tau e]$
2. $\vdash_1 E_0[\text{dyn } \tau e]$
by *inversion*
3. QED by *dynamic dyn hole typing* (2)

CASE $E = \text{stat } E_0$:

1. Contradiction by $\vdash_1 E[\text{dyn } \tau e] : \tau'$

CASE $E = \text{dyn } \tau_0 E_0$:

1. $E[\text{dyn } \tau e] = \text{dyn } \tau_0 E_0[\text{dyn } \tau e]$
2. $\vdash_1 E_0[\text{dyn } \tau e]$
by *inversion*
3. QED by *dynamic dyn hole typing* (2)

CASE $E = \text{stat } \tau_0 E_0$:

1. Contradiction by $\vdash_1 E[\text{dyn } \tau e] : \tau'$

CASE $E = \text{chk } K_0 E_0$:

1. $E[\text{dyn } \tau e] = \text{chk } K_0 E_0[\text{dyn } \tau e]$
2. $\vdash_1 E_0[\text{dyn } \tau e] : \text{Any}$
by *inversion*
3. QED by the induction hypothesis (2)

□

Lemma 4.26 : 1 *dynamic dyn hole typing*

- If $\vdash_1 E[\text{dyn } \tau e]$ then the derivation contains a sub-term $\vdash_1 \text{dyn } \tau e : [\tau]$.

Proof:

By induction on the structure of E .

CASE $E \in E^*$:

1. Contradiction by $\vdash_1 E[\text{dyn } \tau e]$

CASE $E = E_0 e_1$:

1. $E[\text{dyn } \tau e] = E_0[\text{dyn } \tau e] e_1$
2. $\vdash_1 E_0[\text{dyn } \tau e]$
by *inversion*
3. QED by the induction hypothesis (2)

CASE $E = v_0 E_1$:

1. $E[\text{dyn } \tau e] = v_0 E_1[\text{dyn } \tau e]$
2. $\vdash_1 E_1[\text{dyn } \tau e]$
by *inversion*
3. QED by the induction hypothesis (2)

CASE $E = \langle E_0, e_1 \rangle$:

6711 1. $E[\text{dyn } \tau e] = \langle E_0[\text{dyn } \tau e], e_1 \rangle$
6712 2. $\vdash_1 E_0[\text{dyn } \tau e]$
6713 by *inversion*
6714 3. QED by the induction hypothesis (2)
6715 **CASE** $E = \langle v_0, E_1 \rangle$:
6716 1. $E[\text{dyn } \tau e] = \langle v_0, E_1[\text{dyn } \tau e] \rangle$
6717 2. $\vdash_1 E_1[\text{dyn } \tau e]$
6718 by *inversion*
6719 3. QED by the induction hypothesis (2)
6720 **CASE** $E = \text{op}^1 E_0$:
6721 1. $E[\text{dyn } \tau e] = \text{op}^1 E_0[\text{dyn } \tau e]$
6722 2. $\vdash_1 E_0[\text{dyn } \tau e]$
6723 by *inversion*
6724 3. QED by the induction hypothesis (2)
6725 **CASE** $E = \text{op}^2 E_0 e_1$:
6726 1. $E[\text{dyn } \tau e] = \text{op}^2 E_0[\text{dyn } \tau e] e_1$
6727 2. $\vdash_1 E_0[\text{dyn } \tau e]$
6728 by *inversion*
6729 3. QED by the induction hypothesis (2)
6730 **CASE** $E = \text{op}^2 v_0 E_1$:
6731 1. $E[\text{dyn } \tau e] = \text{op}^2 v_0 E_1[\text{dyn } \tau e]$
6732 2. $\vdash_1 E_1[\text{dyn } \tau e]$
6733 by *inversion*
6734 3. QED by the induction hypothesis (2)
6735 **CASE** $E = \text{dyn } E_0$:
6736 1. Contradiction by $\vdash_1 E[\text{dyn } \tau e]$
6737 **CASE** $E = \text{stat } E_0$:
6738 1. $E[\text{dyn } \tau e] = \text{stat } E_0[\text{dyn } \tau e]$
6739 2. $\vdash_1 E_0[\text{dyn } \tau e] : \lfloor \tau_0 \rfloor$
6740 by *inversion*
6741 3. QED by *static dyn hole typing* (2)
6742 **CASE** $E = \text{dyn } \tau E_0$:
6743 1. Contradiction by $\vdash_1 E[\text{dyn } \tau e]$
6744 **CASE** $E = \text{stat } \tau_0 E_0$:
6745 1. $E[\text{dyn } \tau e] = \text{stat } \tau_0 E_0[\text{dyn } \tau e]$
6746 2. $\vdash_1 E_0[\text{dyn } \tau e] : \lfloor \tau_0 \rfloor$
6747 by *inversion*
6748 3. QED by *static dyn hole typing* (2)
6749 **CASE** $E = \text{chk } K_0 E_0$:
6750 1. Contradiction by $\vdash_1 E[\text{dyn } \tau e]$
6751 \square
6752 **Lemma 4.27** : 1 *static stat hole typing*
6753 If $\vdash_1 E[\text{stat } \tau e] : K'$ then the derivation contains a sub-term
6754 $\vdash_1 \text{stat } \tau e$.
6755 *Proof*:
6756 By induction on the structure of E .
6757 **CASE** $E \in E^*$:
6758 1. Contradiction by $\vdash_1 E[\text{stat } \tau e] : \tau'$
6759 **CASE** $E = E_0 e_1$:
6760 1. $E[\text{stat } \tau e] = E_0[\text{stat } \tau e] e_1$
6761 2. $\vdash_1 E_0[\text{stat } \tau e] : K_0$
6762 by *inversion*
6763 3. QED by the induction hypothesis (2)
6764
6765

CASE $E = v_0 E_1$:
6766 1. $E[\text{stat } \tau e] = v_0 E_1[\text{stat } \tau e]$
6767 2. $\vdash_1 E_1[\text{stat } \tau e] : K_1$
6768 by *inversion*
6769 3. QED by the induction hypothesis (2)
6770 **CASE** $E = \langle E_0, e_1 \rangle$:
6771 1. $E[\text{stat } \tau e] = \langle E_0[\text{stat } \tau e], e_1 \rangle$
6772 2. $\vdash_1 E_0[\text{stat } \tau e] : K_0$
6773 by *inversion*
6774 3. QED by the induction hypothesis (2)
6775 **CASE** $E = \langle v_0, E_1 \rangle$:
6776 1. $E[\text{stat } \tau e] = \langle v_0, E_1[\text{stat } \tau e] \rangle$
6777 2. $\vdash_1 E_1[\text{stat } \tau e] : K_1$
6778 by *inversion*
6779 3. QED by the induction hypothesis (2)
6780 **CASE** $E = \text{op}^1 E_0$:
6781 1. $E[\text{stat } \tau e] = \text{op}^1 E_0[\text{stat } \tau e]$
6782 2. $\vdash_1 E_0[\text{stat } \tau e] : K_0$
6783 by *inversion*
6784 3. QED by the induction hypothesis (2)
6785 **CASE** $E = \text{op}^2 E_0 e_1$:
6786 1. $E[\text{stat } \tau e] = \text{op}^2 E_0[\text{stat } \tau e] e_1$
6787 2. $\vdash_1 E_0[\text{stat } \tau e] : K_0$
6788 by *inversion*
6789 3. QED by the induction hypothesis (2)
6790 **CASE** $E = \text{op}^2 v_0 E_1$:
6791 1. $E[\text{stat } \tau e] = \text{op}^2 v_0 E_1[\text{stat } \tau e]$
6792 2. $\vdash_1 E_1[\text{stat } \tau e] : K_1$
6793 by *inversion*
6794 3. QED by the induction hypothesis (2)
6795 **CASE** $E = \text{dyn } E_0$:
6796 1. $E[\text{stat } \tau e] = \text{dyn } E_0[\text{stat } \tau e]$
6797 2. $\vdash_1 E_0[\text{stat } \tau e]$
6798 by *inversion*
6799 3. QED by *dynamic stat hole typing* (2)
6800 **CASE** $E = \text{stat } E_0$:
6801 1. Contradiction by $\vdash_1 E[\text{stat } \tau e] : \tau'$
6802 **CASE** $E = \text{dyn } \tau_0 E_0$:
6803 1. $E[\text{stat } \tau e] = \text{dyn } \tau_0 E_0[\text{stat } \tau e]$
6804 2. $\vdash_1 E_0[\text{stat } \tau e]$
6805 by *inversion*
6806 3. QED by *dynamic stat hole typing* (2)
6807 **CASE** $E = \text{stat } \tau_0 E_0$:
6808 1. Contradiction by $\vdash_1 E[\text{stat } \tau e] : \tau'$
6809 **CASE** $E = \text{chk } K_0 E_0$:
6810 1. $E[\text{stat } \tau e] = \text{chk } K_0 E_0[\text{stat } \tau e]$
6811 2. $\vdash_1 E_0[\text{stat } \tau e] : \text{Any}$
6812 by *inversion*
6813 3. QED by the induction hypothesis (2)
6814 \square
6815 **Lemma 4.28** : 1 *dynamic stat hole typing*
6816 If $\vdash_1 E[\text{stat } \tau e]$ then the derivation contains a sub-term \vdash_1
6817 $\text{stat } \tau e$.
6818 *Proof*:
6819
6820

6821 By induction on the structure of E .
 6822 **CASE** $E \in E^\bullet$:
 6823 1. QED by *dynamic hole typing*
 6824 **CASE** $E = E_0 e_1$:
 6825 1. $E[\text{stat } \tau e] = E_0[\text{stat } \tau e] e_1$
 6826 2. $\vdash_1 E_0[\text{stat } \tau e]$
 6827 by *inversion*
 6828 3. QED by the induction hypothesis (2)
 6829 **CASE** $E = v_0 E_1$:
 6830 1. $E[\text{stat } \tau e] = v_0 E_1[\text{stat } \tau e]$
 6831 2. $\vdash_1 E_1[\text{stat } \tau e]$
 6832 by *inversion*
 6833 3. QED by the induction hypothesis (2)
 6834 **CASE** $E = \langle E_0, e_1 \rangle$:
 6835 1. $E[\text{stat } \tau e] = \langle E_0[\text{stat } \tau e], e_1 \rangle$
 6836 2. $\vdash_1 E_0[\text{stat } \tau e]$
 6837 by *inversion*
 6838 3. QED by the induction hypothesis (2)
 6839 **CASE** $E = \langle v_0, E_1 \rangle$:
 6840 1. $E[\text{stat } \tau e] = \langle v_0, E_1[\text{stat } \tau e] \rangle$
 6841 2. $\vdash_1 E_1[\text{stat } \tau e]$
 6842 by *inversion*
 6843 3. QED by the induction hypothesis (2)
 6844 **CASE** $E = \text{op}^1 E_0$:
 6845 1. $E[\text{stat } \tau e] = \text{op}^1 E_0[\text{stat } \tau e]$
 6846 2. $\vdash_1 E_0[\text{stat } \tau e]$
 6847 by *inversion*
 6848 3. QED by the induction hypothesis (2)
 6849 **CASE** $E = \text{op}^2 E_0 e_1$:
 6850 1. $E[\text{stat } \tau e] = \text{op}^2 E_0[\text{stat } \tau e] e_1$
 6851 2. $\vdash_1 E_0[\text{stat } \tau e]$
 6852 by *inversion*
 6853 3. QED by the induction hypothesis (2)
 6854 **CASE** $E = \text{op}^2 v_0 E_1$:
 6855 1. $E[\text{stat } \tau e] = \text{op}^2 v_0 E_1[\text{stat } \tau e]$
 6856 2. $\vdash_1 E_1[\text{stat } \tau e]$
 6857 by *inversion*
 6858 3. QED by the induction hypothesis (2)
 6859 **CASE** $E = \text{dyn } E_0$:
 6860 1. Contradiction by $\vdash_1 E[\text{stat } \tau e]$
 6861 **CASE** $E = \text{stat } E_0$:
 6862 1. $E[\text{stat } \tau e] = \text{stat } E_0[\text{stat } \tau e]$
 6863 2. $\vdash_1 E_0[\text{stat } \tau e] : \lfloor \tau_0 \rfloor$
 6864 by *inversion*
 6865 3. QED by *static stat hole typing* (2)
 6866 **CASE** $E = \text{dyn } \tau E_0$:
 6867 1. Contradiction by $\vdash_1 E[\text{stat } \tau e]$
 6868 **CASE** $E = \text{stat } \tau_0 E_0$:
 6869 1. $E[\text{stat } \tau e] = \text{stat } \tau_0 E_0[\text{stat } \tau e]$
 6870 2. $\vdash_1 E_0[\text{stat } \tau e] : \lfloor \tau_0 \rfloor$
 6871 by *inversion*
 6872 3. QED by *static stat hole typing* (2)
 6873 **CASE** $E = \text{chk } K_0 E_0$:
 6874 1. Contradiction by $\vdash_1 E[\text{stat } \tau e]$
 6875

□

Lemma 4.29 : 1 *static hole substitution*

If $\vdash_1 E^\bullet[e] : K$ and the derivation contains a sub-term $\vdash_1 e : K'$
 and $\vdash_1 e' : K'$, then $\vdash_1 E^\bullet[e'] : K$

Proof:By induction on the structure of E^\bullet .**CASE** $E^\bullet = []$:

1. $E^\bullet[e] = e$
 $\wedge E^\bullet[e'] = e'$

2. $\vdash_1 e : K$

by (1)

3. $K' = K$

4. QED

CASE $E^\bullet = \langle E^\bullet_0, e_1 \rangle$:1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$ $\wedge E^\bullet[e'] = \langle E^\bullet_0[e'], e_1 \rangle$ 2. $\vdash_1 \langle E^\bullet_0[e], e_1 \rangle : K$ 3. $\vdash_1 E^\bullet_0[e] : K_0$ $\wedge \vdash_1 e_1 : K_1$ by *inversion*4. $\vdash_1 E^\bullet_0[e'] : K_0$

by the induction hypothesis (3)

5. $\vdash_1 \langle E^\bullet_0[e'], e_1 \rangle : K$

by (2, 3, 4)

6. QED by (1, 5)

CASE $E^\bullet = \langle v_0, E^\bullet_1 \rangle$:1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$ $\wedge E^\bullet[e'] = \langle v_0, E^\bullet_1[e'] \rangle$ 2. $\vdash_1 \langle v_0, E^\bullet_1[e] \rangle : K$ 3. $\vdash_1 v_0 : K_0$ $\wedge \vdash_1 E^\bullet_1[e] : K_1$ by *inversion*4. $\vdash_1 E^\bullet_1[e'] : K_1$

by the induction hypothesis (3)

5. $\vdash_1 \langle v_0, E^\bullet_1[e'] \rangle : K$

by (2, 3, 4)

6. QED by (1, 5)

CASE $E^\bullet = E^\bullet_0 e_1$:1. $E^\bullet[e] = E^\bullet_0[e] e_1$ $\wedge E^\bullet[e'] = E^\bullet_0[e'] e_1$ 2. $\vdash_1 E^\bullet_0[e] e_1 : K$ 3. $\vdash_1 E^\bullet_0[e] : K_0$ $\wedge \vdash_1 e_1 : K_1$ by *inversion*4. $\vdash_1 E^\bullet_0[e'] : K_0$

by the induction hypothesis (3)

5. $\vdash_1 E^\bullet_0[e'] e_1 : K$

by (2, 3, 4)

6. QED by (1, 5)

CASE $E^\bullet = v_0 E^\bullet_1$:1. $E^\bullet[e] = v_0 E^\bullet_1[e]$ $\wedge E^\bullet[e'] = v_0 E^\bullet_1[e']$ 2. $\vdash_1 v_0 E^\bullet_1[e] : K$

6931 3. $\vdash v_0 : K_0$
 6932 $\wedge \vdash E^{\bullet}_1[e] : K_1$
 6933 by *inversion*
 6934 4. $\vdash E^{\bullet}_1[e'] : K_1$
 6935 by the induction hypothesis (3)
 6936 5. $\vdash v_0 E^{\bullet}_1[e'] : K$
 6937 by (2, 3, 4)
 6938 6. QED by (1, 5)
 6939 **CASE** $E^{\bullet} = op^1 E^{\bullet}_0 :$
 6940 1. $E^{\bullet}[e] = op^1 E^{\bullet}_0[e]$
 6941 $\wedge E^{\bullet}[e'] = op^1 E^{\bullet}_0[e']$
 6942 2. $\vdash op^1 E^{\bullet}_0[e] : K$
 6943 3. $\vdash E^{\bullet}_0[e] : K_0$
 6944 by *inversion*
 6945 4. $\vdash E^{\bullet}_0[e'] : K_0$
 6946 by the induction hypothesis (3)
 6947 5. $\vdash op^1 E^{\bullet}_0[e'] : K$
 6948 by (2, 3, 4)
 6949 6. QED by (1, 5)
 6950 **CASE** $E^{\bullet} = op^2 E^{\bullet}_0 e_1 :$
 6951 1. $E^{\bullet}[e] = op^2 E^{\bullet}_0[e] e_1$
 6952 $\wedge E^{\bullet}[e'] = op^2 E^{\bullet}_0[e'] e_1$
 6953 2. $\vdash op^2 E^{\bullet}_0[e] e_1 : K$
 6954 3. $\vdash E^{\bullet}_0[e] : K_0$
 6955 $\wedge \vdash e_1 : K_1$
 6956 by *inversion*
 6957 4. $\vdash E^{\bullet}_0[e'] : K_0$
 6958 by the induction hypothesis (3)
 6959 5. $\vdash op^2 E^{\bullet}_0[e'] e_1 : K$
 6960 by (2, 3, 4)
 6961 6. QED by (1, 5)
 6962 **CASE** $E^{\bullet} = op^2 v_0 E^{\bullet}_1 :$
 6963 1. $E^{\bullet}[e] = op^2 v_0 E^{\bullet}_1[e]$
 6964 $\wedge E^{\bullet}[e'] = op^2 v_0 E^{\bullet}_1[e']$
 6965 2. $\vdash op^2 v_0 E^{\bullet}_1[e] : K$
 6966 3. $\vdash v_0 : K_0$
 6967 $\wedge \vdash E^{\bullet}_1[e] : K_1$
 6968 by *inversion*
 6969 4. $\vdash E^{\bullet}_1[e'] : K_1$
 6970 by the induction hypothesis (3)
 6971 5. $\vdash op^2 v_0 E^{\bullet}_1[e'] : K$
 6972 by (2, 3, 4)
 6973 6. QED by (1, 5)
 6974 **CASE** $E^{\bullet} = chk K_c E^{\bullet}_0 :$
 6975 1. $E^{\bullet}[e] = chk K_c E^{\bullet}_0[e]$
 6976 $\wedge E^{\bullet}[e'] = chk K_c E^{\bullet}_0[e']$
 6977 2. $\vdash chk K_c E^{\bullet}_0[e] : K$
 6978 3. $\vdash E^{\bullet}_0[e] : K_0$
 6979 by *inversion*
 6980 4. $\vdash E^{\bullet}_0[e'] : K_0$
 6981 by the induction hypothesis (3)
 6982 5. $\vdash chk K_c E^{\bullet}_0[e'] : K$
 6983 by (2, 3, 4)
 6984 6. QED by (1, 5)
 6985

□

Lemma 4.30 : 1 *dynamic hole substitution*If $\vdash E^{\bullet}[e]$ and $\vdash e'$ then $\vdash E^{\bullet}[e']$ *Proof*:By induction on the structure of E^{\bullet} .**CASE** $E^{\bullet} = [] :$ 1. QED $E^{\bullet}[e'] = e'$ **CASE** $E^{\bullet} = \langle E^{\bullet}_0, e_1 \rangle :$ 1. $E^{\bullet}[e] = \langle E^{\bullet}_0[e], e_1 \rangle$ $\wedge E^{\bullet}[e'] = \langle E^{\bullet}_0[e'], e_1 \rangle$ 2. $\vdash \langle E^{\bullet}_0[e], e_1 \rangle$ 3. $\vdash E^{\bullet}_0[e]$ $\wedge \vdash e_1$ by *inversion*4. $\vdash E^{\bullet}_0[e']$

by the induction hypothesis (3)

5. $\vdash \langle E^{\bullet}_0[e'], e_1 \rangle$

by (3, 4)

6. QED by (1, 5)

CASE $E^{\bullet} = \langle v_0, E^{\bullet}_1 \rangle :$ 1. $E^{\bullet}[e] = \langle v_0, E^{\bullet}_1[e] \rangle$ $\wedge E^{\bullet}[e'] = \langle v_0, E^{\bullet}_1[e'] \rangle$ 2. $\vdash \langle v_0, E^{\bullet}_1[e] \rangle$ 3. $\vdash v_0$ $\wedge \vdash E^{\bullet}_1[e]$ by *inversion*4. $\vdash E^{\bullet}_1[e']$

by the induction hypothesis (3)

5. $\vdash \langle v_0, E^{\bullet}_1[e'] \rangle$

by (3, 4)

6. QED by (1, 5)

CASE $E^{\bullet} = E^{\bullet}_0 e_1 :$ 1. $E^{\bullet}[e] = E^{\bullet}_0[e] e_1$ $\wedge E^{\bullet}[e'] = E^{\bullet}_0[e'] e_1$ 2. $\vdash E^{\bullet}_0[e] e_1$ 3. $\vdash E^{\bullet}_0[e]$ $\wedge \vdash e_1$ by *inversion*4. $\vdash E^{\bullet}_0[e']$

by the induction hypothesis (3)

5. $\vdash E^{\bullet}_0[e'] e_1$

by (3, 4)

6. QED by (1, 5)

CASE $E^{\bullet} = v_0 E^{\bullet}_1 :$ 1. $E^{\bullet}[e] = v_0 E^{\bullet}_1[e]$ $\wedge E^{\bullet}[e'] = v_0 E^{\bullet}_1[e']$ 2. $\vdash v_0 E^{\bullet}_1[e]$ 3. $\vdash v_0$ $\wedge \vdash E^{\bullet}_1[e]$ by *inversion*4. $\vdash E^{\bullet}_1[e']$

by the induction hypothesis (3)

7041 5. $\vdash_1 v_0 E^\bullet_1[e']$
 7042 by (3, 4)
 7043 6. QED by (1, 5)
 7044 **CASE** $E^\bullet = op^1 E^\bullet_0$:
 7045 1. $E^\bullet[e] = op^1 E^\bullet_0[e]$
 7046 $\wedge E^\bullet[e'] = op^1 E^\bullet_0[e']$
 7047 2. $\vdash_1 op^1 E^\bullet_0[e]$
 7048 3. $\vdash_1 E^\bullet_0[e]$
 7049 by *inversion*
 7050 4. $\vdash_1 E^\bullet_0[e']$
 7051 by the induction hypothesis (3)
 7052 5. $\vdash_1 op^1 E^\bullet_0[e']$
 7053 by (3, 4)
 7054 6. QED by (1, 5)
 7055 **CASE** $E^\bullet = op^2 E^\bullet_0 e_1$:
 7056 1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$
 7057 $\wedge E^\bullet[e'] = op^2 E^\bullet_0[e'] e_1$
 7058 2. $\vdash_1 op^2 E^\bullet_0[e] e_1$
 7059 3. $\vdash_1 E^\bullet_0[e]$
 7060 $\wedge \vdash_1 e_1$
 7061 by *inversion*
 7062 4. $\vdash_1 E^\bullet_0[e']$
 7063 by the induction hypothesis (3)
 7064 5. $\vdash_1 op^2 E^\bullet_0[e'] e_1$
 7065 by (3, 4)
 7066 6. QED by (1, 5)
 7067 **CASE** $E^\bullet = op^2 v_0 E^\bullet_1$:
 7068 1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$
 7069 $\wedge E^\bullet[e'] = op^2 v_0 E^\bullet_1[e']$
 7070 2. $\vdash_1 op^2 v_0 E^\bullet_1[e]$
 7071 3. $\vdash_1 v_0$
 7072 $\wedge \vdash_1 E^\bullet_1[e]$
 7073 by *inversion*
 7074 4. $\vdash_1 E^\bullet_1[e']$
 7075 by the induction hypothesis (3)
 7076 5. $\vdash_1 op^2 v_0 E^\bullet_1[e']$
 7077 by (3, 4)
 7078 6. QED by (1, 5)
 7079 **CASE** $E^\bullet = \text{chk } K_c E^\bullet_0$:
 7080 1. Contradiction by $\vdash_1 E^\bullet[e]$
 7081 \square

Lemma 4.31 : 1 *hole substitution*

- If $\vdash_1 E[e] : K$ and the derivation contains a sub-term $\vdash_1 e : K'$ and $\vdash_1 e' : K'$ then $\vdash_1 E[e'] : K$.
- If $\vdash_1 E[e] : K$ and the derivation contains a sub-term $\vdash_1 e$ and $\vdash_1 e'$ then $\vdash_1 E[e'] : K$.
- If $\vdash_1 E[e]$ and the derivation contains a sub-term $\vdash_1 e : K'$ and $\vdash_1 e' : K'$ then $\vdash_1 E[e']$.
- If $\vdash_1 E[e]$ and the derivation contains a sub-term $\vdash_1 e$ and $\vdash_1 e'$ then $\vdash_1 E[e']$.

Proof:

By the following four lemmas: *dynamic context static hole substitution*, *dynamic context dynamic hole substitution*,

static context static hole substitution, and *static context dynamic hole substitution*.

 \square **Lemma 4.32** : 1 *dynamic context static hole substitution*

If $\vdash_1 E[e]$ and contains $\vdash_1 e : K'$, and furthermore $\vdash_1 e' : K'$, then $\vdash_1 E[e']$

Proof:

By induction on the structure of E .

CASE $E \in E^\bullet$:

1. Contradiction by $\vdash_1 E[e]$

CASE $E = E_0 e_1$:

1. $E[e] = E_0[e] e_1$

2. $\vdash_1 E_0[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = v_0 E_1$:

1. $E[e] = v_0 E_1[e]$

2. $\vdash_1 E_1[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \langle E_0, e_1 \rangle$:

1. $E[e] = \langle E_0[e], e_1 \rangle$

2. $\vdash_1 E_0[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \langle v_0, E_1 \rangle$:

1. $E[e] = \langle v_0, E_1[e] \rangle$

2. $\vdash_1 E_1[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = op^1 E_0$:

1. $E[e] = op^1 E_0[e]$

2. $\vdash_1 E_0[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = op^2 E_0 e_1$:

1. $E[e] = op^2 E_0[e] e_1$

2. $\vdash_1 E_0[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = op^2 v_0 E_1$:

1. $E[e] = op^2 v_0 E_1[e]$

2. $\vdash_1 E_1[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \text{dyn } E_0$:

1. Contradiction by $\vdash_1 E[e]$

CASE $E = \text{stat } E_0$:

1. $E[e] = \text{stat } E_0[e]$

2. $\vdash_1 E_0[e] : \text{Any}$

by *inversion*

3. QED by *static context static hole substitution* (2)

CASE $E = \text{dyn } \tau'' E_0$:

7151 1. Contradiction by $\vdash_1 E[e]$
 7152 **CASE** $E = \text{stat } \tau_0 E_0 :$
 7153 1. $E[e] = \text{stat } \tau_0 E_0[e]$
 7154 2. $\vdash_1 E_0[e] : \perp \tau_0$
 7155 by *inversion*
 7156 3. QED by *static context static hole substitution* (2)
 7157 **CASE** $E = \text{chk } K_0 E_0 :$
 7158 1. Contradiction by $\vdash_1 E[e]$
 7159 \square

7160 **Lemma 4.33** : 1 *dynamic context dynamic hole substitution*

7161 If $\vdash_1 E[e]$ and contains $\vdash_1 e$, and furthermore $\vdash_1 e'$, then $\vdash_1 E[e']$

7162 *Proof*:

7163 By induction on the structure of E .

7164 **CASE** $E \in E^\bullet :$

7165 1. QED by *dynamic boundary-free hole substitution*

7166 **CASE** $E = E_0 e_1 :$

7167 1. $E[e] = E_0[e] e_1$

7168 2. $\vdash_1 E_0[e]$

7169 by *inversion*

7170 3. QED by the induction hypothesis (2)

7171 **CASE** $E = v_0 E_1 :$

7172 1. $E[e] = v_0 E_1[e]$

7173 2. $\vdash_1 E_1[e]$

7174 by *inversion*

7175 3. QED by the induction hypothesis (2)

7176 **CASE** $E = \langle E_0, e_1 \rangle :$

7177 1. $E[e] = \langle E_0[e], e_1 \rangle$

7178 2. $\vdash_1 E_0[e]$

7179 by *inversion*

7180 3. QED by the induction hypothesis (2)

7181 **CASE** $E = \langle v_0, E_1 \rangle :$

7182 1. $E[e] = \langle v_0, E_1[e] \rangle$

7183 2. $\vdash_1 E_1[e]$

7184 by *inversion*

7185 3. QED by the induction hypothesis (2)

7186 **CASE** $E = \text{op}^1 E_0 :$

7187 1. $E[e] = \text{op}^1 E_0[e]$

7188 2. $\vdash_1 E_0[e]$

7189 by *inversion*

7190 3. QED by the induction hypothesis (2)

7191 **CASE** $E = \text{op}^2 E_0 e_1 :$

7192 1. $E[e] = \text{op}^2 E_0[e] e_1$

7193 2. $\vdash_1 E_0[e]$

7194 by *inversion*

7195 3. QED by the induction hypothesis (2)

7196 **CASE** $E = \text{op}^2 v_0 E_1 :$

7197 1. $E[e] = \text{op}^2 v_0 E_1[e]$

7198 2. $\vdash_1 E_1[e]$

7199 by *inversion*

7200 3. QED by the induction hypothesis (2)

7201 **CASE** $E = \text{dyn } E_0 :$

7202 1. Contradiction by $\vdash_1 E[e]$

7203 **CASE** $E = \text{stat } E_0 :$

7204 1. $E[e] = \text{stat } E_0[e]$

7205 2. $\vdash_1 E_0[e] : \text{Any}$

7206 by *inversion*

7207 3. QED by *static context dynamic hole substitution* (2)

7208 **CASE** $E = \text{dyn } \tau'' E_0 :$

7209 1. Contradiction by $\vdash_1 E[e]$

7210 **CASE** $E = \text{stat } \tau_0 E_0 :$

7211 1. $E[e] = \text{stat } \tau_0 E_0[e]$

7212 2. $\vdash_1 E_0[e] : \perp \tau_0$

7213 by *inversion*

7214 3. QED by *static context dynamic hole substitution* (2)

7215 **CASE** $E = \text{chk } K_0 E_0 :$

7216 1. Contradiction by $\vdash_1 E[e]$

7217 \square

7218 **Lemma 4.34** : 1 *static context static hole substitution*

7219 If $\vdash_1 E[e] : K$ and contains $\vdash_1 e : K'$, and furthermore $\vdash_1 e' : K'$,
 7220 then $\vdash_1 E[e'] : K$

7221 *Proof*:

7222 By induction on the structure of E .

7223 **CASE** $E \in E^\bullet :$

7224 1. QED by *static boundary-free hole substitution*

7225 **CASE** $E = E_0 e_1 :$

7226 1. $E[e] = E_0[e] e_1$

7227 2. $\vdash_1 E_0[e] : K_0$

7228 by *inversion*

7229 3. QED by the induction hypothesis (2)

7230 **CASE** $E = v_0 E_1 :$

7231 1. $E[e] = v_0 E_1[e]$

7232 2. $\vdash_1 E_1[e] : K_1$

7233 by *inversion*

7234 3. QED by the induction hypothesis (2)

7235 **CASE** $E = \langle E_0, e_1 \rangle :$

7236 1. $E[e] = \langle E_0[e], e_1 \rangle$

7237 2. $\vdash_1 E_0[e] : K_0$

7238 by *inversion*

7239 3. QED by the induction hypothesis (2)

7240 **CASE** $E = \langle v_0, E_1 \rangle :$

7241 1. $E[e] = \langle v_0, E_1[e] \rangle$

7242 2. $\vdash_1 E_1[e] : K_1$

7243 by *inversion*

7244 3. QED by the induction hypothesis (2)

7245 **CASE** $E = \text{op}^1 E_0 :$

7246 1. $E[e] = \text{op}^1 E_0[e]$

7247 2. $\vdash_1 E_0[e] : K_0$

7248 by *inversion*

7249 3. QED by the induction hypothesis (2)

7250 **CASE** $E = \text{op}^2 E_0 e_1 :$

7251 1. $E[e] = \text{op}^2 E_0[e] e_1$

7252 2. $\vdash_1 E_0[e] : K_0$

7253 by *inversion*

7254 3. QED by the induction hypothesis (2)

7255 **CASE** $E = \text{op}^2 v_0 E_1 :$

7256 1. $E[e] = \text{op}^2 v_0 E_1[e]$

7261 2. $\vdash_1 E_1[e] : K_1$
 7262 by *inversion*
 7263 3. QED by the induction hypothesis (2)
 7264 **CASE** $E = \text{dyn } E_0 :$
 7265 1. $E[e] = \text{dyn } E_0[e]$
 7266 2. $\vdash_1 E_0[e]$
 7267 by *inversion*
 7268 3. QED by *static dyn hole typing* (2)
 7269 **CASE** $E = \text{stat } E_0 :$
 7270 1. Contradiction by $\vdash_1 E[e] : K$
 7271 **CASE** $E = \text{dyn } \tau_0 E_0 :$
 7272 1. $E[e] = \text{dyn } \tau_0 E_0[e]$
 7273 2. $\vdash_1 E_0[e]$
 7274 by *inversion*
 7275 3. QED by *static dyn hole typing* (2)
 7276 **CASE** $E = \text{stat } \tau_0 E_0 :$
 7277 1. Contradiction by $\vdash_1 E[e] : K$
 7278 **CASE** $E = \text{chk } K_0 E_0 :$
 7279 1. $E[e] = \text{chk } K_0 E_0[e]$
 7280 2. $\vdash_1 E_0[e] : \text{Any}$
 7281 by *inversion*
 7282 3. QED by the induction hypothesis (2)
 7283 \square
 7284 **Lemma 4.35** : 1 *static context dynamic hole substitution*
 7285 If $\vdash_1 E[e] : K$ and contains $\vdash_1 e$, and furthermore $\vdash_1 e'$, then
 7286 $\vdash_1 E[e'] : K$
 7287 *Proof*:
 7288 By induction on the structure of E .
 7289 **CASE** $E \in E^* :$
 7290 1. Contradiction by $\vdash_1 E[e] : K$
 7291 **CASE** $E = E_0 e_1 :$
 7292 1. $E[e] = E_0[e] e_1$
 7293 2. $\vdash_1 E_0[e] : K_0$
 7294 by *inversion*
 7295 3. QED by the induction hypothesis (2)
 7296 **CASE** $E = v_0 E_1 :$
 7297 1. $E[e] = v_0 E_1[e]$
 7298 2. $\vdash_1 E_1[e] : K_1$
 7299 by *inversion*
 7300 3. QED by the induction hypothesis (2)
 7301 **CASE** $E = \langle E_0, e_1 \rangle :$
 7302 1. $E[e] = \langle E_0[e], e_1 \rangle$
 7303 2. $\vdash_1 E_0[e] : K_0$
 7304 by *inversion*
 7305 3. QED by the induction hypothesis (2)
 7306 **CASE** $E = \langle v_0, E_1 \rangle :$
 7307 1. $E[e] = \langle v_0, E_1[e] \rangle$
 7308 2. $\vdash_1 E_1[e] : K_1$
 7309 by *inversion*
 7310 3. QED by the induction hypothesis (2)
 7311 **CASE** $E = \text{op}^1 E_0 :$
 7312 1. $E[e] = \text{op}^1 E_0[e]$
 7313
 7314
 7315

7316 2. $\vdash_1 E_0[e] : K_0$
 7317 by *inversion*
 7318 3. QED by the induction hypothesis (2)
 7319 **CASE** $E = \text{op}^2 E_0 e_1 :$
 7320 1. $E[e] = \text{op}^2 E_0[e] e_1$
 7321 2. $\vdash_1 E_0[e] : K_0$
 7322 by *inversion*
 7323 3. QED by the induction hypothesis (2)
 7324 **CASE** $E = \text{op}^2 v_0 E_1 :$
 7325 1. $E[e] = \text{op}^2 v_0 E_1[e]$
 7326 2. $\vdash_1 E_1[e] : K_1$
 7327 by *inversion*
 7328 3. QED by the induction hypothesis (2)
 7329 **CASE** $E = \text{dyn } E_0 :$
 7330 1. $E[e] = \text{dyn } E_0[e]$
 7331 2. $\vdash_1 E_0[e]$
 7332 by *inversion*
 7333 3. QED by *dynamic stat hole typing* (2)
 7334 **CASE** $E = \text{stat } E_0 :$
 7335 1. Contradiction by $\vdash_1 E[e] : K$
 7336 **CASE** $E = \text{dyn } \tau_0 E_0 :$
 7337 1. $E[e] = \text{dyn } \tau_0 E_0[e]$
 7338 2. $\vdash_1 E_0[e]$
 7339 by *inversion*
 7340 3. QED by *dynamic stat hole typing* (2)
 7341 **CASE** $E = \text{stat } \tau_0 E_0 :$
 7342 1. Contradiction by $\vdash_1 E[e] : K$
 7343 **CASE** $E = \text{chk } K_0 E_0 :$
 7344 1. $E[e] = \text{chk } K_0 E_0[e]$
 7345 2. $\vdash_1 E_0[e] : \text{Any}$
 7346 by *inversion*
 7347 3. QED by the induction hypothesis (2)
 7348 \square

Lemma 4.36 : 1 *static inversion*

- If $\vdash_1 \langle e_0, e_1 \rangle : K$ then $\vdash_1 e_0 : \text{Any}$ and $\vdash_1 e_1 : \text{Any}$
- If $\vdash_1 \lambda x. e : K$ then $x \vdash_1 e$
- If $\vdash_1 \lambda(x:\tau). e : K$ then $(x:\tau) \vdash_1 e : \text{Any}$
- If $\vdash_1 e_0 e_1 : K$ then $K = \text{Any}$ and $\vdash_1 e_0 : \text{Fun}$ and $\vdash_1 e_1 : \text{Any}$
- If $\vdash_1 \text{op}^1 e_0 : K$ then $K = \text{Any}$ and $\vdash_1 e_0 : \text{Pair}$
- If $\vdash_1 \text{op}^2 e_0 e_1 : K$ then $\vdash_1 e_0 : K_0$ and $\vdash_1 e_1 : K_1$ and $\Delta(\text{op}^2, K_0, K_1) = K'$ and $K' <: K$
- If $\vdash_1 \text{dyn } \tau e : K$ then $\vdash_1 e$ and $\lfloor \tau \rfloor \leqslant K$
- If $\vdash_1 \text{chk } K' e_0 : K$ then $\vdash_1 e_0 : \text{Any}$ and $K' \leqslant K$

Proof:QED by the definition of $\Gamma \vdash_1 e : \tau$ \square **Lemma 4.37** : 1 *dynamic inversion*

- If $\vdash_1 \langle e_0, e_1 \rangle$ then $\vdash_1 e_0$ and $\vdash_1 e_1$
- If $\vdash_1 \lambda x. e$ then $x \vdash_1 e$
- If $\vdash_1 \lambda(x:\tau). e$ then $(x:\tau) \vdash_1 e : \text{Any}$
- If $\vdash_1 e_0 \ e_1$ then $\vdash_1 e_0$ and $\vdash_1 e_1$
- If $\vdash_1 op^1 e_0$ then $\vdash_1 e_0$
- If $\vdash_1 op^2 e_0 \ e_1$ then $\vdash_1 e_0$ and $\vdash_1 e_1$
- If $\vdash_1 \text{stat } \tau \ e$ then $\vdash_1 e : \lfloor \tau \rfloor$
- If $\vdash_1 \text{stat } e$ then $\vdash_1 e : \text{Any}$

Proof:

QED by the definition of $\vdash_1 e$.

