

# Dynamic Updating of Information-Flow Policies

Michael Hicks\*    Boniface Hicks†    Stephen Tse‡    Steve Zdancewic‡  
\* University of Maryland    † Pennsylvania State University    ‡ University of Pennsylvania

March 21, 2005

This report is automatically generated by the tool `lf2tex` from the semantics specification `update.elf` (Twelf source) and the syntactic specification `update.tex` (L<sup>A</sup>T<sub>E</sub>X source).

Some notes about the typesetting used in this report:

- A syntax class is displayed boxed like  $\boxed{e ::= \dots}$  (*terms*).
- A syntax entity is displayed unboxed like  $e ::= \lambda x:t. e$  (*functions*).
- A judgement form is displayed boxed like  $\boxed{\Pi; \Gamma \vdash e : t}$  (*typings*).
- A judgement rule is displayed unboxed like  $\frac{\Pi; \Gamma, x:t_1 \vdash e : t_2}{\Pi; \Gamma \vdash \lambda x:t. e : t_1 \rightarrow t_2}$  (*typing for functions*).
- A theorem is displayed boxed like  $\boxed{\frac{\Pi_1; \Gamma \vdash e_1 : t \quad (\Pi_1; e_1) \longrightarrow (\Pi_2; e_2)}{\Pi_2; \Gamma \vdash e_2 : t}}$  (*preservations*).
- A proof is displayed as a numbered list with the last one of the list being the conclusion. (A rule name with downarrow ( $\downarrow$  ty-fun) means by the inversion of such rule.)

## Contents

<b>1</b>	<b>Syntax</b>	<b>3</b>
1.1	Constants . . . . .	3
1.2	Principals . . . . .	3
1.3	Labels . . . . .	3
1.4	Hierarchies . . . . .	3
1.5	Types . . . . .	3
1.6	Variables . . . . .	3
1.7	Terms . . . . .	3
1.8	Contexts . . . . .	4
<b>2</b>	<b>Static semantics</b>	<b>5</b>
2.1	Substitutions . . . . .	5
2.2	Principal subtypings . . . . .	5
2.3	Label subtypings . . . . .	5
2.4	Hierarchy subtypings . . . . .	6
2.5	Type subtypings . . . . .	6
2.6	Type labels . . . . .	6
2.7	Typings . . . . .	6

<b>3</b>	<b>Dynamic semantics</b>	<b>8</b>
3.1	Values . . . . .	8
3.2	Holes . . . . .	8
3.3	Splits . . . . .	8
3.4	Combines . . . . .	8
3.5	Small-step evaluations . . . . .	8
3.6	Tag checkings . . . . .	9
3.7	Top-level evaluations . . . . .	9
3.8	Totalities . . . . .	9
3.9	Program evaluations . . . . .	10
<b>4</b>	<b>Lemmas</b>	<b>11</b>
4.1	Principal subtypings . . . . .	11
4.2	Label subtypings . . . . .	13
4.3	Hierarchy subtypings . . . . .	14
4.4	Type subtypings . . . . .	15
4.5	Tag checkings . . . . .	18
4.6	Permutations . . . . .	20
4.7	Substitutions . . . . .	22
<b>5</b>	<b>Theorems</b>	<b>25</b>
5.1	Preservation . . . . .	25
5.2	Progress . . . . .	26
5.3	Soundness . . . . .	29
<b>6</b>	<b>Translations</b>	<b>31</b>
6.1	Types . . . . .	31
6.2	Terms . . . . .	31
6.3	Contexts . . . . .	31
6.4	Type labels . . . . .	31
6.5	Subtypings . . . . .	31
6.6	Typings . . . . .	31
6.7	Theorems . . . . .	32

# 1 Syntax

## 1.1 Constants

$\boxed{c ::= \dots}$   $\boxed{c}$

## 1.2 Principals

$\boxed{p ::= \dots}$   $\boxed{p}$

$p ::= c$  (pc)

$p ::= p, p$  (pcat)

## 1.3 Labels

$\boxed{l ::= \dots}$   $\boxed{l}$

$l ::= p: p$  (lp)

$l ::= l, l$  (lcat)

## 1.4 Hierarchies

$\boxed{\Pi ::= \dots}$   $\boxed{a}$

$\Pi ::= \cdot$  (az)

$\Pi ::= \Pi, p \leq p$  (ap)

## 1.5 Types

$\boxed{t ::= \dots}$   $\boxed{t}$

$t ::= \text{bool}_\ell$  (tbool)

$t ::= t \rightarrow t$  (tfun)

## 1.6 Variables

$\boxed{x ::= \dots}$   $\boxed{x}$

## 1.7 Terms

$\boxed{e ::= \dots}$   $\boxed{e}$

$e ::= \text{true}_\ell$  (true)

$e ::= \text{false}_\ell$  (false)

$e ::= x$  (var)

$e ::= \lambda[\Pi]x:t. e$  (fun)

$e ::= e e$  (app)

$e ::= \text{if } e e e$  (ifb)

$e ::= \text{if } (p \leq p) e e$  (ifp)

$e ::= [l \sqsubseteq \ell]e$  (tag)

## 1.8 Contexts

$\Gamma ::= \dots$

$\Gamma ::= \cdot$

$\Gamma ::= \Gamma, x:t$

$\boxed{g}$

$(gz)$

$(gx)$

## 2 Static semantics

### 2.1 Substitutions

$\boxed{e\{e/x\} = e}$	$\boxed{\text{sub}}$
$\text{true}_\ell\{e/x\} = \text{true}_\ell$	(sub-true)
$\text{false}_\ell\{e/x\} = \text{false}_\ell$	(sub-false)
$x\{e/x\} = e$	(sub-var1)
$x_1\{e/x_2\} = x_1$	(sub-var2)
$\frac{e_1\{e/x\} = e_2}{(\lambda[\prod]x_1 : t. e_1)\{e/x\} = (\lambda[\prod]x_1 : t. e_2)}$	(sub-fun)
$\frac{e_1\{e/x\} = e_3 \quad e_2\{e/x\} = e_4}{(e_1 \ e_2)\{e/x\} = (e_3 \ e_4)}$	(sub-app)
$\frac{e_1\{e/x\} = e_4 \quad e_2\{e/x\} = e_5 \quad e_3\{e/x\} = e_6}{(\text{if } e_1 \ e_2 \ e_3)\{e/x\} = (\text{if } e_4 \ e_5 \ e_6)}$	(sub-ifb)
$\frac{e_1\{e/x\} = e_3 \quad e_2\{e/x\} = e_4}{(\text{if } (p_1 \leq p_2) \ e_1 \ e_2)\{e/x\} = (\text{if } (p_1 \leq p_2) \ e_3 \ e_4)}$	(sub-ifp)
$\frac{e_1\{e/x\} = e_2}{([\ell_1 \sqsubseteq \ell_2]e_1)\{e/x\} = ([\ell_1 \sqsubseteq \ell_2]e_2)}$	(sub-tag)

### 2.2 Principal subtypings

$\boxed{\text{some } p}$	$\boxed{\text{psome}}$
$\boxed{\prod \vdash p \leq p}$	$\boxed{\text{pst}}$
$\boxed{\prod \not\vdash p \leq p}$	$\boxed{\text{pnst}}$
$\prod \vdash p \leq p$	(pst-z)
$\frac{\text{some } p_2 \quad \prod \vdash p_1 \leq p_2 \quad \prod \vdash p_2 \leq p_3}{\prod \vdash p_1 \leq p_3}$	(pst-x)
$\prod, p_1 \leq p_2 \vdash p_1 \leq p_2$	(pst-a1)
$\frac{\prod \vdash p_3 \leq p_4}{\prod, p_1 \leq p_2 \vdash p_3 \leq p_4}$	(pst-a2)
$\prod \vdash p_1, p_2 \leq p_1$	(pst-cat1)
$\prod \vdash p_1, p_2 \leq p_2$	(pst-cat2)

### 2.3 Label subtypings

$\boxed{\prod \vdash \ell \sqsubseteq \ell}$	$\boxed{\text{lst}}$
$\boxed{\prod \vdash \ell \not\sqsubseteq \ell}$	$\boxed{\text{lnst}}$
$\boxed{\text{some } \ell}$	$\boxed{\text{lsome}}$
$\prod \vdash \ell \sqsubseteq \ell$	(lst-z)

$$\frac{\text{some } \ell_2 \quad \Pi \vdash \ell_1 \sqsubseteq \ell_2 \quad \Pi \vdash \ell_2 \sqsubseteq \ell_3}{\Pi \vdash \ell_1 \sqsubseteq \ell_3} \quad (\text{lst-x})$$

$$\frac{\Pi \vdash p_1 \leq p_3 \quad \Pi \vdash p_2 \leq p_4}{\Pi \vdash p_1 : p_2 \sqsubseteq p_3 : p_4} \quad (\text{lst-p})$$

$$\Pi \vdash \ell_1 \sqsubseteq \ell_1, \ell_2 \quad (\text{lst-cat1})$$

$$\Pi \vdash \ell_2 \sqsubseteq \ell_1, \ell_2 \quad (\text{lst-cat2})$$

## 2.4 Hierarchy subtypings

$$\boxed{\text{some } \Pi} \quad \boxed{\text{asome}}$$

$$\boxed{\Pi \leq \Pi} \quad \boxed{\text{ast}}$$

$$\Pi \leq \Pi \quad (\text{ast-z})$$

$$\frac{\text{some } \Pi_2 \quad \Pi_1 \leq \Pi_2 \quad \Pi_2 \leq \Pi_3}{\Pi_1 \leq \Pi_3} \quad (\text{ast-x})$$

$$\frac{\Pi_1 \leq \Pi_2}{(\Pi_1, p_1 \leq p_2) \leq \Pi_2} \quad (\text{ast-p1})$$

$$\frac{\Pi_1 \leq \Pi_2 \quad \Pi_1 \vdash p_3 \leq p_4}{\Pi_1 \leq (\Pi_2, p_3 \leq p_4)} \quad (\text{ast-p2})$$