□

Lemma 4.38 : 1 canonical forms

- If $\vdash_1 v : \text{Pair}$ then $v = \langle v_0, v_1 \rangle$
- If $\vdash_1 v : \text{Fun}$ then $v = \lambda x. e'$ or $v = \lambda(x:\tau_d). e'$
- If $\vdash_1 v : \text{Int}$ then $v = i$
- If $\vdash_1 v : \text{Nat}$ then $v \in \mathbb{N}$

Proof:

QED by definition of $\vdash_1 : K$

□

Lemma 4.39 : Δ tag soundness

- If $\vdash_1 v_0 : K_0$ and $\vdash_1 v_1 : K_1$ and $\Delta(op^2, K_0, K_1) = K$ then $\vdash_1 \delta(op^2, v_0, v_1) : K$.

Proof:

By case analysis on Δ .

CASE $\Delta(\text{sum}, \text{Nat}, \text{Nat}) = \text{Nat} :$

1. $v_0 = i_0, i_0 \in \mathbb{N}$
 $\wedge v_1 = i_1, i_1 \in \mathbb{N}$
 by *canonical forms*
2. $\delta(\text{sum}, i_0, i_1) = i_0 + i_1 \in \mathbb{N}$
3. QED

CASE $\Delta(\text{sum}, \text{Int}, \text{Int}) = \text{Int} :$

1. $v_0 = i_0$
 $\wedge v_1 = i_1$
 by *canonical forms*
2. $\delta(\text{sum}, i_0, i_1) = i_0 + i_1 \in i$
3. QED

CASE $\Delta(\text{quotient}, \text{Nat}, \text{Nat}) = \text{Nat} :$

1. $v_0 = i_0, i_0 \in \mathbb{N}$
 $\wedge v_1 = i_1, i_1 \in \mathbb{N}$
 by *canonical forms*
2. **IF** $i_1 = 0 :$
 - a. $\delta(\text{quotient}, i_0, i_1) = \text{BndryErr}$
 - b. QED by $\vdash_1 \text{BndryErr} : K$
- ELSE** $i_1 \neq 0 :$
 - a. $\delta(\text{quotient}, i_0, i_1) = \lfloor i_0/i_1 \rfloor \in \mathbb{N}$
 - b. QED

CASE $\Delta(\text{quotient}, \text{Int}, \text{Int}) = \text{Int} :$

1. $v_0 = i_0$
 $\wedge v_1 = i_1$
 by *canonical forms*
2. **IF** $i_1 = 0 :$
 - a. $\delta(\text{quotient}, i_0, i_1) = \text{BndryErr}$
 - b. QED by $\vdash_1 \text{BndryErr} : K$
- ELSE** $i_1 \neq 0 :$

a. $\delta(\text{quotient}, i_0, i_1) = \lfloor i_0/i_1 \rfloor \in i$

b. QED

□

Lemma 4.40 : δ preservation

- If $\vdash_1 v$ and $\delta(op^1, v) = e$ then $\vdash_1 e$
- If $\vdash_1 v_0$ and $\vdash_1 v_1$ and $\delta(op^2, v_0, v_1) = e$ then $\vdash_1 e$

Proof:

CASE $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0 :$

1. $\vdash_1 v_0$
 by *inversion*
2. QED

CASE $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1 :$

1. $\vdash_1 v_1$
 by *inversion*
2. QED

CASE $\delta(\text{sum}, v_0, v_1) = v_0 + v_1 :$

1. QED

CASE $\delta(\text{quotient}, v_0, v_1) = \lfloor v_0/v_1 \rfloor :$

1. QED

CASE $\delta(op^2, v_0, v_1) = \text{BndryErr} :$

1. QED

□

Lemma 4.41 : Δ preservation

- If $\Delta(op^2, \tau_0, \tau_1) = \tau$ then $\Delta(op^2, \lfloor \tau_0 \rfloor, \lfloor \tau_1 \rfloor) = \lfloor \tau \rfloor$.

Proof:

By case analysis on the definition of Δ

CASE $\Delta(op^2, \text{Nat}, \text{Nat}) = \text{Nat} :$

1. QED by $\lfloor \text{Nat} \rfloor = \text{Nat}$

CASE $\Delta(op^2, \text{Int}, \text{Int}) = \text{Int} :$

1. QED by $\lfloor \text{Int} \rfloor = \text{Int}$

□

Lemma 4.42 : Δ inversion

- If $\Delta(\text{fst}, \tau) = \tau'$ then $\tau = \tau_0 \times \tau_1$ and $\tau' = \tau_0$
- If $\Delta(\text{snd}, \tau) = \tau'$ then $\tau = \tau_0 \times \tau_1$ and $\tau' = \tau_1$

Proof:

QED by the definition of Δ

□

Lemma 4.43 : $<$: preservation

- If $\tau <: \tau'$ then $\lfloor \tau \rfloor \leq \lfloor \tau' \rfloor$

Proof:

By case analysis on the last rule used to show $\tau <: \tau'$.

CASE $\text{Nat} <: \text{Int} :$

1. QED $\lfloor \text{Nat} \rfloor <: \lfloor \text{Int} \rfloor$

CASE $\tau_d \Rightarrow \tau_c <: \tau'_d \Rightarrow \tau'_c :$

1. $\lfloor \tau_d \Rightarrow \tau_c \rfloor = \text{Fun}$
 $\wedge \lfloor \tau'_d \Rightarrow \tau'_c \rfloor = \text{Fun}$
2. QED

CASE $\tau_0 \times \tau_1 <: \tau'_0 \times \tau'_1 :$

1. $\lfloor \tau_0 \times \tau_1 \rfloor = \text{Pair}$
 $\wedge \lfloor \tau'_0 \times \tau'_1 \rfloor = \text{Pair}$
2. QED

□

Lemma 4.44 : 1 static value inversion

7481 If $\vdash v : \text{Any}$ then $\vdash v$

7482 *Proof:*

7483 By induction on the structure of v .

7484 **CASE** $v = i :$

7485 1. QED by $\vdash v$

7486 **CASE** $v = \langle v_0, v_1 \rangle :$

7487 1. $\vdash v_0 : \text{Any}$

7488 $\wedge \vdash v_1 : \text{Any}$

7489 by *inversion*

7490 2. $\vdash v_0$

7491 $\wedge \vdash v_1$

7492 by the induction hypothesis

7493 3. QED by (2)

7494 **CASE** $v = \lambda x. e :$

7495 1. $x \vdash e$

7496 by *inversion*

7497 2. QED

7498 **CASE** $v = \lambda(x:\tau). e :$

7499 1. $(x:\tau) \vdash e : \text{Any}$

7500 by *inversion*

7501 2. QED

7502 \square

7503 **Lemma 4.45** : 1 *dynamic value inversion*

7504 If $\vdash v$ then $\vdash v : \text{Any}$

7505 *Proof:*

7506 By induction on the structure of v .

7507 **CASE** $v = i :$

7508 1. $\vdash v : \text{Int}$

7509 2. QED by $\text{Int} <: \text{Any}$

7510 **CASE** $v = \langle v_0, v_1 \rangle :$

7511 1. $\vdash v_0$

7512 $\wedge \vdash v_1$

7513 by *inversion*

7514 2. $\vdash v_0 : \text{Any}$

7515 $\wedge \vdash v_1 : \text{Any}$

7516 by the induction hypothesis

7517 3. $\vdash \langle v_0, v_1 \rangle : \text{Pair}$

7518 by (2)

7519 4. QED by $\text{Pair} <: \text{Any}$

7520 **CASE** $v = \lambda x. e :$

7521 1. $x \vdash e$

7522 by *inversion*

7523 2. $\vdash \lambda x. e : \text{Fun}$

7524 by (1)

7525 3. QED by $\text{Fun} <: \text{Any}$

7526 **CASE** $v = \lambda(x:\tau). e :$

7527 1. $(x:\tau) \vdash e : \text{Any}$

7528 by *inversion*

7529 2. $\vdash \lambda(x:\tau). e : \text{Fun}$

7530 by (1)

7531 3. QED by $\text{Fun} <: \text{Any}$

7532 \square

7533 **Lemma 4.46** : 1 *substitution*

• If $(x:\tau), \Gamma \vdash e$ and $\vdash v : [\tau]$ then $\Gamma \vdash e[x \leftarrow v]$

• If $x, \Gamma \vdash e$ and $\vdash v$ then $\Gamma \vdash e[x \leftarrow v]$

• If $(x:\tau_x), \Gamma \vdash e : K$ and $\vdash v : [\tau_x]$ then $\Gamma \vdash e[x \leftarrow v] : K$

• If $x, \Gamma \vdash e : K$ and $\vdash v$ then $\Gamma \vdash e[x \leftarrow v] : K$

Proof:

By the following four lemmas: *dynamic context static value substitution*, *dynamic context dynamic value substitution*, *static context static value substitution*, and *static context dynamic value substitution*.

\square

Lemma 4.47 : 1 *dynamic-static substitution*

If $(x:\tau), \Gamma \vdash e$ and $\vdash v : [\tau]$ then $\Gamma \vdash e[x \leftarrow v]$

Proof:

By induction on the structure of e .

CASE $e = x :$

1. $e[x \leftarrow v] = v$

2. $\vdash v : \text{Any}$

by $[\tau] <: \text{Any}$

3. $\vdash v$

by *static value inversion* (2)

4. $\Gamma \vdash v$

by *weakening* (3)

5. QED

CASE $e = x' :$

1. QED by $x'[x \leftarrow v] = x'$

CASE $e = i :$

1. QED by $i[x \leftarrow v] = i$

CASE $e = \lambda x. e' :$

1. QED by $(\lambda x. e')[x \leftarrow v] = \lambda x. e'$

CASE $e = \lambda(x:\tau'). e' :$

1. QED by $(\lambda(x:\tau'). e')[x \leftarrow v] = \lambda(x:\tau'). e'$

CASE $e = \lambda x'. e' :$

1. $e[x \leftarrow v] = \lambda x'. (e'[x \leftarrow v])$

2. $x', (x:\tau), \Gamma \vdash e'$

by *inversion*

3. $x', \Gamma \vdash e'[x \leftarrow v]$

by *dynamic context static value substitution*

4. $\Gamma \vdash \lambda x'. e'[x \leftarrow v]$

by (3)

5. QED

CASE $e = \lambda(x':\tau'). e' :$

1. $e[x \leftarrow v] = \lambda(x':\tau'). (e'[x \leftarrow v])$

2. $(x':\tau'), (x:\tau), \Gamma \vdash e' : \text{Any}$

by *inversion*

3. $(x':\tau'), \Gamma \vdash e'[x \leftarrow v] : \text{Any}$

by *static context static value substitution*

4. $\Gamma \vdash \lambda(x':\tau'). (e'[x \leftarrow v])$

5. QED

CASE $e = \langle e_0, e_1 \rangle :$

1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$

2. $(x:\tau), \Gamma \vdash e_0$

$\wedge (x:\tau), \Gamma \vdash e_1$

by *inversion*

7591 3. $\Gamma \vdash_1 e_0[x \leftarrow v]$
 7592 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v]$
 7593 by the induction hypothesis (2)
 7594 4. $\Gamma \vdash_1 \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
 7595 by (3)
 7596 5. QED
 7597 **CASE** $e = e_0 e_1$:
 7598 1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$
 7599 2. $(x:\tau), \Gamma \vdash_1 e_0$
 7600 $\wedge (x:\tau), \Gamma \vdash_1 e_1$
 7601 by *inversion*
 7602 3. $\Gamma \vdash_1 e_0[x \leftarrow v]$
 7603 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v]$
 7604 by the induction hypothesis (2)
 7605 4. $\Gamma \vdash_1 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 7606 by (3)
 7607 5. QED
 7608 **CASE** $e = op^1 e_0$:
 7609 1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$
 7610 2. $(x:\tau), \Gamma \vdash_1 e_0$
 7611 by *inversion*
 7612 3. $\Gamma \vdash_1 e_0[x \leftarrow v]$
 7613 by the induction hypothesis (2)
 7614 4. $\Gamma \vdash_1 op^1 e_0[x \leftarrow v]$
 7615 by (3)
 7616 5. QED
 7617 **CASE** $e = op^2 e_0 e_1$:
 7618 1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 7619 2. $(x:\tau), \Gamma \vdash_1 e_0$
 7620 $\wedge (x:\tau), \Gamma \vdash_1 e_1$
 7621 by *inversion*
 7622 3. $\Gamma \vdash_1 e_0[x \leftarrow v]$
 7623 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v]$
 7624 by the induction hypothesis (2)
 7625 4. $\Gamma \vdash_1 op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 7626 by (3)
 7627 5. QED
 7628 **CASE** $e = \text{dyn } \tau' e'$
 7629 $\vee e = \text{dyn } e'$
 7630 $\vee e = \text{chk } K' e'$:
 7631 1. Contradiction by $(x:\tau), \Gamma \vdash_1 e$
 7632 **CASE** $e = \text{stat } \tau' e'$:
 7633 1. $e[x \leftarrow v] = \text{stat } \tau' e'[x \leftarrow v]$
 7634 2. $(x:\tau), \Gamma \vdash_1 e' : \lfloor \tau' \rfloor$
 7635 by *inversion*
 7636 3. $\Gamma \vdash_1 e'[x \leftarrow v] : \lfloor \tau' \rfloor$
 7637 by *static context static value substitution* (2)
 7638 4. $\Gamma \vdash_1 \text{stat } \tau' (e'[x \leftarrow v])$
 7639 by (3)
 7640 5. QED
 7641 **CASE** $e = \text{stat } e'$:
 7642 1. $e[x \leftarrow v] = \text{stat } e'[x \leftarrow v]$
 7643 2. $(x:\tau), \Gamma \vdash_1 e' : \text{Any}$
 7644 by *inversion*
 7645

3. $\Gamma \vdash_1 e'[x \leftarrow v] : \text{Any}$
 by *static context static value substitution* (2)
 4. $\Gamma \vdash_1 \text{stat } (e'[x \leftarrow v])$
 by (3)
 5. QED
 \square
Lemma 4.48 : 1 *dynamic-dynamic substitution*
 If $x, \Gamma \vdash_1 e$ and $\Gamma \vdash_1 v$ then $\Gamma \vdash_1 e[x \leftarrow v]$
Proof:
 By induction on the structure of e .
CASE $e = x$:
 1. $e[x \leftarrow v] = v$
 2. $\Gamma \vdash_1 v$
 by *weakening* (3)
 3. QED
CASE $e = x'$:
 1. QED by $x'[x \leftarrow v] = x'$
CASE $e = i$:
 1. QED by $i[x \leftarrow v] = i$
CASE $e = \lambda x. e'$:
 1. QED by $(\lambda x. e')[x \leftarrow v] = \lambda x. e'$
CASE $e = \lambda(x:\tau'). e'$:
 1. QED by $(\lambda(x:\tau'). e')[x \leftarrow v] = \lambda(x:\tau'). e'$
CASE $e = \lambda x'. e'$:
 1. $e[x \leftarrow v] = \lambda x'. (e'[x \leftarrow v])$
 2. $x', x, \Gamma \vdash_1 e'$
 by *inversion*
 3. $x', \Gamma \vdash_1 e'[x \leftarrow v]$
 by the induction hypothesis (2)
 4. $\Gamma \vdash_1 \lambda x'. e'[x \leftarrow v]$
 by (3)
 5. QED
CASE $e = \lambda(x':\tau'). e'$:
 1. $e[x \leftarrow v] = \lambda(x':\tau'). (e'[x \leftarrow v])$
 2. $(x':\tau'), x, \Gamma \vdash_1 e' : \text{Any}$
 by *inversion*
 3. $(x':\tau'), \Gamma \vdash_1 e'[x \leftarrow v] : \text{Any}$
 by *static context dynamic value substitution*
 4. $\Gamma \vdash_1 \lambda(x':\tau'). (e'[x \leftarrow v])$
 5. QED
CASE $e = \langle e_0, e_1 \rangle$:
 1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
 2. $x, \Gamma \vdash_1 e_0$
 $\wedge x, \Gamma \vdash_1 e_1$
 by *inversion*
 3. $\Gamma \vdash_1 e_0[x \leftarrow v]$
 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v]$
 by the induction hypothesis (2)
 4. $\Gamma \vdash_1 \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
 by (3)
 5. QED
CASE $e = e_0 e_1$:
 1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$

7701 2. $x, \Gamma \vdash_1 e_0$
 7702 $\wedge x, \Gamma \vdash_1 e_1$
 7703 by *inversion*
 7704 3. $\Gamma \vdash_1 e_0[x \leftarrow v]$
 7705 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v]$
 7706 by the induction hypothesis (2)
 7707 4. $\Gamma \vdash_1 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 7708 by (3)
 7709 5. QED
 7710 **CASE** $e = op^1 e_0$:
 7711 1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$
 7712 2. $x, \Gamma \vdash_1 e_0$
 7713 by *inversion*
 7714 3. $\Gamma \vdash_1 e_0[x \leftarrow v]$
 7715 by the induction hypothesis (2)
 7716 4. $\Gamma \vdash_1 op^1 e_0[x \leftarrow v]$
 7717 by (3)
 7718 5. QED
 7719 **CASE** $e = op^2 e_0 e_1$:
 7720 1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 7721 2. $x, \Gamma \vdash_1 e_0$
 7722 $\wedge x, \Gamma \vdash_1 e_1$
 7723 by *inversion*
 7724 3. $\Gamma \vdash_1 e_0[x \leftarrow v]$
 7725 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v]$
 7726 by the induction hypothesis (2)
 7727 4. $\Gamma \vdash_1 op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 7728 by (3)
 7729 5. QED
 7730 **CASE** $e = \text{dyn } \tau' e'$
 7731 $\vee e = \text{dyn } e'$
 7732 $\vee e = \text{chk } K' e'$:
 7733 1. Contradiction by $\Gamma \vdash_1 e$
 7734 **CASE** $e = \text{stat } \tau' e'$:
 7735 1. $e[x \leftarrow v] = \text{stat } \tau' e'[x \leftarrow v]$
 7736 2. $x, \Gamma \vdash_1 e' : [\tau']$
 7737 by *inversion*
 7738 3. $\Gamma \vdash_1 e'[x \leftarrow v] : [\tau']$
 7739 by *static context dynamic value substitution* (2)
 7740 4. $\Gamma \vdash_1 \text{stat } \tau' (e'[x \leftarrow v])$
 7741 by (3)
 7742 5. QED
 7743 **CASE** $e = \text{stat } e'$:
 7744 1. $e[x \leftarrow v] = \text{stat } e'[x \leftarrow v]$
 7745 2. $x, \Gamma \vdash_1 e' : \text{Any}$
 7746 by *inversion*
 7747 3. $\Gamma \vdash_1 e'[x \leftarrow v] : \text{Any}$
 7748 by *static context dynamic value substitution* (2)
 7749 4. $\Gamma \vdash_1 \text{stat } (e'[x \leftarrow v])$
 7750 by (3)
 7751 5. QED
 7752 \square

7753 **Lemma 4.49** : 1 *static-static substitution*

7756 If $(x:\tau), \Gamma \vdash_1 e : K$ and $\vdash_1 v : [\tau]$ then $\Gamma \vdash_1 e[x \leftarrow v] : K$

7757 *Proof*:

7758 By induction on the structure of e .

7759 **CASE** $e = x$:

7760 1. $[\tau] \leqslant K$
 7761 by $(x:\tau), \Gamma \vdash_1 x : K$

7762 2. $e[x \leftarrow v] = v$

7763 3. $\vdash_1 v : K$

7764 by (1)

7765 4. $\Gamma \vdash_1 v : K$

7766 by *weakening* (3)

7767 5. QED

7768 **CASE** $e = x'$:

7769 1. QED by $(x'[x \leftarrow v]) = x'$

7770 **CASE** $e = i$:

7771 1. QED by $i[x \leftarrow v] = i$

7772 **CASE** $e = \lambda x. e'$:

7773 1. QED by $(\lambda x. e')[x \leftarrow v] = \lambda x. e'$

7774 **CASE** $e = \lambda x'. e'$:

7775 1. $e[x \leftarrow v] = \lambda x'. (e'[x \leftarrow v])$

7776 2. $x', (x:\tau), \Gamma \vdash_1 e'$

7777 by *inversion*

7778 3. $x', \Gamma \vdash_1 e'[x \leftarrow v]$

7779 by *dynamic context static value substitution*

7780 4. $\Gamma \vdash_1 \lambda x'. e'[x \leftarrow v] : K$

7781 by (3)

7782 5. QED

7783 **CASE** $e = \lambda(x':\tau'). e'$:

7784 1. $e[x \leftarrow v] = \lambda(x':\tau'). (e'[x \leftarrow v])$

7785 2. $(x':\tau'), (x:\tau), \Gamma \vdash_1 e' : \text{Any}$

7786 by *inversion*

7787 3. $(x':\tau'), \Gamma \vdash_1 e'[x \leftarrow v] : \text{Any}$

7788 by the induction hypothesis (2)

7789 4. $\Gamma \vdash_1 \lambda(x':\tau'). (e'[x \leftarrow v]) : K$

7790 5. QED

7791 **CASE** $e = \langle e_0, e_1 \rangle$:

7792 1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$

7793 2. $(x:\tau), \Gamma \vdash_1 e_0 : \text{Any}$

7794 $\wedge (x:\tau), \Gamma \vdash_1 e_1 : \text{Any}$

7795 by *inversion*

7796 3. $\Gamma \vdash_1 e_0[x \leftarrow v] : \text{Any}$

7797 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v] : \text{Any}$

7798 by the induction hypothesis (2)

7799 4. $\Gamma \vdash_1 \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle : K$

7800 by (3)

7801 5. QED

7802 **CASE** $e = e_0 e_1$:

7803 1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$

7804 2. $(x:\tau), \Gamma \vdash_1 e_0 : K_0$

7805 $\wedge (x:\tau), \Gamma \vdash_1 e_1 : K_1$

7806 by *inversion*

7807 3. $\Gamma \vdash_1 e_0[x \leftarrow v] : K_0$

7808 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v] : K_1$

7809 by the induction hypothesis (2)

7811 4. $\Gamma \vdash_1 e_0[x \leftarrow v] \ e_1[x \leftarrow v] : K$
 7812 by (3)
 7813 5. QED
 7814 **CASE** $e = op^1 e_0 :$
 7815 1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$
 7816 2. $(x:\tau), \Gamma \vdash_1 e_0 : K_0$
 7817 by *inversion*
 7818 3. $\Gamma \vdash_1 e_0[x \leftarrow v] : K_0$
 7819 by the induction hypothesis (2)
 7820 4. $\Gamma \vdash_1 op^1 e_0[x \leftarrow v] : K$
 7821 by (3)
 7822 5. QED
 7823 **CASE** $e = op^2 e_0 e_1 :$
 7824 1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 7825 2. $(x:\tau), \Gamma \vdash_1 e_0 : K_0$
 7826 $\wedge (x:\tau), \Gamma \vdash_1 e_1 : K_1$
 7827 by *inversion*
 7828 3. $\Gamma \vdash_1 e_0[x \leftarrow v] : K_0$
 7829 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v] : K_1$
 7830 by the induction hypothesis (2)
 7831 4. $\Gamma \vdash_1 op^2 e_0[x \leftarrow v] e_1[x \leftarrow v] : K$
 7832 by (3)
 7833 5. QED
 7834 **CASE** $e = \text{dyn } \tau' e' :$
 7835 1. $e[x \leftarrow v] = \text{dyn } \tau' e'[x \leftarrow v]$
 7836 2. $(x:\tau), \Gamma \vdash_1 e' :$
 7837 by *inversion*
 7838 3. $\Gamma \vdash_1 e'[x \leftarrow v]$
 7839 by *dynamic context static value substitution* (2)
 7840 4. $\Gamma \vdash_1 \text{dyn } \tau' (e'[x \leftarrow v]) : K$
 7841 by (3)
 7842 5. QED
 7843 **CASE** $e = \text{dyn } e' :$
 7844 1. $e[x \leftarrow v] = \text{dyn } e'[x \leftarrow v]$
 7845 2. $(x:\tau), \Gamma \vdash_1 e' :$
 7846 by *inversion*
 7847 3. $\Gamma \vdash_1 e'[x \leftarrow v]$
 7848 by *dynamic context static value substitution* (2)
 7849 4. $\Gamma \vdash_1 \text{dyn } (e'[x \leftarrow v]) : K$
 7850 by (3)
 7851 5. QED
 7852 **CASE** $e = \text{chk } K' e' :$
 7853 1. $e[x \leftarrow v] = \text{chk } K' (e'[x \leftarrow v])$
 7854 2. $(x:\tau), \Gamma \vdash_1 e' : \text{Any}$
 7855 by *inversion*
 7856 3. $\Gamma \vdash_1 e'[x \leftarrow v] : \text{Any}$
 7857 by the induction hypothesis (2)
 7858 4. $\Gamma \vdash_1 \text{chk } K' (e'[x \leftarrow v]) : K$
 7859 by (3)
 7860 5. QED
 7861 **CASE** $e = \text{stat } \tau' e' :$
 7862 $\vee e = \text{stat } e' :$
 7863 1. Contradiction by $\Gamma \vdash_1 e : K$
 7864
 7865

□

Lemma 4.50 : 1 *static-dynamic substitution*If $x, \Gamma \vdash_1 e : K$ and $\vdash_1 v$ then $\Gamma \vdash_1 e[x \leftarrow v] : K$ *Proof*:By induction on the structure of e .**CASE** $e = x :$ 1. $K = \text{Any}$ by $x, \Gamma \vdash_1 x : K$ 2. $e[x \leftarrow v] = v$ 3. $\vdash_1 v : K$ by *dynamic value inversion*4. $\vdash_1 v : \text{Any}$ by $K \leqslant : \text{Any}$ 5. $\Gamma \vdash_1 v : \text{Any}$ by *weakening* (3)

6. QED

CASE $e = x' :$ 1. QED by $x'[x \leftarrow v] = x'$ **CASE** $e = i :$ 1. QED by $i[x \leftarrow v] = i$ **CASE** $e = \lambda x. e' :$ 1. QED by $(\lambda x. e')[x \leftarrow v] = \lambda x. e'$ **CASE** $e = \lambda(x:\tau'). e' :$ 1. QED by $(\lambda(x:\tau'). e')[x \leftarrow v] = \lambda(x:\tau'). e'$ **CASE** $e = \lambda x'. e' :$ 1. $e[x \leftarrow v] = \lambda x'. (e'[x \leftarrow v])$ 2. $x', x, \Gamma \vdash_1 e' :$ by *inversion*3. $x', \Gamma \vdash_1 e'[x \leftarrow v]$ by *dynamic context dynamic value substitution*4. $\Gamma \vdash_1 \lambda x'. e'[x \leftarrow v] : K$

by (3)

5. QED

CASE $e = \lambda(x':\tau'). e' :$ 1. $e[x \leftarrow v] = \lambda(x':\tau'). (e'[x \leftarrow v])$ 2. $(x':\tau'), x, \Gamma \vdash_1 e' : \text{Any}$ by *inversion*3. $(x':\tau'), \Gamma \vdash_1 e'[x \leftarrow v] : \text{Any}$ by *static context dynamic value substitution*4. $\Gamma \vdash_1 \lambda(x':\tau'). (e'[x \leftarrow v]) : K$

5. QED

CASE $e = \langle e_0, e_1 \rangle :$ 1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$ 2. $x, \Gamma \vdash_1 e_0 : \text{Any}$ $\wedge x, \Gamma \vdash_1 e_1 : \text{Any}$ by *inversion*3. $\Gamma \vdash_1 e_0[x \leftarrow v] : \text{Any}$ $\wedge \Gamma \vdash_1 e_1[x \leftarrow v] : \text{Any}$

by the induction hypothesis (2)

4. $\Gamma \vdash_1 \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle : K$

by (3)

5. QED

CASE $e = e_0 e_1 :$

7921 1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$
 7922 2. $x, \Gamma \vdash_1 e_0 : K_0$
 7923 $\wedge x, \Gamma \vdash_1 e_1 : K_1$
 7924 by *inversion*
 7925 3. $\Gamma \vdash_1 e_0[x \leftarrow v] : K_0$
 7926 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v] : K_1$
 7927 by the induction hypothesis (2)
 7928 4. $\Gamma \vdash_1 e_0[x \leftarrow v] e_1[x \leftarrow v] : K$
 7929 by (3)
 7930 5. QED
 7931 **CASE** $e = op^1 e_0 :$
 7932 1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$
 7933 2. $x, \Gamma \vdash_1 e_0 : K_0$
 7934 by *inversion*
 7935 3. $\Gamma \vdash_1 e_0[x \leftarrow v] : K_0$
 7936 by the induction hypothesis (2)
 7937 4. $\Gamma \vdash_1 op^1 e_0[x \leftarrow v] : K$
 7938 by (3)
 7939 5. QED
 7940 **CASE** $e = op^2 e_0 e_1 :$
 7941 1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
 7942 2. $x, \Gamma \vdash_1 e_0 : K_0$
 7943 $\wedge x, \Gamma \vdash_1 e_1 : K_1$
 7944 by *inversion*
 7945 3. $\Gamma \vdash_1 e_0[x \leftarrow v] : K_0$
 7946 $\wedge \Gamma \vdash_1 e_1[x \leftarrow v] : K_1$
 7947 by the induction hypothesis (2)
 7948 4. $\Gamma \vdash_1 op^2 e_0[x \leftarrow v] e_1[x \leftarrow v] : K$
 7949 by (3)
 7950 5. QED
 7951 **CASE** $e = \text{dyn } \tau' e' :$
 7952 1. $e[x \leftarrow v] = \text{dyn } \tau' e'[x \leftarrow v]$
 7953 2. $x, \Gamma \vdash_1 e' :$
 7954 by *inversion*
 7955 3. $\Gamma \vdash_1 e'[x \leftarrow v]$
 7956 by *dynamic context dynamic value substitution* (2)
 7957 4. $\Gamma \vdash_1 \text{dyn } \tau' (e'[x \leftarrow v]) : K$
 7958 by (3)
 7959 5. QED
 7960 **CASE** $e = \text{dyn } e' :$
 7961 1. $e[x \leftarrow v] = \text{dyn } e'[x \leftarrow v]$
 7962 2. $x, \Gamma \vdash_1 e' :$
 7963 by *inversion*
 7964 3. $\Gamma \vdash_1 e'[x \leftarrow v]$
 7965 by *dynamic context dynamic value substitution* (2)
 7966 4. $\Gamma \vdash_1 \text{dyn } (e'[x \leftarrow v]) : K$
 7967 by (3)
 7968 5. QED
 7969 **CASE** $e = \text{chk } K' e' :$
 7970 1. $e[x \leftarrow v] = \text{chk } K' (e'[x \leftarrow v])$
 7971 2. $x, \Gamma \vdash_1 e' : \text{Any}$
 7972 by *inversion*
 7973 3. $\Gamma \vdash_1 e'[x \leftarrow v] : \text{Any}$
 7974 by the induction hypothesis (2)
 7975

4. $\Gamma \vdash_1 \text{chk } K' (e'[x \leftarrow v]) : K$
 by (3)
 5. QED
CASE $e = \text{stat } \tau' e' :$
 $\vee e = \text{stat } e' :$
 1. Contradiction by $\Gamma \vdash_1 e : K$
 \square
Lemma 4.51 : weakening

- If $\Gamma \vdash_1 e$ then $x, \Gamma \vdash_1 e$
- If $\Gamma \vdash_1 e : \tau$ then $(x : \tau'), \Gamma \vdash_1 e : \tau$

Proof:

- e is closed under Γ
 by $\Gamma \vdash_1 e$
 $\vee \Gamma \vdash_1 e : \tau$ QED
 \square

Lemma 4.52 : unique static evaluation contexts

If $\vdash e : \tau$ and e is boundary-free then one of the following holds:

- e is a value
- $e = E^\bullet[v_0 v_1]$
- $e = E^\bullet[op^1 v]$
- $e = E^\bullet[op^2 v_0 v_1]$
- $e = E^\bullet[\text{Err}]$

Proof:

By induction on the structure of e .

CASE $e = x :$

1. Contradiction by $\vdash e : \tau$

CASE $e = i$

$$\vee e = \lambda(x : \tau_d). e' :$$

1. QED e is a value

CASE $e = \langle e_0, e_1 \rangle :$

IF $e_0 \notin v :$

1. $e_0 = E^\bullet_0[e'_0]$
by the induction hypothesis
2. $E^\bullet = \langle E^\bullet_0, e_1 \rangle$
3. QED by $e = E^\bullet[e'_0]$

IF $e_0 \in v$

$$\wedge e_1 \notin v :$$

1. $e_1 = E^\bullet_1[e'_1]$
by the induction hypothesis
2. $E^\bullet = \langle e_0, E^\bullet_1 \rangle$
3. QED by $e = E^\bullet[e'_1]$

ELSE $e_0 \in v$

$$\wedge e_1 \in v :$$

1. $E^\bullet = []$
2. QED $e = E^\bullet[\langle e_0, e_1 \rangle]$

CASE $e = e_0 e_1 :$

IF $e_0 \notin v :$

1. $e_0 = E^\bullet_0[e'_0]$
by the induction hypothesis
2. $E^\bullet = E^\bullet_0 e_1$
3. QED by $e = E^\bullet[e'_0]$

8031 **IF** $e_0 \in v$
 8032 $\wedge e_1 \notin v :$
 8033 1. $e_1 = E^\bullet_1[e'_1]$
 8034 by the induction hypothesis
 8035 2. $E^\bullet = e_0 E^\bullet_1$
 8036 3. QED by $e = E^\bullet[e'_1]$
 8037 **ELSE** $e_0 \in v$
 8038 $\wedge e_1 \in v :$
 8039 1. $E^\bullet = []$
 8040 2. QED $e = E^\bullet[e_0 e_1]$
 8041 **CASE** $e = op^1 e_0 :$
 8042 **IF** $e_0 \notin v :$
 8043 1. $e_0 = E^\bullet_0[e'_0]$
 8044 by the induction hypothesis
 8045 2. $E^\bullet = op^1 E^\bullet_0$
 8046 3. QED $e = E^\bullet[e'_0]$
 8047 **ELSE** $e_0 \in v :$
 8048 1. $E^\bullet = []$
 8049 2. QED $e = E^\bullet[op^1 e_0]$
 8050 **CASE** $e = op^2 e_0 e_1 :$
 8051 **IF** $e_0 \notin v :$
 8052 1. $e_0 = E^\bullet_0[e'_0]$
 8053 by the induction hypothesis
 8054 2. $E^\bullet = op^2 E^\bullet_0 e_1$
 8055 3. QED $e = E^\bullet[e'_0]$
 8056 **IF** $e_0 \in v$
 8057 $\wedge e_1 \notin v :$
 8058 1. $e_1 = E^\bullet_1[e'_1]$
 8059 by the induction hypothesis
 8060 2. $E^\bullet = op^2 e_0 E^\bullet_1$
 8061 3. QED $e = E^\bullet[e'_1]$
 8062 **ELSE** $e_0 \in v$
 8063 $\wedge e_1 \in v :$
 8064 1. $E^\bullet = []$
 8065 2. QED $e = E^\bullet[op^2 e_0 e_1]$
 8066 **CASE** $e = chk K' e' :$
 8067 1. Contradiction by $\vdash e : \tau$
 8068 **CASE** $e = dyn e_0 :$
 8069 1. Contradiction by $\vdash e : \tau$
 8070 **CASE** $e = stat e' :$
 8071 1. Contradiction by $\vdash e : \tau$
 8072 **CASE** $e = dyn \tau e_0 :$
 8073 1. QED e is boundary-free
 8074 **CASE** $e = stat \tau e' :$
 8075 1. Contradiction by $\vdash e : \tau$
 8076 **CASE** $e = Err :$
 8077 1. $E^\bullet = []$
 8078 2. QED
 8079 \square

8080 **Lemma 4.53** : \vdash static inversion

- If $\Gamma \vdash x : \tau$ then $(x : \tau') \in \Gamma$ and $\tau' \leq \tau$ 8086
- If $\Gamma \vdash \lambda(x : \tau'_d). e' : \tau$ then $(x : \tau'_d), \Gamma \vdash e' : \tau'_c$ and $\tau'_d \Rightarrow \tau'_c \leq \tau$ 8087
- If $\Gamma \vdash \langle e_0, e_1 \rangle : \tau$ then $\Gamma \vdash e_0 : \tau_0$ and $\Gamma \vdash e_1 : \tau_1$ and $\tau_0 \times \tau_1 \leq \tau$ 8088
- If $\Gamma \vdash e_0 e_1 : \tau_c$ then $\Gamma \vdash e_0 : \tau'_d \Rightarrow \tau'_c$ and $\Gamma \vdash e_1 : \tau'_d$ and $\tau'_c \leq \tau_c$ 8089
- If $\Gamma \vdash fst e : \tau$ then $\Gamma \vdash e : \tau_0 \times \tau_1$ and $\Delta(fst, \tau_0 \times \tau_1) = \tau_0$ and $\tau_0 \leq \tau$ 8090
- If $\Gamma \vdash snd e : \tau$ then $\Gamma \vdash e : \tau_0 \times \tau_1$ and $\Delta(snd, \tau_0 \times \tau_1) = \tau_1$ and $\tau_1 \leq \tau$ 8091
- If $\Gamma \vdash op^2 e_0 e_1 : \tau$ then $\Gamma \vdash e_0 : \tau_0$ and $\Gamma \vdash e_1 : \tau_1$ and $\Delta(op^2, \tau_0, \tau_1) = \tau'$ and $\tau' \leq \tau$ 8092
- If $\Gamma \vdash dyn \tau' e' : \tau$ then $\Gamma \vdash e'$ and $\tau' \leq \tau$ 8093

Proof:

QED by the definition of $\Gamma \vdash e : \tau$

\square

Lemma 4.54 : canonical forms

- If $\vdash v : \tau_0 \times \tau_1$ then $v = \langle v_0, v_1 \rangle$ 8103
- If $\vdash v : \tau_d \Rightarrow \tau_c$ then $v = \lambda(x : \tau_x). e'$ 8104
- $\wedge \tau_d \leq \tau_x$ 8105
- If $\vdash v : Int$ then $v = i$ 8106
- If $\vdash v : Nat$ then $v = i$ and $v \in \mathbb{N}$ 8107

Proof:

QED by definition of $\vdash e : \tau$

\square

Lemma 4.55 : substitution

If $(x : \tau_x), \Gamma \vdash e : \tau$, and e is boundary-free and $\vdash v : \tau_x$ then $\Gamma \vdash e[x \leftarrow v] : \tau$

Proof:

By induction on the structure of e .

CASE $e = x :$

1. $e[x \leftarrow v] = v$

2. $\tau_x = \tau$

3. $\Gamma \vdash v : \tau$

by weakening

4. QED

CASE $e = x' :$

1. QED by $x'[x \leftarrow v] = x'$

CASE $e = i :$

1. QED by $i[x \leftarrow v] = i$

CASE $e = \lambda x. e' :$

1. Contradiction by $(x : \tau_x), \Gamma \vdash e : \tau$

CASE $e = \lambda(x : \tau'). e' :$

1. QED by $(\lambda(x : \tau'). e')[x \leftarrow v] = \lambda(x : \tau'). e'$

CASE $e = \lambda(x' : \tau'). e' :$

1. $e[x \leftarrow v] = \lambda(x' : \tau'). (e'[x \leftarrow v])$

2. $(x' : \tau'), x, \Gamma \vdash e'$

by static inversion forms

3. $(x' : \tau'), \Gamma \vdash e'[x \leftarrow v]$

by the induction hypothesis (2)

4. $\Gamma \vdash \lambda(x' : \tau'). (e'[x \leftarrow v])$

by (3)

5. QED

8141 **CASE** $e = \langle e_0, e_1 \rangle :$
8142 1. $e[x \leftarrow v] = \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
8143 2. $x, \Gamma \vdash e_0$
8144 $\wedge x, \Gamma \vdash e_1$
8145 by *static inversion forms*
8146 3. $\Gamma \vdash e_0[x \leftarrow v]$
8147 $\wedge \Gamma \vdash e_1[x \leftarrow v]$
8148 by the induction hypothesis (2)
8149 4. $\Gamma \vdash \langle e_0[x \leftarrow v], e_1[x \leftarrow v] \rangle$
8150 by (3)
8151 5. QED
8152 **CASE** $e = e_0 e_1 :$
8153 1. $e[x \leftarrow v] = e_0[x \leftarrow v] e_1[x \leftarrow v]$
8154 2. $x, \Gamma \vdash e_0$
8155 $\wedge x, \Gamma \vdash e_1$
8156 by *static inversion forms*
8157 3. $\Gamma \vdash e_0[x \leftarrow v]$
8158 $\wedge \Gamma \vdash e_1[x \leftarrow v]$
8159 by the induction hypothesis (2)
8160 4. $\Gamma \vdash e_0[x \leftarrow v] e_1[x \leftarrow v]$
8161 by (3)
8162 5. QED
8163 **CASE** $e = op^1 e_0 :$
8164 1. $e[x \leftarrow v] = op^1 e_0[x \leftarrow v]$
8165 2. $x, \Gamma \vdash e_0$
8166 by *static inversion forms*
8167 3. $\Gamma \vdash e_0[x \leftarrow v]$
8168 by the induction hypothesis (2)
8169 4. $\Gamma \vdash op^1 e_0[x \leftarrow v]$
8170 by (3)
8171 5. QED
8172 **CASE** $e = op^2 e_0 e_1 :$
8173 1. $e[x \leftarrow v] = op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
8174 2. $x, \Gamma \vdash e_0$
8175 $\wedge x, \Gamma \vdash e_1$
8176 by *static inversion forms*
8177 3. $\Gamma \vdash e_0[x \leftarrow v]$
8178 $\wedge \Gamma \vdash e_1[x \leftarrow v]$
8179 by the induction hypothesis (2)
8180 4. $\Gamma \vdash op^2 e_0[x \leftarrow v] e_1[x \leftarrow v]$
8181 by (3)
8182 5. QED
8183 **CASE** $e = \text{chk } K' e' :$
8184 1. Contradiction by $\vdash e : \tau$
8185 **CASE** $e = \text{dyn } e' :$
8186 1. Contradiction by $\vdash e : \tau$
8187 **CASE** $e = \text{stat } e' :$
8188 1. Contradiction by $\vdash e : \tau$
8189 **CASE** $e = \text{dyn } \tau' e' :$
8190 1. Contradiction by e is boundary-free
8191 **CASE** $e = \text{stat } \tau' e' :$
8192 1. Contradiction by $\vdash e : \tau$
8193 **CASE** $e = \text{Err} :$
8194 1. QED $\text{Err}[x \leftarrow v] = \text{Err}$
8195

□

Lemma 4.56 : δ preservation

- If $\vdash v$ and $\delta(op^1, v) = v'$ then $\vdash e'$
- If $\vdash v_0$ and $\vdash v_1$ and $\delta(op^2, v_0, v_1) = e'$ then $\vdash v'$

*Proof:***CASE** $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0 :$ 1. $\vdash v_0$ by *static inversion forms*

2. QED

CASE $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1 :$ 1. $\vdash v_1$ by *static inversion forms*

2. QED

CASE $\delta(\text{sum}, v_0, v_1) = v_0 + v_1 :$

1. QED

CASE $\delta(\text{quotient}, v_0, v_1) = \lfloor v_0/v_1 \rfloor :$

1. QED

CASE $\delta(\text{quotient}, v_0, v_1) = \text{BndryErr} :$

1. QED

□

Lemma 4.57 : *weakening*

- If $\Gamma \vdash e$ then $x, \Gamma \vdash e$
- If $\Gamma \vdash e$ then $(x : \tau), \Gamma \vdash e$

*Proof:*QED because e is closed under Γ

□

A.5 (HC) Co-Natural Embedding

A.5.1 Co-Natural Definitions

Language HC

$e = x \mid v \mid \langle e, e \rangle \mid e e \mid op^1 e \mid op^2 e e \mid$
 $\text{dyn } \tau e \mid \text{stat } \tau e \mid \text{Err}$
 $v = i \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x:\tau). e$
 $\text{mon}(\tau \Rightarrow \tau) v \mid \text{mon}(\tau \times \tau) v$
 $\tau = \text{Nat} \mid \text{Int} \mid \tau \times \tau \mid \tau \Rightarrow \tau$
 $\Gamma = \cdot \mid x, \Gamma \mid (x:\tau), \Gamma$
 $\text{Err} = \text{BndryErr} \mid \text{TagErr}$
 $r = v \mid \text{Err}$
 $E^\bullet = [] \mid E^\bullet e \mid v E^\bullet \mid \langle E^\bullet, e \rangle \mid \langle v, E^\bullet \rangle \mid$
 $op^1 E^\bullet \mid op^2 E^\bullet e \mid op^2 v E^\bullet$
 $E = E^\bullet \mid E e \mid v E \mid \langle E, e \rangle \mid \langle v, E \rangle \mid op^1 E \mid$
 $op^2 E e \mid op^2 v E \mid \text{dyn } \tau E \mid \text{stat } \tau E$

$\Delta : op^1 \times \tau \longrightarrow \tau$

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

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

$\Delta : op^2 \times \tau \times \tau \longrightarrow \tau$

$\Delta(op^2, \text{Nat}, \text{Nat}) = \text{Nat}$

$\Delta(op^2, \text{Int}, \text{Int}) = \text{Int}$

$\tau \leqslant : \tau$

$\text{Nat} \leqslant : \text{Int} \quad \frac{\tau'_d \leqslant : \tau_d \quad \tau_c \leqslant : \tau'_c}{\tau_d \Rightarrow \tau_c \leqslant : \tau'_d \Rightarrow \tau'_c} \quad \frac{\tau_0 \leqslant : \tau'_0 \quad \tau_1 \leqslant : \tau'_1}{\tau_0 \times \tau_1 \leqslant : \tau'_0 \times \tau'_1}$

$\frac{\tau \leqslant : \tau' \quad \tau' \leqslant : \tau''}{\tau \leqslant : \tau''}$

$\Gamma \vdash e$

$\frac{x \in \Gamma}{\Gamma \vdash x} \quad \frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e} \quad \frac{}{\Gamma \vdash i} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle}$

$\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1} \quad \frac{\Gamma \vdash e}{\Gamma \vdash op^1 e} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash \text{Err}}$

$\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e}$

$\Gamma \vdash e : \tau$

$\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau} \quad \frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} \quad \frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}}$

$\frac{}{\Gamma \vdash i : \text{Int}} \quad \frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c}$

$\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash op^1 e_0 : \tau} \quad \frac{\Gamma \vdash e_1 : \tau_1 \quad \Delta(op^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash op^2 e_0 e_1 : \tau} \quad \frac{\Gamma \vdash e : \tau' \quad \tau' \leqslant : \tau}{\Gamma \vdash e : \tau} \quad \frac{}{\Gamma \vdash \text{Err} : \tau}$

$\frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau}$

$\Gamma \vdash_C e$

$\frac{x \in \Gamma}{\Gamma \vdash_C x} \quad \frac{x, \Gamma \vdash_C e}{\Gamma \vdash_C \lambda x. e} \quad \frac{}{\Gamma \vdash_C i} \quad \frac{\Gamma \vdash_C e_0 \quad \Gamma \vdash_C e_1}{\Gamma \vdash_C \langle e_0, e_1 \rangle}$

$\frac{\Gamma \vdash_C e_0 \quad \Gamma \vdash_C e_1}{\Gamma \vdash_C e_0 e_1} \quad \frac{\Gamma \vdash_C e}{\Gamma \vdash_C op^1 e} \quad \frac{\Gamma \vdash_C e_0 \quad \Gamma \vdash_C e_1}{\Gamma \vdash_C op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash_C \text{Err}}$

$\frac{\Gamma \vdash_C e : \tau}{\Gamma \vdash_C \text{stat } \tau e} \quad \frac{\Gamma \vdash_C v : \tau_0 \times \tau_1}{\Gamma \vdash_C \text{mon}(\tau_0 \times \tau_1) v} \quad \frac{\Gamma \vdash_C v : \tau_d \Rightarrow \tau_c}{\Gamma \vdash_C \text{mon}(\tau_d \Rightarrow \tau_c) v}$

$\Gamma \vdash_C e : \tau$

$\frac{(x:\tau) \in \Gamma}{\Gamma \vdash_C x : \tau} \quad \frac{(x:\tau_d), \Gamma \vdash_C e : \tau_c}{\Gamma \vdash_C \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} \quad \frac{i \in \mathbb{N}}{\Gamma \vdash_C i : \text{Nat}}$

$\frac{}{\Gamma \vdash_C i : \text{Int}} \quad \frac{\Gamma \vdash_C e_0 : \tau_0 \quad \Gamma \vdash_C e_1 : \tau_1}{\Gamma \vdash_C \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma \vdash_C e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash_C e_1 : \tau_d}{\Gamma \vdash_C e_0 e_1 : \tau_c}$

$\frac{\Gamma \vdash_C e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash_C op^1 e_0 : \tau} \quad \frac{\Gamma \vdash_C e_1 : \tau_1 \quad \Delta(op^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash_C op^2 e_0 e_1 : \tau} \quad \frac{\Gamma \vdash_C e : \tau' \quad \tau' < : \tau}{\Gamma \vdash_C e : \tau}$

$\frac{}{\Gamma \vdash_C \text{Err} : \tau} \quad \frac{\Gamma \vdash_C e}{\Gamma \vdash_C \text{dyn } \tau e : \tau}$

$\frac{\Gamma \vdash_C v}{\Gamma \vdash_C \text{mon}(\tau_0 \times \tau_1) v : (\tau_0 \times \tau_1)}$

$\frac{\Gamma \vdash_C v}{\Gamma \vdash_C \text{mon}(\tau_d \Rightarrow \tau_c) v : (\tau_d \Rightarrow \tau_c)}$

8361 $\delta(op^1, v) = e$
8362 $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$
8363 $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$
8364 $\delta(op^2, v, v) = e$
8365 $\delta(\text{sum}, i_0, i_1) = i_0 + i_1$
8366 $\delta(\text{quotient}, i_0, 0) = \text{BndryErr}$
8367 $\delta(\text{quotient}, i_0, i_1) = \lfloor i_0 / i_1 \rfloor$
8368 if $i_1 \neq 0$
8370 $\mathcal{D}_C : \tau \times v \longrightarrow e$
8371 $\mathcal{D}_C(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v$
8372 if $v = \lambda x. e$ or $v = \text{mon}(\tau'_d \Rightarrow \tau'_c) v'$
8373 $\mathcal{D}_C(\tau_0 \times \tau_1, v) = \text{mon}(\tau_0 \times \tau_1) v$
8374 if $v = \langle v_0, v_1 \rangle$ or $v = \text{mon}(\tau'_0 \times \tau'_1) v'$
8375 $\mathcal{D}_C(\text{Int}, i) = i$
8376 $\mathcal{D}_C(\text{Nat}, i) = i$
8377 if $i \in \mathbb{N}$
8378 $\mathcal{D}_C(\tau, v) = \text{BndryErr}$
8379 otherwise
8380 $\mathcal{S}_C : \tau \times v \longrightarrow e$
8381 $\mathcal{S}_C(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v$
8382 $\mathcal{S}_C(\tau_0 \times \tau_1, v) = \text{mon}(\tau_0 \times \tau_1) v$
8383 $\mathcal{S}_C(\tau, v) = v$
8384 otherwise
8386 $e \triangleright_{S-C} e$
8387 $\text{dyn } \tau v \triangleright_{S-C} \mathcal{D}_C(\tau, v)$
8388 $(\text{mon}(\tau_d \Rightarrow \tau_c) v_f) v \triangleright_{S-C} \text{dyn } \tau_c (v_f e')$
8389 where $e' = \text{stat } \tau_d v$
8390 $(\lambda(x:\tau). e) v \triangleright_{S-C} e[x \leftarrow v]$
8391 $\text{fst}(\text{mon}(\tau_0 \times \tau_1) v) \triangleright_{S-C} \text{dyn } \tau_0 (\text{fst } v)$
8392 $\text{snd}(\text{mon}(\tau_0 \times \tau_1) v) \triangleright_{S-C} \text{dyn } \tau_1 (\text{snd } v)$
8393 $op^1 v \triangleright_{S-C} \delta(op^1, v)$
8394 $op^2 v_0 v_1 \triangleright_{S-C} \delta(op^2, v_0, v_1)$
8395 $e \triangleright_{D-C} e$
8396 $\text{stat } \tau v \triangleright_{D-C} \mathcal{S}_C(\tau, v)$
8397 $v_0 v_1 \triangleright_{D-C} \text{TagErr}$
8398 if $v_0 \in \mathbb{Z}$ or $v_0 = \langle v, v' \rangle$
8399 $(\text{mon}(\tau_d \Rightarrow \tau_c) v_f) v \triangleright_{D-C} \text{stat } \tau_c (v_f e')$
8400 where $e' = \text{dyn } \tau_d v$
8401 $(\lambda x. e) v \triangleright_{D-C} e[x \leftarrow v]$
8402 $\text{fst}(\text{mon}(\tau_0 \times \tau_1) v) \triangleright_{D-C} \text{stat } \tau_0 (\text{fst } v)$
8403 $\text{snd}(\text{mon}(\tau_0 \times \tau_1) v) \triangleright_{D-C} \text{stat } \tau_1 (\text{snd } v)$
8404 $op^1 v \triangleright_{D-C} \text{TagErr}$
8405 if $\delta(op^1, v)$ is undefined
8406 $op^1 v \triangleright_{D-C} \delta(op^1, v)$
8407 $op^2 v_0 v_1 \triangleright_{D-C} \text{TagErr}$
8408 if $\delta(op^2, v_0, v_1)$ is undefined
8409 $op^2 v_0 v_1 \triangleright_{D-C} \delta(op^2, v_0, v_1)$
8410
8411
8412
8413
8414
8415

$e \rightarrow_{C-S} e$
 $E^\bullet[e] \rightarrow_{C-S} E^\bullet[e']$
if $e \triangleright_{S-C} e'$
 $E[\text{stat } \tau E^\bullet[e]] \rightarrow_{C-S} E[\text{stat } \tau E^\bullet[e']]$
if $e \triangleright_{S-C} e'$
 $E[\text{dyn } \tau E^\bullet[e]] \rightarrow_{C-S} E[\text{dyn } \tau E^\bullet[e']]$
if $e \triangleright_{D-C} e'$
 $E[\text{Err}] \rightarrow_{C-S} \text{Err}$
 $e \rightarrow_{C-D} e$
 $E^\bullet[e] \rightarrow_{C-D} E^\bullet[e']$
if $e \triangleright_{D-C} e'$
 $E[\text{stat } \tau E^\bullet[e]] \rightarrow_{C-D} E[\text{stat } \tau E^\bullet[e']]$
if $e \triangleright_{S-C} e'$
 $E[\text{dyn } \tau E^\bullet[e]] \rightarrow_{C-D} E[\text{dyn } \tau E^\bullet[e']]$
if $e \triangleright_{D-C} e'$
 $E[\text{Err}] \rightarrow_{C-D} \text{Err}$
 $e \rightarrow_{C-S}^* e$ reflexive, transitive closure of \rightarrow_{C-S}
 $e \rightarrow_{C-D}^* e$ reflexive, transitive closure of \rightarrow_{C-D}

8416
8417
8418
8419
8420
8421
8422
8423
8424
8425
8426
8427
8428
8429
8430
8431
8432
8433
8434
8435
8436
8437
8438
8439
8440
8441
8442
8443
8444
8445
8446
8447
8448
8449
8450
8451
8452
8453
8454
8455
8456
8457
8458
8459
8460
8461
8462
8463
8464
8465
8466
8467
8468
8469
8470

A.5.2 Co-Natural Theorems

Theorem 5.0 : static HC soundness

If $\vdash e : \tau$ then $\vdash_C e : \tau$ and one of the following holds:

- $e \rightarrow_{C-S}^* v$ and $\vdash_C v : \tau$
- $e \rightarrow_{C-S}^* E[\text{dyn } \tau' e']$ and $e' \triangleright_{D-C} \text{TagErr}$
- $e \rightarrow_{C-S}^* \text{BndryErr}$
- e diverges

Proof:

1. $\vdash_C e : \tau$
by *static subset*
 2. QED by *static progress* and *static preservation*.
-

Theorem 5.1 : dynamic HC-soundness

If $\vdash e$ then $\vdash_C e$ and one of the following holds:

- $e \rightarrow_{C-D}^* v$ and $\vdash_C v$
- $e \rightarrow_{C-D}^* E[e']$ and $e' \triangleright_{D-C} \text{TagErr}$
- $e \rightarrow_{C-D}^* \text{BndryErr}$
- e diverges

Proof:

1. $\vdash_C e$
by *dynamic subset*
 2. QED by *dynamic progress* and *dynamic preservation*.
-

Corollary 5.2 : HC static soundness

If $\vdash e : \tau$ and e is boundary-free, then one of the following holds:

- $e \rightarrow_{C-S}^* v$ and $\vdash_C v : \tau$
- $e \rightarrow_{C-S}^* \text{BndryErr}$
- e diverges

Proof:

Consequence of the proof for *static HC-soundness*

□

A.5.3 Co-Natural Lemmas

Lemma 5.3 : \mathcal{D}_C soundness

If $\vdash_C v$ then $\vdash_C \mathcal{D}_C(\tau, v) : \tau$

Proof:

CASE $\mathcal{D}_C(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v :$

1. $\vdash_C \text{mon}(\tau_d \Rightarrow \tau_c) v : \tau_d \Rightarrow \tau_c$
by $\vdash_C v$
2. QED

CASE $\mathcal{D}_C(\tau_0 \times \tau_1, v) = \text{mon}(\tau_0 \times \tau_1) v :$

1. $\vdash_C \text{mon}(\tau_0 \times \tau_1) v : \tau_0 \times \tau_1$
by $\vdash_C v$
2. QED

CASE $v = i$

$\wedge \mathcal{D}_C(\text{Int}, v) = v :$

1. QED

CASE $v \in \mathbb{N}$

$\wedge \mathcal{D}_C(\text{Nat}, v) = v :$

1. QED

CASE $\mathcal{D}_C(\tau, v) = \text{BndryErr} :$

1. QED

□

Lemma 5.4 : \mathcal{S}_C soundness

If $\vdash_C v : \tau$ then $\vdash_C \mathcal{S}_C(\tau, v)$

Proof:

CASE $\vdash_C v : \tau_d \Rightarrow \tau_c$

$\wedge \mathcal{S}_C(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v :$

1. QED

CASE $\vdash_C v : \tau_0 \times \tau_1$

$\wedge \mathcal{S}_C(\tau_0 \times \tau_1, v) = \text{mon}(\tau_0 \times \tau_1) v :$

1. QED

CASE $\vdash_C v : \text{Int}$

$\wedge \mathcal{S}_C(\text{Int}, v) = v :$

1. QED

CASE $\vdash_C v : \text{Nat}$

$\wedge \mathcal{S}_C(\text{Nat}, v) = v :$

1. QED

□

Corollary 5.5 : HC static subset

If $\Gamma \vdash e : \tau$ then $\Gamma \vdash_C e : \tau$.

Proof:

Consequence of the proof for the higher-order *static subset* lemma; both \vdash_C and \vdash_H have the same typing rules for surface-language expressions.

□

Corollary 5.6 : HC dynamic subset

If $\Gamma \vdash e$ then $\Gamma \vdash_C e$.

Proof:

Consequence of the proof for the higher-order *dynamic subset* lemma.

□

Lemma 5.7 : HC static progress

If $\vdash_C e : \tau$ then one of the following holds:

- e is a value
- $e \in \text{Err}$
- $e \rightarrow_{C-S} e'$
- $e \rightarrow_{C-S} \text{BndryErr}$
- $e = E[\text{dyn } \tau' e']$ and $e' \rightarrow_{C-D} \text{TagErr}$

Proof:

By the *boundary factoring* lemma, there are seven possible cases.

CASE e is a value :

1. QED

CASE $e = E^\bullet[v_0 v_1] :$

1. $\vdash_C v_0 v_1 : \tau'$
by *static hole typing*

2. $\vdash_C v_0 : \tau_d \Rightarrow \tau_c$

$\wedge \vdash_C v_1 : \tau_d$

by *inversion*

3. $v_0 = \lambda(x : \tau'_d). e'$
 $\vee v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) v_f$
by *canonical forms*

4. **IF** $v_0 = \lambda(x : \tau'_d). e' :$

- a. $e \rightarrow_{C-S} E^\bullet[e'[x \leftarrow v_1]]$
by $v_0 v_1 \triangleright_{S-C} e'[x \leftarrow v_1]$

- b. QED

ELSE $v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) v_f :$

- a. $e \rightarrow_{C-S} E^\bullet[\text{dyn } \tau'_c (v_f (\text{stat } \tau'_d v_1))]$
by $v_0 v_1 \triangleright_{S-C} \text{dyn } \tau'_c (v_f (\text{stat } \tau'_d v_1))$

- b. QED

CASE $e = E^\bullet[op^1 v] :$

1. $\vdash_C op^1 v : \tau'$

by *static hole typing*

2. $\vdash_C v : \tau_0 \times \tau_1$

by *inversion*

3. $v = \langle v_0, v_1 \rangle$

$\vee v = \text{mon}(\tau_0 \times \tau_1) v'$

by *canonical forms*

4. **IF** $v = \langle v_0, v_1 \rangle$

$\wedge op^1 = \text{fst} :$

- a. $\delta(op^1, \langle v_0, v_1 \rangle) = v_0$
by *definition*

- b. $e \rightarrow_{C-S} E^\bullet[v_0]$
by $op^1 v \triangleright_{S-C} v_0$

- c. QED

IF $v = \langle v_0, v_1 \rangle$

$\wedge op^1 = \text{snd} :$

- a. $\delta(op^1, \langle v_0, v_1 \rangle) = v_1$
by *definition*

- b. $e \rightarrow_{C-S} E^\bullet[v_1]$
by $op^1 v \triangleright_{S-C} v_1$

- c. QED

IF $v = \text{mon}(\tau_0 \times \tau_1) v'$

$\wedge op^1 = \text{fst} :$

- a. $e \rightarrow_{C-S} E^\bullet[\text{dyn } \tau_0 (op^1 v')]$
by *definition*

8691 b. QED
8692 **ELSE** $v = \text{mon}(\tau_0 \times \tau_1) v'$
8693 $\wedge \text{op}^1 = \text{snd} :$
8694 a. $e \rightarrow_{\text{C-S}} E^{\bullet}[\text{dyn } \tau_1 (\text{op}^1 v')]$
8695 by definition
8696 b. QED
8697 **CASE** $e = E^{\bullet}[\text{op}^2 v_0 v_1] :$
8698 1. $\vdash_{\text{C}} \text{op}^2 v_0 v_1 : \tau'$
8699 by *static hole typing*
8700 2. $\vdash_{\text{C}} v_0 : \tau_0$
8701 $\wedge \vdash_{\text{C}} v_1 : \tau_1$
8702 $\wedge \Delta(\text{op}^2, \tau_0, \tau_1) = \tau''$
8703 by *inversion*
8704 3. $\delta(\text{op}^2, v_0, v_1) = e'$
8705 by Δ *type soundness* (2)
8706 4. $\text{op}^2 v_0 v_1 \triangleright_{\text{S-C}} e'$
8707 by (3)
8708 5. QED by $e \rightarrow_{\text{C-S}} E^{\bullet}[e']$
8709 **CASE** $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :
8710 1. e' is a value
8711 $\vee e' \in \text{Err}$
8712 $\vee e' \rightarrow_{\text{C-D}} e''$
8713 $\vee e' \rightarrow_{\text{C-D}} \text{BndryErr}$
8714 $\vee e' = E'[e'']$ and $e'' \triangleright_{\text{D-C}} \text{TagErr}$
8715 by *dynamic progress*
8716 2. **IF** e' is a value :
8717 a. QED $e \rightarrow_{\text{C-S}} E[\mathcal{D}_{\text{C}}(\tau', e')]$
8718 **IF** $e' \in \text{Err} :$
8719 a. QED $e \rightarrow_{\text{C-S}} e'$
8720 **IF** $e' \rightarrow_{\text{C-D}} e'' :$
8721 a. QED $e \rightarrow_{\text{C-S}} E[\text{dyn } \tau' e'']$
8722 **IF** $e' \rightarrow_{\text{C-D}} \text{BndryErr} :$
8723 a. QED $e \rightarrow_{\text{C-S}} E[\text{dyn } \tau' \text{BndryErr}]$
8724 **ELSE** $e' = E'[e'']$ and $e'' \triangleright_{\text{D-C}} \text{TagErr} :$
8725 a. $E' \in E^{\bullet}$
8726 by e' is boundary-free
8727 b. QED
8728 **CASE** $e = E[\text{stat } \tau' e']$ and e' is boundary-free :
8729 1. e' is a value
8730 $\vee e' \in \text{Err}$
8731 $\vee e' \rightarrow_{\text{C-S}} e''$
8732 $\vee e' \rightarrow_{\text{C-S}} \text{BndryErr}$
8733 $\vee e' = E''[\text{dyn } \tau'' E^{\bullet}][e'']$ and $e'' \triangleright_{\text{D-C}} \text{TagErr}$
8734 by *static progress*
8735 2. **IF** e' is a value :
8736 a. QED $e \rightarrow_{\text{C-S}} E[\mathcal{S}_{\text{C}}(\tau', e')]$
8737 **IF** $e' \in \text{Err} :$
8738 a. QED $e \rightarrow_{\text{C-S}} e'$
8739 **IF** $e' \rightarrow_{\text{C-S}} e'' :$
8740 a. QED $e \rightarrow_{\text{C-S}} E[\text{stat } \tau' e'']$
8741 **IF** $e' \rightarrow_{\text{C-S}} \text{BndryErr} :$
8742 a. QED $e \rightarrow_{\text{C-S}} E[\text{stat } \tau' \text{BndryErr}]$
8743
8744
8745

8746 **ELSE** $e' = E''[\text{dyn } \tau'' E^{\bullet}][e'']$ and $e'' \triangleright_{\text{D-C}} \text{TagErr}$
8747 :
8748 a. Contradiction by e' is boundary-free
8749 **CASE** $e = E[\text{Err}] :$
8750 1. QED $e \rightarrow_{\text{C-S}} \text{Err}$
8751 □
8752 **Lemma 5.8** : HC *dynamic progress*
8753 If $\vdash_{\text{C}} e$ then one of the following holds:
8754 • e is a value
8755 • $e \in \text{Err}$
8756 • $e \rightarrow_{\text{C-D}} e'$
8757 • $e \rightarrow_{\text{C-D}} \text{BndryErr}$
8758 • $e \rightarrow_{\text{C-D}} \text{TagErr}$
8759 *Proof*:
8760 By the *boundary factoring* lemma, there are seven cases.
8761 **CASE** e is a value :
8762 1. QED
8763 **CASE** $e = E^{\bullet}[v_0 v_1] :$
8764 **IF** $v_0 = \lambda x. e' :$
8765 1. $e \rightarrow_{\text{C-D}} E^{\bullet}[e'[x \leftarrow v_1]]$
8766 by $v_0 v_1 \triangleright_{\text{D-C}} e'[x \leftarrow v_1]$
8767 2. QED
8768 **IF** $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) v_f :$
8769 1. $e \rightarrow_{\text{C-D}} E^{\bullet}[\text{stat } \tau_c (v_f (\text{dyn } \tau_d v_1))]$
8770 by $v_0 v_1 \triangleright_{\text{D-C}} \text{stat } \tau_c (v_f (\text{dyn } \tau_d v_1))$
8771 2. QED
8772 **ELSE** $v_0 = i$
8773 $\vee v_0 = \langle v, v' \rangle :$
8774 1. $e \rightarrow_{\text{C-D}} \text{TagErr}$
8775 by $(v_0 v_1) \triangleright_{\text{D-C}} \text{TagErr}$
8776 2. QED
8777 **CASE** $e = E^{\bullet}[\text{op}^1 v] :$
8778 **IF** $v = \text{mon}(\tau_0 \times \tau_1) v' :$
8779 $\wedge \text{op}^1 = \text{fst} :$
8780 1. $e \rightarrow_{\text{C-D}} E^{\bullet}[\text{stat } \tau_0 \text{op}^1 v']$
8781 by $\text{op}^1 v \triangleright_{\text{D-C}} \text{stat } \tau_0 \text{op}^1 v'$
8782 2. QED
8783 **IF** $v = \text{mon}(\tau_0 \times \tau_1) v' :$
8784 $\wedge \text{op}^1 = \text{snd} :$
8785 1. $e \rightarrow_{\text{C-D}} E^{\bullet}[\text{stat } \tau_1 \text{op}^1 v']$
8786 by $\text{op}^1 v \triangleright_{\text{D-C}} \text{stat } \tau_1 \text{op}^1 v'$
8787 2. QED
8788 **IF** $\delta(\text{op}^1, v) = e' :$
8789 1. $(\text{op}^1 v) \triangleright_{\text{D-C}} e'$
8790 2. QED
8791 **ELSE** $\delta(\text{op}^1, v)$ is undefined :
8792 1. $e \rightarrow_{\text{C-D}} \text{TagErr}$
8793 by $(\text{op}^1 v) \triangleright_{\text{D-C}} \text{TagErr}$
8794 2. QED
8795 **CASE** $e = E^{\bullet}[\text{op}^2 v_0 v_1] :$
8796 **IF** $\delta(\text{op}^2, v_0, v_1) = e'' :$
8797 1. $\text{op}^2 v_0 v_1 \triangleright_{\text{D-C}} e''$
8798 2. QED
8799 **ELSE** $\delta(\text{op}^2, v_0, v_1)$ is undefined :
8800