## 2.5 Type subtypings

$$\boxed{\Pi \vdash t \preceq t} \quad \boxed{\text{tst}}$$

$$\frac{\Pi \vdash \ell_1 \sqsubseteq \ell_2}{\Pi \vdash \text{bool}_{\ell_1} \preceq \text{bool}_{\ell_2}} \quad (\text{tst-bool})$$

$$\frac{\Pi \vdash t_3 \preceq t_1 \quad \Pi \vdash t_2 \preceq t_4}{\Pi \vdash t_1 \rightarrow t_2 \preceq t_3 \rightarrow t_4} \quad (\text{tst-fun})$$

## 2.6 Type labels

$$\boxed{\text{lab}(t) = \ell} \quad \boxed{\text{lab}}$$

$$\text{lab}(\text{bool}_{\ell}) = \ell \quad (\text{lab-bool})$$

$$\frac{\text{lab}(t_2) = \ell}{\text{lab}(t_1 \rightarrow t_2) = \ell} \quad (\text{lab-fun})$$

## 2.7 Typings

$$\boxed{\Pi; \Gamma \vdash e : t} \quad \boxed{\text{ty}}$$

$$\Pi; \Gamma \vdash \text{true}_{\ell} : \text{bool}_{\ell} \quad (\text{ty-true})$$

$$\Pi; \Gamma \vdash \text{false}_{\ell} : \text{bool}_{\ell} \quad (\text{ty-false})$$

$$\frac{\Pi; \Gamma \vdash e_1 : \text{bool}_{\ell} \quad \Pi; \Gamma \vdash e_2 : t \quad \Pi; \Gamma \vdash e_3 : t \quad \text{lab}(t) = \ell}{\Pi; \Gamma \vdash \text{if } e_1 \ e_2 \ e_3 : t} \quad (\text{ty-ifb})$$

$$\Pi; \Gamma, x : t \vdash x : t \quad (\text{ty-var1})$$

$$\frac{\Pi; \Gamma \vdash x_2 : t_2}{\Pi; \Gamma, x_1 : t_1 \vdash x_2 : t_2} \quad (\text{ty-var2})$$

$$\frac{\Pi \leq \Pi_1 \quad \Pi_1; \Gamma, x : t_1 \vdash e : t_2}{\Pi; \Gamma \vdash \lambda[\Pi_1]x : t_1. e : t_1 \rightarrow t_2} \quad (\text{ty-fun})$$

$$\frac{\Pi; \Gamma \vdash e_1 : t_1 \rightarrow t_2 \quad \Pi; \Gamma \vdash e_2 : t_1}{\Pi; \Gamma \vdash e_1 e_2 : t_2} \quad (\text{ty-app})$$

$$\frac{\Pi, p_1 \leq p_2; \Gamma \vdash e_1 : t \quad \Pi; \Gamma \vdash e_2 : t}{\Pi; \Gamma \vdash \text{if } (p_1 \leq p_2) e_1 e_2 : t} \quad (\text{ty-ifp})$$

$$\frac{\Pi \vdash \ell_1 \sqsubseteq \ell_2 \quad \Pi; \Gamma \vdash e : \text{bool}_{\ell_1}}{\Pi; \Gamma \vdash [\ell_1 \sqsubseteq \ell_2]e : \text{bool}_{\ell_2}} \quad (\text{ty-tag})$$

### 3 Dynamic semantics

#### 3.1 Values

$\text{val } e$	$\text{val}$
$\text{val true}_\ell$	(val-true)
$\text{val false}_\ell$	(val-false)
$\text{val } (\lambda[\Pi]x:t. e)$	(val-fun)

#### 3.2 Holes

$\mathcal{E} ::= \dots$	$q$
$\mathcal{E} ::= \mathcal{E} e$	(qappa)
$\mathcal{E} ::= e \mathcal{E}$	(qappb)
$\mathcal{E} ::= \text{if } \mathcal{E} e e$	(qifb)
$\mathcal{E} ::= [\ell \sqsubseteq \ell] \mathcal{E}$	(qtag)

#### 3.3 Splits

$e = \mathcal{E}[e]$	$\text{split}$
$\text{if } e_1 e_2 e_3 = \text{if } \mathcal{E} e_2 e_3[e_1]$	(split-ifb)
$e_1 e_2 = \mathcal{E} e_2[e_1]$	(split-app1)
$e_1 e_2 = e_1 \mathcal{E}[e_2]$	(split-app2)
$[\ell_1 \sqsubseteq \ell_2] e = [\ell_1 \sqsubseteq \ell_2] \mathcal{E}[e]$	(split-tag)

#### 3.4 Combines

$\mathcal{E}[e] = e$	$\text{combine}$
$\mathcal{E} e_2[e_1] = e_1 e_2$	(combine-app1)
$e_1 \mathcal{E}[e_2] = e_1 e_2$	(combine-app2)
$\text{if } \mathcal{E} e_2 e_3[e_1] = \text{if } e_1 e_2 e_3$	(combine-ifb)
$[\ell_1 \sqsubseteq \ell_2] \mathcal{E}[e] = [\ell_1 \sqsubseteq \ell_2] e$	(combine-tag)

#### 3.5 Small-step evaluations

$\Pi \vdash e \longrightarrow e$	$\text{ev}$
$\frac{\text{val } e_2 \quad e_1 \{e_2/x\} = e_3}{\Pi \vdash (\lambda[\Pi_1]x:t. e_1) e_2 \longrightarrow e_3}$	(ev-app)
$\Pi \vdash \text{if true}_\ell e_1 e_2 \longrightarrow e_1$	(ev-ifb1)
$\Pi \vdash \text{if false}_\ell e_1 e_2 \longrightarrow e_2$	(ev-ifb2)
$\frac{\Pi \vdash p_1 \leq p_2}{\Pi \vdash \text{if } (p_1 \leq p_2) e_1 e_2 \longrightarrow e_1}$	(ev-ifp1)

$$\frac{\Pi \not\vdash p_1 \leq p_2}{\Pi \vdash \text{if } (p_1 \leq p_2) e_1 e_2 \longrightarrow e_2} \quad (\text{ev-ifp2})$$

$$\Pi \vdash [\ell_1 \sqsubseteq \ell_2] \text{true}_{\ell_1} \longrightarrow \text{true}_{\ell_2} \quad (\text{ev-tag1})$$

$$\Pi \vdash [\ell_1 \sqsubseteq \ell_2] \text{false}_{\ell_1} \longrightarrow \text{false}_{\ell_2} \quad (\text{ev-tag2})$$

$$\frac{e_1 = \mathcal{E}[e_2] \quad \Pi \vdash e_2 \longrightarrow e_3 \quad \mathcal{E}[e_3] = e_4}{\Pi \vdash e_1 \longrightarrow e_4} \quad (\text{ev-hole})$$

### 3.6 Tag checkings

$$\boxed{\Pi \vdash e} \quad \boxed{\text{ae}}$$

$$\Pi \vdash \text{true}_{\ell} \quad (\text{ae-true})$$

$$\Pi \vdash \text{false}_{\ell} \quad (\text{ae-false})$$

$$\frac{\Pi \leq \Pi_1}{\Pi \vdash \lambda[\Pi_1]x:t. e} \quad (\text{ae-fun})$$

$$\frac{\Pi \vdash e_1 \quad \Pi \vdash e_2}{\Pi \vdash e_1 e_2} \quad (\text{ae-app})$$

$$\frac{\Pi \vdash e_1 \quad \Pi \vdash e_2 \quad \Pi \vdash e_3}{\Pi \vdash \text{if } e_1 e_2 e_3} \quad (\text{ae-ifb})$$

$$\frac{\Pi, p_1 \leq p_2 \vdash e_1 \quad \Pi \vdash e_2}{\Pi \vdash \text{if } (p_1 \leq p_2) e_1 e_2} \quad (\text{ae-ifp})$$

$$\frac{\Pi \vdash \ell_1 \sqsubseteq \ell_2 \quad \Pi \vdash e}{\Pi \vdash [\ell_1 \sqsubseteq \ell_2]e} \quad (\text{ae-tag})$$

### 3.7 Top-level evaluations

$$\boxed{\langle \Pi; e \rangle | \Pi \longrightarrow \langle \Pi; e \rangle} \quad \boxed{\text{topev}}$$

$$\frac{\Pi \vdash e_1 \longrightarrow e_2}{\langle \Pi; e_1 \rangle | \Pi \longrightarrow \langle \Pi; e_2 \rangle} \quad (\text{topev-ev})$$

$$\frac{\Pi_2 \vdash e}{\langle \Pi_1; e \rangle | \Pi_2 \longrightarrow \langle \Pi_2; e \rangle} \quad (\text{topev-upd})$$

### 3.8 Totalities

$$\boxed{\text{some } \Pi} \quad \boxed{\text{asome-total}}$$

$$\boxed{e_1 \{e/x\} = e_2} \quad \boxed{\text{sub-total}}$$

$$\boxed{\Pi \vdash p \diamond p} \quad \boxed{\text{psty}}$$

$$\frac{\Pi \vdash p_1 \leq p_2}{\Pi \vdash p_1 \diamond p_2} \quad (\text{psty-pst})$$

$$\frac{\Pi \not\vdash p_1 \leq p_2}{\Pi \vdash p_1 \diamond p_2} \quad (\text{psty-pnst})$$

$$\boxed{\Pi \vdash p_1 \diamond p_2} \quad \boxed{\text{pst-total}}$$

### 3.9 Program evaluations

$$\begin{array}{c}
 \boxed{\langle \Pi; \mathbf{e} \rangle \Downarrow \langle \Pi; \mathbf{e} \rangle} \\
 \frac{\text{val } \mathbf{e}}{\langle \Pi; \mathbf{e} \rangle \Downarrow \langle \Pi; \mathbf{e} \rangle} \\
 \frac{\text{some } \Pi \quad \langle \Pi_1; \mathbf{e}_1 \rangle \mid \Pi \longrightarrow \langle \Pi_2; \mathbf{e}_2 \rangle \quad \langle \Pi_2; \mathbf{e}_2 \rangle \Downarrow \langle \Pi_3; \mathbf{e}_3 \rangle}{\langle \Pi_1; \mathbf{e}_1 \rangle \Downarrow \langle \Pi_2; \mathbf{e}_3 \rangle}
 \end{array}
 \begin{array}{l}
 \boxed{\text{big ev}} \\
 (\text{big ev-v}) \\
 (\text{big ev-e})
 \end{array}$$

## 4 Lemmas

### 4.1 Principal subtypings

$\frac{\Pi \vdash p_1 \leq p_2}{\Pi, p_3 \leq p_4 \vdash p_1 \leq p_2}$	appst
1: $\Pi \vdash p_1 \leq p_1$ 2: $\Pi, p_2 \leq p_3 \vdash p_1 \leq p_1$	(appst-z) *given pst-z
1: $\Pi \vdash p_5 \leq p_2$ 2: <b>some</b> $p_1$ 3: $\Pi \vdash p_5 \leq p_1$ 4: $\Pi, p_3 \leq p_4 \vdash p_5 \leq p_1$ 5: $\Pi \vdash p_1 \leq p_2$ 6: $\Pi, p_3 \leq p_4 \vdash p_1 \leq p_2$ 7: $\Pi, p_3 \leq p_4 \vdash p_5 \leq p_2$	(appst-x) *given $\downarrow$ pst-x: 1 $\downarrow$ pst-x: 1 appst: 3 $\downarrow$ pst-x: 1 appst: 5 pst-x: 2,4,6
1: $\Pi, p_1 \leq p_2 \vdash p_1 \leq p_2$ 2: $(\Pi, p_1 \leq p_2), p_3 \leq p_4 \vdash p_1 \leq p_2$	(appst-a1) *given pst-a2: 1
1: $\Pi, p_3 \leq p_4 \vdash p_1 \leq p_2$ 2: $\Pi \vdash p_1 \leq p_2$ 3: $(\Pi, p_3 \leq p_4), p_5 \leq p_6 \vdash p_1 \leq p_2$	(appst-a2) *given $\downarrow$ pst-a2: 1 pst-a2: 1
1: $\Pi \vdash p_1, p_2 \leq p_1$ 2: $\Pi, p_3 \leq p_4 \vdash p_1, p_2 \leq p_1$	(appst-cat1) *given pst-cat1
1: $\Pi \vdash p_1, p_2 \leq p_2$ 2: $\Pi, p_3 \leq p_4 \vdash p_1, p_2 \leq p_2$	(appst-cat2) *given pst-cat2
$\frac{\Pi, p_1 \leq p_2 \vdash p_3 \leq p_4 \quad \Pi \vdash p_1 \leq p_2}{\Pi \vdash p_3 \leq p_4}$	pstpst
1: $\Pi, p_1 \leq p_2 \vdash p_3 \leq p_3$ 2: $\Pi \vdash p_1 \leq p_2$ 3: $\Pi \vdash p_3 \leq p_3$	(pstpst-z) *given *given pst-z
1: $\Pi, p_1 \leq p_2 \vdash p_5 \leq p_4$ 2: <b>some</b> $p_3$ 3: $\Pi, p_1 \leq p_2 \vdash p_5 \leq p_3$ 4: $\Pi \vdash p_1 \leq p_2$ 5: $\Pi \vdash p_5 \leq p_3$ 6: $\Pi, p_1 \leq p_2 \vdash p_3 \leq p_4$ 7: $\Pi \vdash p_3 \leq p_4$ 8: $\Pi \vdash p_5 \leq p_4$	(pstpst-x) *given $\downarrow$ pst-x: 1 $\downarrow$ pst-x: 1 *given pstpst: 3,4 $\downarrow$ pst-x: 1 pstpst: 6,4 pst-x: 2,5,7

1:  $\Pi, p_1 \leq p_2 \vdash p_1 \leq p_2$   
 2:  $\Pi \vdash p_1 \leq p_2$

(pstpst-a1)  
 \*given  
 \*given

1:  $\Pi \vdash p_1 \leq p_2$   
 2:  $\Pi, p_1 \leq p_2 \vdash p_3 \leq p_4$   
 3:  $\Pi \vdash p_3 \leq p_4$

(pstpst-a2)  
 \*given  
 \*given  
 $\downarrow$ pst-a2: 2

1:  $\Pi, p_1 \leq p_2 \vdash p_3, p_4 \leq p_3$   
 2:  $\Pi \vdash p_1 \leq p_2$   
 3:  $\Pi \vdash p_3, p_4 \leq p_3$

(pstpst-cat1)  
 \*given  
 \*given  
 pst-cat1

1:  $\Pi, p_1 \leq p_2 \vdash p_3, p_4 \leq p_4$   
 2:  $\Pi \vdash p_1 \leq p_2$   
 3:  $\Pi \vdash p_3, p_4 \leq p_4$

(pstpst-cat2)  
 \*given  
 \*given  
 pst-cat2

$$\frac{\Pi_1 \vdash p_1 \leq p_2 \quad \Pi_2 \leq \Pi_1}{\Pi_2 \vdash p_1 \leq p_2}$$

astpst

1:  $\Pi_1 \vdash p \leq p$   
 2:  $\Pi_2 \leq \Pi_1$   
 3:  $\Pi_2 \vdash p \leq p$

(astpst-z)  
 \*given  
 \*given  
 pst-z

1:  $\Pi_1 \vdash p_3 \leq p_2$   
 2: some  $p_1$   
 3:  $\Pi_1 \vdash p_3 \leq p_1$   
 4:  $\Pi_2 \leq \Pi_1$   
 5:  $\Pi_2 \vdash p_3 \leq p_1$   
 6:  $\Pi_1 \vdash p_1 \leq p_2$   
 7:  $\Pi_2 \vdash p_1 \leq p_2$   
 8:  $\Pi_2 \vdash p_3 \leq p_2$

(astpst-x)  
 \*given  
 $\downarrow$ pst-x: 1  
 $\downarrow$ pst-x: 1  
 \*given  
 astpst: 3,4  
 $\downarrow$ pst-x: 1  
 astpst: 6,4  
 pst-x: 2,5,7

1:  $\Pi_1, p_1 \leq p_2 \vdash p_1 \leq p_2$   
 2:  $(\Pi_2, p_1 \leq p_2) \leq (\Pi_1, p_1 \leq p_2)$   
 3:  $\Pi_2, p_1 \leq p_2 \vdash p_1 \leq p_2$

(astpst-a1)  
 \*given  
 \*given  
 pst-a1

1:  $\Pi_2 \leq (\Pi_1, p_3 \leq p_4)$   
 2:  $\Pi_2 \vdash p_3 \leq p_4$   
 3:  $\Pi_1, p_3 \leq p_4 \vdash p_1 \leq p_2$   
 4:  $\Pi_1 \vdash p_1 \leq p_2$   
 5:  $\Pi_2 \leq \Pi_1$   
 6:  $\Pi_2 \vdash p_1 \leq p_2$

(astpst-a2)  
 \*given  
 $\downarrow$ ast-p2: 1  
 \*given  
 $\downarrow$ pst-a2: 3  
 $\downarrow$ ast-p2: 1  
 astpst: 4,5

1:  $\Pi_1 \vdash p_1, p_2 \leq p_1$   
 2:  $\Pi_2 \leq \Pi_1$   
 3:  $\Pi_2 \vdash p_1, p_2 \leq p_1$

(astpst-cat1)  
 \*given  
 \*given  
 pst-cat1

1: $\Pi_1 \vdash p_1, p_2 \leq p_2$	(astpst-cat2)
2: $\Pi_2 \leq \Pi_1$	*given
3: $\Pi_2 \vdash p_1, p_2 \leq p_2$	*given
	pst-cat2

## 4.2 Label subtypings

$$\frac{\Pi, p_1 \leq p_2 \vdash \ell_1 \sqsubseteq \ell_2 \quad \Pi \vdash p_1 \leq p_2}{\Pi \vdash \ell_1 \sqsubseteq \ell_2}$$

pstlst

1: $\Pi, p_1 \leq p_2 \vdash \ell \sqsubseteq \ell$	(pstlst-z)
2: $\Pi \vdash p_1 \leq p_2$	*given
3: $\Pi \vdash \ell \sqsubseteq \ell$	*given
	lst-z

1: $\Pi, p_1 \leq p_2 \vdash \ell_3 \sqsubseteq \ell_2$	(pstlst-x)
2: <b>some</b> $\ell_1$	*given
3: $\Pi, p_1 \leq p_2 \vdash \ell_3 \sqsubseteq \ell_1$	↓lst-x: 1
4: $\Pi \vdash p_1 \leq p_2$	↓lst-x: 1
5: $\Pi \vdash \ell_3 \sqsubseteq \ell_1$	*given
6: $\Pi, p_1 \leq p_2 \vdash \ell_1 \sqsubseteq \ell_2$	pstlst: 3,4
7: $\Pi \vdash \ell_1 \sqsubseteq \ell_2$	↓lst-x: 1
8: $\Pi \vdash \ell_3 \sqsubseteq \ell_2$	pstlst: 6,4
	lst-x: 2,5,7