8801 1. $e \rightarrow_{C-D} \text{TagErr}$
 8802 by $op^2 v_0 v_1 \triangleright_{D-C} \text{TagErr}$
 8803 2. QED
 8804 **CASE** $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :
 8805 1. e' is a value
 8806 $\vee e' \in \text{Err}$
 8807 $\vee e' \rightarrow_{C-D} e''$
 8808 $\vee e' \rightarrow_{C-D} \text{BndryErr}$
 8809 $\vee e' = E[e'']$ and $e'' \triangleright_{D-C} \text{TagErr}$
 8810 by *dynamic progress*
 8811 2. **IF** e' is a value :
 8812 a. QED $e \rightarrow_{C-D} E[\mathcal{D}_C(\tau', e')]$
 8813 **IF** $e' \in \text{Err}$:
 8814 a. QED $e \rightarrow_{C-D} e'$
 8815 **IF** $e' \rightarrow_{C-D} e''$:
 8816 a. QED $e \rightarrow_{C-S} E[\text{dyn } \tau' e'']$
 8817 **IF** $e' \rightarrow_{C-D} \text{BndryErr}$:
 8818 a. QED $e \rightarrow_{C-D} E[\text{dyn } \tau' \text{BndryErr}]$
 8819 **ELSE** $e' = E[e'']$ and $e'' \triangleright_{D-C} \text{TagErr}$:
 8820 a. $E \in E^\bullet$
 8821 by e' is boundary-free
 8822 b. QED
 8823 **CASE** $e = E[\text{stat } \tau' e']$ and e' is boundary-free :
 8824 1. e' is a value
 8825 $\vee e' \in \text{Err}$
 8826 $\vee e' \rightarrow_{C-S} e''$
 8827 $\vee e' \rightarrow_{C-S} \text{BndryErr}$
 8828 $\vee e' = E''[\text{dyn } \tau'' E''[e'']]$ and $e'' \triangleright_{D-C} \text{TagErr}$
 8829 by *static progress*
 8830 2. **IF** e' is a value :
 8831 a. QED $e \rightarrow_{C-S} E[\mathcal{S}_C(\tau', e')]$
 8832 **IF** $e' \in \text{Err}$:
 8833 a. QED $e \rightarrow_{C-S} e'$
 8834 **IF** $e' \rightarrow_{C-S} e''$:
 8835 a. QED $e \rightarrow_{C-S} E[\text{stat } \tau' e'']$
 8836 **IF** $e' \rightarrow_{C-S} \text{BndryErr}$:
 8837 a. QED $e \rightarrow_{C-S} E[\text{stat } \tau' \text{BndryErr}]$
 8838 **ELSE** $e' = E''[\text{dyn } \tau'' E''[e'']]$ and $e'' \triangleright_{D-C} \text{TagErr}$
 8839 :
 8840 a. Contradiction by e' is boundary-free
 8841 **CASE** $e = E[\text{Err}]$:
 8842 1. QED $e \rightarrow_{C-D} \text{Err}$
 8843 \square

Lemma 5.9 : HC *static preservation*

8845 If $\vdash_C e : \tau$ and $e \rightarrow_{C-S} e'$ then $\vdash_C e' : \tau$

8846 *Proof*:

8847 By the *boundary factoring* lemma there are seven cases.

8848 **CASE** e is a value :

8849 1. Contradiction by $e \rightarrow_{C-S} e'$

8850 **CASE** $e = E^\bullet[v_0 v_1]$:

8851 **IF** $v_0 = \lambda(x : \tau_x). e'$

8852 $\wedge e \rightarrow_{C-S} E^\bullet[e'[x \leftarrow v_1]]$:

8853 1. $\vdash_C v_0 v_1 : \tau'$
 8854 by *static hole typing*
 8855 2. $\vdash_C v_0 : \tau_d \Rightarrow \tau_c$
 8856 $\wedge \vdash_C v_1 : \tau_d$
 8857 $\wedge \tau_c \leq \tau'$
 8858 by *inversion*
 8859 3. $\tau_d \leq \tau_x$
 8860 by *canonical forms* (2)
 8861 4. $(x : \tau_x) \vdash_C e' : \tau_c$
 8862 by *inversion* (2)
 8863 5. $\vdash_C v_1 : \tau_x$
 8864 by (2, 3)
 8865 6. $\vdash_C e'[x \leftarrow v_1] : \tau_c$
 8866 by *substitution* (4, 5)
 8867 7. $\vdash_C e'[x \leftarrow v_1] : \tau'$
 8868 by (2, 6)
 8869 8. QED by *hole substitution* (7)
 8870 **ELSE** $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) v_f$
 8871 $\wedge e \rightarrow_{C-S} E^\bullet[\text{dyn } \tau_c (v_f (\text{stat } \tau_d v_1))]$:
 8872 1. $\vdash_C v_0 v_1 : \tau'$
 8873 by *static hole typing*
 8874 2. $\vdash_C v_0 : \tau'_d \Rightarrow \tau'_c$
 8875 $\wedge \vdash_C v_1 : \tau'_d$
 8876 $\wedge \tau'_c \leq \tau'$
 8877 by *inversion*
 8878 3. $\vdash_C v_f$
 8879 by *inversion* (2)
 8880 4. $\tau_d \Rightarrow \tau_c \leq \tau'_d \Rightarrow \tau'_c$
 8881 by *canonical forms* (2)
 8882 5. $\tau'_d \leq \tau_d$
 8883 $\wedge \tau_c \leq \tau'_c$
 8884 by (4)
 8885 6. $\vdash_C v_1 : \tau_d$
 8886 by (2, 5)
 8887 7. $\vdash_C \text{stat } \tau_d v_1$
 8888 by (6)
 8889 8. $\vdash_C v_f (\text{stat } \tau_d v_1)$
 8890 by (3, 7)
 8891 9. $\vdash_C \text{dyn } \tau_c (v_f (\text{stat } \tau_d v_1)) : \tau_c$
 8892 by (8)
 8893 10. $\vdash_C \text{dyn } \tau_c (v_f (\text{stat } \tau_d v_1)) : \tau'$
 8894 by (2, 5, 9)
 8895 11. QED by *hole substitution* (10)
 8896 **CASE** $e = E^\bullet[op^1 v]$:
 8897 **IF** $v = \text{mon}(\tau_0 \times \tau_1) v'$
 8898 $\wedge op^1 = \text{fst}$
 8899 $\wedge e \rightarrow_{C-S} E^\bullet[\text{dyn } \tau_0 (\text{fst } v')]$:
 8900 1. $\vdash_C \text{fst } v : \tau'$
 8901 by *static hole typing*
 8902 2. $\vdash_C v : \tau'_0 \times \tau'_1$
 8903 $\wedge \tau'_0 < \tau'$
 8904 by *inversion*
 8905 3. $\vdash_C v'$
 8906 by *inversion* (2)

8911	4. $\tau_0 \times \tau_1 \leq \tau'_0 \times \tau'_1$	4. $\vdash_C v_1 : \tau'$	8966
8912	by <i>canonical forms</i> (2)	by (2, 3)	8967
8913	5. $\tau_0 \leq \tau'_0$	5. QED by <i>hole substitution</i> (4)	8968
8914	6. $\vdash_C \text{fst } v'$	CASE $e = E^\bullet[op^2 v_0 v_1] :$	8969
8915	by (3)	1. $e \rightarrow_{C-S} E^\bullet[\delta(op^2, v_0, v_1)]$	8970
8916	7. $\vdash_C \text{dyn } \tau_0 (\text{fst } v') : \tau_0$	by $e \rightarrow_{C-S} e'$	8971
8917	by (6)	2. $\vdash_C op^2 v_0 v_1 : \tau'$	8972
8918	8. $\vdash_C \text{dyn } \tau_0 (\text{fst } v') : \tau'$	by <i>static hole typing</i>	8973
8919	by (2, 5, 7)	3. $\vdash_C v_0 : \tau_0$	8974
8920	9. QED by <i>hole substitution</i>	$\wedge \vdash_C v_1 : \tau_1$	8975
8921	IF $v = \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	$\wedge \Delta(op^2, \tau_0, \tau_1) = \tau''$	8976
8922	$\wedge op^1 = \text{snd}$	$\wedge \tau'' \leq \tau'$	8977
8923	$\wedge e \rightarrow_{C-S} E^\bullet[\text{dyn } \tau_0 (\text{snd } v')]$	by <i>inversion</i> (1)	8978
8924	1. $\vdash_C \text{snd } v : \tau'$	4. $\vdash_C \delta(op^2, v_0, v_1) : \tau''$	8979
8925	by <i>static hole typing</i>	by Δ <i>type soundness</i> (2)	8980
8926	2. $\vdash_C v : \tau'_0 \times \tau'_1$	5. $\vdash_C \delta(op^2, v_0, v_1) : \tau'$	8981
8927	$\wedge \tau'_1 < \tau'$	by (2, 3)	8982
8928	by <i>inversion</i>	6. QED by <i>hole substitution</i> (4)	8983
8929	3. $\vdash_C v'$	CASE $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :	8984
8930	by <i>inversion</i> (2)	IF e' is a value :	8985
8931	4. $\tau_0 \times \tau_1 \leq \tau'_0 \times \tau'_1$	1. $e \rightarrow_{C-S} E[\mathcal{D}_C(\tau', e')]$	8986
8932	by <i>canonical forms</i> (2)	2. $\vdash_C \text{dyn } \tau' e' : \tau'$	8987
8933	5. $\tau_1 \leq \tau'_1$	by <i>boundary hole typing</i>	8988
8934	6. $\vdash_C \text{snd } v'$	3. $\vdash_C e'$	8989
8935	by (3)	by <i>inversion</i> (2)	8990
8936	7. $\vdash_C \text{dyn } \tau_0 (\text{snd } v') : \tau_0$	4. $\vdash_C \mathcal{D}_C(\tau', e') : \tau'$	8991
8937	by (5)	by \mathcal{D}_C <i>soundness</i> (3)	8992
8938	8. $\vdash_C \text{dyn } \tau_0 (\text{snd } v') : \tau'$	5. QED by <i>hole substitution</i> (4)	8993
8939	by (2, 5, 7)	ELSE $e' \rightarrow_{C-D} e'' :$	8994
8940	9. QED by <i>hole substitution</i>	1. $e \rightarrow_{C-S} E[\text{dyn } \tau' e'']$	8995
8941	IF $v = \langle v_0, v_1 \rangle$	2. $\vdash_C \text{dyn } \tau' e' : \tau'$	8996
8942	$\wedge op^1 = \text{fst}$	by <i>boundary hole typing</i>	8997
8943	$\wedge e \rightarrow_{C-S} E^\bullet[v_0] :$	3. $\vdash_C e'$	8998
8944	1. $\vdash_C \text{fst } \langle v_0, v_1 \rangle : \tau'$	by <i>inversion</i> (2)	8999
8945	by <i>static hole typing</i>	4. $\vdash_C e''$	9000
8946	2. $\vdash_C \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$	by <i>dynamic preservation</i> (3)	9001
8947	$\wedge \tau_0 \leq \tau'$	5. $\vdash_C \text{dyn } \tau' e'' : \tau'$	9002
8948	by <i>inversion</i> (1)	by (4)	9003
8949	3. $\vdash_C v_0 : \tau_0$	6. QED by <i>hole substitution</i> (5)	9004
8950	by <i>inversion</i> (2)	CASE $e = E[\text{stat } \tau' e']$ and e' is boundary-free :	9005
8951	4. $\vdash_C v_0 : \tau'$	IF e' is a value :	9006
8952	by (2, 3)	1. $e \rightarrow_{C-S} E[\mathcal{S}_C(\tau', e')]$	9007
8953	5. QED by <i>hole substitution</i> (4)	2. $\vdash_C \text{stat } \tau' e'$	9008
8954	ELSE $v = \langle v_0, v_1 \rangle$	by <i>boundary hole typing</i>	9009
8955	$\wedge op^1 = \text{snd}$	3. $\vdash_C e' : \tau'$	9010
8956	$\wedge e \rightarrow_{C-S} E^\bullet[v_1] :$	by <i>inversion</i> (2)	9011
8957	1. $\vdash_C \text{snd } \langle v_0, v_1 \rangle : \tau'$	4. $\vdash_C \mathcal{S}_C(\tau', e')$	9012
8958	by <i>static hole typing</i>	by \mathcal{S}_C <i>soundness</i> (3)	9013
8959	2. $\vdash_C \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$	5. QED by <i>hole substitution</i> (4)	9014
8960	$\wedge \tau_1 \leq \tau'$	ELSE $e' \rightarrow_{C-S} e'' :$	9015
8961	by <i>inversion</i> (1)	1. $e \rightarrow_{C-S} E[\text{stat } \tau' e'']$	9016
8962	3. $\vdash_C v_1 : \tau_1$	2. $\vdash_C \text{stat } \tau' e'$	9017
8963	by <i>inversion</i> (2)	by <i>boundary hole typing</i>	9018
8964			9019
8965			9020

9021 3. $\vdash_C e' : \tau'$
 9022 by *inversion* (2)
 9023 4. $\vdash_C e'' : \tau'$
 9024 by *static preservation* (3)
 9025 5. $\vdash_C \text{stat } \tau' e''$
 9026 by (4)
 9027 6. QED by *hole substitution* (5)
 9028 **CASE** $e = E[\text{Err}]$:
 9029 1. $e \rightarrow_{C-S} \text{Err}$
 9030 2. QED by $\vdash_C \text{Err} : \tau$
 9031 \square

Lemma 5.10 : HC dynamic preservation

If $\vdash_C e$ and $e \rightarrow_{C-D} e'$ then $\vdash_C e'$

Proof:

By the *boundary factoring* lemma, there are seven cases.

CASE e is a value :

1. Contradiction by $e \rightarrow_{C-D} e'$

CASE $e = E^\bullet[v_0 v_1]$:

IF $v_0 = \lambda x. e'$

$\wedge e \rightarrow_{C-D} E^\bullet[e'[x \leftarrow v_1]]$:

1. $\vdash_C v_0 v_1$
by *dynamic hole typing*

2. $\vdash_C v_0$
 $\wedge \vdash_C v_1$
by *inversion* (1)

3. $x \vdash_C e'$
by *inversion* (2)

4. $\vdash_C e'[x \leftarrow v_1]$
by *substitution* (2, 3)

5. QED *hole substitution* (4)

ELSE $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) v_f$

$\wedge e \rightarrow_{C-D} E^\bullet[\text{stat } \tau_c (v_f (\text{dyn } \tau_d v_1))]$:

1. $\vdash_C v_0 v_1$
by *dynamic hole typing*

2. $\vdash_C v_0$
 $\wedge \vdash_C v_1$
by *inversion* (1)

3. $\vdash_C v_f : \tau_d \Rightarrow \tau_c$
by *inversion* (2)

4. $\vdash_C \text{dyn } \tau_d v_1 : \tau_d$
by (2)

5. $\vdash_C v_f (\text{dyn } \tau_d v_1) : \tau_c$
by (3, 4)

6. $\vdash_C \text{stat } \tau_c (v_f (\text{dyn } \tau_d v_1))$
by (5)

7. QED by *hole substitution*

CASE $e = E^\bullet[op^1 v]$:

IF $v = \text{mon}(\tau_0 \times \tau_1) v'$

$\wedge op^1 = \text{fst}$

$\wedge e \rightarrow_{C-D} E[\text{stat } \tau_0 (\text{fst } v')]$:

1. $\vdash_C op^1 v$
by *dynamic hole typing*

2. $\vdash_C \text{mon}(\tau_0 \times \tau_1) v'$
by *inversion* (1)
 3. $\vdash_C v' : \tau_0 \times \tau_1$
by *inversion* (2)
 4. $\vdash_C \text{fst } v' : \tau_0$
by (3)
 5. $\vdash_C \text{stat } \tau_0 (\text{fst } v')$
by (4)
 6. QED by *hole substitution*
IF $v = \text{mon}(\tau_0 \times \tau_1) v'$
 $\wedge op^1 = \text{snd}$
 $\wedge e \rightarrow_{C-D} E[\text{stat } \tau_0 (\text{snd } v')]$:

1. $\vdash_C op^1 v$
by *dynamic hole typing*

2. $\vdash_C \text{mon}(\tau_0 \times \tau_1) v'$
by *inversion* (1)

3. $\vdash_C v' : \tau_0 \times \tau_1$
by *inversion* (2)

4. $\vdash_C \text{snd } v' : \tau_1$
by (3)

5. $\vdash_C \text{stat } \tau_1 (\text{snd } v')$
by (4)

6. QED by *hole substitution*

IF $v = \langle v_0, v_1 \rangle$

$\wedge op^1 = \text{fst}$

$\wedge e \rightarrow_{C-D} E^\bullet[v_0]$:

1. $\vdash_C op^1 v$
by *dynamic hole typing*

2. $\vdash_C v$
by *inversion* (1)

3. $\vdash_C v_0$
by *inversion* (2)

4. QED by *hole substitution*

ELSE $v = \langle v_0, v_1 \rangle$

$\wedge op^1 = \text{snd}$

$\wedge e \rightarrow_{C-D} E^\bullet[v_1]$:

1. $\vdash_C op^1 v$
by *dynamic hole typing*

2. $\vdash_C v$
by *inversion* (1)

3. $\vdash_C v_1$
by *inversion* (2)

4. QED by *hole substitution*

CASE $e = E^\bullet[op^2 v_0 v_1]$:

1. $e \rightarrow_{C-D} E^\bullet[\delta(op^2, v_0, v_1)]$

2. $\vdash_C op^2 v_0 v_1$
by *dynamic hole typing*

3. $\vdash_C v_0$
 $\wedge \vdash_C v_1$
by *inversion* (1)

4. $\vdash_C \delta(op^2, v_0, v_1)$
by δ *preservation* (2)

5. QED by *hole substitution* (3)

CASE $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :

IF e' is a value :

1. $e \rightarrow_{C-D} E[\mathcal{D}_C(\tau', e')]$
2. $\vdash_C \text{dyn } \tau' e' : \tau'$
by *boundary hole typing*
3. $\vdash_C e'$
by *inversion* (2)
4. $\vdash_C \mathcal{D}_C(\tau', e') : \tau'$
by \mathcal{D}_C *soundness* (3)
5. QED by *hole substitution* (4)

ELSE $e' \rightarrow_{C-D} e''$:

1. $e \rightarrow_{C-D} E[\text{dyn } \tau' e'']$
2. $\vdash_C \text{dyn } \tau' e' : \tau'$
by *boundary hole typing*
3. $\vdash_C e'$
 $\wedge \tau' \leq \tau''$
by *inversion* (2)
4. $\vdash_C e''$
by *dynamic preservation* (3)
5. $\vdash_C \text{dyn } \tau' e'' : \tau'$
by (4)
6. QED by *hole substitution* (5)

CASE $e = E[\text{stat } \tau' e']$ and e' is boundary-free :

IF $e' \in v$:

1. $e \rightarrow_{C-D} E[\mathcal{S}_C(\tau', e')]$
2. $\vdash_C \text{stat } \tau' e'$
by *boundary hole typing*
3. $\vdash_C e' : \tau'$
by *inversion* (2)
4. $\vdash_C \mathcal{S}_C(\tau', e')$
by \mathcal{S}_C *soundness* (3)
5. QED by *hole substitution* (5)

ELSE $e' \rightarrow_{C-S} e''$:

1. $e \rightarrow_{C-D} E[\text{stat } \tau' e'']$
2. $\vdash_C \text{stat } \tau' e'$
by *boundary hole typing*
3. $\vdash_C e' : \tau'$
by *inversion* (2)
4. $\vdash_C e'' : \tau'$
by *static preservation* (3)
5. $\vdash_C \text{stat } \tau' e''$
by (4)
6. QED by *hole substitution* (5)

CASE $e = E[\text{Err}]$:

1. $e \rightarrow_{C-D} \text{Err}$
2. QED $\vdash_C \text{Err}$

□

Lemma 5.11 : HC *static boundary factoring*

If $\vdash_C e : \tau$ then one of the following holds:

- e is a value
- $e = E^\bullet[v_0 v_1]$
- $e = E^\bullet[\text{op}^1 v]$
- $e = E^\bullet[\text{op}^2 v_0 v_1]$
- $e = E[\text{dyn } \tau e']$ where e' is boundary-free
- $e = E[\text{stat } \tau e']$ where e' is boundary-free
- $e = E[\text{Err}]$

Proof:

By the *boundary factoring* lemma for the higher-order embedding. (The only difference is the meaning of e is a value.)

□

Lemma 5.12 : HC *dynamic boundary factoring*

If $\vdash_C e$ then one of the following holds:

- e is a value
- $e = E^\bullet[v_0 v_1]$
- $e = E^\bullet[\text{op}^1 v]$
- $e = E^\bullet[\text{op}^2 v_0 v_1]$
- $e = E[\text{dyn } \tau e']$ where e' is boundary-free
- $e = E[\text{stat } \tau e']$ where e' is boundary-free
- $e = E[\text{Err}]$

Proof:

By the *boundary factoring* lemma for the higher-order embedding.

□

Lemma 5.13 : HC *static hole typing*

If $\vdash_C E^\bullet[e] : \tau$ then the derivation contains a sub-term $\vdash_C e : \tau'$

Proof (sketch): Similar to the *static hole typing* lemma for the higher-order embedding. □

Lemma 5.14 : HC *dynamic hole typing*

If $\vdash_C E^\bullet[e]$ then the derivation contains a sub-term $\vdash_C e$

Proof (sketch): Similar to the *static hole typing* lemma for the higher-order embedding. □

Lemma 5.15 : HC *boundary hole typing*

- If $\vdash_C E[\text{dyn } \tau e] : \tau'$ then the derivation contains a sub-term $\vdash_C \text{dyn } \tau e : \tau$
- If $\vdash_C E[\text{dyn } \tau e]$ then the derivation contains a sub-term $\vdash_C \text{dyn } \tau e : \tau$
- If $\vdash_C E[\text{stat } \tau e] : \tau'$ then the derivation contains a sub-term $\vdash_C \text{stat } \tau e$
- If $\vdash_C E[\text{stat } \tau e]$ then the derivation contains a sub-term $\vdash_C \text{stat } \tau e$

Proof (sketch): Similar to the proof for the higher-order *boundary hole typing* lemma. □

Lemma 5.16 : HC *hole substitution*

- If $\vdash_C E[e]$ and the derivation contains a sub-term $\vdash_C e : \tau'$ and $\vdash_C e' : \tau'$ then $\vdash_C E[e']$.
- If $\vdash_C E[e]$ and the derivation contains a sub-term $\vdash_C e$ and $\vdash_C e'$ then $\vdash_C E[e']$.
- If $\vdash_C E[e] : \tau$ and the derivation contains a sub-term $\vdash_C e : \tau'$ and $\vdash_C e' : \tau'$ then $\vdash_C E[e'] : \tau$.
- If $\vdash_C E[e] : \tau$ and the derivation contains a sub-term $\vdash_C e$ and $\vdash_C e'$ then $\vdash_C E[e'] : \tau$.

Proof (sketch): Similar to the proof of the higher-order *hole substitution* lemma, just replacing \vdash_H with \vdash_C . \square

Lemma 5.17 : \vdash_C static inversion

- If $\Gamma \vdash_C x : \tau$ then $(x : \tau') \in \Gamma$ and $\tau' \leq \tau$
- If $\Gamma \vdash_C \lambda(x : \tau'_d). e' : \tau$ then $(x : \tau'_d), \Gamma \vdash_C e' : \tau'_c$ and $\tau'_d \Rightarrow \tau'_c \leq \tau$
- If $\Gamma \vdash_C \langle e_0, e_1 \rangle : \tau_0 \times \tau_1$ then $\Gamma \vdash_C e_0 : \tau'_0$ and $\Gamma \vdash_C e_1 : \tau'_1$ and $\tau'_0 \leq \tau_0$ and $\tau'_1 \leq \tau_1$
- If $\Gamma \vdash_C e_0 e_1 : \tau_c$ then $\Gamma \vdash_C e_0 : \tau'_d \Rightarrow \tau'_c$ and $\Gamma \vdash_C e_1 : \tau'_d$ and $\tau'_c \leq \tau_c$
- If $\Gamma \vdash_C \text{fst } e : \tau$ then $\Gamma \vdash_C e : \tau_0 \times \tau_1$ and $\Delta(\text{fst}, \tau_0 \times \tau_1) = \tau_0$ and $\tau_0 \leq \tau$
- If $\Gamma \vdash_C \text{snd } e : \tau$ then $\Gamma \vdash_C e : \tau_0 \times \tau_1$ and $\Delta(\text{snd}, \tau_0 \times \tau_1) = \tau_1$ and $\tau_1 \leq \tau$
- If $\Gamma \vdash_C \text{op}^2 e_0 e_1 : \tau$ then $\Gamma \vdash_C e_0 : \tau_0$ and $\Gamma \vdash_C e_1 : \tau_1$ and $\Delta(\text{op}^2, \tau_0, \tau_1) = \tau'$ and $\tau' \leq \tau$
- If $\Gamma \vdash_C \text{mon } \tau'_0 \times \tau'_1 v' : \tau_0 \times \tau_1$ then $\Gamma \vdash_C v'$ and $\tau'_0 \times \tau'_1 \leq \tau_0 \times \tau_1$
- If $\Gamma \vdash_C \text{mon } \tau'_d \Rightarrow \tau'_c v' : \tau_d \Rightarrow \tau_c$ then $\Gamma \vdash_C v'$ and $\tau'_d \Rightarrow \tau'_c \leq \tau_d \Rightarrow \tau_c$
- If $\Gamma \vdash_C \text{dyn } \tau' e' : \tau$ then $\Gamma \vdash_C e'$ and $\tau' \leq \tau$

Proof:

QED by the definition of $\Gamma \vdash_C e : \tau$

\square

Lemma 5.18 : \vdash_C dynamic inversion

- If $\Gamma \vdash_C x$ then $x \in \Gamma$
- If $\Gamma \vdash_C \lambda x. e'$ then $x, \Gamma \vdash_C e'$
- If $\Gamma \vdash_C \langle e_0, e_1 \rangle$ then $\Gamma \vdash_C e_0$ and $\Gamma \vdash_C e_1$
- If $\Gamma \vdash_C e_0 e_1$ then $\Gamma \vdash_C e_0$ and $\Gamma \vdash_C e_1$
- If $\Gamma \vdash_C \text{op}^1 e_0$ then $\Gamma \vdash_C e_0$
- If $\Gamma \vdash_C \text{op}^2 e_0 e_1$ then $\Gamma \vdash_C e_0$ and $\Gamma \vdash_C e_1$
- If $\Gamma \vdash_C \text{mon } \tau_d \Rightarrow \tau_c v'$ then $\Gamma \vdash_C v' : \tau_d \Rightarrow \tau_c$
- If $\Gamma \vdash_C \text{mon } \tau_0 \times \tau_1 v'$ then $\Gamma \vdash_C v' : \tau_0 \times \tau_1$
- If $\Gamma \vdash_C \text{stat } \tau' e'$ then $\Gamma \vdash_C e' : \tau'$

Proof:

QED by the definition of $\Gamma \vdash_C e$

\square

Lemma 5.19 : HC canonical forms

- If $\vdash_C v : \tau_0 \times \tau_1$ then either:
 - $v = \langle v_0, v_1 \rangle$
 - or $v = \text{mon}(\tau'_0 \times \tau'_1) v'$
 - $\wedge \tau'_0 \times \tau'_1 \leq \tau_0 \times \tau_1$
- If $\vdash_C v : \tau_d \Rightarrow \tau_c$ then either:
 - $v = \lambda(x : \tau_x). e'$
 - $\wedge \tau_d \leq \tau_x$
 - or $v = \text{mon}(\tau'_d \Rightarrow \tau'_c) v'$
 - $\wedge \tau'_d \Rightarrow \tau'_c \leq \tau_d \Rightarrow \tau_c$
- If $\vdash_C v : \text{Int}$ then $v = i$
- If $\vdash_C v : \text{Nat}$ then $v = i$ and $v \in \mathbb{N}$

Proof:

QED by definition of $\vdash_C e : \tau$

\square

Lemma 5.20 : Δ type soundness

If $\vdash_C v_0 : \tau_0$ and $\vdash_C v_1 : \tau_1$ and $\Delta(\text{op}^2, \tau_0, \tau_1) = \tau$ then one of the following holds:

- $\delta(\text{op}^2, v_0, v_1) = v$ and $\vdash_C v : \tau$, or
- $\delta(\text{op}^2, v_0, v_1) = \text{BndryErr}$

Proof (sketch): Similar to the proof for the higher-order Δ type soundness lemma. \square

Lemma 5.21 : δ preservation

- If $\vdash_C v$ and $\delta(\text{op}^1, v) = v'$ then $\vdash_C v'$
- If $\vdash_C v_0$ and $\vdash_C v_1$ and $\delta(\text{op}^2, v_0, v_1) = v'$ then $\vdash_C v'$

Proof (sketch): Similar to the proof for the higher-order δ preservation lemma. \square

Lemma 5.22 : HC substitution

- If $(x : \tau_x), \Gamma \vdash_C e$ and $\vdash_C v : \tau_x$ then $\Gamma \vdash_C e[x \leftarrow v]$
- If $x, \Gamma \vdash_C e$ and $\vdash_C v$ then $\Gamma \vdash_C e[x \leftarrow v]$
- If $(x : \tau_x), \Gamma \vdash_C e : \tau$ and $\vdash_C v : \tau_x$ then $\Gamma \vdash_C e[x \leftarrow v] : \tau$
- If $x, \Gamma \vdash_C e : \tau$ and $\vdash_C v$ then $\Gamma \vdash_C e[x \leftarrow v] : \tau$

Proof (sketch): Similar to the proof for the higher-order substitution lemma. \square

Lemma 5.23 : weakening

- If $\Gamma \vdash_C e$ then $x, \Gamma \vdash_C e$
- If $\Gamma \vdash_C e : \tau$ then $(x : \tau'), \Gamma \vdash_C e : \tau$

Proof:

QED because e is closed under Γ

\square

A.6 (HF) Forgetful Embedding

A.6.1 Forgetful Definitions

Language HF

$e = x \mid v \mid \langle e, e \rangle \mid e e \mid op^1 e \mid op^2 e e \mid$
 $\text{dyn } \tau e \mid \text{stat } \tau e \mid \text{Err} \mid \text{chk } \tau e$
 $v = i \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x:\tau). e \mid$
 $\text{mon}(\tau \Rightarrow \tau)(\lambda x. e) \mid \text{mon}(\tau \Rightarrow \tau)(\lambda(x:\tau). e) \mid$
 $\text{mon}(\tau \times \tau) \langle v, v \rangle$
 $\tau = \text{Nat} \mid \text{Int} \mid \tau \times \tau \mid \tau \Rightarrow \tau$
 $\Gamma = \cdot \mid x, \Gamma \mid (x:\tau), \Gamma$
 $\text{Err} = \text{BndryErr} \mid \text{TagErr}$
 $r = v \mid \text{Err}$
 $E^\bullet = [] \mid E^\bullet e \mid v E^\bullet \mid \langle E^\bullet, e \rangle \mid \langle v, E^\bullet \rangle \mid$
 $op^1 E^\bullet \mid op^2 E^\bullet e \mid op^2 v E^\bullet$
 $E = E^\bullet \mid E e \mid v E \mid \langle E, e \rangle \mid \langle v, E \rangle \mid op^1 E \mid$
 $op^2 E e \mid op^2 v E \mid \text{dyn } \tau e \mid \text{stat } \tau e$

$\Delta : op^1 \times \tau \longrightarrow \tau$

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

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

$\Delta : op^2 \times \tau \times \tau \longrightarrow \tau$

$\Delta(op^2, \text{Nat}, \text{Nat}) = \text{Nat}$

$\Delta(op^2, \text{Int}, \text{Int}) = \text{Int}$

$\tau \leqslant \tau$

$\text{Nat} \leqslant \text{Int} \quad \frac{\tau'_d \leqslant \tau_d \quad \tau_c \leqslant \tau'_c}{\tau_d \Rightarrow \tau_c \leqslant \tau'_d \Rightarrow \tau'_c} \quad \frac{\tau_0 \leqslant \tau'_0 \quad \tau_1 \leqslant \tau'_1}{\tau_0 \times \tau_1 \leqslant \tau'_0 \times \tau'_1}$

$\frac{\tau \leqslant \tau'}{\tau \leqslant \tau} \quad \frac{\tau \leqslant \tau' \quad \tau' \leqslant \tau''}{\tau \leqslant \tau''}$

$\Gamma \vdash e$

$\frac{x \in \Gamma}{\Gamma \vdash x} \quad \frac{x, \Gamma \vdash e}{\Gamma \vdash \lambda x. e} \quad \frac{}{\Gamma \vdash i} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash \langle e_0, e_1 \rangle}$

$\frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash e_0 e_1} \quad \frac{\Gamma \vdash e}{\Gamma \vdash op^1 e} \quad \frac{\Gamma \vdash e_0 \quad \Gamma \vdash e_1}{\Gamma \vdash op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash \text{Err}}$

$\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{stat } \tau e}$

$\Gamma \vdash e : \tau$

$\frac{(x:\tau) \in \Gamma}{\Gamma \vdash x : \tau} \quad \frac{(x:\tau_d), \Gamma \vdash e : \tau_c}{\Gamma \vdash \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c} \quad \frac{i \in \mathbb{N}}{\Gamma \vdash i : \text{Nat}}$

$\frac{}{\Gamma \vdash i : \text{Int}} \quad \frac{\Gamma \vdash e_0 : \tau_0 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \langle e_0, e_1 \rangle : \tau_0 \times \tau_1} \quad \frac{\Gamma \vdash e_0 : \tau_d \Rightarrow \tau_c \quad \Gamma \vdash e_1 : \tau_d}{\Gamma \vdash e_0 e_1 : \tau_c}$

$\frac{\Gamma \vdash e_0 : \tau_0 \quad \Delta(op^1, \tau_0) = \tau}{\Gamma \vdash op^1 e_0 : \tau} \quad \frac{\Gamma \vdash e_1 : \tau_1 \quad \Delta(op^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash op^2 e_0 e_1 : \tau} \quad \frac{\Gamma \vdash e : \tau' \quad \tau' \leqslant \tau}{\Gamma \vdash e : \tau} \quad \frac{}{\Gamma \vdash \text{Err} : \tau}$

$\frac{\Gamma \vdash e}{\Gamma \vdash \text{dyn } \tau e : \tau}$

$\Gamma \vdash_F e$

$\frac{x \in \Gamma}{\Gamma \vdash_F x} \quad \frac{x, \Gamma \vdash_F e}{\Gamma \vdash_F \lambda x. e} \quad \frac{}{\Gamma \vdash_F i} \quad \frac{\Gamma \vdash_F e_0 \quad \Gamma \vdash_F e_1}{\Gamma \vdash_F \langle e_0, e_1 \rangle}$

$\frac{\Gamma \vdash_F e_0 \quad \Gamma \vdash_F e_1}{\Gamma \vdash_F e_0 e_1} \quad \frac{\Gamma \vdash_F e}{\Gamma \vdash_F op^1 e} \quad \frac{\Gamma \vdash_F e_0 \quad \Gamma \vdash_F e_1}{\Gamma \vdash_F op^2 e_0 e_1} \quad \frac{}{\Gamma \vdash_F \text{Err}}$

$\frac{\Gamma \vdash_F e : \tau}{\Gamma \vdash_F \text{stat } \tau e} \quad \frac{\Gamma \vdash_F v_0 : \tau'_0 \quad \Gamma \vdash_F v_1 : \tau'_1}{\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle}$

$\frac{\Gamma \vdash_F v_0 \quad \Gamma \vdash_F v_1}{\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle} \quad \frac{\Gamma \vdash_F \lambda x. e}{\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) \lambda x. e}$

$\frac{\Gamma \vdash_F \lambda(x:\tau'_d). e : \tau'_d \Rightarrow \tau'_c}{\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) \lambda(x:\tau'_d). e}$