1: $\Pi, p_1 \leq p_2 \vdash p_5 : p_3 \sqsubseteq p_6 : p_4$	(pstlst-p)
2: $\Pi, p_1 \leq p_2 \vdash p_5 \leq p_6$	*given
3: $\Pi \vdash p_1 \leq p_2$	↓lst-p: 1
4: $\Pi \vdash p_5 \leq p_6$	*given
5: $\Pi, p_1 \leq p_2 \vdash p_3 \leq p_4$	pstpst: 2,3
6: $\Pi \vdash p_3 \leq p_4$	↓lst-p: 1
7: $\Pi \vdash p_5 : p_3 \sqsubseteq p_6 : p_4$	pstpst: 5,3
	lst-p: 4,6

1: $\Pi, p_1 \leq p_2 \vdash \ell_1 \sqsubseteq \ell_1, \ell_2$	(pstlst-cat1)
2: $\Pi \vdash p_1 \leq p_2$	*given
3: $\Pi \vdash \ell_1 \sqsubseteq \ell_1, \ell_2$	*given
	lst-cat1

1: $\Pi, p_1 \leq p_2 \vdash \ell_1 \sqsubseteq \ell_2, \ell_1$	(pstlst-cat2)
2: $\Pi \vdash p_1 \leq p_2$	*given
3: $\Pi \vdash \ell_1 \sqsubseteq \ell_2, \ell_1$	*given
	lst-cat2

$$\frac{\Pi_1 \vdash \ell_1 \sqsubseteq \ell_2 \quad \Pi_2 \leq \Pi_1}{\Pi_2 \vdash \ell_1 \sqsubseteq \ell_2}$$

astlst

1: $\Pi_1 \vdash \ell \sqsubseteq \ell$	(astlst-z)
2: $\Pi_2 \leq \Pi_1$	*given
3: $\Pi_2 \vdash \ell \sqsubseteq \ell$	*given
	lst-z

1: $\Pi_1 \vdash \ell_3 \sqsubseteq \ell_2$	(astlst-x)
2: <b>some</b> $\ell_1$	*given
3: $\Pi_1 \vdash \ell_3 \sqsubseteq \ell_1$	↓lst-x: 1
	↓lst-x: 1

4: $\Pi_2 \leq \Pi_1$	* given
5: $\Pi_2 \vdash \ell_3 \sqsubseteq \ell_1$	astlst: 3,4
6: $\Pi_1 \vdash \ell_1 \sqsubseteq \ell_2$	$\downarrow$ lst-x: 1
7: $\Pi_2 \vdash \ell_1 \sqsubseteq \ell_2$	astlst: 6,4
8: $\Pi_2 \vdash \ell_3 \sqsubseteq \ell_2$	lst-x: 2,5,7

1: $\Pi_1 \vdash p_3 : p_1 \sqsubseteq p_4 : p_2$	(astlst-p)
2: $\Pi_1 \vdash p_3 \leq p_4$	* given
3: $\Pi_2 \leq \Pi_1$	$\downarrow$ lst-p: 1
4: $\Pi_2 \vdash p_3 \leq p_4$	* given
5: $\Pi_1 \vdash p_1 \leq p_2$	astpst: 2,3
6: $\Pi_2 \vdash p_1 \leq p_2$	$\downarrow$ lst-p: 1
7: $\Pi_2 \vdash p_3 : p_1 \sqsubseteq p_4 : p_2$	astpst: 5,3
	lst-p: 4,6

1: $\Pi_1 \vdash \ell_1 \sqsubseteq \ell_1, \ell_2$	(astlst-cat1)
2: $\Pi_2 \leq \Pi_1$	* given
3: $\Pi_2 \vdash \ell_1 \sqsubseteq \ell_1, \ell_2$	* given
	lst-cat1

1: $\Pi_1 \vdash \ell_1 \sqsubseteq \ell_2, \ell_1$	(astlst-cat2)
2: $\Pi_2 \leq \Pi_1$	* given
3: $\Pi_2 \vdash \ell_1 \sqsubseteq \ell_2, \ell_1$	* given
	lst-cat2

### 4.3 Hierarchy subtypings

$\frac{(\Pi_1, p_1 \leq p_2) \leq \Pi_2 \quad \Pi_1 \vdash p_1 \leq p_2}{\Pi_1 \leq \Pi_2}$	pstast
---------------------------------------------------------------------------------------------	--------

1: $(\Pi_1, p_1 \leq p_2) \leq \Pi_3$	(pstast-x)
2: some $\Pi_2$	* given
3: $(\Pi_1, p_1 \leq p_2) \leq \Pi_2$	$\downarrow$ ast-x: 1
4: $\Pi_1 \vdash p_1 \leq p_2$	$\downarrow$ ast-x: 1
5: $\Pi_1 \leq \Pi_2$	* given
6: $\Pi_2 \leq \Pi_3$	pstast: 3,4
7: $\Pi_1 \leq \Pi_3$	$\downarrow$ ast-x: 1
	ast-x: 2,5,6

1: $\Pi_1 \vdash p_1 \leq p_2$	(pstast-p1)
2: $(\Pi_1, p_1 \leq p_2) \leq \Pi_2$	* given
3: $\Pi_1 \leq \Pi_2$	* given
	$\downarrow$ ast-p1: 2

1: $(\Pi_1, p_1 \leq p_2) \leq (\Pi_2, p_3 \leq p_4)$	(pstast-p2)
2: $(\Pi_1, p_1 \leq p_2) \leq \Pi_2$	* given
3: $\Pi_1 \vdash p_1 \leq p_2$	$\downarrow$ ast-p2: 1
4: $\Pi_1 \leq \Pi_2$	* given
5: $\Pi_1, p_1 \leq p_2 \vdash p_3 \leq p_4$	pstast: 2,3
6: $\Pi_1 \vdash p_3 \leq p_4$	$\downarrow$ ast-p2: 1
7: $\Pi_1 \leq (\Pi_2, p_3 \leq p_4)$	pstpst: 5,3
	ast-p2: 4,6

$\frac{\Pi_1 \leq \Pi_2}{(\Pi_1, p_1 \leq p_2) \leq \Pi_2}$	apast
-------------------------------------------------------------	-------

1:  $\Pi \leq \Pi$  (apast-z)  
 2:  $(\Pi, p_1 \leq p_2) \leq \Pi$  \*given  
 ast-p1: 1

1:  $\Pi_1 \leq \Pi_3$  (apast-x)  
 2: **some**  $\Pi_2$  \*given  
 3:  $\Pi_1 \leq \Pi_2$   $\downarrow$ ast-x: 1  
 4:  $(\Pi_1, p_1 \leq p_2) \leq \Pi_2$   $\downarrow$ ast-x: 1  
 5:  $\Pi_2 \leq \Pi_3$  apast: 3  
 6:  $(\Pi_1, p_1 \leq p_2) \leq \Pi_3$   $\downarrow$ ast-x: 1  
 ast-x: 2,4,5

1:  $(\Pi_1, p_1 \leq p_2) \leq \Pi_2$  (apast-p1)  
 2:  $\Pi_1 \leq \Pi_2$  \*given  
 3:  $((\Pi_1, p_1 \leq p_2), p_3 \leq p_4) \leq \Pi_2$   $\downarrow$ ast-p1: 1  
 ast-p1: 1

1:  $\Pi_1 \leq (\Pi_2, p_1 \leq p_2)$  (apast-p2)  
 2:  $\Pi_1 \leq \Pi_2$  \*given  
 3:  $(\Pi_1, p_3 \leq p_4) \leq \Pi_2$   $\downarrow$ ast-p2: 1  
 4:  $\Pi_1 \vdash p_1 \leq p_2$  apast: 2  
 5:  $\Pi_1, p_3 \leq p_4 \vdash p_1 \leq p_2$   $\downarrow$ ast-p2: 1  
 6:  $(\Pi_1, p_3 \leq p_4) \leq (\Pi_2, p_1 \leq p_2)$  appst: 4  
 ast-p2: 3,5

$$\frac{\Pi_1 \leq \Pi_2}{(\Pi_1, p_1 \leq p_2) \leq (\Pi_2, \ell_1 \leq \ell_2)}$$

apapast

1:  $\Pi_1 \leq \Pi_2$  (apapast-l)  
 2:  $(\Pi_1, p_1 \leq p_2) \leq \Pi_2$  \*given  
 3:  $\Pi_1, p_1 \leq p_2 \vdash p_1 \leq p_2$  apast: 1  
 4:  $(\Pi_1, p_1 \leq p_2) \leq (\Pi_2, p_1 \leq p_2)$  pst-a1  
 ast-p2: 2,3

## 4.4 Type subtypings

$$\frac{\Pi, p_1 \leq p_2; \Gamma \vdash e : t \quad \Pi \vdash p_1 \leq p_2}{\Pi; \Gamma \vdash e : t}$$

pstty

1:  $\Pi, p_1 \leq p_2; \Gamma \vdash \text{true}_\ell : \text{bool}_\ell$  (pstty-true)  
 2:  $\Pi \vdash p_1 \leq p_2$  \*given  
 3:  $\Pi; \Gamma \vdash \text{true}_\ell : \text{bool}_\ell$  \*given  
 ty-true

1:  $\Pi, p_1 \leq p_2; \Gamma \vdash \text{false}_\ell : \text{bool}_\ell$  (pstty-false)  
 2:  $\Pi \vdash p_1 \leq p_2$  \*given  
 3:  $\Pi; \Gamma \vdash \text{false}_\ell : \text{bool}_\ell$  \*given  
 ty-false

1:  $\Pi, p_1 \leq p_2; \Gamma \vdash \text{if } e_1 e_2 e_1 : \text{bool}_\ell$  (pstty-iffb)  
 2:  $\Pi, p_1 \leq p_2; \Gamma \vdash e_1 : \text{bool}_\ell$  \*given  
 3:  $\Pi \vdash p_1 \leq p_2$   $\downarrow$ ty-iffb: 1  
 4:  $\Pi; \Gamma \vdash e_1 : \text{bool}_\ell$  \*given  
 5:  $\Pi, p_1 \leq p_2; \Gamma \vdash e_2 : \text{bool}_\ell$  pstty: 2,3  
 6:  $\Pi; \Gamma \vdash e_2 : \text{bool}_\ell$   $\downarrow$ ty-iffb: 1  
 pstty: 5,3

7:  $\Pi, p_1 \leq p_2; \Gamma \vdash e_1 : \text{bool}_\ell$   $\downarrow$ ty-afb: 1  
8:  $\Pi; \Gamma \vdash e_1 : \text{bool}_\ell$  pstty: 7,3  
9:  $\text{lab}(\text{bool}_\ell) = \ell$   $\downarrow$ ty-afb: 1  
10:  $\Pi; \Gamma \vdash \text{if } e_1 \ e_2 \ e_1 : \text{bool}_\ell$  ty-afb: 4,6,8,9

(pstty-var1)  
1:  $\Pi, p_1 \leq p_2; \Gamma, x:t \vdash x : t$  \*given  
2:  $\Pi \vdash p_1 \leq p_2$  \*given  
3:  $\Pi; \Gamma, x:t \vdash x : t$  ty-var1

(pstty-var2)  
1:  $\Pi, p_1 \leq p_2; \Gamma, x_2:t_2 \vdash x_1 : t_1$  \*given  
2:  $\Pi, p_1 \leq p_2; \Gamma \vdash x_1 : t_1$   $\downarrow$ ty-var2: 1  
3:  $\Pi \vdash p_1 \leq p_2$  \*given  
4:  $\Pi; \Gamma \vdash x_1 : t_1$  pstty: 2,3  
5:  $\Pi; \Gamma, x_2:t_2 \vdash x_1 : t_1$  ty-var2: 4

(pstty-fun)  
1:  $\Pi_1, p_1 \leq p_2; \Gamma \vdash \lambda[\Pi_2]x:t_1. e : t_1 \rightarrow t_2$  \*given  
2:  $(\Pi_1, p_1 \leq p_2) \leq \Pi_2$   $\downarrow$ ty-fun: 1  
3:  $\Pi_1 \vdash p_1 \leq p_2$  \*given  
4:  $\Pi_1 \leq \Pi_2$  pstast: 2,3  
5:  $\Pi_2; \Gamma, x:t_1 \vdash e : t_2$   $\downarrow$ ty-fun: 1  
6:  $\Pi_1; \Gamma \vdash \lambda[\Pi_2]x:t_1. e : t_1 \rightarrow t_2$  ty-fun: 4,5

(pstty-app)  
1:  $\Pi, p_1 \leq p_2; \Gamma \vdash e_2 \ e_1 : t_2$  \*given  
2:  $\Pi, p_1 \leq p_2; \Gamma \vdash e_2 : t_1 \rightarrow t_2$   $\downarrow$ ty-app: 1  
3:  $\Pi \vdash p_1 \leq p_2$  \*given  
4:  $\Pi; \Gamma \vdash e_2 : t_1 \rightarrow t_2$  pstty: 2,3  
5:  $\Pi, p_1 \leq p_2; \Gamma \vdash e_1 : t_1$   $\downarrow$ ty-app: 1  
6:  $\Pi; \Gamma \vdash e_1 : t_1$  pstty: 5,3  
7:  $\Pi; \Gamma \vdash e_2 \ e_1 : t_2$  ty-app: 4,6

(pstty-ifp)  
1:  $\Pi, p_1 \leq p_2; \Gamma \vdash \text{if } (p_1 \leq p_2) \ e_2 \ e_1 : t$  \*given  
2:  $(\Pi, p_1 \leq p_2), p_1 \leq p_2; \Gamma \vdash e_2 : t$   $\downarrow$ ty-ifp: 1  
3:  $\Pi \vdash p_1 \leq p_2$  \*given  
4:  $\Pi, p_1 \leq p_2 \vdash p_1 \leq p_2$  appst: 3  
5:  $\Pi, p_1 \leq p_2; \Gamma \vdash e_2 : t$  pstty: 2,4  
6:  $\Pi, p_1 \leq p_2; \Gamma \vdash e_1 : t$   $\downarrow$ ty-ifp: 1  
7:  $\Pi; \Gamma \vdash e_1 : t$  pstty: 6,3  
8:  $\Pi; \Gamma \vdash \text{if } (p_1 \leq p_2) \ e_2 \ e_1 : t$  ty-ifp: 5,7

(pstty-tag)  
1:  $\Pi, p_1 \leq p_2; \Gamma \vdash [\ell_1 \sqsubseteq \ell_2]e : \text{bool}_{\ell_2}$  \*given  
2:  $\Pi, p_1 \leq p_2 \vdash \ell_1 \sqsubseteq \ell_2$   $\downarrow$ ty-tag: 1  
3:  $\Pi \vdash p_1 \leq p_2$  \*given  
4:  $\Pi \vdash \ell_1 \sqsubseteq \ell_2$  pstlst: 2,3  
5:  $\Pi, p_1 \leq p_2; \Gamma \vdash e : \text{bool}_{\ell_1}$   $\downarrow$ ty-tag: 1  
6:  $\Pi; \Gamma \vdash e : \text{bool}_{\ell_1}$  pstty: 5,3  
7:  $\Pi; \Gamma \vdash [\ell_1 \sqsubseteq \ell_2]e : \text{bool}_{\ell_2}$  ty-tag: 4,6

$$\frac{\Pi_1; \Gamma \vdash e : t \quad \Pi_2 \leq \Pi_1}{\Pi_2; \Gamma \vdash e : t}$$

astty

1: $\Pi_1; \Gamma \vdash \text{true}_\ell : \text{bool}_\ell$	(astty-true)
2: $\Pi_2 \leq \Pi_1$	*given
3: $\Pi_2; \Gamma \vdash \text{true}_\ell : \text{bool}_\ell$	*given
	ty-true
1: $\Pi_1; \Gamma \vdash \text{false}_\ell : \text{bool}_\ell$	(astty-false)
2: $\Pi_2 \leq \Pi_1$	*given
3: $\Pi_2; \Gamma \vdash \text{false}_\ell : \text{bool}_\ell$	*given
	ty-false
1: $\Pi_1; \Gamma \vdash \text{if } e_1 \ e_2 \ e_1 : \text{bool}_\ell$	(astty-ifb)
2: $\Pi_1; \Gamma \vdash e_1 : \text{bool}_\ell$	*given
3: $\Pi_2 \leq \Pi_1$	$\downarrow$ ty-ifb: 1
4: $\Pi_2; \Gamma \vdash e_1 : \text{bool}_\ell$	*given
5: $\Pi_1; \Gamma \vdash e_2 : \text{bool}_\ell$	astty: 2,3
6: $\Pi_2; \Gamma \vdash e_2 : \text{bool}_\ell$	$\downarrow$ ty-ifb: 1
7: $\Pi_1; \Gamma \vdash e_1 : \text{bool}_\ell$	astty: 5,3
8: $\Pi_2; \Gamma \vdash e_1 : \text{bool}_\ell$	$\downarrow$ ty-ifb: 1
9: $\text{lab}(\text{bool}_\ell) = \ell$	astty: 7,3
10: $\Pi_2; \Gamma \vdash \text{if } e_1 \ e_2 \ e_1 : \text{bool}_\ell$	$\downarrow$ ty-ifb: 1
	ty-ifb: 4,6,8,9
1: $\Pi_1; \Gamma, x:t \vdash x : t$	(astty-var1)
2: $\Pi_2 \leq \Pi_1$	*given
3: $\Pi_2; \Gamma, x:t \vdash x : t$	*given
	ty-var1
1: $\Pi_1; \Gamma, x_2:t_2 \vdash x_1 : t_1$	(astty-var2)
2: $\Pi_1; \Gamma \vdash x_1 : t_1$	*given
3: $\Pi_2 \leq \Pi_1$	$\downarrow$ ty-var2: 1
4: $\Pi_2; \Gamma \vdash x_1 : t_1$	*given
5: $\Pi_2; \Gamma, x_2:t_2 \vdash x_1 : t_1$	astty: 2,3
	ty-var2: 4
1: <b>some</b> $\Pi_1$	(astty-fun)
2: $\Pi_3 \leq \Pi_1$	asome-total
3: $\Pi_1; \Gamma \vdash \lambda[\Pi_2]x:t_1. e : t_1 \rightarrow t_2$	*given
4: $\Pi_1 \leq \Pi_2$	*given
5: $\Pi_3 \leq \Pi_2$	$\downarrow$ ty-fun: 3
6: $\Pi_2; \Gamma, x:t_1 \vdash e : t_2$	ast-x: 1,2,4
7: $\Pi_3; \Gamma \vdash \lambda[\Pi_2]x:t_1. e : t_1 \rightarrow t_2$	$\downarrow$ ty-fun: 3
	ty-fun: 5,6
1: $\Pi_1; \Gamma \vdash e_2 \ e_1 : t_2$	(astty-app)
2: $\Pi_1; \Gamma \vdash e_2 : t_1 \rightarrow t_2$	*given
3: $\Pi_2 \leq \Pi_1$	$\downarrow$ ty-app: 1
4: $\Pi_2; \Gamma \vdash e_2 : t_1 \rightarrow t_2$	*given
5: $\Pi_1; \Gamma \vdash e_1 : t_1$	astty: 2,3
6: $\Pi_2; \Gamma \vdash e_1 : t_1$	$\downarrow$ ty-app: 1
7: $\Pi_2; \Gamma \vdash e_2 \ e_1 : t_2$	astty: 5,3
	ty-app: 4,6
1: $\Pi_1; \Gamma \vdash \text{if } (p_1 \leq p_2) \ e_2 \ e_1 : t$	(astty-ifp)
2: $\Pi_1, p_1 \leq p_2; \Gamma \vdash e_2 : t$	*given
3: $\Pi_2 \leq \Pi_1$	$\downarrow$ ty-ifp: 1
4: $(\Pi_2, p_1 \leq p_2) \leq (\Pi_1, p_1 \leq p_2)$	*given
5: $\Pi_2, p_1 \leq p_2; \Gamma \vdash e_2 : t$	apapast: 3
	astty: 2,4