9461	$\boxed{\Gamma \vdash_F e : \tau}$	
9462	$\frac{(x:\tau) \in \Gamma}{\Gamma \vdash_F x : \tau}$	
9463	$\frac{(x:\tau_d), \Gamma \vdash_F e : \tau_c}{\Gamma \vdash_F \lambda(x:\tau_d). e : \tau_d \Rightarrow \tau_c}$	
9464	$\frac{i \in \mathbb{N}}{\Gamma \vdash_F i : \text{Nat}}$	
9465		
9466	$\frac{\Gamma \vdash_F e_0 : \tau_0}{\Gamma \vdash_F e_1 : \tau_1}$	$\frac{\Gamma \vdash_F e_0 : \tau_d \Rightarrow \tau_c}{\Gamma \vdash_F e_1 : \tau_d}$
9467	$\frac{}{\Gamma \vdash_F i : \text{Int}}$	$\frac{}{\Gamma \vdash_F \langle e_0, e_1 \rangle : \tau_0 \times \tau_1}$
9468	$\frac{}{\Gamma \vdash_F i : \text{Int}}$	$\frac{}{\Gamma \vdash_F e_0 e_1 : \tau_c}$
9469		
9470		
9471	$\frac{\Gamma \vdash_F e_0 : \tau_0}{\Delta(op^1, \tau_0) = \tau}$	$\frac{\Gamma \vdash_F e_1 : \tau_1}{\Delta(op^2, \tau_0, \tau_1) = \tau}$
9472	$\frac{\Delta(op^1, \tau_0) = \tau}{\Gamma \vdash_F op^1 e_0 : \tau}$	$\frac{\Delta(op^2, \tau_0, \tau_1) = \tau}{\Gamma \vdash_F op^2 e_0 e_1 : \tau}$
9473	$\frac{}{\Gamma \vdash_F op^1 e_0 : \tau}$	$\frac{}{\Gamma \vdash_F e : \tau'}$
9474	$\frac{}{\Gamma \vdash_F op^1 e_0 : \tau}$	$\frac{}{\Gamma \vdash_F e : \tau}$
9475		
9476	$\frac{}{\Gamma \vdash_F \text{Err} : \tau}$	$\frac{\Gamma \vdash_F e}{\Gamma \vdash_F \text{dyn } \tau e : \tau}$
9477	$\frac{}{\Gamma \vdash_F \text{Err} : \tau}$	$\frac{}{\Gamma \vdash_F \text{dyn } \tau e : \tau}$
9478		
9479	$\frac{\Gamma \vdash_F v_0 : \tau'_0 \quad \Gamma \vdash_F v_1 : \tau'_1}{\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : (\tau_0 \times \tau_1)}$	
9480	$\frac{}{\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : (\tau_0 \times \tau_1)}$	
9481		
9482	$\frac{\Gamma \vdash_F v_0 \quad \Gamma \vdash_F v_1}{\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : (\tau_0 \times \tau_1)}$	
9483	$\frac{}{\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : (\tau_0 \times \tau_1)}$	
9484	$\frac{}{\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : (\tau_0 \times \tau_1)}$	
9485		
9486	$\frac{\Gamma \vdash_F \lambda x. e}{\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) \lambda x. e : (\tau_d \Rightarrow \tau_c)}$	
9487	$\frac{}{\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) \lambda x. e : (\tau_d \Rightarrow \tau_c)}$	
9488		
9489	$\frac{\Gamma \vdash_F \lambda(x:\tau'_d). e : \tau'_d \Rightarrow \tau'_c}{\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) \lambda(x:\tau'_d). e : (\tau_d \Rightarrow \tau_c)}$	$\frac{\Gamma \vdash_F e : \tau'}{\Gamma \vdash_F \text{chk } \tau e : \tau}$
9490	$\frac{}{\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) \lambda(x:\tau'_d). e : (\tau_d \Rightarrow \tau_c)}$	$\frac{}{\Gamma \vdash_F \text{chk } \tau e : \tau}$
9491	$\boxed{\delta(op^1, v) = e}$	
9492	$\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$	
9493	$\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$	
9494	$\delta(\text{sum}, i_0, i_1) = i_0 + i_1$	
9495	$\delta(\text{quotient}, i_0, 0) = \text{BndryErr}$	
9496	$\delta(\text{quotient}, i_0, i_1) = \lfloor i_0 / i_1 \rfloor$	
9497	$\text{if } i_1 \neq 0$	
9498	$\boxed{\mathcal{D}_F : \tau \times v \longrightarrow e}$	
9499	$\mathcal{D}_F(\tau, v) = \mathcal{X}(\tau, v)$	
9500	$\boxed{\mathcal{S}_F : \tau \times v \longrightarrow e}$	
9501	$\mathcal{S}_F(\tau, v) = \mathcal{X}(\tau, v)$	
9502		
9503		
9504		
9505		
9506		
9507		
9508		
9509		
9510		
9511		
9512		
9513		
9514		
9515		

9516	$\boxed{\mathcal{X} : \tau \times v \longrightarrow e}$	
9517	$\mathcal{X}(\tau_d \Rightarrow \tau_c, \lambda x. e) = \text{mon}(\tau_d \Rightarrow \tau_c) (\lambda x. e)$	
9518	$\mathcal{X}(\tau_d \Rightarrow \tau_c, \lambda(x:\tau). e) = \text{mon}(\tau_d \Rightarrow \tau_c) (\lambda(x:\tau). e)$	
9519	$\mathcal{X}(\tau_d \Rightarrow \tau_c, \text{mon}(\tau'_d \Rightarrow \tau'_c) v') = \text{mon}(\tau_d \Rightarrow \tau_c) v'$	
9520	$\mathcal{X}(\tau_0 \times \tau_1, \langle v_0, v_1 \rangle) = \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	
9521	$\mathcal{X}(\tau_0 \times \tau_1, \text{mon}(\tau'_0 \times \tau'_1) v') = \text{mon}(\tau_0 \times \tau_1) v'$	
9522	$\mathcal{X}(\text{Int}, i) = i$	
9523	$\mathcal{X}(\text{Nat}, i) = i$	
9524	$\text{if } i \in \mathbb{N}$	
9525	$\mathcal{X}(\tau, v) = \text{BndryErr}$	
9526	otherwise	
9527	$\boxed{e \triangleright_{S-1} e}$	
9528	$\text{dyn } \tau v \triangleright_{S-1} \mathcal{D}_F(\tau, v)$	
9529	$\text{chk } \tau v \triangleright_{S-1} \mathcal{X}(\tau, v)$	
9530	$(\text{mon}(\tau_d \Rightarrow \tau_c) (\lambda x. e)) v \triangleright_{S-1} \text{dyn } \tau_c e'$	
9531	$\text{where } e' = (\lambda x. e) (\mathcal{X}(\tau_d, v))$	
9532	$(\text{mon}(\tau_d \Rightarrow \tau_c) (\lambda(x:\tau). e)) v \triangleright_{S-1} \text{chk } \tau_c e'$	
9533	$\text{where } e' = (\lambda(x:\tau). e) (\mathcal{X}(\tau, v))$	
9534	$\text{fst}(\text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle) \triangleright_{S-1} \mathcal{X}(\tau_0, v_0)$	
9535	$\text{snd}(\text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle) \triangleright_{S-1} \mathcal{X}(\tau_1, v_1)$	
9536	$(\lambda(x:\tau). e) v \triangleright_{S-1} e[x \leftarrow v]$	
9537	$op^1 v \triangleright_{S-1} \delta(op^1, v)$	
9538	$op^2 v_0 v_1 \triangleright_{S-1} \delta(op^2, v_0, v_1)$	
9539	$\boxed{e \triangleright_{D-1} e}$	
9540	$\text{stat } \tau v \triangleright_{D-1} \mathcal{S}_F(\tau, v)$	
9541	$v_0 v_1 \triangleright_{D-1} \text{TagErr}$	
9542	$\text{if } v_0 \in \mathbb{Z} \text{ or } v_0 = \langle v, v' \rangle$	
9543	$(\text{mon}(\tau_d \Rightarrow \tau_c) (\lambda x. e)) v \triangleright_{D-1} (\lambda x. e) v$	
9544	$(\text{mon}(\tau_d \Rightarrow \tau_c) (\lambda(x:\tau). e)) v \triangleright_{D-1} \text{stat } \tau_c e'$	
9545	$\text{where } e' = \text{chk } \tau_c ((\lambda(x:\tau). e) (\mathcal{X}(\tau, v)))$	
9546	$(\lambda x. e) v \triangleright_{H-D} e[x \leftarrow v]$	
9547	$\text{fst}(\text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle) \triangleright_{D-1} \mathcal{X}(\tau_0, v_0)$	
9548	$\text{snd}(\text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle) \triangleright_{D-1} \mathcal{X}(\tau_1, v_1)$	
9549	$op^1 v \triangleright_{H-D} \text{TagErr}$	
9550	$\text{if } \delta(op^1, v) \text{ is undefined}$	
9551	$op^1 v \triangleright_{H-D} \delta(op^1, v)$	
9552	$op^2 v_0 v_1 \triangleright_{H-D} \text{TagErr}$	
9553	$\text{if } \delta(op^2, v_0, v_1) \text{ is undefined}$	
9554	$op^2 v_0 v_1 \triangleright_{H-D} \delta(op^2, v_0, v_1)$	
9555	$\boxed{e \rightarrow_{F-S} e}$	
9556	$E^\bullet[e] \rightarrow_{F-S} E^\bullet[e']$	
9557	$\text{if } e \triangleright_{S-1} e'$	
9558	$E[\text{stat } \tau E^\bullet[e]] \rightarrow_{F-S} E[\text{stat } \tau E^\bullet[e']]$	
9559	$\text{if } e \triangleright_{S-1} e'$	
9560	$E[\text{dyn } \tau E^\bullet[e]] \rightarrow_{F-S} E[\text{dyn } \tau E^\bullet[e']]$	
9561	$\text{if } e \triangleright_{D-1} e'$	
9562	$E[\text{Err}] \rightarrow_{F-S} \text{Err}$	
9563		
9564		
9565		
9566		
9567		
9568		
9569		
9570		

9571	$e \rightarrow_{F-D} e$	9626
9572	$E^\bullet[e] \rightarrow_{F-D} E^\bullet[e']$	9627
9573	if $e \triangleright_{D-1} e'$	9628
9574	$E[\text{stat } \tau E^\bullet[e]] \rightarrow_{F-D} E[\text{stat } \tau E^\bullet[e']]$	9629
9575	if $e \triangleright_{S-1} e'$	9630
9576	$E[\text{dyn } \tau E^\bullet[e]] \rightarrow_{F-D} E[\text{dyn } \tau E^\bullet[e']]$	9631
9577	if $e \triangleright_{D-1} e'$	9632
9578	$E[\text{Err}] \rightarrow_{F-D} \text{Err}$	9633
9579	$e \rightarrow_{F-S}^* e$ reflexive, transitive closure of \rightarrow_{F-S}	9634
9580		9635
9581	$e \rightarrow_{F-D}^* e$ reflexive, transitive closure of \rightarrow_{F-D}	9636
9582		9637
9583		9638
9584		9639
9585		9640
9586		9641
9587		9642
9588		9643
9589		9644
9590		9645
9591		9646
9592		9647
9593		9648
9594		9649
9595		9650
9596		9651
9597		9652
9598		9653
9599		9654
9600		9655
9601		9656
9602		9657
9603		9658
9604		9659
9605		9660
9606		9661
9607		9662
9608		9663
9609		9664
9610		9665
9611		9666
9612		9667
9613		9668
9614		9669
9615		9670
9616		9671
9617		9672
9618		9673
9619		9674
9620		9675
9621		9676
9622		9677
9623		9678
9624		9679
9625		9680

A.6.2 Forgetful Theorems

Theorem 6.0 : static HF-soundness

If $\vdash e : \tau$ then $\vdash_F e : \tau$ and one of the following holds:

- $e \rightarrow_{F-S}^* v$ and $\vdash_F v : \tau$
- $e \rightarrow_{F-S}^* E[\text{dyn } \tau' e']$ and $e' \triangleright_{D-1} \text{TagErr}$
- $e \rightarrow_{F-S}^* \text{BndryErr}$
- e diverges

Proof:

1. $\vdash_F e : \tau$
by *static subset*
2. QED by *static progress* and *static preservation*.

□

Theorem 6.1 : dynamic HF-soundness

If $\vdash e$ then $\vdash_F e$ and one of the following holds:

- $e \rightarrow_{F-D}^* v$ and $\vdash_F v$
- $e \rightarrow_{F-D}^* E[e']$ and $e' \triangleright_{D-1} \text{TagErr}$
- $e \rightarrow_{F-D}^* \text{BndryErr}$
- e diverges

Proof:

1. $\vdash_F e$
by *dynamic subset*
2. QED by *dynamic progress* and *dynamic preservation*.

□

Corollary 6.2 : HF static soundness

If $\vdash e : \tau$ and e is boundary-free, then one of the following holds:

- $e \rightarrow_{F-S}^* v$ and $\vdash_F v : \tau$
- $e \rightarrow_{F-S}^* \text{BndryErr}$
- e diverges

Proof:

Consequence of the proof for *static HF-soundness*

□

A.6.3 Forgetful Lemmas

Lemma 6.3 : $\mathcal{X}(\cdot, \cdot)$ soundness

If $\Gamma \vdash_F v$ or $\Gamma \vdash_F v : \tau$
 and $\mathcal{X}(\tau', v) = v'$,
 then $\Gamma \vdash_F v'$ and $\Gamma \vdash_F v' : \tau'$

Proof:

By case analysis of the definition of $\mathcal{X}(\cdot, \cdot)$.

CASE $\mathcal{X}(\tau_d \Rightarrow \tau_c, v) = \text{mon}(\tau_d \Rightarrow \tau_c) v :$

IF $v = \lambda x. e$

$\wedge \Gamma \vdash_F v :$

1. $\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) v$
by $\Gamma \vdash_F v$
2. $\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) v : \tau_d \Rightarrow \tau_c$
by $\Gamma \vdash_F v$
3. QED

ELSE $v = \lambda(x : \tau_x). e$

$\wedge \Gamma \vdash_F v : \tau'_d \Rightarrow \tau'_c :$

1. $\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) v$
by $\Gamma \vdash_F v : \tau'_d \Rightarrow \tau'_c$
2. $\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) v : \tau_d \Rightarrow \tau_c$
by $\Gamma \vdash_F v : \tau'_d \Rightarrow \tau'_c$
3. QED

CASE $\mathcal{X}(\tau_d \Rightarrow \tau_c, \text{mon}(\tau'_d \Rightarrow \tau'_c) v') = \text{mon}(\tau_d \Rightarrow \tau_c) v' :$

IF $\Gamma \vdash_F \text{mon}(\tau'_d \Rightarrow \tau'_c) v' :$

IF $v' = \lambda x. e'$

$\wedge \Gamma \vdash_F v' :$

1. $\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) v'$
by $\Gamma \vdash_F v'$
2. $\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) v' : \tau_d \Rightarrow \tau_c$
by $\Gamma \vdash_F v'$
3. QED

ELSE $v' = \lambda(x : \tau_x). e'$

$\wedge \Gamma \vdash_F v' : \tau''_d \Rightarrow \tau''_c :$

1. $\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) v'$
by $\Gamma \vdash_F v' : \tau''_d \Rightarrow \tau''_c$
2. $\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) v' : \tau_d \Rightarrow \tau_c$
by $\Gamma \vdash_F v' : \tau''_d \Rightarrow \tau''_c$
3. QED

ELSE $\Gamma \vdash_F \text{mon}(\tau'_d \Rightarrow \tau'_c) v' : \tau'_d \Rightarrow \tau'_c :$

IF $v' = \lambda x. e'$

$\wedge \Gamma \vdash_F v' :$

1. $\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) v'$
by $\Gamma \vdash_F v'$
2. $\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) v' : \tau_d \Rightarrow \tau_c$
by $\Gamma \vdash_F v'$
3. QED

ELSE $v' = \lambda(x : \tau_x). e'$

$\wedge \Gamma \vdash_F v' : \tau''_d \Rightarrow \tau''_c :$

1. $\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) v'$
by $\Gamma \vdash_F v' : \tau''_d \Rightarrow \tau''_c$
2. $\Gamma \vdash_F \text{mon}(\tau_d \Rightarrow \tau_c) v' : \tau_d \Rightarrow \tau_c$
by $\Gamma \vdash_F v' : \tau''_d \Rightarrow \tau''_c$
3. QED

CASE $\mathcal{X}(\tau_0 \times \tau_1, \langle v_0, v_1 \rangle) = \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle :$

IF $\Gamma \vdash_F \langle v_0, v_1 \rangle :$

1. $\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$
by $\Gamma \vdash_F \langle v_0, v_1 \rangle$
2. $\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$
by $\Gamma \vdash_F \langle v_0, v_1 \rangle$
3. QED

ELSE $\Gamma \vdash_F \langle v_0, v_1 \rangle : \tau'_0 \times \tau'_1 :$

1. $\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$
by $\Gamma \vdash_F \langle v_0, v_1 \rangle : \tau'_0 \times \tau'_1$
2. $\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$
by $\Gamma \vdash_F \langle v_0, v_1 \rangle : \tau'_0 \times \tau'_1$
3. QED

CASE $\mathcal{X}(\tau_0 \times \tau_1, \text{mon}(\tau'_0 \times \tau'_1) \langle v_0, v_1 \rangle) = \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$

:

IF $\Gamma \vdash_F \langle v_0, v_1 \rangle :$

1. $\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$
by $\Gamma \vdash_F \langle v_0, v_1 \rangle$
2. $\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$
by $\Gamma \vdash_F \langle v_0, v_1 \rangle$
3. QED

ELSE $\Gamma \vdash_F \langle v_0, v_1 \rangle : \tau''_0 \times \tau''_1 :$

1. $\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$
by $\Gamma \vdash_F \langle v_0, v_1 \rangle : \tau''_0 \times \tau''_1$
2. $\Gamma \vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$
by $\Gamma \vdash_F \langle v_0, v_1 \rangle : \tau''_0 \times \tau''_1$
3. QED

CASE $\mathcal{X}(\text{Int}, i) = i :$

1. $\Gamma \vdash_F i$
2. $\Gamma \vdash_F i : \text{Int}$
3. QED

CASE $\mathcal{X}(\text{Nat}, i) = i :$

1. $\Gamma \vdash_F i$
2. $\Gamma \vdash_F i : \text{Nat}$
by $i \in \mathbb{N}$
3. QED

□

Corollary 6.4 : \mathcal{D}_F soundness

If $\vdash_F v$ then $\vdash_F \mathcal{D}_F(\tau, v) : \tau$

Proof:

QED by \mathcal{X} soundness

□

Corollary 6.5 : \mathcal{S}_F soundness

If $\vdash_F v : \tau$ then $\vdash_F \mathcal{S}_F(\tau, v)$

Proof:

QED by \mathcal{X} soundness

□

Corollary 6.6 : HF static subset

If $\Gamma \vdash e : \tau$ then $\Gamma \vdash_F e : \tau$.

Proof:

Consequence of the proof for the higher-order *static subset* lemma; both \vdash_F and \vdash_H have the same typing rules for surface-language expressions.

□

Corollary 6.7 : HF *dynamic subset*If $\Gamma \vdash e$ then $\Gamma \vdash_F e$.*Proof*:Consequence of the proof for the higher-order *dynamic subset* lemma.

□

Lemma 6.8 : HF *static progress*If $\vdash_F e : \tau$ then one of the following holds:

- e is a value
- $e \in \text{Err}$
- $e \rightarrow_{F-S} e'$
- $e \rightarrow_{F-S} \text{BndryErr}$
- $e = E[\text{dyn } \tau' e']$ and $e' \rightarrow_{F-D} \text{TagErr}$

Proof:By the *boundary factoring* lemma, there are eight possible cases.**CASE** e is a value :

1. QED

CASE $e = E^*[v_0 v_1]$:

- 1.
- $\vdash_F v_0 v_1 : \tau'$

by *static hole typing*

- 2.
- $\vdash_F v_0 : \tau_d \Rightarrow \tau_c$

 $\wedge \vdash_F v_1 : \tau_d$ by *inversion*

- 3.
- $v_0 = \lambda(x:\tau'_d). e'$

 $\vee v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) \lambda x. e'$ $\vee v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) \lambda(x:\tau_x). e'$ by *canonical forms*

- 4.
- IF**
- $v_0 = \lambda(x:\tau'_d). e'$
- :

- a.
- $e \rightarrow_{F-S} E^*[e'[x \leftarrow v_1]]$

by $v_0 v_1 \triangleright_{S-1} e'[x \leftarrow v_1]$

- b. QED

IF $v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) \lambda x. e'$ $\wedge X(\tau'_d, v_1) = v'_1 :$

- a.
- $e \rightarrow_{F-S} E^*[\text{dyn } \tau'_c (e'[x \leftarrow v'_1])]$

by $v_0 v_1 \triangleright_{S-1} \text{dyn } \tau'_c (e'[x \leftarrow v'_1])$

- b. QED

IF $v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) \lambda x. e'$ $\wedge X(\tau'_d, v_1) = \text{BndryErr} :$

- a.
- $e \rightarrow_{F-S} \text{BndryErr}$

by $v_0 v_1 \triangleright_{S-1} \text{BndryErr}$

- b. QED

IF $v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) \lambda(x:\tau_x). e'$ $\wedge X(\tau_x, v_1) = v'_1 :$

- a.
- $e \rightarrow_{F-S} E^*[\text{stat } \tau'_c (\text{chk } \tau'_c e'[x \leftarrow v'_1])]$

by $v_0 v_1 \triangleright_{S-1} \text{stat } \tau'_c (\text{chk } \tau'_c e'[x \leftarrow v'_1])$

- b. QED

ELSE $v_0 = \text{mon}(\tau'_d \Rightarrow \tau'_c) \lambda(x:\tau_x). e'$ $\wedge X(\tau_x, v_1) = \text{BndryErr} :$

- a.
- $e \rightarrow_{F-S} \text{BndryErr}$

by $v_0 v_1 \triangleright_{S-1} \text{BndryErr}$

- b. QED

CASE $e = E^*[op^1 v]$:

- 1.
- $\vdash_F op^1 v : \tau'$

by *static hole typing*

- 2.
- $\vdash_F v : \tau_0 \times \tau_1$

by *inversion*

- 3.
- $v = \langle v_0, v_1 \rangle$

 $\vee v = \text{mon}(\tau'_0 \times \tau'_1) \langle v_0, v_1 \rangle$ by *canonical forms*

- 4.
- IF**
- $v = \langle v_0, v_1 \rangle$

 $\wedge op^1 = \text{fst} :$

- a.
- $\delta(\text{fst}, \langle v_0, v_1 \rangle) = v_0$

- b.
- $e \rightarrow_{F-S} E^*[v_0]$

by $op^1 v \triangleright_{S-1} v_0$

- c. QED

IF $v = \langle v_0, v_1 \rangle$ $\wedge op^1 = \text{snd} :$

- a.
- $\delta(\text{snd}, \langle v_0, v_1 \rangle) = v_1$

- b.
- $e \rightarrow_{F-S} E^*[v_1]$

by $op^1 v \triangleright_{S-1} v_1$

- c. QED

IF $v = \text{mon}(\tau'_0 \times \tau'_1) \langle v_0, v_1 \rangle$ $\wedge op^1 = \text{fst}$ $\wedge X(\tau'_0, v_0) = v'_0 :$

- a.
- $e \rightarrow_{F-S} E^*[v'_0]$

by $\text{fst } v \triangleright_{S-1} v'_0$

- b. QED

IF $v = \text{mon}(\tau'_0 \times \tau'_1) \langle v_0, v_1 \rangle$ $\wedge op^1 = \text{fst}$ $\wedge X(\tau'_0, v_0) = \text{BndryErr} :$

- a.
- $e \rightarrow_{F-S} \text{BndryErr}$

by $\text{fst } v \triangleright_{S-1} \text{BndryErr}$

- b. QED

IF $v = \text{mon}(\tau'_0 \times \tau'_1) \langle v_0, v_1 \rangle$ $\wedge op^1 = \text{snd}$ $\wedge X(\tau'_1, v_1) = v'_1 :$

- a.
- $e \rightarrow_{F-S} E^*[v'_1]$

by $\text{snd } v \triangleright_{S-1} v'_1$

- b. QED

ELSE $v = \text{mon}(\tau'_0 \times \tau'_1) \langle v_0, v_1 \rangle$ $\wedge op^1 = \text{snd}$ $\wedge X(\tau'_1, v_1) = \text{BndryErr} :$

- a.
- $e \rightarrow_{F-S} \text{BndryErr}$

by $\text{snd } v \triangleright_{S-1} \text{BndryErr}$

- b. QED

CASE $e = E^*[op^2 v_0 v_1]$:

- 1.
- $\vdash_F op^2 v_0 v_1 : \tau'$

by *static hole typing*

- 2.
- $\vdash_F v_0 : \tau_0$

 $\wedge \vdash_F v_1 : \tau_1$ $\wedge \Delta(op^2, \tau_0, \tau_1) = \tau''$ by *inversion*

- 3.
- $\delta(op^2, v_0, v_1) = e'$

by Δ *type soundness* (2)

10011 4. $op^2 v_0 v_1 \triangleright_{S-1} e'$
 10012 by (3)
 10013 5. QED by $e \rightarrow_{F-S} E^\bullet[e']$
 10014 **CASE** $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :
 10015 1. e' is a value
 10016 $\vee e' \in \text{Err}$
 10017 $\vee e' \rightarrow_{F-D} e''$
 10018 $\vee e' \rightarrow_{F-D} \text{BndryErr}$
 10019 $\vee e' = E'[e'']$ and $e'' \triangleright_{D-1} \text{TagErr}$
 10020 by *dynamic progress*
 10021 2. **IF** e' is a value :
 10022 a. QED $e \rightarrow_{F-S} E[\mathcal{D}_F(\tau', e')]$
 10023 **IF** $e' \in \text{Err}$:
 10024 a. QED $e \rightarrow_{F-S} e'$
 10025 **IF** $e' \rightarrow_{F-D} e''$:
 10026 a. QED $e \rightarrow_{F-S} E[\text{dyn } \tau' e'']$
 10027 **IF** $e' \rightarrow_{F-D} \text{BndryErr}$:
 10028 a. QED $e \rightarrow_{F-S} E[\text{dyn } \tau' \text{BndryErr}]$
 10029 **ELSE** $e' = E'[e'']$ and $e'' \triangleright_{D-1} \text{TagErr}$:
 10030 a. $E' \in E^\bullet$
 10031 by e' is boundary-free
 10032 b. QED
 10033 **CASE** $e = E[\text{stat } \tau' e']$ and e' is boundary-free :
 10034 1. e' is a value
 10035 $\vee e' \in \text{Err}$
 10036 $\vee e' \rightarrow_{F-S} e''$
 10037 $\vee e' \rightarrow_{F-S} \text{BndryErr}$
 10038 $\vee e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{D-1} \text{TagErr}$
 10039 by *static progress*
 10040 2. **IF** e' is a value :
 10041 a. QED $e \rightarrow_{F-S} E[\mathcal{S}_F(\tau', e')]$
 10042 **IF** $e' \in \text{Err}$:
 10043 a. QED $e \rightarrow_{F-S} e'$
 10044 **IF** $e' \rightarrow_{F-S} e''$:
 10045 a. QED $e \rightarrow_{F-S} E[\text{stat } \tau' e'']$
 10046 **IF** $e' \rightarrow_{F-S} \text{BndryErr}$:
 10047 a. QED $e \rightarrow_{F-S} E[\text{stat } \tau' \text{BndryErr}]$
 10048 **ELSE** $e' = E''[\text{dyn } \tau'' E^{\bullet\bullet}[e'']]$ and $e'' \triangleright_{D-1} \text{TagErr}$
 10049 :
 10050 a. Contradiction by e' is boundary-free
 10051 **CASE** $e = E[\text{Err}]$:
 10052 1. QED $e \rightarrow_{F-S} \text{Err}$
 10053 **CASE** $e = E^\bullet[\text{chk } \tau' v]$:
 10054 **IF** $X(\tau, v) = v'$:
 10055 1. $e \rightarrow_{F-S} E^\bullet[v']$
 10056 by $(\text{chk } \tau v) \triangleright_{S-1} v'$
 10057 2. QED
 10058 **ELSE** $X(\tau, v) = \text{BndryErr}$:
 10059 1. $e \rightarrow_{F-S} \text{BndryErr}$
 10060 by $(\text{chk } \tau v) \triangleright_{S-1} \text{BndryErr}$
 10061 2. QED
 10062 \square

10063 **Lemma 6.9** : HF *dynamic progress*
 10064
 10065

If $\vdash_F e$ then one of the following holds:

- e is a value
- $e \in \text{Err}$
- $e \rightarrow_{F-D} e'$
- $e \rightarrow_{F-D} \text{BndryErr}$
- $e \rightarrow_{F-D} \text{TagErr}$

Proof:

By the *boundary factoring* lemma, there are seven cases.

CASE e is a value :

1. QED

CASE $e = E^\bullet[v_0 v_1]$:

IF $v_0 = \lambda x. e'$:

1. $e \rightarrow_{F-D} E^\bullet[e'[x \leftarrow v_1]]$
by $v_0 v_1 \triangleright_{D-1} e'[x \leftarrow v_1]$

2. QED

IF $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c)(\lambda x. e')$:

1. $e \rightarrow_{F-D} E^\bullet[e'[x \leftarrow v_1]]$
by $v_0 v_1 \triangleright_{D-1} e'[x \leftarrow v_1]$

2. QED

IF $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c)(\lambda(x : \tau_x). e')$

$\wedge X(\tau_x, v_1) = v'_1$:

1. $e \rightarrow_{F-D} E^\bullet[\text{stat } \tau_c (\text{chk } \tau_c e'[x \leftarrow v'_1])]$
by $v_0 v_1 \triangleright_{D-1} \text{stat } \tau_c (\text{chk } \tau_c e'[x \leftarrow v'_1])$

2. QED

IF $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c)(\lambda(x : \tau_x). e')$

$\wedge X(\tau_x, v_1) = \text{BndryErr}$:

1. $e \rightarrow_{F-D} \text{BndryErr}$
by $v_0 v_1 \triangleright_{D-1} \text{BndryErr}$

2. QED

IF $v_0 = \lambda(x : \tau_x). e'$:

1. Contradiction by $\vdash_F e$

ELSE $v_0 = i$

$\vee v_0 = \langle v, v' \rangle$

$\vee v_0 = \text{mon } \tau_0 \times \tau_1 v'$:

1. $e \rightarrow_{F-D} \text{TagErr}$
by $(v_0 v_1) \triangleright_{D-1} \text{TagErr}$

2. QED

CASE $e = E^\bullet[op^1 v]$:

IF $v = \text{mon } \tau_0 \times \tau_1 \langle v_0, v_1 \rangle$

$\wedge op^1 = \text{fst}$

$\wedge X(\tau_0, v_0) = v'_0$:

1. $e \rightarrow_{F-D} E^\bullet[v'_0]$
by $op^1 v \triangleright_{D-1} v'_0$

2. QED

IF $v = \text{mon } \tau_0 \times \tau_1 \langle v_0, v_1 \rangle$

$\wedge op^1 = \text{fst}$

$\wedge X(\tau_0, v_0) = \text{BndryErr}$:

1. $e \rightarrow_{F-D} \text{BndryErr}$
by $op^1 v \triangleright_{D-1} \text{BndryErr}$

2. QED

IF $v = \text{mon } \tau_0 \times \tau_1 \langle v_0, v_1 \rangle$

$\wedge op^1 = \text{snd}$

$\wedge X(\tau_1, v_1) = v'_1$:

10121 1. $e \rightarrow_{F-D} E^\bullet[v_1']$
 10122 by $op^1 v \triangleright_{D-1} v_1'$
 10123 2. QED
 10124 **IF** $v = \text{mon } \tau_0 \times \tau_1 \langle v_0, v_1 \rangle$
 10125 $\wedge op^1 = \text{snd}$
 10126 $\wedge X(\tau_1, v_1) = \text{BndryErr}$:
 10127 1. $e \rightarrow_{F-D} \text{BndryErr}$
 10128 by $op^1 v \triangleright_{D-1} \text{BndryErr}$
 10129 2. QED
 10130 **IF** $\delta(op^1, v) = e'$:
 10131 1. $(op^1 v) \triangleright_{D-1} e'$
 10132 2. QED by $e \rightarrow_{F-D} E^\bullet[e']$
 10133 **ELSE** $\delta(op^1, v)$ is undefined :
 10134 1. $e \rightarrow_{F-D} \text{TagErr}$
 10135 by $(op^1 v) \triangleright_{D-1} \text{TagErr}$
 10136 2. QED
 10137 **CASE** $e = E^\bullet[op^2 v_0 v_1]$:
 10138 **IF** $\delta(op^2, v_0, v_1) = e''$:
 10139 1. $op^2 v_0 v_1 \triangleright_{D-1} e''$
 10140 2. QED
 10141 **ELSE** $\delta(op^2, v_0, v_1)$ is undefined :
 10142 1. $e \rightarrow_{F-D} \text{TagErr}$
 10143 by $op^2 v_0 v_1 \triangleright_{D-1} \text{TagErr}$
 10144 2. QED
 10145 **CASE** $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :
 10146 1. e' is a value
 10147 $\vee e' \in \text{Err}$
 10148 $\vee e' \rightarrow_{F-D} e''$
 10149 $\vee e' \rightarrow_{F-D} \text{BndryErr}$
 10150 $\vee e' = E^\bullet[e'']$ and $e'' \triangleright_{D-1} \text{TagErr}$
 10151 by *dynamic progress*
 10152 2. **IF** e' is a value :
 10153 a. QED $e \rightarrow_{F-D} E[\mathcal{D}_F(\tau', e')]$
 10154 **IF** $e' \in \text{Err}$:
 10155 a. QED $e \rightarrow_{F-D} e'$
 10156 **IF** $e' \rightarrow_{F-D} e''$:
 10157 a. QED $e \rightarrow_{F-S} E[\text{dyn } \tau' e'']$
 10158 **IF** $e' \rightarrow_{F-D} \text{BndryErr}$:
 10159 a. QED $e \rightarrow_{F-D} E[\text{dyn } \tau' \text{BndryErr}]$
 10160 **ELSE** $e' = E[e'']$ and $e'' \triangleright_{D-1} \text{TagErr}$:
 10161 a. $E \in E^\bullet$
 10162 by e' is boundary-free
 10163 b. QED
 10164 **CASE** $e = E[\text{stat } \tau' e']$ and e' is boundary-free :
 10165 1. e' is a value
 10166 $\vee e' \in \text{Err}$
 10167 $\vee e' \rightarrow_{F-S} e''$
 10168 $\vee e' \rightarrow_{F-S} \text{BndryErr}$
 10169 $\vee e' = E''[\text{dyn } \tau'' E'''[e'']]$ and $e'' \triangleright_{D-1} \text{TagErr}$
 10170 by *static progress*
 10171 2. **IF** e' is a value :
 10172 a. QED $e \rightarrow_{F-S} E[\mathcal{S}_F(\tau', e')]$
 10173 **IF** $e' \in \text{Err}$:
 10174
 10175

a. QED $e \rightarrow_{F-S} e'$
IF $e' \rightarrow_{F-S} e''$:
 a. QED $e \rightarrow_{F-S} E[\text{stat } \tau' e'']$
IF $e' \rightarrow_{F-S} \text{BndryErr}$:
 a. QED $e \rightarrow_{F-S} E[\text{stat } \tau' \text{BndryErr}]$
ELSE $e' = E''[\text{dyn } \tau'' E'''[e'']]$ and $e'' \triangleright_{D-1} \text{TagErr}$
 :
 a. Contradiction by e' is boundary-free

CASE $e = E[\text{Err}]$:

1. QED $e \rightarrow_{F-D} \text{Err}$

□

Lemma 6.10 : HF *static preservation*

■ If $\vdash_F e : \tau$ and $e \rightarrow_{F-S} e'$ then $\vdash_F e' : \tau$

Proof:

By the *boundary factoring* lemma there are eight cases.