6: $\Pi_1; \Gamma \vdash e_1 : t$	↓ty-ifp: 1
7: $\Pi_2; \Gamma \vdash e_1 : t$	astty: 6,3
8: $\Pi_2; \Gamma \vdash \text{if } (p_1 \leq p_2) e_2 e_1 : t$	ty-ifp: 5,7

1: $\Pi_1; \Gamma \vdash [l_1 \sqsubseteq l_2]e : \text{bool}_{\ell_2}$	(astty-tag)
2: $\Pi_1 \vdash l_1 \sqsubseteq l_2$	*given
3: $\Pi_2 \leq \Pi_1$	↓ty-tag: 1
4: $\Pi_2 \vdash l_1 \sqsubseteq l_2$	*given
5: $\Pi_1; \Gamma \vdash e : \text{bool}_{\ell_1}$	astlst: 2,3
6: $\Pi_2; \Gamma \vdash e : \text{bool}_{\ell_1}$	↓ty-tag: 1
7: $\Pi_2; \Gamma \vdash [l_1 \sqsubseteq l_2]e : \text{bool}_{\ell_2}$	astty: 5,3
	ty-tag: 4,6

## 4.5 Tag checkings

$\Pi; \cdot \vdash e : t$
$\Pi \vdash e$

tyae
------

1: $\Pi; \cdot \vdash \text{true}_{\ell} : \text{bool}_{\ell}$	(tyae-true)
2: $\Pi \vdash \text{true}_{\ell}$	*given
	ae-true

1: $\Pi; \cdot \vdash \text{false}_{\ell} : \text{bool}_{\ell}$	(tyae-false)
2: $\Pi \vdash \text{false}_{\ell}$	*given
	ae-false

1: $\Pi; \cdot \vdash \text{if } e_3 e_2 e_1 : t$	(tyae-ifb)
2: $\text{lab}(t) = \ell$	*given
3: $\Pi; \cdot \vdash e_3 : \text{bool}_{\ell}$	↓ty-ifb: 1
4: $\Pi \vdash e_3$	↓ty-ifb: 1
5: $\Pi; \cdot \vdash e_2 : t$	tyae: 3
6: $\Pi \vdash e_2$	↓ty-ifb: 1
7: $\Pi; \cdot \vdash e_1 : t$	tyae: 5
8: $\Pi \vdash e_1$	↓ty-ifb: 1
9: $\Pi \vdash \text{if } e_3 e_2 e_1$	tyae: 7
	ae-ifb: 4,6,8

1: $\Pi_1; \cdot \vdash \lambda[\Pi_2]x:t_1. e : t_1 \rightarrow t_2$	(tyae-fun)
2: $\Pi_2; \cdot, x:t_1 \vdash e : t_2$	*given
3: $\Pi_1 \leq \Pi_2$	↓ty-fun: 1
4: $\Pi_1 \vdash \lambda[\Pi_2]x:t_1. e$	↓ty-fun: 1
	ae-fun: 3

1: $\Pi; \cdot \vdash e_2 e_1 : t_2$	(tyae-app)
2: $\Pi; \cdot \vdash e_2 : t_1 \rightarrow t_2$	*given
3: $\Pi \vdash e_2$	↓ty-app: 1
4: $\Pi; \cdot \vdash e_1 : t_1$	tyae: 2
5: $\Pi \vdash e_1$	↓ty-app: 1
6: $\Pi \vdash e_2 e_1$	tyae: 4
	ae-app: 3,5

1: $\Pi; \cdot \vdash \text{if } (p_1 \leq p_2) e_2 e_1 : t$	(tyae-ifp)
2: $\Pi, p_1 \leq p_2; \cdot \vdash e_2 : t$	*given
3: $\Pi, p_1 \leq p_2 \vdash e_2$	↓ty-ifp: 1
4: $\Pi; \cdot \vdash e_1 : t$	tyae: 2
5: $\Pi \vdash e_1$	↓ty-ifp: 1
	tyae: 4

6: $\Pi \vdash \text{if } (p_1 \leq p_2) e_2 e_1$	ae-ifp: 3,5
1: $\Pi; \cdot \vdash [\ell_1 \sqsubseteq \ell_2]e : \text{bool}_{\ell_2}$ 2: $\Pi \vdash \ell_1 \sqsubseteq \ell_2$ 3: $\Pi; \cdot \vdash e : \text{bool}_{\ell_1}$ 4: $\Pi \vdash e$ 5: $\Pi \vdash [\ell_1 \sqsubseteq \ell_2]e$	(tyae-tag) *given $\downarrow$ ty-tag: 1 $\downarrow$ ty-tag: 1 tyae: 3 ae-tag: 2,4
$\frac{\Pi_1; \cdot \vdash e : t \quad \Pi_2 \vdash e}{\Pi_2; \cdot \vdash e : t}$	<div style="border: 1px solid black; padding: 2px; display: inline-block;">aety</div>
1: $\Pi_1; \cdot \vdash \text{true}_{\ell} : \text{bool}_{\ell}$ 2: $\Pi_2 \vdash \text{true}_{\ell}$ 3: $\Pi_2; \cdot \vdash \text{true}_{\ell} : \text{bool}_{\ell}$	(aety-true) *given *given ty-true
1: $\Pi_1; \cdot \vdash \text{false}_{\ell} : \text{bool}_{\ell}$ 2: $\Pi_2 \vdash \text{false}_{\ell}$ 3: $\Pi_2; \cdot \vdash \text{false}_{\ell} : \text{bool}_{\ell}$	(aety-false) *given *given ty-false
1: $\Pi_1; \cdot \vdash \text{if } e_3 e_2 e_1 : t$ 2: $\Pi_1; \cdot \vdash e_3 : \text{bool}_{\ell}$ 3: $\Pi_2 \vdash \text{if } e_3 e_2 e_1$ 4: $\Pi_2 \vdash e_3$ 5: $\Pi_2; \cdot \vdash e_3 : \text{bool}_{\ell}$ 6: $\Pi_1; \cdot \vdash e_2 : t$ 7: $\Pi_2 \vdash e_2$ 8: $\Pi_2; \cdot \vdash e_2 : t$ 9: $\Pi_1; \cdot \vdash e_1 : t$ 10: $\Pi_2 \vdash e_1$ 11: $\Pi_2; \cdot \vdash e_1 : t$ 12: $\text{lab}(t) = \ell$ 13: $\Pi_2; \cdot \vdash \text{if } e_3 e_2 e_1 : t$	(aety-ifb) *given $\downarrow$ ty-ifb: 1 *given $\downarrow$ ae-ifb: 3 aety: 2,4 $\downarrow$ ty-ifb: 1 $\downarrow$ ae-ifb: 3 aety: 6,7 $\downarrow$ ty-ifb: 1 $\downarrow$ ae-ifb: 3 aety: 9,10 $\downarrow$ ty-ifb: 1 ty-ifb: 5,8,11,12
1: $\Pi_1; \cdot \vdash \lambda[\Pi_2]x:t_1. e : t_1 \rightarrow t_2$ 2: $\Pi_1 \leq \Pi_2$ 3: $\Pi_3 \vdash \lambda[\Pi_2]x:t_1. e$ 4: $\Pi_3 \leq \Pi_2$ 5: $\Pi_2; \cdot, x:t_1 \vdash e : t_2$ 6: $\Pi_3; \cdot \vdash \lambda[\Pi_2]x:t_1. e : t_1 \rightarrow t_2$	(aety-fun) *given $\downarrow$ ty-fun: 1 *given $\downarrow$ ae-fun: 3 $\downarrow$ ty-fun: 1 ty-fun: 4,5
1: $\Pi_1; \cdot \vdash e_2 e_1 : t_2$ 2: $\Pi_1; \cdot \vdash e_2 : t_1 \rightarrow t_2$ 3: $\Pi_2 \vdash e_2 e_1$ 4: $\Pi_2 \vdash e_2$ 5: $\Pi_2; \cdot \vdash e_2 : t_1 \rightarrow t_2$ 6: $\Pi_1; \cdot \vdash e_1 : t_1$ 7: $\Pi_2 \vdash e_1$ 8: $\Pi_2; \cdot \vdash e_1 : t_1$ 9: $\Pi_2; \cdot \vdash e_2 e_1 : t_2$	(aety-app) *given $\downarrow$ ty-app: 1 *given $\downarrow$ ae-app: 3 aety: 2,4 $\downarrow$ ty-app: 1 $\downarrow$ ae-app: 3 aety: 6,7 ty-app: 5,8

1:	$\Pi_1; \cdot \vdash \text{if } (p_1 \leq p_2) e_2 e_1 : t$	(aety-ifp) *given
2:	$\Pi_1, p_1 \leq p_2; \cdot \vdash e_2 : t$	↓ty-ifp: 1
3:	$\Pi_2 \vdash \text{if } (p_1 \leq p_2) e_2 e_1$	*given
4:	$\Pi_2, p_1 \leq p_2 \vdash e_2$	↓ae-ifp: 3
5:	$\Pi_2, p_1 \leq p_2; \cdot \vdash e_2 : t$	aety: 2,4
6:	$\Pi_1; \cdot \vdash e_1 : t$	↓ty-ifp: 1
7:	$\Pi_2 \vdash e_1$	↓ae-ifp: 3
8:	$\Pi_2; \cdot \vdash e_1 : t$	aety: 6,7
9:	$\Pi_2; \cdot \vdash \text{if } (p_1 \leq p_2) e_2 e_1 : t$	ty-ifp: 5,8

1:	$\Pi_1; \cdot \vdash [l_1 \sqsubseteq l_2]e : \text{bool}_{\ell_2}$	(aety-tag) *given
2:	$\Pi_1 \vdash l_1 \sqsubseteq l_2$	↓ty-tag: 1
3:	$\Pi_2 \vdash [l_1 \sqsubseteq l_2]e$	*given
4:	$\Pi_2 \vdash l_1 \sqsubseteq l_2$	↓ae-tag: 3
5:	$\Pi_1; \cdot \vdash e : \text{bool}_{\ell_1}$	↓ty-tag: 1
6:	$\Pi_2 \vdash e$	↓ae-tag: 3
7:	$\Pi_2; \cdot \vdash e : \text{bool}_{\ell_1}$	aety: 5,6
8:	$\Pi_2; \cdot \vdash [l_1 \sqsubseteq l_2]e : \text{bool}_{\ell_2}$	ty-tag: 4,7

## 4.6 Permutations

	$\boxed{\Gamma \equiv \Gamma}$	$\boxed{\text{perm}}$
	$(\Gamma, x_1 : t_1), x_2 : t_2 \equiv (\Gamma, x_2 : t_2), x_1 : t_1$	(perm-x1)
	$\frac{\Gamma_1 \equiv \Gamma_2}{\Gamma_1, x : t \equiv \Gamma_2, x : t}$	(perm-x2)
	$\boxed{\frac{\Pi; \Gamma_1 \vdash e : t \quad \Gamma_1 \equiv \Gamma_2}{\Pi; \Gamma_2 \vdash e : t}}$	$\boxed{\text{permty}}$
1:	$\Pi; \Gamma_1 \vdash \text{true}_{\ell} : \text{bool}_{\ell}$	(permty-true) *given
2:	$\Gamma_1 \equiv \Gamma_2$	*given
3:	$\Pi; \Gamma_2 \vdash \text{true}_{\ell} : \text{bool}_{\ell}$	ty-true
1:	$\Pi; \Gamma_1 \vdash \text{false}_{\ell} : \text{bool}_{\ell}$	(permty-false) *given
2:	$\Gamma_1 \equiv \Gamma_2$	*given
3:	$\Pi; \Gamma_2 \vdash \text{false}_{\ell} : \text{bool}_{\ell}$	ty-false
1:	$\Pi; \Gamma_1 \vdash \text{if } e_1 e_2 e_1 : \text{bool}_{\ell}$	(permty-ifb) *given
2:	$\Pi; \Gamma_1 \vdash e_1 : \text{bool}_{\ell}$	↓ty-ifb: 1
3:	$\Gamma_1 \equiv \Gamma_2$	*given
4:	$\Pi; \Gamma_2 \vdash e_1 : \text{bool}_{\ell}$	permty: 2,3
5:	$\Pi; \Gamma_1 \vdash e_2 : \text{bool}_{\ell}$	↓ty-ifb: 1
6:	$\Pi; \Gamma_2 \vdash e_2 : \text{bool}_{\ell}$	permty: 5,3
7:	$\Pi; \Gamma_1 \vdash e_1 : \text{bool}_{\ell}$	↓ty-ifb: 1
8:	$\Pi; \Gamma_2 \vdash e_1 : \text{bool}_{\ell}$	permty: 7,3
9:	$\text{lab}(\text{bool}_{\ell}) = \ell$	↓ty-ifb: 1
10:	$\Pi; \Gamma_2 \vdash \text{if } e_1 e_2 e_1 : \text{bool}_{\ell}$	ty-ifb: 4,6,8,9
1:	$\Pi; \Gamma_1, x : t \vdash x : t$	(permty-var1) *given
2:	$\Gamma_1, x : t \equiv \Gamma_2, x : t$	*given

3: $\Pi; \Gamma_2, x:t \vdash x : t$	ty-var1
1: $\Pi; (\Gamma, x_1:t_1), x_2:t_2 \vdash x_1 : t_1$ 2: $\Pi; \Gamma, x_1:t_1 \vdash x_1 : t_1$ 3: $(\Gamma, x_1:t_1), x_2:t_2 \equiv (\Gamma, x_2:t_2), x_1:t_1$ 4: $\Pi; (\Gamma, x_2:t_2), x_1:t_1 \vdash x_1 : t_1$	(permtty-var2) *given $\downarrow$ ty-var2: 1 *given ty-var1
1: $(\Gamma, x_1:t_1), x_2:t_2 \equiv (\Gamma, x_2:t_2), x_1:t_1$ 2: $\Pi; (\Gamma, x_1:t_1), x_2:t_2 \vdash x_3 : t_3$ 3: $\Pi; \Gamma, x_1:t_1 \vdash x_3 : t_3$ 4: $\Pi; \Gamma \vdash x_3 : t_3$ 5: $\Pi; \Gamma, x_2:t_2 \vdash x_3 : t_3$ 6: $\Pi; (\Gamma, x_2:t_2), x_1:t_1 \vdash x_3 : t_3$	(permtty-var3) *given *given $\downarrow$ ty-var2: 2 $\downarrow$ ty-var2: 3 ty-var2: 4 ty-var2: 5
1: $\Pi; \Gamma_1, x_2:t_2 \vdash x_1 : t_1$ 2: $\Pi; \Gamma_1 \vdash x_1 : t_1$ 3: $\Gamma_1, x_2:t_2 \equiv \Gamma_2, x_2:t_2$ 4: $\Gamma_1 \equiv \Gamma_2$ 5: $\Pi; \Gamma_2 \vdash x_1 : t_1$ 6: $\Pi; \Gamma_2, x_2:t_2 \vdash x_1 : t_1$	(permtty-var4) *given $\downarrow$ ty-var2: 1 *given $\downarrow$ perm-x2: 3 permtty: 2,4 ty-var2: 5
1: $\Pi_2; \Gamma_1 \vdash \lambda[\Pi_1]x:t_1. e : t_1 \rightarrow t_2$ 2: $\Pi_2 \leq \Pi_1$ 3: $\Pi_1; \Gamma_1, x:t_1 \vdash e : t_2$ 4: $\Gamma_1 \equiv \Gamma_2$ 5: $\Gamma_1, x:t_1 \equiv \Gamma_2, x:t_1$ 6: $\Pi_1; \Gamma_2, x:t_1 \vdash e : t_2$ 7: $\Pi_2; \Gamma_2 \vdash \lambda[\Pi_1]x:t_1. e : t_1 \rightarrow t_2$	(permtty-fun) *given $\downarrow$ ty-fun: 1 $\downarrow$ ty-fun: 1 *given perm-x2: 4 permtty: 3,5 ty-fun: 2,6
1: $\Pi; \Gamma_1 \vdash e_2 e_1 : t_2$ 2: $\Pi; \Gamma_1 \vdash e_2 : t_1 \rightarrow t_2$ 3: $\Gamma_1 \equiv \Gamma_2$ 4: $\Pi; \Gamma_2 \vdash e_2 : t_1 \rightarrow t_2$ 5: $\Pi; \Gamma_1 \vdash e_1 : t_1$ 6: $\Pi; \Gamma_2 \vdash e_1 : t_1$ 7: $\Pi; \Gamma_2 \vdash e_2 e_1 : t_2$	(permtty-app) *given $\downarrow$ ty-app: 1 *given permtty: 2,3 $\downarrow$ ty-app: 1 permtty: 5,3 ty-app: 4,6
1: $\Pi; \Gamma_1 \vdash \text{if } (p_1 \leq p_2) e_2 e_1 : t$ 2: $\Pi, p_1 \leq p_2; \Gamma_1 \vdash e_2 : t$ 3: $\Gamma_1 \equiv \Gamma_2$ 4: $\Pi, p_1 \leq p_2; \Gamma_2 \vdash e_2 : t$ 5: $\Pi; \Gamma_1 \vdash e_1 : t$ 6: $\Pi; \Gamma_2 \vdash e_1 : t$ 7: $\Pi; \Gamma_2 \vdash \text{if } (p_1 \leq p_2) e_2 e_1 : t$	(permtty-ifp) *given $\downarrow$ ty-ifp: 1 *given permtty: 2,3 $\downarrow$ ty-ifp: 1 permtty: 5,3 ty-ifp: 4,6
1: $\Pi; \Gamma_1 \vdash [\ell_1 \sqsubseteq \ell_2]e : \text{bool}_{\ell_2}$ 2: $\Pi \vdash \ell_1 \sqsubseteq \ell_2$ 3: $\Pi; \Gamma_1 \vdash e : \text{bool}_{\ell_1}$ 4: $\Gamma_1 \equiv \Gamma_2$ 5: $\Pi; \Gamma_2 \vdash e : \text{bool}_{\ell_1}$ 6: $\Pi; \Gamma_2 \vdash [\ell_1 \sqsubseteq \ell_2]e : \text{bool}_{\ell_2}$	(permtty-tag) *given $\downarrow$ ty-tag: 1 $\downarrow$ ty-tag: 1 *given permtty: 3,4 ty-tag: 2,5