CASE e is a value :

1. Contradiction by $e \rightarrow_{F-S} e'$

CASE $e = E^\bullet[v_0 v_1]$:

IF $v_0 = \lambda(x:\tau_x). e'$

$\wedge e \rightarrow_{F-S} e'[x \leftarrow v_1]$:

1. $\vdash_F v_0 v_1 : \tau'$

by *static hole typing*

2. $\vdash_F v_0 : \tau_d \Rightarrow \tau_c$

$\wedge \vdash_F v_1 : \tau_d$

$\wedge \tau_c \leq \tau'$

by *inversion*

3. $(x:\tau_x) \vdash_F e' : \tau_c$

by *inversion* (2)

4. $\tau_d \leq \tau_x$

by *canonical forms* (2)

5. $\vdash_F v_1 : \tau_x$

by (2, 4)

6. $\vdash_F e'[x \leftarrow v_1] : \tau_c$

by *substitution* (3, 5)

7. $\vdash_F e'[x \leftarrow v_1] : \tau'$

by (2, 6)

8. QED by *hole substitution*

IF $v_0 = \text{mon } \tau_d \Rightarrow \tau_c \lambda x. e'$

$\wedge e \rightarrow_{F-S} E^\bullet[\text{dyn } \tau_c ((\lambda x. e') (X(\tau_d, v_1)))]$:

1. $\vdash_F v_0 v_1 : \tau'$

by *static hole typing*

2. $\vdash_F v_0 : \tau'_d \Rightarrow \tau'_c$

$\wedge \tau'_c \leq \tau'$

by *inversion*

3. $\tau_d \Rightarrow \tau_c \leq \tau'_d \Rightarrow \tau'_c$

by *canonical forms* (2)

4. $\vdash_F \lambda x. e'$

by *inversion* (2)

5. $\tau'_d \leq \tau_d$

$\wedge \tau_c \leq \tau'_c$

by (3)

6. $\vdash_F X(\tau_d, v_1)$

by *X soundness*

10231	7. $\vdash_{\mathbb{F}} (\lambda x. e') \mathcal{X}(\tau_d, v_1)$	2. $\vdash_{\mathbb{F}} \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$	10286
10232	by (4, 6)	$\wedge \tau_1 \leq \tau'$	10287
10233	8. $\vdash_{\mathbb{F}} \text{dyn } \tau_c ((\lambda x. e') \mathcal{X}(\tau_d, v_1)) : \tau_c$	by <i>inversion</i>	10288
10234	by (7)	3. $\vdash_{\mathbb{F}} v_1 : \tau_1$	10289
10235	9. $\vdash_{\mathbb{F}} \text{dyn } \tau_c ((\lambda x. e') \mathcal{X}(\tau_d, v_1)) : \tau'$	by <i>inversion</i>	10290
10236	by (2, 5, 8)	4. $\vdash_{\mathbb{F}} v_1 : \tau'$	10291
10237	10. QED by <i>hole substitution</i>	by (2)	10292
10238	ELSE $v_0 = \text{mon } \tau_d \Rightarrow \tau_c (\lambda(x:\tau_x). e')$	5. QED by <i>hole substitution</i>	10293
10239	$\wedge e \rightarrow_{\mathbb{F}\text{-S}} E^*[\text{stat } \tau_c (\text{chk } \tau_c ((\lambda(x:\tau_x). e') \mathcal{X}(\tau_x, v_1)))]$	IF $v = \text{mon } (\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	10294
10240	:	$\wedge \text{op}^1 = \text{fst}$	10295
10241	1. $\vdash_{\mathbb{F}} v_0 v_1 : \tau'$	$\wedge e \rightarrow_{\mathbb{F}\text{-S}} E^*[\mathcal{X}(\tau_0, v_0)] :$	10296
10242	by <i>static hole typing</i>	1. $\vdash_{\mathbb{F}} \text{fst } v : \tau'$	10297
10243	2. $\vdash_{\mathbb{F}} v_0 : \tau'_d \Rightarrow \tau'_c$	by <i>static hole typing</i>	10298
10244	$\wedge \vdash_{\mathbb{F}} v_1 : \tau'_d$	2. $\vdash_{\mathbb{F}} v : \tau'_0 \times \tau'_1$	10299
10245	$\wedge \tau'_c \leq \tau'$	$\wedge \tau'_0 < \tau'$	10300
10246	by <i>inversion</i>	by <i>inversion</i> (1)	10301
10247	3. $\vdash_{\mathbb{F}} \lambda(x:\tau_x). e' : \tau_x \Rightarrow \tau'_x$	3. $\tau_0 \leq \tau'_0$	10302
10248	by <i>inversion</i>	by <i>canonical forms</i> (2)	10303
10249	4. $\tau_d \Rightarrow \tau_c \leq \tau'_d \Rightarrow \tau'_c$	4. $\vdash_{\mathbb{F}} \langle v_0, v_1 \rangle$	10304
10250	by <i>canonical forms</i> (2)	$\vee \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle : \tau''$	10305
10251	5. $\tau_c \leq \tau'_c$	by <i>inversion</i> (2)	10306
10252	by (4)	5. $\vdash_{\mathbb{F}} v_0$	10307
10253	6. $\vdash_{\mathbb{F}} \mathcal{X}(\tau_x, v_1) : \tau_x$	$\vee \vdash_{\mathbb{F}} v_0 : \tau'''$	10308
10254	by <i>X soundness</i>	by <i>inversion</i> (4)	10309
10255	7. $\vdash_{\mathbb{F}} (\lambda(x:\tau_x). e') \mathcal{X}(\tau_x, v_1) : \tau'_x$	6. $\vdash_{\mathbb{F}} \mathcal{X}(\tau_0, v_0) : \tau_0$	10310
10256	by (3, 6)	by <i>X soundness</i> (5)	10311
10257	8. $\vdash_{\mathbb{F}} \text{chk } \tau_c ((\lambda(x:\tau_x). e') \mathcal{X}(\tau_x, v_1)) : \tau_c$	7. $\vdash_{\mathbb{F}} \mathcal{X}(\tau_0, v_0) : \tau'$	10312
10258	by (7)	by (2, 3, 6)	10313
10259	9. $\vdash_{\mathbb{F}} \text{stat } \tau_c (\text{chk } \tau_c ((\lambda(x:\tau_x). e') \mathcal{X}(\tau_x, v_1))) : \tau_c$	8. QED by <i>hole substitution</i>	10314
10260	by (8)	ELSE $v = \text{mon } (\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	10315
10261	10. $\vdash_{\mathbb{F}} \text{stat } \tau_c (\text{chk } \tau_c ((\lambda(x:\tau_x). e') \mathcal{X}(\tau_x, v_1))) : \tau'$	$\wedge \text{op}^1 = \text{snd}$	10316
10262	by (2, 5, 9)	$\wedge e \rightarrow_{\mathbb{F}\text{-S}} E^*[\mathcal{X}(\tau_1, v_1)] :$	10317
10263	11. QED by <i>hole substitution</i>	1. $\vdash_{\mathbb{F}} \text{snd } v : \tau'$	10318
10264	CASE $e = E^*[\text{op}^1 v] :$	by <i>static hole typing</i>	10319
10265	IF $v = \langle v_0, v_1 \rangle$	2. $\vdash_{\mathbb{F}} v : \tau'_0 \times \tau'_1$	10320
10266	$\wedge \text{op}^1 = \text{fst}$	$\wedge \tau'_1 < \tau'$	10321
10267	$\wedge e \rightarrow_{\mathbb{F}\text{-S}} E^*[v_0] :$	by <i>inversion</i> (1)	10322
10268	1. $\vdash_{\mathbb{F}} \text{fst } \langle v_0, v_1 \rangle : \tau'$	3. $\tau_1 \leq \tau'_1$	10323
10269	by <i>static hole typing</i>	by <i>canonical forms</i> (2)	10324
10270	2. $\vdash_{\mathbb{F}} \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$	4. $\vdash_{\mathbb{F}} \langle v_0, v_1 \rangle$	10325
10271	$\wedge \tau_0 \leq \tau'$	$\vee \vdash_{\mathbb{F}} \langle v_0, v_1 \rangle : \tau''$	10326
10272	by <i>inversion</i>	by <i>inversion</i> (2)	10327
10273	3. $\vdash_{\mathbb{F}} v_0 : \tau_0$	5. $\vdash_{\mathbb{F}} v_1$	10328
10274	by <i>inversion</i>	$\vee \vdash_{\mathbb{F}} v_1 : \tau'''$	10329
10275	4. $\vdash_{\mathbb{F}} v_0 : \tau'$	by <i>inversion</i> (4)	10330
10276	by (2)	6. $\vdash_{\mathbb{F}} \mathcal{X}(\tau_1, v_1) : \tau_1$	10331
10277	5. QED by <i>hole substitution</i>	by <i>X soundness</i> (5)	10332
10278	IF $v = \langle v_0, v_1 \rangle$	7. $\vdash_{\mathbb{F}} \mathcal{X}(\tau_1, v_1) : \tau'$	10333
10279	$\wedge \text{op}^1 = \text{snd}$	by (2, 3, 6)	10334
10280	$\wedge e \rightarrow_{\mathbb{F}\text{-S}} E^*[v_1] :$	8. QED by <i>hole substitution</i>	10335
10281	1. $\vdash_{\mathbb{F}} \text{snd } \langle v_0, v_1 \rangle : \tau'$	CASE $e = E^*[\text{op}^2 v_0 v_1]$	10336
10282	by <i>static hole typing</i>	$\wedge \delta(\text{op}^2, v_0, v_1) = v$	10337
10283		$\wedge e \rightarrow_{\mathbb{F}\text{-S}} E^*[v] :$	10338
10284			10339
10285			10340

10341 1. $\vdash_F op^2 v_0 v_1 : \tau'$
 10342 by *static hole typing*
 10343 2. $\vdash_F v_0 : \tau_0$
 10344 $\wedge \vdash_F v_1 : \tau_1$
 10345 $\wedge \Delta(op^2, \tau_0, \tau_1) = \tau''$
 10346 $\wedge \tau'' \leq \tau'$
 10347 by *inversion*
 10348 3. $\vdash_F v : \tau''$
 10349 by Δ *type soundness* (2)
 10350 4. $\vdash_F v : \tau'$
 10351 by (2, 3)
 10352 5. QED by *hole substitution* (4)
 10353 **CASE** $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :
 10354 **IF** e' is a value :
 10355 1. $e \rightarrow_{F-S} E[\mathcal{D}_F(\tau', e')]$
 10356 2. $\vdash_F \text{dyn } \tau' e' : \tau'$
 10357 by *boundary hole typing*
 10358 3. $\vdash_F e'$
 10359 by *inversion* (2)
 10360 4. $\vdash_F \mathcal{D}_F(\tau', e') : \tau'$
 10361 by \mathcal{D}_F *soundness* (3)
 10362 5. QED by *hole substitution* (4)
 10363 **ELSE** $e' \rightarrow_{F-D} e''$:
 10364 1. $e \rightarrow_{F-S} E[\text{dyn } \tau' e'']$
 10365 2. $\vdash_F \text{dyn } \tau' e' : \tau'$
 10366 by *boundary hole typing*
 10367 3. $\vdash_F e'$
 10368 by *inversion* (2)
 10369 4. $\vdash_F e''$
 10370 by *dynamic preservation* (3)
 10371 5. $\vdash_F \text{dyn } \tau' e'' : \tau'$
 10372 by (4)
 10373 6. QED by *hole substitution* (5)
 10374 **CASE** $e = E[\text{stat } \tau' e']$ and e' is boundary-free :
 10375 **IF** e' is a value :
 10376 1. $e \rightarrow_{F-S} E[\mathcal{S}_F(\tau', e')]$
 10377 2. $\vdash_F \text{stat } \tau' e'$
 10378 by *boundary hole typing*
 10379 3. $\vdash_F e' : \tau'$
 10380 by *inversion* (2)
 10381 4. $\vdash_F \mathcal{S}_F(\tau', e')$
 10382 by \mathcal{S}_F *soundness* (3)
 10383 5. QED by *hole substitution* (4)
 10384 **ELSE** $e' \rightarrow_{F-S} e''$:
 10385 1. $e \rightarrow_{F-S} E[\text{stat } \tau' e'']$
 10386 2. $\vdash_F \text{stat } \tau' e'$
 10387 by *boundary hole typing*
 10388 3. $\vdash_F e' : \tau'$
 10389 by *inversion* (2)
 10390 4. $\vdash_F e'' : \tau'$
 10391 by *static preservation* (3)
 10392 5. $\vdash_F \text{stat } \tau' e''$
 10393 by (4)
 10394
 10395

6. QED by *hole substitution* (5)
CASE $e = E[\text{Err}]$:
 1. $e \rightarrow_{F-S} \text{Err}$
 2. QED by $\vdash_F \text{Err} : \tau$
CASE $e = E^\bullet[\text{chk } \tau v]$:
 1. $\vdash_F \text{chk } \tau v : \tau$
 by *static hole typing*
 2. $\vdash_F v : \tau'$
 by *inversion* (1)
 3. $\vdash_F X(\tau, v') : \tau$
 by X *soundness* (2)
 4. QED by *hole substitution* (3)
 □
Lemma 6.11 : HF *dynamic preservation*
 If $\vdash_F e$ and $e \rightarrow_{F-D} e'$ then $\vdash_F e'$
Proof:
 By the *boundary factoring* lemma, there are seven cases.
CASE e is a value :
 1. Contradiction by $e \rightarrow_{F-D} e'$
CASE $e = E^\bullet[v_0 v_1]$:
IF $v_0 = \lambda x. e'$
 $\wedge e \rightarrow_{F-D} E^\bullet[e'[x \leftarrow v_1]]$:
 1. $\vdash_F v_0 v_1$
 by *dynamic hole typing*
 2. $\vdash_F v_0$
 $\wedge \vdash_F v_1$
 by *inversion* (1)
 3. $x \vdash_F e'$
 by *inversion* (2)
 4. $\vdash_F e'[x \leftarrow v_1]$
 by *substitution* (2, 3)
 5. QED *hole substitution* (4)
IF $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) \lambda x. e'$
 $\wedge e \rightarrow_{F-D} E^\bullet[(\lambda x. e') v_1]$:
 1. $\vdash_F v_0 v_1$
 by *dynamic hole typing*
 2. $\vdash_F v_0$
 $\wedge \vdash_F v_1$
 by *inversion* (1)
 3. $\vdash_F (\lambda x. e') v_1$
 by (2)
 4. QED *hole substitution* (5)
ELSE $v_0 = \text{mon}(\tau_d \Rightarrow \tau_c) \lambda(x : \tau_x). e'$
 $\wedge e \rightarrow_{F-D} E^\bullet[\text{stat } \tau_c (\text{chk } \tau_c ((\lambda(x : \tau_x). e') X(\tau_x, v_1)))]$:
 1. $\vdash_F v_0 v_1$
 by *dynamic hole typing*
 2. $\vdash_F v_0$
 $\wedge \vdash_F v_1$
 by *inversion*
 3. $\vdash_F \lambda(x : \tau_x). e' : \tau_x \Rightarrow \tau'_x$
 by *inversion* (2)

10451	4. $\vdash_F X(\tau_x, v_1) : \tau_x$	4. $\vdash_F X(\tau_1, v_1)$	10506
10452	by X soundness (2)	by X soundness (3)	10507
10453	5. $\vdash_F ((\lambda(x:\tau_x). e') X(\tau_x, v_1)) : \tau'_x$	5. QED by hole substitution	10508
10454	by (3, 4)	CASE $e = E^\bullet[op^2 v_0 v_1]$	10509
10455	6. $\vdash_F \text{chk } \tau_c ((\lambda(x:\tau_x). e') X(\tau_x, v_1)) : \tau_c$	$\wedge \delta(op^2, v_0, v_1) = v$	10510
10456	by (5)	$\wedge e \rightarrow_{F-D} E^\bullet[v] :$	10511
10457	7. $\vdash_F \text{stat } \tau_c (\text{chk } \tau_c ((\lambda(x:\tau_x). e') X(\tau_x, v_1)))$	1. $\vdash_F op^2 v_0 v_1$	10512
10458	by (6)	by dynamic hole typing	10513
10459	8. QED hole substitution	2. $\vdash_F v_0$	10514
10460	CASE $e = E^\bullet[op^1 v] :$	$\wedge \vdash_F v_1$	10515
10461	IF $v = \langle v_0, v_1 \rangle$	by inversion (1)	10516
10462	$\wedge op^1 = \text{fst}$	3. $\vdash_F v$	10517
10463	$\wedge e \rightarrow_{F-D} E^\bullet[v_0] :$	by δ preservation (2)	10518
10464	1. $\vdash_F op^1 v$	4. QED by hole substitution (3)	10519
10465	by dynamic hole typing	CASE $e = E[\text{dyn } \tau' e']$ and e' is boundary-free :	10520
10466	2. $\vdash_F v$	IF e' is a value :	10521
10467	by inversion (1)	1. $e \rightarrow_{F-D} E[\mathcal{D}_F(\tau', e')]$	10522
10468	3. $\vdash_F v_0$	2. $\vdash_F \text{dyn } \tau' e' : \tau'$	10523
10469	by inversion (2)	by boundary hole typing	10524
10470	4. QED by hole substitution	3. $\vdash_F e'$	10525
10471	IF $v = \langle v_0, v_1 \rangle$	by inversion (2)	10526
10472	$\wedge op^1 = \text{snd}$	4. $\vdash_F \mathcal{D}_F(\tau', e') : \tau'$	10527
10473	$\wedge e \rightarrow_{F-D} E^\bullet[v_1] :$	by \mathcal{D}_F soundness (3)	10528
10474	1. $\vdash_F op^1 v$	5. QED by hole substitution (4)	10529
10475	by dynamic hole typing	ELSE $e' \rightarrow_{F-D} e'' :$	10530
10476	2. $\vdash_F v$	1. $e \rightarrow_{F-D} E[\text{dyn } \tau' e'']$	10531
10477	by inversion (1)	2. $\vdash_F \text{dyn } \tau' e' : \tau'$	10532
10478	3. $\vdash_F v_1$	by boundary hole typing	10533
10479	by inversion (2)	3. $\vdash_F e'$	10534
10480	4. QED by hole substitution	$\wedge \tau' \leq \tau''$	10535
10481	IF $v = \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	by inversion (2)	10536
10482	$\wedge op^1 = \text{fst}$	4. $\vdash_F e''$	10537
10483	$\wedge e \rightarrow_{F-D} E^\bullet[X(\tau_0, v_0)] :$	by dynamic preservation (3)	10538
10484	1. $\vdash_F op^1 v$	5. $\vdash_F \text{dyn } \tau' e'' : \tau'$	10539
10485	by dynamic hole typing	by (4)	10540
10486	2. $\vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	6. QED by hole substitution (5)	10541
10487	by inversion (1)	CASE $e = E[\text{stat } \tau' e']$ and e' is boundary-free :	10542
10488	3. $\vdash_F v_0$	IF $e' \in v :$	10543
10489	$\vee \vdash_F v_0 : \tau'_0$	1. $e \rightarrow_{F-D} E[\mathcal{S}_F(\tau', e')]$	10544
10490	by inversion (2)	2. $\vdash_F \text{stat } \tau' e'$	10545
10491	4. $\vdash_F X(\tau_0, v_0)$	by boundary hole typing	10546
10492	by X soundness (3)	3. $\vdash_F e' : \tau'$	10547
10493	5. QED by hole substitution	by inversion (2)	10548
10494	ELSE $v = \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	4. $\vdash_F \mathcal{S}_F(\tau', e')$	10549
10495	$\wedge op^1 = \text{snd}$	by \mathcal{S}_F soundness (3)	10550
10496	$\wedge e \rightarrow_{F-D} E^\bullet[X(\tau_1, v_1)] :$	5. QED by hole substitution (5)	10551
10497	1. $\vdash_F op^1 v$	ELSE $e' \rightarrow_{F-S} e'' :$	10552
10498	by dynamic hole typing	1. $e \rightarrow_{F-D} E[\text{stat } \tau' e'']$	10553
10499	2. $\vdash_F \text{mon}(\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$	2. $\vdash_F \text{stat } \tau' e'$	10554
10500	by inversion (1)	by boundary hole typing	10555
10501	3. $\vdash_F v_1$	3. $\vdash_F e' : \tau'$	10556
10502	$\vee \vdash_F v_1 : \tau'_1$	by inversion (2)	10557
10503	by inversion (2)	4. $\vdash_F e'' : \tau'$	10558
10504		by static preservation (3)	10559
10505			10560

10561 5. $\vdash_F \text{stat } \tau' e''$
 10562 by (4)
 10563 6. QED by *hole substitution* (5)
 10564 **CASE** $e = E[\text{Err}]$:
 10565 1. $e \rightarrow_{F-D} \text{Err}$
 10566 2. QED $\vdash_F \text{Err}$
 10567 \square
 10568 **Lemma 6.12** : HF *static boundary factoring*
 10569 If $\vdash_F e : \tau$ then one of the following holds:
 10570 • e is a value
 10571 • $e = E^\bullet[v_0 v_1]$
 10572 • $e = E^\bullet[op^1 v]$
 10573 • $e = E^\bullet[op^2 v_0 v_1]$
 10574 • $e = E^\bullet[\text{chk } \tau v]$
 10575 • $e = E[\text{dyn } \tau e']$ where e' is boundary-free
 10576 • $e = E[\text{stat } \tau e']$ where e' is boundary-free
 10577 • $e = E[\text{Err}]$

10578 *Proof*:

10579 By the *unique static evaluation contexts* lemma, there are
 10580 eight cases.
 10581 **CASE** e is a value :
 10582 1. QED
 10583 **CASE** $e = E[v_0 v_1]$:
 10584 1. $E = E^\bullet$
 10585 $\vee E = E'[\text{dyn } \tau E^\bullet]$
 10586 $\vee E = E'[\text{stat } \tau E^\bullet]$
 10587 by *inner boundary*
 10588 2. **IF** $E = E^\bullet$:
 10589 a. QED $e = E^\bullet[v_0 v_1]$
 10590 **IF** $E = E'[\text{dyn } \tau E^\bullet]$:
 10591 a. QED $e = E'[\text{dyn } \tau E^\bullet[v_0 v_1]]$
 10592 **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:
 10593 a. QED $e = E'[\text{stat } \tau E^\bullet[v_0 v_1]]$
 10594 **CASE** $e = E[op^1 v]$:
 10595 1. $E = E^\bullet$
 10596 $\vee E = E'[\text{dyn } \tau E^\bullet]$
 10597 $\vee E = E'[\text{stat } \tau E^\bullet]$
 10598 by *inner boundary*
 10599 2. **IF** $E = E^\bullet$:
 10600 a. QED $e = E^\bullet[op^1 v]$
 10601 **IF** $E = E'[\text{dyn } \tau E^\bullet]$:
 10602 a. QED $e = E'[\text{dyn } \tau E^\bullet[op^1 v]]$
 10603 **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:
 10604 a. QED $e = E'[\text{stat } \tau E^\bullet[op^1 v]]$
 10605 **CASE** $e = E[op^2 v_0 v_1]$:
 10606 1. $E = E^\bullet$
 10607 $\vee E = E'[\text{dyn } \tau E^\bullet]$
 10608 $\vee E = E'[\text{stat } \tau E^\bullet]$
 10609 by *inner boundary*
 10610 2. **IF** $E = E^\bullet$:
 10611 a. QED $e = E^\bullet[op^2 v_0 v_1]$
 10612 **IF** $E = E'[\text{dyn } \tau E^\bullet]$:
 10613 a. QED $e = E'[\text{dyn } \tau E^\bullet[op^2 v_0 v_1]]$
 10614 **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:
 10615

a. QED $e = E'[\text{stat } \tau E^\bullet[op^2 v_0 v_1]]$
 10616
 10617 **CASE** $e = E[\text{chk } \tau v]$:
 10618 1. $E = E^\bullet$
 10619 $\vee E = E'[\text{dyn } \tau E^\bullet]$
 10620 $\vee E = E'[\text{stat } \tau E^\bullet]$
 10621 by *inner boundary*
 10622 2. **IF** $E = E^\bullet$:
 10623 a. QED $e = E^\bullet[\text{chk } \tau v]$
 10624 **IF** $E = E'[\text{dyn } \tau E^\bullet]$:
 10625 a. Contradiction by $\vdash_F e : \tau$
 10626 **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:
 10627 a. QED $e = E'[\text{stat } \tau E^\bullet[\text{chk } \tau v]]$
 10628 **CASE** $e = E[\text{dyn } \tau v]$:
 10629 1. QED v is boundary-free
 10630 **CASE** $e = E[\text{stat } \tau v]$:
 10631 1. QED v is boundary-free
 10632 **CASE** $e = E[\text{Err}]$:
 10633 1. QED
 10634 \square

10635 **Lemma 6.13** : HF *unique static evaluation contexts*

10636 If $\vdash_F e : \tau$ then one of the following holds:

- 10637 • e is a value
- 10638 • $e = E[v_0 v_1]$
- 10639 • $e = E[op^1 v]$
- 10640 • $e = E[op^2 v_0 v_1]$
- 10641 • $e = E[\text{chk } \tau v]$
- 10642 • $e = E[\text{dyn } \tau v]$
- 10643 • $e = E[\text{stat } \tau v]$
- 10644 • $e = E[\text{Err}]$

10645 *Proof*:

10646 By induction on the structure of e .

10647 **CASE** $e = x$
 10648 $\vee e = \lambda x. e'$
 10649 $\vee e = \text{stat } \tau e'$
 10650 1. Contradiction by $\vdash_F e : \tau$
 10651 **CASE** $e = i$
 10652 $\vee e = \lambda(x : \tau_d). e'$
 10653 $\vee e = \text{mon}(\tau_d \Rightarrow \tau_c) v$
 10654 1. QED e is a value
 10655 **CASE** $e = \langle e_0, e_1 \rangle$:
 10656 **IF** $e_0 \notin v$:
 10657 1. $\vdash_F e_0 : \tau_0$
 10658 by *inversion*
 10659 2. $e_0 = E_0[e'_0]$
 10660 by the induction hypothesis (1)
 10661 3. $E = \langle E_0, e_1 \rangle$
 10662 4. QED $e = E[e'_0]$
 10663 **IF** $e_0 \in v$
 10664 $\wedge e_1 \notin v$:
 10665 1. $\vdash_F e_1 : \tau_1$
 10666 by *inversion*
 10667 2. $e_1 = E_1[e'_1]$
 10668 by the induction hypothesis (1)
 10669 3. $E = \langle e_0, E_1 \rangle$
 10670

10671 4. QED $e = E[e'_1]$
 10672 **ELSE** $e_0 \in v$
 10673 $\wedge e_1 \in v :$
 10674 1. $E = []$
 10675 2. QED e is a value
 10676 **CASE** $e = e_0 e_1 :$
 10677 **IF** $e_0 \notin v :$
 10678 1. $\vdash_F e_0 : \tau_0$
 10679 by *inversion*
 10680 2. $e_0 = E_0[e'_0]$
 10681 by the induction hypothesis (1)
 10682 3. $E = E_0 e_1$
 10683 4. QED $e = E[e'_0]$
 10684 **IF** $e_0 \in v$
 10685 $\wedge e_1 \notin v :$
 10686 1. $\vdash_F e_1 : \tau_1$
 10687 by *inversion*
 10688 2. $e_1 = E_1[e'_1]$
 10689 by the induction hypothesis (1)
 10690 3. $E = e_0 E_1$
 10691 4. QED $e = E[e'_1]$
 10692 **ELSE** $e_0 \in v$
 10693 $\wedge e_1 \in v :$
 10694 1. $E = []$
 10695 2. QED $e = E[e_0 e_1]$
 10696 **CASE** $e = op^1 e_0 :$
 10697 **IF** $e_0 \notin v :$
 10698 1. $\vdash_F e_0 : \tau_0$
 10699 by *inversion*
 10700 2. $e_0 = E_0[e'_0]$
 10701 by the induction hypothesis (1)
 10702 3. $E = op^1 E_0$
 10703 4. QED $e = E[e'_0]$
 10704 **ELSE** $e_0 \in v :$
 10705 1. $E = []$
 10706 2. QED $e = E[op^1 e_0]$
 10707 **CASE** $e = op^2 e_0 e_1 :$
 10708 **IF** $e_0 \notin v :$
 10709 1. $\vdash_F e_0 : \tau_0$
 10710 by *inversion*
 10711 2. $e_0 = E_0[e'_0]$
 10712 by the induction hypothesis (1)
 10713 3. $E = op^2 E_0 e_1$
 10714 4. QED $e = E[e'_0]$
 10715 **IF** $e_0 \in v$
 10716 $\wedge e_1 \notin v :$
 10717 1. $\vdash_F e_1 : \tau_1$
 10718 by *inversion*
 10719 2. $e_1 = E_1[e'_1]$
 10720 by the induction hypothesis (1)
 10721 3. $E = op^2 e_0 E_1$
 10722 4. QED $e = E[e'_1]$
 10723 **ELSE** $e_0 \in v$
 10724 $\wedge e_1 \in v :$
 10725

1. $E = []$
 2. QED $e = E[op^2 e_0 e_1]$
CASE $e = \text{chk } \tau e_0 :$
IF $e_0 \notin v :$
 1. $\vdash_F e_0 : \tau_0$
 by *inversion*
 2. $e_0 = E_0[e'_0]$
 by the induction hypothesis (1)
 3. $E = \text{chk } \tau E_0$
 4. QED $e = E[e'_0]$
ELSE $e_0 \in v :$
 1. $E = []$
 2. QED $e = E[\text{chk } \tau e_0]$
CASE $e = \text{dyn } \tau e_0 :$
IF $e_0 \notin v :$
 1. $\vdash_F e_0$
 by *inversion*
 2. $e_0 = E_0[e'_0]$
 by *unique dynamic evaluation contexts* (1)
 3. $E = \text{dyn } \tau E_0$
 4. QED $e = E[e'_0]$
ELSE $e_0 \in v :$
 1. $E = []$
 2. QED $e = E[\text{dyn } \tau e_0]$
CASE $e = \text{Err} :$
 1. $E = []$
 2. QED $e = E[\text{Err}]$

□

Lemma 6.14 : HF *inner boundary*For all contexts E , one of the following holds:

- $E = E^\bullet$
- $E = E'[\text{dyn } \tau E^\bullet]$
- $E = E'[\text{stat } \tau E^\bullet]$

Proof:By induction on the structure of E .**CASE** $E = E^\bullet :$

1. QED

CASE $E = E_0 e_1 :$ 1. $E_0 = E^\bullet$ $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$ $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$

by the induction hypothesis

2. **IF** $E_0 = E^\bullet :$ a. QED E is boundary-free**IF** $E_0 = E'_0[\text{dyn } \tau E^\bullet] :$ a. $E' = E'_0 e_1$ b. QED $E = E'[\text{dyn } \tau E^\bullet]$ **ELSE** $E_0 = E'_0[\text{stat } \tau E^\bullet] :$ a. $E' = E'_0 e_1$ b. QED $E = E'[\text{stat } \tau E^\bullet]$ **CASE** $E = v_0 E_1 :$ 1. $E_1 = E^\bullet$ $\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$

10781 $\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$
 10782 by the induction hypothesis
 10783 2. **IF** $E_1 = E^\bullet$:
 10784 a. QED E is boundary-free
 10785 **IF** $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:
 10786 a. $E' = v_0 E'_1$
 10787 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 10788 **ELSE** $E_1 = E'_1[\text{stat } \tau E^\bullet]$:
 10789 a. $E' = v_0 E'_1$
 10790 b. QED $E = E'[\text{stat } \tau E^\bullet]$
 10791 **CASE** $E = \langle E_0, e_1 \rangle$:
 10792 1. $E_0 = E^\bullet$
 10793 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
 10794 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
 10795 by the induction hypothesis
 10796 2. **IF** $E_0 = E^\bullet$:
 10797 a. QED E is boundary-free
 10798 **IF** $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:
 10799 a. $E' = \langle E'_0, e_1 \rangle$
 10800 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 10801 **ELSE** $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
 10802 a. $E' = \langle E'_0, e_1 \rangle$
 10803 b. QED $E = E'[\text{stat } \tau E^\bullet]$
 10804 **CASE** $E = \langle v_0, E_1 \rangle$:
 10805 1. $E_1 = E^\bullet$
 10806 $\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$
 10807 $\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$
 10808 by the induction hypothesis
 10809 2. **IF** $E_1 = E^\bullet$:
 10810 a. QED E is boundary-free
 10811 **IF** $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:
 10812 a. $E' = \langle v_0, E'_1 \rangle$
 10813 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 10814 **ELSE** $E_1 = E'_1[\text{stat } \tau E^\bullet]$:
 10815 a. $E' = \langle v_0, E'_1 \rangle$
 10816 b. QED $E = E'[\text{stat } \tau E^\bullet]$
 10817 **CASE** $E = op^1 E_0$:
 10818 1. $E_0 = E^\bullet$
 10819 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
 10820 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
 10821 by the induction hypothesis
 10822 2. **IF** $E_0 = E^\bullet$:
 10823 a. QED E is boundary-free
 10824 **IF** $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:
 10825 a. $E' = op^1 E'_0$
 10826 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 10827 **ELSE** $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
 10828 a. $E' = op^1 E'_0$
 10829 b. QED $E = E'[\text{stat } \tau E^\bullet]$
 10830 **CASE** $E = op^2 E_0 e_1$:
 10831 1. $E_0 = E^\bullet$
 10832 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
 10833
 10834
 10835

10836 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
 10837 by the induction hypothesis
 10838 2. **IF** $E_0 = E^\bullet$:
 10839 a. QED E is boundary-free
 10840 **IF** $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:
 10841 a. $E' = op^2 E'_0 e_1$
 10842 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 10843 **ELSE** $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
 10844 a. $E' = op^2 E'_0 e_1$
 10845 b. QED $E = E'[\text{stat } \tau E^\bullet]$
 10846 **CASE** $E = op^2 v_0 E_1$:
 10847 1. $E_1 = E^\bullet$
 10848 $\vee E_1 = E'_1[\text{dyn } \tau E^\bullet]$
 10849 $\vee E_1 = E'_1[\text{stat } \tau E^\bullet]$
 10850 by the induction hypothesis
 10851 2. **IF** $E_1 = E^\bullet$:
 10852 a. QED E is boundary-free
 10853 **IF** $E_1 = E'_1[\text{dyn } \tau E^\bullet]$:
 10854 a. $E' = op^2 v_0 E'_1$
 10855 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 10856 **ELSE** $E_1 = E'_1[\text{stat } \tau E^\bullet]$:
 10857 a. $E' = op^2 v_0 E'_1$
 10858 b. QED $E = E'[\text{stat } \tau E^\bullet]$
 10859 **CASE** $E = \text{chk } \tau E_0$:
 10860 1. $E_0 = E^\bullet$
 10861 $\vee E_0 = E'_0[\text{dyn } \tau E^\bullet]$
 10862 $\vee E_0 = E'_0[\text{stat } \tau E^\bullet]$
 10863 by the induction hypothesis
 10864 2. **IF** $E_0 = E^\bullet$:
 10865 a. QED E is boundary-free
 10866 **IF** $E_0 = E'_0[\text{dyn } \tau E^\bullet]$:
 10867 a. $E' = \text{chk } \tau E'_0$
 10868 b. QED $E = E'[\text{dyn } \tau E^\bullet]$
 10869 **ELSE** $E_0 = E'_0[\text{stat } \tau E^\bullet]$:
 10870 a. $E' = \text{chk } \tau E'_0$
 10871 b. QED $E = E'[\text{stat } \tau E^\bullet]$
 10872 **CASE** $E = \text{dyn } \tau E_0$:
 10873 1. $E_0 = E^\bullet$
 10874 $\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$
 10875 $\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$
 10876 by the induction hypothesis
 10877 2. **IF** $E_0 = E^\bullet$:
 10878 a. QED
 10879 **IF** $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:
 10880 a. $E' = \text{dyn } \tau E'_0$
 10881 b. QED $E = E'[\text{dyn } \tau' E^\bullet]$
 10882 **ELSE** $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:
 10883 a. $E' = \text{dyn } \tau E'_0$
 10884 b. QED $E = E'[\text{stat } \tau' E^\bullet]$
 10885 **CASE** $E = \text{stat } \tau E_0$:
 10886 1. $E_0 = E^\bullet$
 10887 $\vee E_0 = E'_0[\text{dyn } \tau' E^\bullet]$
 10888
 10889
 10890

10891 $\vee E_0 = E'_0[\text{stat } \tau' E^\bullet]$
 10892 by the induction hypothesis
 10893 2. **IF** $E_0 = E^\bullet$:
 10894 a. QED
 10895 **IF** $E_0 = E'_0[\text{dyn } \tau' E^\bullet]$:
 10896 a. $E' = \text{stat } \tau E'_0$
 10897 b. QED $E = E'[\text{dyn } \tau' E^\bullet]$
 10898 **ELSE** $E_0 = E'_0[\text{stat } \tau' E^\bullet]$:
 10899 a. $E' = \text{stat } \tau E'_0$
 10900 b. QED $E = E'[\text{stat } \tau' E^\bullet]$

□

Lemma 6.15 : HF *dynamic boundary factoring*If $\vdash_F e$ then one of the following holds:

- e is a value
- $e = E^\bullet[v_0 v_1]$
- $e = E^\bullet[op^1 v]$
- $e = E^\bullet[op^2 v_0 v_1]$
- $e = E[\text{dyn } \tau e']$ where e' is boundary-free
- $e = E[\text{stat } \tau e']$ where e' is boundary-free
- $e = E[\text{Err}]$

Proof:

By the *unique dynamic evaluation contexts* lemma, there are eight cases.

CASE e is a value :

1. QED

CASE $e = E[v_0 v_1]$:1. $E = E^\bullet$ $\vee E = E'[\text{dyn } \tau E^\bullet]$ $\vee E = E'[\text{stat } \tau E^\bullet]$ by *inner boundary*2. **IF** $E = E^\bullet$:a. QED $e = E^\bullet[v_0 v_1]$ **IF** $E = E'[\text{dyn } \tau E^\bullet]$:a. QED $e = E'[\text{dyn } \tau E^\bullet[v_0 v_1]]$ **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:a. QED $e = E'[\text{stat } \tau E^\bullet[v_0 v_1]]$ **CASE** $e = E[op^1 v]$:1. $E = E^\bullet$ $\vee E = E'[\text{dyn } \tau E^\bullet]$ $\vee E = E'[\text{stat } \tau E^\bullet]$ by *inner boundary*2. **IF** $E = E^\bullet$:a. QED $e = E^\bullet[op^1 v]$ **IF** $E = E'[\text{dyn } \tau E^\bullet]$:a. QED $e = E'[\text{dyn } \tau E^\bullet[op^1 v]]$ **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:a. QED $e = E'[\text{stat } \tau E^\bullet[op^1 v]]$ **CASE** $e = E[op^2 v_0 v_1]$:1. $E = E^\bullet$ $\vee E = E'[\text{dyn } \tau E^\bullet]$ $\vee E = E'[\text{stat } \tau E^\bullet]$ by *inner boundary*2. **IF** $E = E^\bullet$:a. QED $e = E^\bullet[op^2 v_0 v_1]$ **IF** $E = E'[\text{dyn } \tau E^\bullet]$:a. QED $e = E'[\text{dyn } \tau E^\bullet[op^2 v_0 v_1]]$ **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:a. QED $e = E'[\text{stat } \tau E^\bullet[op^2 v_0 v_1]]$ **CASE** $e = E[\text{chk } \tau' v]$:1. $E = E^\bullet$ $\vee E = E'[\text{dyn } \tau E^\bullet]$ $\vee E = E'[\text{stat } \tau E^\bullet]$ by *inner boundary*2. **IF** $E = E^\bullet$:a. Contradiction by $\vdash_F e$ **IF** $E = E'[\text{dyn } \tau E^\bullet]$:a. Contradiction by $\vdash_F e$ **ELSE** $E = E'[\text{stat } \tau E^\bullet]$:a. QED $e = E'[\text{stat } \tau E^\bullet[\text{chk } \tau' v]]$ **CASE** $e = E[\text{dyn } \tau v]$:1. QED v is boundary-free**CASE** $e = E[\text{stat } \tau v]$:1. QED v is boundary-free**CASE** $e = E[\text{Err}]$:

1. QED

□

Lemma 6.16 : HF *unique dynamic evaluation contexts*If $\vdash_F e$ then one of the following holds:

- e is a value
- $e = E[v_0 v_1]$
- $e = E[op^1 v]$
- $e = E[op^2 v_0 v_1]$
- $e = E[\text{chk } \tau v]$
- $e = E[\text{dyn } \tau v]$
- $e = E[\text{stat } \tau v]$
- $e = E[\text{Err}]$

*Proof:*By induction on the structure of e .**CASE** $e = x$ $\vee e = \lambda(x:\tau). e'$ $\vee e = \text{dyn } \tau e'$ 1. Contradiction by $\vdash_F e$ **CASE** $e = i$ $\vee e = \lambda x. e'$ $\vee e = \text{mon}(\tau_d \Rightarrow \tau_c) v$ 1. QED e is a value**CASE** $e = \text{Err}$:1. $E = []$ 2. QED $e = E[\text{Err}]$ **CASE** $e = \langle e_0, e_1 \rangle$:**IF** $e_0 \notin v$:1. $\vdash_F e_0$ by *inversion*2. $e_0 = E'_0[e'_0]$

by the induction hypothesis (1)

3. $E = \langle E_0, e_1 \rangle$ 4. QED $e = E[e'_0]$

11001 **IF** $e_0 \in v$
 11002 $\wedge e_1 \notin v :$
 11003 1. $\vdash_F e_1$
 11004 by *inversion*
 11005 2. $e_1 = E_1[e'_1]$
 11006 by the induction hypothesis (1)
 11007 3. $E = \langle e_0, E_1 \rangle$
 11008 4. QED $e = E[e'_1]$
 11009 **ELSE** $e_0 \in v$
 11010 $\wedge e_1 \in v :$
 11011 1. $E = []$
 11012 2. QED e is a value
 11013 **CASE** $e = e_0 e_1 :$
 11014 **IF** $e_0 \notin v :$
 11015 1. $\vdash_F e_0$
 11016 by *inversion*
 11017 2. $e_0 = E_0[e'_0]$
 11018 by the induction hypothesis (1)
 11019 3. $E = E_0 e_1$
 11020 4. QED $e = E[e'_0]$
 11021 **IF** $e_0 \in v$
 11022 $\wedge e_1 \notin v :$
 11023 1. $\vdash_F e_1$
 11024 by *inversion*
 11025 2. $e_1 = E_1[e'_1]$
 11026 by the induction hypothesis (1)
 11027 3. $E = e_0 E_1$
 11028 4. QED $e = E[e'_1]$
 11029 **ELSE** $e_0 \in v$
 11030 $\wedge e_1 \in v :$
 11031 1. $E = []$
 11032 2. QED $e = E[e_0 e_1]$
 11033 **CASE** $e = op^1 e_0 :$
 11034 **IF** $e_0 \notin v :$
 11035 1. $\vdash_F e_0$
 11036 by *inversion*
 11037 2. $e_0 = E_0[e'_0]$
 11038 by the induction hypothesis (1)
 11039 3. $E = op^1 E_0$
 11040 4. QED $e = E[e'_0]$
 11041 **ELSE** $e_0 \in v :$
 11042 1. $E = []$
 11043 2. QED $e = E[op^1 e_0]$
 11044 **CASE** $e = op^2 e_0 e_1 :$
 11045 **IF** $e_0 \notin v :$
 11046 1. $\vdash_F e_0$
 11047 by *inversion*
 11048 2. $e_0 = E_0[e'_0]$
 11049 by the induction hypothesis (1)
 11050 3. $E = op^2 E_0 e_1$
 11051 4. QED $e = E[e'_0]$
 11052 **IF** $e_0 \in v$
 11053 $\wedge e_1 \notin v :$

1. $\vdash_F e_1$
 by *inversion*
 2. $e_1 = E_1[e'_1]$
 by the induction hypothesis (1)
 3. $E = op^2 e_0 E_1$
 4. QED $e = E[e'_1]$
ELSE $e_0 \in v$
 $\wedge e_1 \in v :$
 1. $E = []$
 2. QED $e = E[op^2 e_0 e_1]$
CASE $e = \text{chk } \tau e_0 :$
 Contradiction by $\vdash_F e$
CASE $e = \text{stat } \tau e_0 :$
IF $e_0 \notin v :$
 1. $\vdash_F e_0$
 by *inversion*
 2. $e_0 = E_0[e'_0]$
 by *unique static evaluation contexts* (1)
 3. $E = \text{stat } \tau E_0$
 4. QED $e = E[e'_0]$
ELSE $e_0 \in v :$
 1. $E = []$
 2. QED $e = E[\text{stat } \tau e_0]$

□

Lemma 6.17 : HF *static hole typing*If $\vdash_F E[e] : \tau$ then the derivation contains a sub-term $\vdash_F e : \tau'$ *Proof*:By induction on the structure of E^\bullet .**CASE** $E^\bullet = [] :$ 1. QED $E^\bullet[e] = e$ **CASE** $E^\bullet = E^\bullet_0 e_1 :$ 1. $E^\bullet[e] = E^\bullet_0[e] e_1$ 2. $\vdash_F E^\bullet_0[e] : \tau_d \Rightarrow \tau_c$ by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = v_0 E^\bullet_1 :$ 1. $E^\bullet[e] = v_0 E^\bullet_1[e]$ 2. $\vdash_F E^\bullet_1[e] : \tau_d$ by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = \langle E^\bullet_0, e_1 \rangle :$ 1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$ 2. $\vdash_F E^\bullet_0[e] : \tau_0$ by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = \langle v_0, E^\bullet_1 \rangle :$ 1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$ 2. $\vdash_F E^\bullet_1[e] : \tau_1$ by *inversion*

3. QED by the induction hypothesis (2)

CASE $E^\bullet = op^1 E^\bullet_0 :$ 1. $E^\bullet[e] = op^1 E^\bullet_0[e]$

11111 2. $\vdash_F E^\bullet_0[e] : \tau_0$
 11112 by *inversion*
 11113 3. QED by the induction hypothesis (2)
 11114 **CASE** $E^\bullet = op^2 E^\bullet_0 e_1 :$
 11115 1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$
 11116 2. $\vdash_F E^\bullet_0[e] : \tau_0$
 11117 by *inversion*
 11118 3. QED by the induction hypothesis (2)
 11119 **CASE** $E^\bullet = op^2 v_0 E^\bullet_1 :$
 11120 1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$
 11121 2. $\vdash_F E^\bullet_1[e] : \tau_1$
 11122 by *inversion*
 11123 3. QED by the induction hypothesis (2)
 11124 **CASE** $E^\bullet = chk \tau E^\bullet_0 :$
 11125 1. $E^\bullet[e] = chk \tau E^\bullet_0[e]$
 11126 2. $\vdash_F E^\bullet_0[e] : \tau_0$
 11127 by *inversion*
 11128 3. QED by the induction hypothesis (2)
 11129 \square
 11130 **Lemma 6.18** : HF *dynamic hole typing*
 11131 If $\vdash_F E^\bullet[e]$ then the derivation contains a sub-term $\vdash_F e$
 11132 *Proof*:
 11133 By induction on the structure of E^\bullet .
 11134 **CASE** $E^\bullet = [] :$
 11135 1. QED $E^\bullet[e] = e$
 11136 **CASE** $E^\bullet = E^\bullet_0 e_1 :$
 11137 1. $E^\bullet[e] = E^\bullet_0[e] e_1$
 11138 2. $\vdash_F E^\bullet_0[e]$
 11139 by *inversion*
 11140 3. QED by the induction hypothesis (2)
 11141 **CASE** $E^\bullet = v_0 E^\bullet_1 :$
 11142 1. $E^\bullet[e] = v_0 E^\bullet_1[e]$
 11143 2. $\vdash_F E^\bullet_1[e]$
 11144 by *inversion*
 11145 3. QED by the induction hypothesis (2)
 11146 **CASE** $E^\bullet = \langle E^\bullet_0, e_1 \rangle :$
 11147 1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$
 11148 2. $\vdash_F E^\bullet_0[e]$
 11149 by *inversion*
 11150 3. QED by the induction hypothesis (2)
 11151 **CASE** $E^\bullet = \langle v_0, E^\bullet_1 \rangle :$
 11152 1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$
 11153 2. $\vdash_F E^\bullet_1[e]$
 11154 by *inversion*
 11155 3. QED by the induction hypothesis (2)
 11156 **CASE** $E^\bullet = op^1 E^\bullet_0 :$
 11157 1. $E^\bullet[e] = op^1 E^\bullet_0[e]$
 11158 2. $\vdash_F E^\bullet_0[e]$
 11159 by *inversion*
 11160 3. QED by the induction hypothesis (2)
 11161 **CASE** $E^\bullet = op^2 E^\bullet_0 e_1 :$
 11162 1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$
 11163
 11164
 11165

11166 2. $\vdash_F E^\bullet_0[e]$
 11167 by *inversion*
 11168 3. QED by the induction hypothesis (2)
 11169 **CASE** $E^\bullet = op^2 v_0 E^\bullet_1 :$
 11170 1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$
 11171 2. $\vdash_F E^\bullet_1[e]$
 11172 by *inversion*
 11173 3. QED by the induction hypothesis (2)
 11174 \square
 11175 **Lemma 6.19** : HF *boundary hole typing*
 11176 • If $\vdash_F E[\text{dyn } \tau e] : \tau'$ then the derivation contains a sub-term
 11177 $\vdash_F \text{dyn } \tau e : \tau$
 11178 • If $\vdash_F E[\text{dyn } \tau e]$ then the derivation contains a sub-term
 11179 $\vdash_F \text{dyn } \tau e : \tau$
 11180 • If $\vdash_F E[\text{stat } \tau e] : \tau'$ then the derivation contains a sub-term
 11181 $\vdash_F \text{stat } \tau e$
 11182 • If $\vdash_F E[\text{stat } \tau e]$ then the derivation contains a sub-term
 11183 $\vdash_F \text{stat } \tau e$
 11184 *Proof*:
 11185 By the following four lemmas: *static dyn hole typing*,
 11186 *dynamic dyn hole typing*, *static stat hole typing*, and
 11187 *dynamic stat hole typing*.
 11188 \square
 11189 **Lemma 6.20** : HF *static dyn hole typing*
 11190 If $\vdash_F E[\text{dyn } \tau e] : \tau'$ then the derivation contains a sub-term
 11191 $\vdash_F \text{dyn } \tau e : \tau$.
 11192 *Proof*:
 11193 By induction on the structure of E .
 11194 **CASE** $E \in E^\bullet :$
 11195 1. $\vdash_F \text{dyn } \tau e : \tau''$
 11196 by *static hole typing*
 11197 2. $\vdash_F \text{dyn } \tau e : \tau$
 11198 by *inversion* (1)
 11199 3. QED
 11200 **CASE** $E = E_0 e_1 :$
 11201 1. $E[\text{dyn } \tau e] = E_0[\text{dyn } \tau e] e_1$
 11202 2. $\vdash_F E_0[\text{dyn } \tau e] : \tau_0$
 11203 by *inversion*
 11204 3. QED by the induction hypothesis (2)
 11205 **CASE** $E = v_0 E_1 :$
 11206 1. $E[\text{dyn } \tau e] = v_0 E_1[\text{dyn } \tau e]$
 11207 2. $\vdash_F E_1[\text{dyn } \tau e] : \tau_1$
 11208 by *inversion*
 11209 3. QED by the induction hypothesis (2)
 11210 **CASE** $E = \langle E_0, e_1 \rangle :$
 11211 1. $E[\text{dyn } \tau e] = \langle E_0[\text{dyn } \tau e], e_1 \rangle$
 11212 2. $\vdash_F E_0[\text{dyn } \tau e] : \tau_0$
 11213 by *inversion*
 11214 3. QED by the induction hypothesis (2)
 11215 **CASE** $E = \langle v_0, E_1 \rangle :$
 11216 1. $E[\text{dyn } \tau e] = \langle v_0, E_1[\text{dyn } \tau e] \rangle$
 11217 2. $\vdash_F E_1[\text{dyn } \tau e] : \tau_1$
 11218 by *inversion*
 11219
 11220

11221 3. QED by the induction hypothesis (2)
 11222 **CASE** $E = op^1 E_0$:
 11223 1. $E[\text{dyn } \tau e] = op^1 E_0[\text{dyn } \tau e]$
 11224 2. $\vdash_F E_0[\text{dyn } \tau e] : \tau_0$
 11225 by *inversion*
 11226 3. QED by the induction hypothesis (2)
 11227 **CASE** $E = op^2 E_0 e_1$:
 11228 1. $E[\text{dyn } \tau e] = op^2 E_0[\text{dyn } \tau e] e_1$
 11229 2. $\vdash_F E_0[\text{dyn } \tau e] : \tau_0$
 11230 by *inversion*
 11231 3. QED by the induction hypothesis (2)
 11232 **CASE** $E = op^2 v_0 E_1$:
 11233 1. $E[\text{dyn } \tau e] = op^2 v_0 E_1[\text{dyn } \tau e]$
 11234 2. $\vdash_F E_1[\text{dyn } \tau e] : \tau_1$
 11235 by *inversion*
 11236 3. QED by the induction hypothesis (2)
 11237 **CASE** $E = \text{chk } \tau'' E_0$:
 11238 1. $E[\text{dyn } \tau e] = \text{chk } \tau'' E_0[\text{dyn } \tau e]$
 11239 2. $\vdash_F E_0[\text{dyn } \tau e] : \tau_0$
 11240 by *inversion*
 11241 3. QED by the induction hypothesis (2)
 11242 **CASE** $E = \text{dyn } \tau_0 E_0$:
 11243 1. $E[\text{dyn } \tau e] = \text{dyn } \tau_0 E_0[\text{dyn } \tau e]$
 11244 2. $\vdash_F E_0[\text{dyn } \tau e]$
 11245 by *inversion*
 11246 3. QED by *dynamic dyn hole typing* (2)
 11247 **CASE** $E = \text{stat } \tau_0 E_0$:
 11248 1. Contradiction by $\vdash_F E[\text{dyn } \tau e] : \tau'$
 11249 \square
 11250 **Lemma 6.21** : HF *dynamic dyn hole typing*
 11251 If $\vdash_F E[\text{dyn } \tau e]$ then the derivation contains a sub-term
 11252 $\vdash_F \text{dyn } \tau e : \tau$.
 11253 *Proof*:
 11254 By induction on the structure of E .
 11255 **CASE** $E \in E^*$:
 11256 1. Contradiction by $\vdash_F E[\text{dyn } \tau e]$
 11257 **CASE** $E = E_0 e_1$:
 11258 1. $E[\text{dyn } \tau e] = E_0[\text{dyn } \tau e] e_1$
 11259 2. $\vdash_F E_0[\text{dyn } \tau e]$
 11260 by *inversion*
 11261 3. QED by the induction hypothesis (2)
 11262 **CASE** $E = v_0 E_1$:
 11263 1. $E[\text{dyn } \tau e] = v_0 E_1[\text{dyn } \tau e]$
 11264 2. $\vdash_F E_1[\text{dyn } \tau e]$
 11265 by *inversion*
 11266 3. QED by the induction hypothesis (2)
 11267 **CASE** $E = \langle E_0, e_1 \rangle$:
 11268 1. $E[\text{dyn } \tau e] = \langle E_0[\text{dyn } \tau e], e_1 \rangle$
 11269 2. $\vdash_F E_0[\text{dyn } \tau e]$
 11270 by *inversion*
 11271 3. QED by the induction hypothesis (2)
 11272 **CASE** $E = \langle v_0, E_1 \rangle$:
 11273 1. $E[\text{dyn } \tau e] = \langle v_0, E_1[\text{dyn } \tau e] \rangle$
 11274
 11275

2. $\vdash_F E_1[\text{dyn } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^1 E_0$:
 1. $E[\text{dyn } \tau e] = op^1 E_0[\text{dyn } \tau e]$
 2. $\vdash_F E_0[\text{dyn } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^2 E_0 e_1$:
 1. $E[\text{dyn } \tau e] = op^2 E_0[\text{dyn } \tau e] e_1$
 2. $\vdash_F E_0[\text{dyn } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^2 v_0 E_1$:
 1. $E[\text{dyn } \tau e] = op^2 v_0 E_1[\text{dyn } \tau e]$
 2. $\vdash_F E_1[\text{dyn } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{chk } \tau'' E_0$:
 1. Contradiction by $\vdash_F E[\text{dyn } \tau e]$
 \square
CASE $E = \text{dyn } \tau E_0$:
 1. Contradiction by $\vdash_F E[\text{dyn } \tau e]$
CASE $E = \text{stat } \tau_0 E_0$:
 1. $E[\text{dyn } \tau e] = \text{stat } \tau_0 E_0[\text{dyn } \tau e]$
 2. $\vdash_F E_0[\text{dyn } \tau e] : \tau_0$
 by *inversion*
 3. QED by *static dyn hole typing* (2)
 $\}$
Lemma 6.22 : HF *static stat hole typing*
 If $\vdash_F E[\text{stat } \tau e] : \tau'$ then the derivation contains a sub-term
 $\vdash_F \text{stat } \tau e$.
Proof:
 By induction on the structure of E .
CASE $E \in E^*$:
 1. Contradiction by $\vdash_F E[\text{stat } \tau e] : \tau'$
CASE $E = E_0 e_1$:
 1. $E[\text{stat } \tau e] = E_0[\text{stat } \tau e] e_1$
 2. $\vdash_F E_0[\text{stat } \tau e] : \tau_0$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = v_0 E_1$:
 1. $E[\text{stat } \tau e] = v_0 E_1[\text{stat } \tau e]$
 2. $\vdash_F E_1[\text{stat } \tau e] : \tau_1$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \langle E_0, e_1 \rangle$:
 1. $E[\text{stat } \tau e] = \langle E_0[\text{stat } \tau e], e_1 \rangle$
 2. $\vdash_F E_0[\text{stat } \tau e] : \tau_0$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \langle v_0, E_1 \rangle$:
 1. $E[\text{stat } \tau e] = \langle v_0, E_1[\text{stat } \tau e] \rangle$
 11276
 11277
 11278
 11279
 11280
 11281
 11282
 11283
 11284
 11285
 11286
 11287
 11288
 11289
 11290
 11291
 11292
 11293
 11294
 11295
 11296
 11297
 11298
 11299
 11300
 11301
 11302
 11303
 11304
 11305
 11306
 11307
 11308
 11309
 11310
 11311
 11312
 11313
 11314
 11315
 11316
 11317
 11318
 11319
 11320
 11321
 11322
 11323
 11324
 11325
 11326
 11327
 11328
 11329
 11330

11331 2. $\vdash_F E_1[\text{stat } \tau e] : \tau_1$
 11332 by *inversion*
 11333 3. QED by the induction hypothesis (2)
 11334 **CASE** $E = op^1 E_0$:
 11335 1. $E[\text{stat } \tau e] = op^1 E_0[\text{stat } \tau e]$
 11336 2. $\vdash_F E_0[\text{stat } \tau e] : \tau_0$
 11337 by *inversion*
 11338 3. QED by the induction hypothesis (2)
 11339 **CASE** $E = op^2 E_0 e_1$:
 11340 1. $E[\text{stat } \tau e] = op^2 E_0[\text{stat } \tau e] e_1$
 11341 2. $\vdash_F E_0[\text{stat } \tau e] : \tau_0$
 11342 by *inversion*
 11343 3. QED by the induction hypothesis (2)
 11344 **CASE** $E = op^2 v_0 E_1$:
 11345 1. $E[\text{stat } \tau e] = op^2 v_0 E_1[\text{stat } \tau e]$
 11346 2. $\vdash_F E_1[\text{stat } \tau e] : \tau_1$
 11347 by *inversion*
 11348 3. QED by the induction hypothesis (2)
 11349 **CASE** $E = \text{chk } \tau'' E_0$:
 11350 1. $E[\text{stat } \tau e] = \text{chk } \tau'' E_0[\text{stat } \tau e]$
 11351 2. $\vdash_F E_0[\text{stat } \tau e] : \tau_0$
 11352 by *inversion*
 11353 3. QED by the induction hypothesis (2)
 11354 **CASE** $E = \text{dyn } \tau_0 E_0$:
 11355 1. $E[\text{stat } \tau e] = \text{dyn } \tau_0 E_0[\text{stat } \tau e]$
 11356 2. $\vdash_F E_0[\text{stat } \tau e]$
 11357 by *inversion*
 11358 3. QED by *dynamic stat hole typing* (2)
 11359 **CASE** $E = \text{stat } \tau_0 E_0$:
 11360 1. Contradiction by $\vdash_F E[\text{stat } \tau e] : \tau'$
 11361 \square
 11362 **Lemma 6.23** : HF *dynamic stat hole typing*
 11363 If $\vdash_F E[\text{stat } \tau e]$ then the derivation contains a sub-term \vdash_F
 11364 $\text{stat } \tau e$.
 11365 *Proof*:
 11366 By induction on the structure of E .
 11367 **CASE** $E \in E^\bullet$:
 11368 1. QED by *dynamic hole typing*
 11369 **CASE** $E = E_0 e_1$:
 11370 1. $E[\text{stat } \tau e] = E_0[\text{stat } \tau e] e_1$
 11371 2. $\vdash_F E_0[\text{stat } \tau e]$
 11372 by *inversion*
 11373 3. QED by the induction hypothesis (2)
 11374 **CASE** $E = v_0 E_1$:
 11375 1. $E[\text{stat } \tau e] = v_0 E_1[\text{stat } \tau e]$
 11376 2. $\vdash_F E_1[\text{stat } \tau e]$
 11377 by *inversion*
 11378 3. QED by the induction hypothesis (2)
 11379 **CASE** $E = \langle E_0, e_1 \rangle$:
 11380 1. $E[\text{stat } \tau e] = \langle E_0[\text{stat } \tau e], e_1 \rangle$
 11381 2. $\vdash_F E_0[\text{stat } \tau e]$
 11382 by *inversion*
 11383 3. QED by the induction hypothesis (2)
 11384 **CASE** $E = \langle v_0, E_1 \rangle$:
 11385

1. $E[\text{stat } \tau e] = \langle v_0, E_1[\text{stat } \tau e] \rangle$
 2. $\vdash_F E_1[\text{stat } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^1 E_0$:
 1. $E[\text{stat } \tau e] = op^1 E_0[\text{stat } \tau e]$
 2. $\vdash_F E_0[\text{stat } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^2 E_0 e_1$:
 1. $E[\text{stat } \tau e] = op^2 E_0[\text{stat } \tau e] e_1$
 2. $\vdash_F E_0[\text{stat } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = op^2 v_0 E_1$:
 1. $E[\text{stat } \tau e] = op^2 v_0 E_1[\text{stat } \tau e]$
 2. $\vdash_F E_1[\text{stat } \tau e]$
 by *inversion*
 3. QED by the induction hypothesis (2)
CASE $E = \text{chk } \tau'' E_0$:
 1. Contradiction by $\vdash_F E[\text{stat } \tau e]$
CASE $E = \text{dyn } \tau_0 E_0$:
 1. Contradiction by $\vdash_F E[\text{stat } \tau e]$
CASE $E = \text{stat } \tau_0 E_0$:
 1. $E[\text{stat } \tau e] = \text{stat } \tau_0 E_0[\text{stat } \tau e]$
 2. $\vdash_F E_0[\text{stat } \tau e] : \tau_0$
 by *inversion*
 3. QED by *static stat hole typing* (2)
 \square
Lemma 6.24 : HF *static boundary-free hole substitution*
 If $\vdash_F E^\bullet[e] : \tau$ and the derivation contains a sub-term $\vdash_F e : \tau'$
 and $\vdash_F e' : \tau'$ then $\vdash_F E^\bullet[e'] : \tau$.
Proof:
 By induction on the structure of E^\bullet
CASE $E^\bullet = []$:
 1. $E^\bullet[e] = e$
 $\wedge E^\bullet[e'] = e'$
 2. $\vdash_F e : \tau$
 by (1)
 3. $\tau' = \tau$
 4. $\vdash_F e' : \tau$
 5. QED by (1, 4)
CASE $E^\bullet = E^\bullet_0 e_1$:
 1. $E^\bullet[e] = E^\bullet_0[e] e_1$
 $\wedge E^\bullet[e'] = E^\bullet_0[e'] e_1$
 2. $\vdash_F E^\bullet_0[e] e_1 : \tau$
 3. $\vdash_F E^\bullet_0[e] : \tau_0$
 $\wedge \vdash_F e_1 : \tau_1$
 by *inversion*
 4. $\vdash_F E^\bullet_0[e'] : \tau_0$
 by the induction hypothesis (3)
 5. $\vdash_F E^\bullet_0[e'] e_1 : \tau$
 by (2, 3, 4)

11441 6. QED by (1, 5)
 11442 **CASE** $E^\bullet = v_0 E^\bullet_1 :$
 11443 1. $E^\bullet[e] = v_0 E^\bullet_1[e]$
 11444 $\wedge E^\bullet[e'] = v_0 E^\bullet_1[e']$
 11445 2. $\vdash_F v_0 E^\bullet_1[e] : \tau$
 11446 3. $\vdash_F v_0 : \tau_0$
 11447 $\wedge \vdash_F E^\bullet_1[e] : \tau_1$
 11448 by *inversion*
 11449 4. $\vdash_F E^\bullet_1[e'] : \tau_1$
 11450 by the induction hypothesis (3)
 11451 5. $\vdash_F v_0 E^\bullet_1[e'] : \tau$
 11452 by (2, 3, 4)
 11453 6. QED by (1, 5)
 11454 **CASE** $E^\bullet = op^1 E^\bullet_0 :$
 11455 1. $E^\bullet[e] = op^1 E^\bullet_0[e]$
 11456 $\wedge E^\bullet[e'] = op^1 E^\bullet_0[e']$
 11457 2. $\vdash_F op^1 E^\bullet_0[e] : \tau$
 11458 3. $\vdash_F E^\bullet_0[e] : \tau_0$
 11459 by *inversion*
 11460 4. $\vdash_F E^\bullet_0[e'] : \tau_0$
 11461 by the induction hypothesis (3)
 11462 5. $\vdash_F op^1 E^\bullet_0[e'] : \tau$
 11463 by (2, 3, 4)
 11464 6. QED by (1, 5)
 11465 **CASE** $E^\bullet = \langle E^\bullet_0, e_1 \rangle :$
 11466 1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$
 11467 $\wedge E^\bullet[e'] = \langle E^\bullet_0[e'], e_1 \rangle$
 11468 2. $\vdash_F \langle E^\bullet_0[e], e_1 \rangle : \tau$
 11469 3. $\vdash_F E^\bullet_0[e] : \tau_0$
 11470 $\wedge \vdash_F e_1 : \tau_1$
 11471 by *inversion*
 11472 4. $\vdash_F E^\bullet_0[e'] : \tau_0$
 11473 by the induction hypothesis (3)
 11474 5. $\vdash_F \langle E^\bullet_0[e'], e_1 \rangle : \tau$
 11475 by (2, 3, 4)
 11476 6. QED by (1, 5)
 11477 **CASE** $E^\bullet = \langle v_0, E^\bullet_1 \rangle :$
 11478 1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$
 11479 $\wedge E^\bullet[e'] = \langle v_0, E^\bullet_1[e'] \rangle$
 11480 2. $\vdash_F \langle v_0, E^\bullet_1[e] \rangle : \tau$
 11481 3. $\vdash_F v_0 : \tau_0$
 11482 $\wedge \vdash_F E^\bullet_1[e] : \tau_1$
 11483 by *inversion*
 11484 4. $\vdash_F E^\bullet_1[e'] : \tau_1$
 11485 by the induction hypothesis (3)
 11486 5. $\vdash_F \langle v_0, E^\bullet_1[e'] \rangle : \tau$
 11487 by (2, 3, 4)
 11488 6. QED by (1, 5)
 11489 **CASE** $E^\bullet = op^2 E^\bullet_0 e_1 :$
 11490 1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$
 11491 $\wedge E^\bullet[e'] = op^2 E^\bullet_0[e'] e_1$
 11492 2. $\vdash_F op^2 E^\bullet_0[e] e_1 : \tau$
 11493
 11494
 11495

3. $\vdash_F E^\bullet_0[e] : \tau_0$
 $\wedge \vdash_F e_1 : \tau_1$
 by *inversion*
 4. $\vdash_F E^\bullet_0[e'] : \tau_0$
 by the induction hypothesis (3)
 5. $\vdash_F op^2 E^\bullet_0[e'] e_1 : \tau$
 by (2, 3, 4)
 6. QED by (1, 5)
CASE $E^\bullet = op^2 v_0 E^\bullet_1 :$
 1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$
 $\wedge E^\bullet[e'] = op^2 v_0 E^\bullet_1[e']$
 2. $\vdash_F op^2 v_0 E^\bullet_1[e] : \tau$
 3. $\vdash_F v_0 : \tau_0$
 $\wedge \vdash_F E^\bullet_1[e] : \tau_1$
 by *inversion*
 4. $\vdash_F E^\bullet_1[e'] : \tau_1$
 by the induction hypothesis (3)
 5. $\vdash_F op^2 v_0 E^\bullet_1[e'] : \tau$
 by (2, 3, 4)
 6. QED by (1, 5)
CASE $E^\bullet = \text{chk } \tau'' E^\bullet_0 :$
 1. $E^\bullet[e] = \text{chk } \tau'' E^\bullet_0[e]$
 $\wedge E^\bullet[e'] = \text{chk } \tau'' E^\bullet_0[e']$
 2. $\vdash_F \text{chk } \tau'' E^\bullet_0[e] : \tau$
 3. $\vdash_F E^\bullet_0[e] : \tau_0$
 by *inversion*
 4. $\vdash_F E^\bullet_0[e'] : \tau_0$
 by the induction hypothesis (3)
 5. $\vdash_F \text{chk } \tau'' E^\bullet_0[e'] : \tau$
 by (2, 3, 4)
 6. QED by (1, 5)
 □

Lemma 6.25 : HF *dynamic hole substitution*

■ If $\vdash_F E^\bullet[e]$ and $\vdash_F e'$ then $\vdash_F E^\bullet[e']$

Proof:

By induction on the structure of E^\bullet

CASE $E^\bullet = [] :$

1. QED $E^\bullet[e'] = e'$

CASE $E^\bullet = \langle E^\bullet_0, e_1 \rangle :$

1. $E^\bullet[e] = \langle E^\bullet_0[e], e_1 \rangle$
 $\wedge E^\bullet[e'] = \langle E^\bullet_0[e'], e_1 \rangle$

2. $\vdash_F \langle E^\bullet_0[e], e_1 \rangle$

3. $\vdash_F E^\bullet_0[e]$

$\wedge \vdash_F e_1$

by *inversion*

4. $\vdash_F E^\bullet_0[e']$

by the induction hypothesis (3)

5. $\vdash_F \langle E^\bullet_0[e'], e_1 \rangle$

by (3, 4)

6. QED by (1, 5)

CASE $E^\bullet = \langle v_0, E^\bullet_1 \rangle :$

1. $E^\bullet[e] = \langle v_0, E^\bullet_1[e] \rangle$

$\wedge E^\bullet[e'] = \langle v_0, E^\bullet_1[e'] \rangle$

11551 2. $\vdash_F \langle v_0, E^\bullet_1[e] \rangle$
 11552 3. $\vdash_F v_0$
 11553 $\wedge \vdash_F E^\bullet_1[e]$
 11554 by *inversion*
 11555 4. $\vdash_F E^\bullet_1[e']$
 11556 by the induction hypothesis (3)
 11557 5. $\vdash_F \langle v_0, E^\bullet_1[e'] \rangle$
 11558 by (3, 4)
 11559 6. QED by (1, 5)
 11560 **CASE** $E^\bullet = E^\bullet_0 e_1$:
 11561 1. $E^\bullet[e] = E^\bullet_0[e] e_1$
 11562 $\wedge E^\bullet[e'] = E^\bullet_0[e'] e_1$
 11563 2. $\vdash_F E^\bullet_0[e] e_1$
 11564 3. $\vdash_F E^\bullet_0[e]$
 11565 $\wedge \vdash_F e_1$
 11566 by *inversion*
 11567 4. $\vdash_F E^\bullet_0[e']$
 11568 by the induction hypothesis (3)
 11569 5. $\vdash_F E^\bullet_0[e'] e_1$
 11570 by (3, 4)
 11571 6. QED by (1, 5)
 11572 **CASE** $E^\bullet = v_0 E^\bullet_1$:
 11573 1. $E^\bullet[e] = v_0 E^\bullet_1[e]$
 11574 $\wedge E^\bullet[e'] = v_0 E^\bullet_1[e']$
 11575 2. $\vdash_F v_0 E^\bullet_1[e]$
 11576 3. $\vdash_F v_0$
 11577 $\wedge \vdash_F E^\bullet_1[e]$
 11578 by *inversion*
 11579 4. $\vdash_F E^\bullet_1[e']$
 11580 by the induction hypothesis (3)
 11581 5. $\vdash_F v_0 E^\bullet_1[e']$
 11582 by (3, 4)
 11583 6. QED by (1, 5)
 11584 **CASE** $E^\bullet = op^1 E^\bullet_0$:
 11585 1. $E^\bullet[e] = op^1 E^\bullet_0[e]$
 11586 $\wedge E^\bullet[e'] = op^1 E^\bullet_0[e']$
 11587 2. $\vdash_F op^1 E^\bullet_0[e]$
 11588 3. $\vdash_F E^\bullet_0[e]$
 11589 by *inversion*
 11590 4. $\vdash_F E^\bullet_0[e']$
 11591 by the induction hypothesis (3)
 11592 5. $\vdash_F op^1 E^\bullet_0[e']$
 11593 by (4)
 11594 6. QED by (1, 5)
 11595 **CASE** $E^\bullet = op^2 E^\bullet_0 e_1$:
 11596 1. $E^\bullet[e] = op^2 E^\bullet_0[e] e_1$
 11597 $\wedge E^\bullet[e'] = op^2 E^\bullet_0[e'] e_1$
 11598 2. $\vdash_F op^2 E^\bullet_0[e] e_1$
 11599 3. $\vdash_F E^\bullet_0[e]$
 11600 $\wedge \vdash_F e_1$
 11601 by *inversion*
 11602 4. $\vdash_F E^\bullet_0[e']$
 11603 by the induction hypothesis (3)

5. $\vdash_F op^2 E^\bullet_0[e'] e_1$
 by (3, 4)
 6. QED by (1, 5)
CASE $E^\bullet = op^2 v_0 E^\bullet_1$:
 1. $E^\bullet[e] = op^2 v_0 E^\bullet_1[e]$
 $\wedge E^\bullet[e'] = op^2 v_0 E^\bullet_1[e']$
 2. $\vdash_F op^2 v_0 E^\bullet_1[e]$
 3. $\vdash_F v_0$
 $\wedge \vdash_F E^\bullet_1[e]$
 by *inversion*
 4. $\vdash_F E^\bullet_1[e']$
 by the induction hypothesis (3)
 5. $\vdash_F op^2 v_0 E^\bullet_1[e']$
 by (3, 4)
 6. QED by (1, 5)
CASE $E^\bullet = \text{chk } \tau_0 E^\bullet_0$:
 1. Contradiction by $\vdash_F E^\bullet[e]$
 □

Lemma 6.26 : HF *hole substitution*

- If $\vdash_F E[e]$ and the derivation contains a sub-term $\vdash_F e : \tau'$ and $\vdash_F e' : \tau'$ then $\vdash_F E[e']$.
- If $\vdash_F E[e]$ and the derivation contains a sub-term $\vdash_F e$ and $\vdash_F e'$ then $\vdash_F E[e']$.
- If $\vdash_F E[e] : \tau$ and the derivation contains a sub-term $\vdash_F e : \tau'$ and $\vdash_F e' : \tau'$ then $\vdash_F E[e'] : \tau$.
- If $\vdash_F E[e] : \tau$ and the derivation contains a sub-term $\vdash_F e$ and $\vdash_F e'$ then $\vdash_F E[e'] : \tau$.

Proof:

By the following four lemmas: *dynamic context static hole substitution*, *dynamic context dynamic hole substitution*, *static context static hole substitution*, and *static context dynamic hole substitution*.

□

Lemma 6.27 : HF *dynamic context static hole substitution*

- If $\vdash_F E[e]$ and contains $\vdash_F e : \tau'$, and furthermore $\vdash_F e' : \tau'$, then $\vdash_F E[e']$

Proof:

By induction on the structure of E .

CASE $E \in E^\bullet$:

1. Contradiction by $\vdash_F E[e]$

CASE $E = E_0 e_1$:

1. $E[e] = E_0[e] e_1$
2. $\vdash_F E_0[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = v_0 E_1$:

1. $E[e] = v_0 E_1[e]$
2. $\vdash_F E_1[e]$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \langle E_0, e_1 \rangle$:

1. $E[e] = \langle E_0[e], e_1 \rangle$

11661 2. $\vdash_F E_0[e]$
 11662 by *inversion*
 11663 3. QED by the induction hypothesis (2)
 11664 **CASE** $E = \langle v_0, E_1 \rangle :$
 11665 1. $E[e] = \langle v_0, E_1[e] \rangle$
 11666 2. $\vdash_F E_1[e]$
 11667 by *inversion*
 11668 3. QED by the induction hypothesis (2)
 11669 **CASE** $E = op^1 E_0 :$
 11670 1. $E[e] = op^1 E_0[e]$
 11671 2. $\vdash_F E_0[e]$
 11672 by *inversion*
 11673 3. QED by the induction hypothesis (2)
 11674 **CASE** $E = op^2 E_0 e_1 :$
 11675 1. $E[e] = op^2 E_0[e] e_1$
 11676 2. $\vdash_F E_0[e]$
 11677 by *inversion*
 11678 3. QED by the induction hypothesis (2)
 11679 **CASE** $E = op^2 v_0 E_1 :$
 11680 1. $E[e] = op^2 v_0 E_1[e]$
 11681 2. $\vdash_F E_1[e]$
 11682 by *inversion*
 11683 3. QED by the induction hypothesis (2)
 11684 **CASE** $E = \text{chk } \tau'' E_0 :$
 11685 1. $E[e] = \text{chk } \tau'' E_0[e]$
 11686 2. $\vdash_F E_0[e]$
 11687 by *inversion*
 11688 3. QED by the induction hypothesis (2)
 11689 **CASE** $E = \text{dyn } \tau'' E_0 :$
 11690 1. Contradiction by $\vdash_F E[e]$
 11691 **CASE** $E = \text{stat } \tau_0 E_0 :$
 11692 1. $E[e] = \text{stat } \tau_0 E_0[e]$
 11693 2. $\vdash_F E_0[e] : \tau_0$
 11694 by *inversion*
 11695 3. QED by *static context static hole substitution* (2)
 11696 \square
 11697 **Lemma 6.28** : HF *dynamic context dynamic hole substitution*
 11698 If $\vdash_F E[e]$ and contains $\vdash_F e$, and furthermore $\vdash_F e'$, then $\vdash_F E[e']$
 11699 *Proof*:
 11700 By induction on the structure of E .
 11701 **CASE** $E \in E^\bullet :$
 11702 1. QED by *dynamic boundary-free hole substitution*
 11703 **CASE** $E = E_0 e_1 :$
 11704 1. $E[e] = E_0[e] e_1$
 11705 2. $\vdash_F E_0[e]$
 11706 by *inversion*
 11707 3. QED by the induction hypothesis (2)
 11708 **CASE** $E = v_0 E_1 :$
 11709 1. $E[e] = v_0 E_1[e]$
 11710 2. $\vdash_F E_1[e]$
 11711 by *inversion*
 11712 3. QED by the induction hypothesis (2)
 11713 **CASE** $E = \langle E_0, e_1 \rangle :$
 11714 1. $E[e] = \langle E_0[e], e_1 \rangle$
 11715 2. $\vdash_F E_0[e]$
 11716 by *inversion*
 11717 3. QED by the induction hypothesis (2)
 11718 **CASE** $E = op^1 E_0 :$
 11719 1. $E[e] = op^1 E_0[e]$
 11720 2. $\vdash_F E_0[e]$
 11721 by *inversion*
 11722 3. QED by the induction hypothesis (2)
 11723 **CASE** $E = op^2 E_0 e_1 :$
 11724 1. $E[e] = op^2 E_0[e] e_1$
 11725 2. $\vdash_F E_0[e]$
 11726 by *inversion*
 11727 3. QED by the induction hypothesis (2)
 11728 **CASE** $E = op^2 v_0 E_1 :$
 11729 1. $E[e] = op^2 v_0 E_1[e]$
 11730 2. $\vdash_F E_1[e]$
 11731 by *inversion*
 11732 3. QED by the induction hypothesis (2)
 11733 **CASE** $E = \text{chk } \tau'' E_0 :$
 11734 1. Contradiction by $\vdash_F E[e]$
 11735 **CASE** $E = \text{dyn } \tau'' E_0 :$
 11736 1. Contradiction by $\vdash_F E[e]$
 11737 **CASE** $E = \text{stat } \tau_0 E_0 :$
 11738 1. $E[e] = \text{stat } \tau_0 E_0[e]$
 11739 2. $\vdash_F E_0[e] : \tau_0$
 11740 by *inversion*
 11741 3. QED by *static context dynamic hole substitution* (2)
 11742 \square

11716 1. $E[e] = \langle E_0[e], e_1 \rangle$
 11717 2. $\vdash_F E_0[e]$
 11718 by *inversion*
 11719 3. QED by the induction hypothesis (2)
 11720 **CASE** $E = \langle v_0, E_1 \rangle :$
 11721 1. $E[e] = \langle v_0, E_1[e] \rangle$
 11722 2. $\vdash_F E_1[e]$
 11723 by *inversion*
 11724 3. QED by the induction hypothesis (2)
 11725 **CASE** $E = op^1 E_0 :$
 11726 1. $E[e] = op^1 E_0[e]$
 11727 2. $\vdash_F E_0[e]$
 11728 by *inversion*
 11729 3. QED by the induction hypothesis (2)
 11730 **CASE** $E = op^2 E_0 e_1 :$
 11731 1. $E[e] = op^2 E_0[e] e_1$
 11732 2. $\vdash_F E_0[e]$
 11733 by *inversion*
 11734 3. QED by the induction hypothesis (2)
 11735 **CASE** $E = op^2 v_0 E_1 :$
 11736 1. $E[e] = op^2 v_0 E_1[e]$
 11737 2. $\vdash_F E_1[e]$
 11738 by *inversion*
 11739 3. QED by the induction hypothesis (2)
 11740 **CASE** $E = \text{chk } \tau'' E_0 :$
 11741 1. Contradiction by $\vdash_F E[e]$
 11742 **CASE** $E = \text{dyn } \tau'' E_0 :$
 11743 1. Contradiction by $\vdash_F E[e]$
 11744 **CASE** $E = \text{stat } \tau_0 E_0 :$
 11745 1. $E[e] = \text{stat } \tau_0 E_0[e]$
 11746 2. $\vdash_F E_0[e] : \tau_0$
 11747 by *inversion*
 11748 3. QED by *static context dynamic hole substitution* (2)
 11749 \square
 11750 **Lemma 6.29** : HF *static context static hole substitution*
 11751 If $\vdash_F E[e] : \tau$ and contains $\vdash_F e : \tau'$, and furthermore $\vdash_F e' : \tau'$,
 11752 then $\vdash_F E[e'] : \tau$
 11753 *Proof*:
 11754 By induction on the structure of E .
 11755 **CASE** $E \in E^\bullet :$
 11756 1. QED by *static boundary-free hole substitution*
 11757 **CASE** $E = E_0 e_1 :$
 11758 1. $E[e] = E_0[e] e_1$
 11759 2. $\vdash_F E_0[e] : \tau_0$
 11760 by *inversion*
 11761 3. QED by the induction hypothesis (2)
 11762 **CASE** $E = v_0 E_1 :$
 11763 1. $E[e] = v_0 E_1[e]$
 11764 2. $\vdash_F E_1[e] : \tau_1$
 11765 by *inversion*
 11766 3. QED by the induction hypothesis (2)
 11767 **CASE** $E = \langle E_0, e_1 \rangle :$
 11768 1. $E[e] = \langle E_0[e], e_1 \rangle$
 11769 2. $\vdash_F E_0[e]$
 11770 by *inversion*
 11771 3. QED by the induction hypothesis (2)

11771 2. $\vdash_F E_0[e] : \tau_0$
 11772 by *inversion*
 11773 3. QED by the induction hypothesis (2)
 11774 **CASE** $E = \langle v_0, E_1 \rangle :$
 11775 1. $E[e] = \langle v_0, E_1[e] \rangle$
 11776 2. $\vdash_F E_1[e] : \tau_1$
 11777 by *inversion*
 11778 3. QED by the induction hypothesis (2)
 11779 **CASE** $E = op^1 E_0 :$
 11780 1. $E[e] = op^1 E_0[e]$
 11781 2. $\vdash_F E_0[e] : \tau_0$
 11782 by *inversion*
 11783 3. QED by the induction hypothesis (2)
 11784 **CASE** $E = op^2 E_0 e_1 :$
 11785 1. $E[e] = op^2 E_0[e] e_1$
 11786 2. $\vdash_F E_0[e] : \tau_0$
 11787 by *inversion*
 11788 3. QED by the induction hypothesis (2)
 11789 **CASE** $E = op^2 v_0 E_1 :$
 11790 1. $E[e] = op^2 v_0 E_1[e]$
 11791 2. $\vdash_F E_1[e] : \tau_1$
 11792 by *inversion*
 11793 3. QED by the induction hypothesis (2)
 11794 **CASE** $E = \text{chk } \tau'' E_0 :$
 11795 1. $E[e] = \text{chk } \tau'' E_0[e]$
 11796 2. $\vdash_F E_0[e] : \tau_0$
 11797 by *inversion*
 11798 3. QED by the induction hypothesis (2)
 11799 **CASE** $E = \text{dyn } \tau_0 E_0 :$
 11800 1. $E[e] = \text{dyn } \tau_0 E_0[e]$
 11801 2. $\vdash_F E_0[e]$
 11802 by *inversion*
 11803 3. QED by *static dyn hole typing* (2)
 11804 **CASE** $E = \text{stat } \tau_0 E_0 :$
 11805 1. Contradiction by $\vdash_F E[e] : \tau$
 11806 \square

11807 **Lemma 6.30** : HF *static context dynamic hole substitution*

11808 If $\vdash_F E[e] : \tau$ and contains $\vdash_F e$, and furthermore $\vdash_F e'$, then
 11809 $\vdash_F E[e'] : \tau$

11810 *Proof*:

11811 By induction on the structure of E .

11812 **CASE** $E \in E^* :$

11813 1. Contradiction by $\vdash_F E[e] : \tau$

11814 **CASE** $E = E_0 e_1 :$

11815 1. $E[e] = E_0[e] e_1$

11816 2. $\vdash_F E_0[e] : \tau_0$

11817 by *inversion*

11818 3. QED by the induction hypothesis (2)

11819 **CASE** $E = v_0 E_1 :$

11820 1. $E[e] = v_0 E_1[e]$

11821 2. $\vdash_F E_1[e] : \tau_1$

11822 by *inversion*

11823 3. QED by the induction hypothesis (2)

11824

11825

CASE $E = \langle E_0, e_1 \rangle :$

1. $E[e] = \langle E_0[e], e_1 \rangle$

2. $\vdash_F E_0[e] : \tau_0$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \langle v_0, E_1 \rangle :$

1. $E[e] = \langle v_0, E_1[e] \rangle$

2. $\vdash_F E_1[e] : \tau_1$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = op^1 E_0 :$

1. $E[e] = op^1 E_0[e]$

2. $\vdash_F E_0[e] : \tau_0$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = op^2 E_0 e_1 :$

1. $E[e] = op^2 E_0[e] e_1$

2. $\vdash_F E_0[e] : \tau_0$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = op^2 v_0 E_1 :$

1. $E[e] = op^2 v_0 E_1[e]$

2. $\vdash_F E_1[e] : \tau_1$

by *inversion*

3. QED by the induction hypothesis (2)

CASE $E = \text{chk } \tau'' E_0 :$

1. Contradiction by $\vdash_F E[e] : \tau$

CASE $E = \text{dyn } \tau_0 E_0 :$

1. $E[e] = \text{dyn } \tau_0 E_0[e]$

2. $\vdash_F E_0[e]$

by *inversion*

3. QED by *dynamic stat hole typing* (2)

CASE $E = \text{stat } \tau_0 E_0 :$

1. Contradiction by $\vdash_F E[e] : \tau$

\square

Lemma 6.31 : \vdash_F *static inversion*

- If $\Gamma \vdash_F x : \tau$ then $(x : \tau') \in \Gamma$ and $\tau' \leq \tau$
- If $\Gamma \vdash_F \lambda(x : \tau'_d). e' : \tau$ then $(x : \tau'_d), \Gamma \vdash_F e' : \tau'_c$ and $\tau'_d \Rightarrow \tau'_c \leq \tau$
- If $\Gamma \vdash_F \langle e_0, e_1 \rangle : \tau_0 \times \tau_1$ then $\Gamma \vdash_F e_0 : \tau'_0$ and $\Gamma \vdash_F e_1 : \tau'_1$ and $\tau'_0 \leq \tau_0$ and $\tau'_1 \leq \tau_1$
- If $\Gamma \vdash_F e_0 e_1 : \tau_c$ then $\Gamma \vdash_F e_0 : \tau'_d \Rightarrow \tau'_c$ and $\Gamma \vdash_F e_1 : \tau'_d$ and $\tau'_c \leq \tau_c$
- If $\Gamma \vdash_F \text{fst } e : \tau$ then $\Gamma \vdash_F e : \tau_0 \times \tau_1$ and $\Delta(\text{fst}, \tau_0 \times \tau_1) = \tau_0$ and $\tau_0 \leq \tau$
- If $\Gamma \vdash_F \text{snd } e : \tau$ then $\Gamma \vdash_F e : \tau_0 \times \tau_1$ and $\Delta(\text{snd}, \tau_0 \times \tau_1) = \tau_1$ and $\tau_1 \leq \tau$
- If $\Gamma \vdash_F \text{op}^2 e_0 e_1 : \tau$ then $\Gamma \vdash_F e_0 : \tau_0$ and $\Gamma \vdash_F e_1 : \tau_1$ and $\Delta(\text{op}^2, \tau_0, \tau_1) = \tau'$ and $\tau' \leq \tau$
- If $\Gamma \vdash_F \text{mon } \tau'_0 \times \tau'_1 \langle v_0, v_1 \rangle : \tau_0 \times \tau_1$ then either:
 - $\Gamma \vdash_F \langle v_0, v_1 \rangle$
 - or $\Gamma \vdash_F \langle v_0, v_1 \rangle : \tau$
- If $\Gamma \vdash_F \text{mon } \tau'_d \Rightarrow \tau'_c \lambda x. e : \tau_d \Rightarrow \tau_c$ then $\Gamma \vdash_F \lambda x. e$ and $\tau'_d \Rightarrow \tau'_c \leq \tau_d \Rightarrow \tau_c$
- If $\Gamma \vdash_F \text{mon } \tau'_d \Rightarrow \tau'_c \lambda(x : \tau'_d). e : \tau_d \Rightarrow \tau_c$ then $\Gamma \vdash_F \lambda(x : \tau_x). e : \tau''_d \Rightarrow \tau''_c$ and $\tau'_d \Rightarrow \tau'_c \leq \tau_d \Rightarrow \tau_c$
- If $\Gamma \vdash_F \text{dyn } \tau' e' : \tau$ then $\Gamma \vdash_F e'$ and $\tau' \leq \tau$
- If $\Gamma \vdash_F \text{chk } \tau e' : \tau$ then $\Gamma \vdash_F e' : \tau'$

Proof:

QED by the definition of $\Gamma \vdash_F e : \tau$

□

Lemma 6.32 : \vdash_F dynamic inversion

- If $\Gamma \vdash_F x$ then $x \in \Gamma$
- If $\Gamma \vdash_F \lambda x. e'$ then $x, \Gamma \vdash_F e'$
- If $\Gamma \vdash_F \langle e_0, e_1 \rangle$ then $\Gamma \vdash_F e_0$ and $\Gamma \vdash_F e_1$
- If $\Gamma \vdash_F e_0 e_1$ then $\Gamma \vdash_F e_0$ and $\Gamma \vdash_F e_1$
- If $\Gamma \vdash_F \text{op}^1 e_0$ then $\Gamma \vdash_F e_0$
- If $\Gamma \vdash_F \text{op}^2 e_0 e_1$ then $\Gamma \vdash_F e_0$ and $\Gamma \vdash_F e_1$
- If $\Gamma \vdash_F \text{mon } (\tau_d \Rightarrow \tau_c) \lambda x. e$ then $\Gamma \vdash_F \lambda x. e$
- If $\Gamma \vdash_F \text{mon } (\tau_d \Rightarrow \tau_c) \lambda(x : \tau_x). e$ then $\Gamma \vdash_F \lambda(x : \tau_x). e : \tau_x \Rightarrow \tau'_c$
- If $\Gamma \vdash_F \text{mon } (\tau_0 \times \tau_1) \langle v_0, v_1 \rangle$ then either:
 - $\Gamma \vdash_F \langle v_0, v_1 \rangle$
 - or $\Gamma \vdash_F \langle v_0, v_1 \rangle : \tau'$
- If $\Gamma \vdash_F \text{stat } \tau' e'$ then $\Gamma \vdash_F e' : \tau'$

Proof:

QED by the definition of $\Gamma \vdash_F e$

□

Lemma 6.33 : HF canonical forms

- If $\Gamma \vdash_F v : \tau_0 \times \tau_1$ then either:
 - $v = \langle v_0, v_1 \rangle$
 - or $v = \text{mon } \tau'_0 \times \tau'_1 \langle v_0, v_1 \rangle$
 $\wedge \tau'_0 \times \tau'_1 \leq \tau_0 \times \tau_1$
- If $\Gamma \vdash_F v : \tau_d \Rightarrow \tau_c$ then either:
 - $v = \lambda(x : \tau_x). e'$
 $\wedge \tau_d \leq \tau_x$
 - or $v = \text{mon } (\tau'_d \Rightarrow \tau'_c) (\lambda x. e)$
 $\wedge \tau'_d \Rightarrow \tau'_c \leq \tau_d \Rightarrow \tau_c$
 - or $v = \text{mon } (\tau'_d \Rightarrow \tau'_c) \lambda(x : \tau_x). e$
 $\wedge \tau'_d \Rightarrow \tau'_c \leq \tau_d \Rightarrow \tau_c$
- If $\Gamma \vdash_F v : \text{Int}$ then $v = i$
- If $\Gamma \vdash_F v : \text{Nat}$ then $v = i$ and $v \in \mathbb{N}$

Proof:

QED by definition of $\vdash_F : \tau$

□

Lemma 6.34 : Δ type soundness

If $\Gamma \vdash_F v_0 : \tau_0$ and $\Gamma \vdash_F v_1 : \tau_1$ and $\Delta(\text{op}^2, \tau_0, \tau_1) = \tau$ then one of the following holds:

- $\delta(\text{op}^2, v_0, v_1) = v$ and $\Gamma \vdash_F v : \tau$, or
- $\delta(\text{op}^2, v_0, v_1) = \text{BndryErr}$

Proof (sketch): Similar to the proof for the higher-order Δ type soundness lemma. □

Lemma 6.35 : δ preservation

- If $\Gamma \vdash_F v$ and $\delta(\text{op}^1, v) = v'$ then $\Gamma \vdash_F v'$
- If $\Gamma \vdash_F v_0$ and $\Gamma \vdash_F v_1$ and $\delta(\text{op}^2, v_0, v_1) = v'$ then $\Gamma \vdash_F v'$

Proof:

Similar to the proof for the higher-order δ preservation lemma.

□

Lemma 6.36 : HF substitution

- If $(x : \tau_x), \Gamma \vdash_F e$ and $\Gamma \vdash_F v : \tau_x$ then $\Gamma \vdash_F e[x \leftarrow v]$
- If $x, \Gamma \vdash_F e$ and $\Gamma \vdash_F v$ then $\Gamma \vdash_F e[x \leftarrow v]$
- If $(x : \tau_x), \Gamma \vdash_F e : \tau$ and $\Gamma \vdash_F v : \tau_x$ then $\Gamma \vdash_F e[x \leftarrow v] : \tau$
- If $x, \Gamma \vdash_F e : \tau$ and $\Gamma \vdash_F v$ then $\Gamma \vdash_F e[x \leftarrow v] : \tau$

Proof:

Similar to the proof for the higher-order substitution lemma.

□

Lemma 6.37 : weakening

- If $\Gamma \vdash_F e$ then $x, \Gamma \vdash_F e$
- If $\Gamma \vdash_F e : \tau$ then $(x : \tau'), \Gamma \vdash_F e : \tau$

Proof:

QED because e is closed under Γ

□

A.7 Embeddings Summary

The paragraphs in this section summarize the five embeddings with four slogans. Each slogan pertains to one aspect of the embedding:

1. What kinds of checks does the embedding perform when a value reaches a type boundary?
2. When, if ever, does the embedding wrap a value in a monitor?
3. If an ill-typed value reaches a type boundary, when does the embedding signal an error?
4. How do types affect behavior?

These embeddings are ordered on a speculative scale from "most guarantees" to "least guarantees".

Higher-Order embedding

1. recursively check read-only values;
2. monitor functional and mutable values;
3. detect boundary errors as early as possible;
4. types globally constrain behavior.

Co-Natural embedding

1. tag-check all values;
2. monitor all data structures and functions;
3. detect boundary errors as late as possible;
4. types globally constrain behavior

Forgetful embedding

1. tag-check all values;
2. apply at most one monitor to each value;
3. detect boundary errors as late as possible;
4. types (of values) locally constrain behavior.

First-Order embedding

1. tag-check all values;
2. never allocate a monitor;
3. detect boundary errors as late as possible;
4. types (of contexts) locally constrain behavior.

Erasure embedding

1. never check values;
2. never allocate a monitor;
3. never detect a type boundary error;
4. types do not affect behavior

A.8 Simulation Lemmas

A.8.1 Definitions

Combined Language

$$\begin{aligned}
 e &= x \mid v \mid \langle e, e \rangle \mid ee \mid op^1 e \mid op^2 ee \mid \\
 &\quad dyn \tau e \mid stat \tau e \mid Err \mid chk K e \mid dyn e \mid stat e \\
 v &= i \mid \langle v, v \rangle \mid \lambda x. e \mid \lambda(x:\tau). e \mid mon(\tau \Rightarrow \tau) v \\
 E^\bullet &= [] \mid E^\bullet e \mid v E^\bullet \mid \langle E^\bullet, e \rangle \mid \langle v, E^\bullet \rangle \mid \\
 &\quad op^1 E^\bullet \mid op^2 E^\bullet e \mid op^2 v E^\bullet \mid chk K E^\bullet \\
 E &= E^\bullet \mid E e \mid v E \mid \langle E, e \rangle \mid \langle v, E \rangle \mid op^1 E \mid \\
 &\quad op^2 E e \mid op^2 v E \mid dyn \tau E \mid stat \tau E \\
 &\quad chk K E \mid dyn E \mid stat E
 \end{aligned}$$

$e \text{ } 1 \lesssim_E e$

$$\begin{aligned}
 &\frac{}{Err \text{ } 1 \lesssim_E Err} \quad \frac{}{Err \text{ } 1 \lesssim_E e^E} \quad \frac{e^1 \text{ } 1 \lesssim_E e^E}{chk K e^1 \text{ } 1 \lesssim_E e^E} \\
 &\frac{e^1 \text{ } 1 \lesssim_E e^E}{dyn e^1 \text{ } 1 \lesssim_E e^E} \quad \frac{e^1 \text{ } 1 \lesssim_E e^E}{stat e^1 \text{ } 1 \lesssim_E e^E} \quad \frac{}{x \text{ } 1 \lesssim_E x} \quad \frac{}{i \text{ } 1 \lesssim_E i} \\
 &\frac{e^1 \text{ } 1 \lesssim_E e^E}{\lambda x. e^1 \text{ } 1 \lesssim_E \lambda x. e^E} \quad \frac{e^1 \text{ } 1 \lesssim_E e^E}{\lambda(x:\tau). e^1 \text{ } 1 \lesssim_E \lambda(x:\tau). e^E} \\
 &\frac{e_0^1 \text{ } 1 \lesssim_E e_0^E \quad e_1^1 \text{ } 1 \lesssim_E e_1^E}{e_0^1 e_1^1 \text{ } 1 \lesssim_E e_0^E e_1^E} \quad \frac{e_0^1 \text{ } 1 \lesssim_E e_0^E \quad e_1^1 \text{ } 1 \lesssim_E e_1^E}{\langle e_0^1, e_1^1 \rangle \text{ } 1 \lesssim_E \langle e_0^E, e_1^E \rangle} \\
 &\frac{e_0^1 \text{ } 1 \lesssim_E e_0^E}{op^1 e_0^1 \text{ } 1 \lesssim_E op^1 e_0^E} \quad \frac{e_0^1 \text{ } 1 \lesssim_E e_0^E \quad e_1^1 \text{ } 1 \lesssim_E e_1^E}{op^2 e_0^1 e_1^1 \text{ } 1 \lesssim_E op^2 e_0^E e_1^E} \\
 &\frac{e_0^1 \text{ } 1 \lesssim_E e_0^E}{dyn \tau e_0^1 \text{ } 1 \lesssim_E dyn \tau e_0^E} \quad \frac{e_0^1 \text{ } 1 \lesssim_E e_0^E}{stat \tau e_0^1 \text{ } 1 \lesssim_E stat \tau e_0^E}
 \end{aligned}$$

$E \text{ } 1 \lesssim_E E$

$$\begin{aligned}
 &\frac{E^1 \text{ } 1 \lesssim_E E^E}{chk K E^1 \text{ } 1 \lesssim_E E^E} \quad \frac{E^1 \text{ } 1 \lesssim_E E^E}{dyn E^1 \text{ } 1 \lesssim_E E^E} \quad \frac{E^1 \text{ } 1 \lesssim_E E^E}{stat E^1 \text{ } 1 \lesssim_E E^E} \\
 &\frac{E^1 \text{ } 1 \lesssim_E E^E \quad e^1 \text{ } 1 \lesssim_E e^E}{E^1 e^1 \text{ } 1 \lesssim_E E^E e^E} \quad \frac{v_0 \text{ } 1 \lesssim_E v_1 \quad E^1 \text{ } 1 \lesssim_E E^E}{v_0 E^1 \text{ } 1 \lesssim_E v_1 E^E} \\
 &\frac{E^1 \text{ } 1 \lesssim_E E^E \quad e^1 \text{ } 1 \lesssim_E e^E}{\langle E^1, e^1 \rangle \text{ } 1 \lesssim_E \langle E^E, e^E \rangle} \quad \frac{v_0 \text{ } 1 \lesssim_E v_1 \quad E^1 \text{ } 1 \lesssim_E E^E}{\langle v_0, E^1 \rangle \text{ } 1 \lesssim_E \langle v_1, E^E \rangle} \\
 &\frac{E^1 \text{ } 1 \lesssim_E E^E}{op^1 E^1 \text{ } 1 \lesssim_E op^1 E^E} \quad \frac{E^1 \text{ } 1 \lesssim_E E^E \quad e^1 \text{ } 1 \lesssim_E e^E}{op^2 E^1 e^1 \text{ } 1 \lesssim_E op^2 E^E e^E} \\
 &\frac{v_0 \text{ } 1 \lesssim_E v_1 \quad E^1 \text{ } 1 \lesssim_E E^E}{op^2 v_0 E^1 \text{ } 1 \lesssim_E op^2 v_1 E^E} \quad \frac{E^1 \text{ } 1 \lesssim_E E^E}{dyn \tau E^1 \text{ } 1 \lesssim_E dyn \tau E^E} \\
 &\frac{E^1 \text{ } 1 \lesssim_E E^E}{stat \tau E^1 \text{ } 1 \lesssim_E stat \tau E^E}
 \end{aligned}$$

A.8.2 Theorems

Theorem 8.0 : Err approximation

If $e \in es$ and $\vdash e : \tau$ then the following statements hold:

- if $e \rightarrow_{E-S}^* Err$ then $e \rightarrow_{1-S}^* Err$
- if $e \rightarrow_{1-S}^* Err$ then $e \rightarrow_{H-S}^* Err$

Proof:

QED by 1-E approximation and H-1 approximation.

□

A.8.3 Lemmas

Lemma 8.1 : 1-E approximation

If $e \in es$ and $\vdash e : \tau$ and $e \rightarrow_{E-S}^* Err$ then $\vdash_1 e \rightsquigarrow e'' : \lfloor \tau \rfloor$ and $e'' \rightarrow_{1-S}^* Err$

Proof:

- $e'' \text{ } 1 \lesssim_E e$
by 1-E reflexivity
- QED by 1-E simulation

□

Lemma 8.2 : reflexivity

If $\vdash e : \tau$ and $\vdash_1 e \rightsquigarrow e'' : \lfloor \tau \rfloor$ then $e'' \text{ } 1 \lesssim_E e$.

Proof:

- e and e'' are identical up to chk expressions
by definition of \rightsquigarrow
- QED by definition of $1 \lesssim_E$

□

Lemma 8.3 : E-1 simulation

If $e_0^1 \text{ } 1 \lesssim_E e_0^E$ and $e_0^E \rightarrow_{E-S} e_1^E$ and $e_0^1 \notin Err$ then:

- $e_0^1 \rightarrow_{1-S} \dots \rightarrow_{1-S} e_n^1$
- $\forall i \in \{1..n-1\}. e_i^1 \text{ } 1 \lesssim_E e_0^E$
- $e_n^1 \text{ } 1 \lesssim_E e_1^E$

Proof:

12211 **CASE** $e_0^E = E^E[e_0^E]$
 12212 $\wedge e_{0'}^E \triangleright_{E-S} e_1^E$
 12213 $\wedge e_1^E = E^E[e_1^E]$:
 12214 1. $e_0^1 = E^1[e_0^1]$
 12215 $\wedge E^1 \underset{1}{\lesssim}_E E^E$
 12216 $\wedge e_{0'}^1 \underset{1}{\lesssim}_E e_{0'}^E$
 12217 by 1-E context factoring
 12218 2. $E^1[e_0^1] \rightarrow_{1-S} \dots \rightarrow_{1-S} E^1[e_{n-1}^1]$
 12219 $\wedge \forall i \in \{1..n-1\}. E^1[e_i^1] \underset{1}{\lesssim}_E E^E[e_i^E]$
 12220 $\wedge e_{n-1}^1 \neq \text{chk } \tau \ e$
 12221 $\wedge e_{n-1}^1 \neq \text{dyn } e$
 12222 $\wedge e_{n-1}^1 \neq \text{stat } e$
 12223 by repeated uses of 1-E stutter (1)
 12224 3. **IF** $e_{n-1}^1 \in \text{Err}$:
 12225 a. QED $e_0^1 \rightarrow_{1-S}^* \text{Err}$
 12226 **ELSE** $e_{n-1}^1 \notin \text{Err}$:
 12227 a. $E^1[e_{n-1}^1] \rightarrow_{1-S} E^1[e_n^1]$
 12228 $\wedge e_n^1 \underset{1}{\lesssim}_E e_1^E$
 12229 by 1-E step (1, 2)
 12230 b. QED 1-E context congruence
 12231 \square

12232 **Lemma 8.4 : 1-E context factoring**

12233 If $e_0^1 \underset{1}{\lesssim}_E e_0^E$ and $e_0^E = E_0^E[e_1^E]$ then $e_0^1 = E_0^1[e_{0'}^1]$ and $E_0^1 \underset{1}{\lesssim}_E E_0^E$
 12234 and $e_{0'}^1 \underset{1}{\lesssim}_E e_{0'}^E$

12235 *Proof:*

12236 QED by structural induction on the derivation of $e_0^1 \underset{1}{\lesssim}_E$
 12237 e_0^E
 12238 \square

12239 **Lemma 8.5 : 1-E stutter**

12240 If $E^1[e^1] \underset{1}{\lesssim}_E E^E[e^E]$ and $e^1 = E_0^1[\text{Err}]$
 12241 $\vee e^1 = E_0^1[\text{chk } K \ v_0]$
 12242 $\vee e^1 = E_0^1[\text{dyn } v_0]$
 12243 $\vee e^1 = E_0^1[\text{stat } v_0]$
 12244 then $E^1[e^1] \rightarrow_{1-S} E^1[e_1^1]$ and $E^1[e_1^1] \underset{1}{\lesssim}_E E^E[e^E]$.
 12245 *Proof:*

12246 **CASE** $e^1 = E_0^1[\text{Err}]$:
 12247 1. QED $E^1[e^1] \rightarrow_{1-S} \text{Err}$
 12248 **CASE** $e^1 = E_0^1[\text{chk } K \ v_0]$:
 12249 **IF** $X(K, v_0) = \text{BndryErr}$:
 12250 1. QED $E^1[E_0^1[\text{chk } K \ v_0]] \rightarrow_{1-S} \text{BndryErr}$
 12251 **ELSE** $X(K, v_0) = v_0$:
 12252 1. $E^1[E_0^1[\text{chk } K \ v_0]] \rightarrow_{1-S} E^1[E_0^1[v_0]]$
 12253 2. $E^1[E_0^1[v_0]] \underset{1}{\lesssim}_E E^E[e^E]$
 12254 by $E^1[E_0^1[\text{chk } K \ v_0]] \underset{1}{\lesssim}_E E^E[e^E]$
 12255 3. QED
 12256 **CASE** $e^1 = E_0^1[\text{dyn } v_0]$:
 12257 1. $E^1[E_0^1[\text{dyn } v_0]] \rightarrow_{1-S} E^1[E_0^1[v_0]]$
 12258 2. $E^1[E_0^1[v_0]] \underset{1}{\lesssim}_E E^E[e^E]$
 12259 by $E^1[E_0^1[\text{dyn } v_0]] \underset{1}{\lesssim}_E E^E[e^E]$
 12260 3. QED
 12261 **CASE** $e^1 = E_0^1[\text{stat } v_0]$:
 12262 1. $E^1[E_0^1[\text{stat } v_0]] \rightarrow_{1-S} E^1[E_0^1[v_0]]$
 12263 \square

12264 2. $E^1[E_0^1[v_0]] \underset{1}{\lesssim}_E E^E[e^E]$
 12265 by $E^1[E_0^1[\text{stat } v_0]] \underset{1}{\lesssim}_E E^E[e^E]$
 12266 3. QED
 12267 \square

12268 **Lemma 8.6 : 1-E step**

12269 If $E^1[e^1] \underset{1}{\lesssim}_E E^E[e^E]$ and $e^1 \notin \{\text{chk } \tau \ e, \text{dyn } e, \text{stat } e\}$ and
 12270 $e^E \triangleright_{E-S} e_1^E$ then $E^1[e^1] \rightarrow_{1-S} E^1[e_1^1]$ and $e_1^1 \underset{1}{\lesssim}_E e_1^E$

12271 *Proof:*

12272 By boundary factoring and static hole typing, the inner
 12273 expression e^1 is either typed or untyped.

12274 **CASE** $\vdash_1 e^1$:

12275 QED by case analysis on $e^E \triangleright_{E-S} e_1^E$; either e^1 steps in
 12276 the same manner, or e^1 steps to a boundary error due
 12277 to the application of a typed function to an invalid
 12278 argument

12279 **CASE** $\vdash_1 e^1 : K$:

12280 QED by case analysis on $e^E \triangleright_{E-S} e_1^E$; note that $e_1^E \notin$
 12281 TagErr since e^1 is well-typed.
 12282 \square

12283 **Lemma 8.7 : 1-E context congruence**

12284 If $e^1 \underset{1}{\lesssim}_E e^E$ and $E^1 \underset{1}{\lesssim}_E E^E$ then $E^1[e^1] \underset{1}{\lesssim}_E E^E[e^E]$

12285 *Proof:*

12286 QED by definition of $\underset{1}{\lesssim}_E$
 12287 \square

12288 **Lemma 8.8 : reflexivity**

12289 If $\vdash e : \tau$ then $e \underset{1}{\lesssim}_E e$.

12290 *Proof:*

12291 By structural induction on the derivation of $\vdash e : \tau$.
 12292 TODO
 12293 \square

12294 **Lemma 8.9 : 1-H simulation**

12295 yolo

12296 *Proof:*

12297 nooo
 12298 \square