## 4.7 Substitutions

$$\frac{\Pi; \Gamma, x:t_1 \vdash e_1 : t_2 \quad ; \cdot \vdash e_2 : t_1 \quad e_1\{e_2/x\} = e_3}{\Pi; \Gamma \vdash e_3 : t_2}$$

subty

1:  $\Pi; \Gamma, x:t \vdash \text{true}_\ell : \text{bool}_\ell$   
 2:  $; \cdot \vdash e : t$   
 3:  $\text{true}_\ell\{e/x\} = \text{true}_\ell$   
 4:  $\Pi; \Gamma \vdash \text{true}_\ell : \text{bool}_\ell$

(subty-true)  
 \*given  
 \*given  
 \*given  
 ty-true

1:  $\Pi; \Gamma, x:t \vdash \text{false}_\ell : \text{bool}_\ell$   
 2:  $; \cdot \vdash e : t$   
 3:  $\text{false}_\ell\{e/x\} = \text{false}_\ell$   
 4:  $\Pi; \Gamma \vdash \text{false}_\ell : \text{bool}_\ell$

(subty-false)  
 \*given  
 \*given  
 \*given  
 ty-false

1:  $\Pi; \Gamma, x:t_1 \vdash \text{if } e_6 \text{ } e_4 \text{ } e_1 : t_2$   
 2:  $\Pi; \Gamma, x:t_1 \vdash e_6 : \text{bool}_\ell$   
 3:  $; \cdot \vdash e_2 : t_1$   
 4:  $(\text{if } e_6 \text{ } e_4 \text{ } e_1)\{e_2/x\} = (\text{if } e_7 \text{ } e_5 \text{ } e_3)$   
 5:  $e_6\{e_2/x\} = e_7$   
 6:  $\Pi; \Gamma \vdash e_7 : \text{bool}_\ell$   
 7:  $\Pi; \Gamma, x:t_1 \vdash e_4 : t_2$   
 8:  $e_4\{e_2/x\} = e_5$   
 9:  $\Pi; \Gamma \vdash e_5 : t_2$   
 10:  $\Pi; \Gamma, x:t_1 \vdash e_1 : t_2$   
 11:  $e_1\{e_2/x\} = e_3$   
 12:  $\Pi; \Gamma \vdash e_3 : t_2$   
 13:  $\text{lab}(t_2) = \ell$   
 14:  $\Pi; \Gamma \vdash \text{if } e_7 \text{ } e_5 \text{ } e_3 : t_2$

(subty-if)  
 \*given  
 $\downarrow$ ty-ifb: 1  
 \*given  
 \*given  
 $\downarrow$ sub-ifb: 4  
 subty: 2,3,5  
 $\downarrow$ ty-ifb: 1  
 $\downarrow$ sub-ifb: 4  
 subty: 7,3,8  
 $\downarrow$ ty-ifb: 1  
 $\downarrow$ sub-ifb: 4  
 subty: 10,3,11  
 $\downarrow$ ty-ifb: 1  
 ty-ifb: 6,9,12,13

1:  $; \cdot, x:t \vdash x : t$   
 2:  $x\{e/x\} = e$   
 3:  $; \cdot \vdash e : t$

(subty-var1)  
 \*given  
 \*given  
 \*given

1:  $x_2\{x_2/x_1\} = x_2$   
 2:  $; \cdot, x_1:t \vdash x_2 : t$   
 3:  $; \cdot \vdash x_2 : t$

(subty-var2)  
 \*given  
 \*given  
 $\downarrow$ ty-var2: 2

1:  $\Pi_2; \Gamma, x_2:t_2 \vdash \lambda[\Pi_1]x_1:t_1. e_1 : t_1 \rightarrow t_3$   
 2:  $\Pi_2 \leq \Pi_1$   
 3:  $\Pi_1; (\Gamma, x_2:t_2), x_1:t_1 \vdash e_1 : t_3$   
 4:  $(\Gamma, x_2:t_2), x_1:t_1 \equiv (\Gamma, x_1:t_1), x_2:t_2$   
 5:  $\Pi_1; (\Gamma, x_1:t_1), x_2:t_2 \vdash e_1 : t_3$   
 6:  $; \cdot \vdash e_2 : t_2$   
 7:  $(\lambda[\Pi_1]x_1:t_1. e_1)\{e_2/x_2\} = (\lambda[\Pi_1]x_1:t_1. e_3)$   
 8:  $e_1\{e_2/x_2\} = e_3$   
 9:  $\Pi_1; \Gamma, x_1:t_1 \vdash e_3 : t_3$   
 10:  $\Pi_2; \Gamma \vdash \lambda[\Pi_1]x_1:t_1. e_3 : t_1 \rightarrow t_3$

(subty-fun)  
 \*given  
 $\downarrow$ ty-fun: 1  
 $\downarrow$ ty-fun: 1  
 perm-x1  
 permty: 3,4  
 \*given  
 \*given  
 $\downarrow$ sub-fun: 7  
 subty: 5,6,8  
 ty-fun: 2,9

1: $\Pi; \Gamma; x:t_1 \vdash e_4 e_1 : t_3$ 2: $\Pi; \Gamma; x:t_1 \vdash e_4 : t_2 \rightarrow t_3$ 3: $\cdot \vdash e_2 : t_1$ 4: $(e_4 e_1)\{e_2/x\} = (e_5 e_3)$ 5: $e_4\{e_2/x\} = e_5$ 6: $\Pi; \Gamma \vdash e_5 : t_2 \rightarrow t_3$ 7: $\Pi; \Gamma; x:t_1 \vdash e_1 : t_2$ 8: $e_1\{e_2/x\} = e_3$ 9: $\Pi; \Gamma \vdash e_3 : t_2$ 10: $\Pi; \Gamma \vdash e_5 e_3 : t_3$	(subty-app) *given $\downarrow$ ty-app: 1 *given *given $\downarrow$ sub-app: 4 subty: 2,3,5 $\downarrow$ ty-app: 1 $\downarrow$ sub-app: 4 subty: 7,3,8 ty-app: 6,9
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

$$\frac{\Pi; \Gamma \vdash e_1 : t_1 \quad e_1 = \mathcal{E}[e_2]}{\Pi; \Gamma \vdash e_2 : t_2}$$

splitty

1: $\Pi; \Gamma \vdash \text{if } e_1 e_2 e_3 : t$ 2: $\Pi; \Gamma \vdash e_2 : t$ 3: $\Pi; \Gamma \vdash e_3 : t$ 4: $\text{lab}(t) = \ell$ 5: $\text{if } e_1 e_2 e_3 = \text{if } \mathcal{E} e_2 e_3[e_1]$ 6: $\Pi; \Gamma \vdash e_1 : \text{bool}_\ell$	(splitty-afb) *given $\downarrow$ ty-afb: 1 $\downarrow$ ty-afb: 1 $\downarrow$ ty-afb: 1 *given $\downarrow$ ty-afb: 1
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------

1: $\Pi; \Gamma \vdash e_1 e_2 : t_1$ 2: $\Pi; \Gamma \vdash e_2 : t_2$ 3: $e_1 e_2 = \mathcal{E} e_2[e_1]$ 4: $\Pi; \Gamma \vdash e_1 : t_2 \rightarrow t_1$	(splitty-app1) *given $\downarrow$ ty-app: 1 *given $\downarrow$ ty-app: 1
------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------

1: $\Pi; \Gamma \vdash e_1 e_2 : t_1$ 2: $\Pi; \Gamma \vdash e_1 : t_2 \rightarrow t_1$ 3: $e_1 e_2 = e_1 \mathcal{E}[e_2]$ 4: $\Pi; \Gamma \vdash e_2 : t_2$	(splitty-app2) *given $\downarrow$ ty-app: 1 *given $\downarrow$ ty-app: 1
------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------

1: $\Pi; \Gamma \vdash [\ell_1 \sqsubseteq \ell_2]e : \text{bool}_{\ell_2}$ 2: $\Pi \vdash \ell_1 \sqsubseteq \ell_2$ 3: $[\ell_1 \sqsubseteq \ell_2]e = [\ell_1 \sqsubseteq \ell_2]\mathcal{E}[e]$ 4: $\Pi; \Gamma \vdash e : \text{bool}_{\ell_1}$	(splitty-tag) *given $\downarrow$ ty-tag: 1 *given $\downarrow$ ty-tag: 1
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------

$$\frac{\Pi; \Gamma \vdash e_1 : t_1 \quad e_1 = \mathcal{E}[e_2] \quad \Pi; \Gamma \vdash e_2 : t_2 \quad \Pi; \Gamma \vdash e_3 : t_2 \quad \mathcal{E}[e_3] = e_4}{\Pi; \Gamma \vdash e_4 : t_1}$$

combinety

1: $\Pi; \Gamma \vdash \text{if } e_1 e_2 e_3 : t$ 2: $\Pi; \Gamma \vdash e_1 : \text{bool}_\ell$ 3: $\text{if } e_1 e_2 e_3 = \text{if } \mathcal{E} e_2 e_3[e_1]$ 4: $\text{if } \mathcal{E} e_2 e_3[e_4] = \text{if } e_4 e_2 e_3$ 5: $\Pi; \Gamma \vdash e_4 : \text{bool}_\ell$ 6: $\Pi; \Gamma \vdash e_2 : t$ 7: $\Pi; \Gamma \vdash e_3 : t$ 8: $\text{lab}(t) = \ell$ 9: $\Pi; \Gamma \vdash \text{if } e_4 e_2 e_3 : t$	(combinety-afb) *given $\downarrow$ ty-afb: 1 *given *given *given $\downarrow$ ty-afb: 1 $\downarrow$ ty-afb: 1 $\downarrow$ ty-afb: 1 ty-afb: 5,6,7,8
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

1: $\Pi; \Gamma \vdash e_1 e_2 : t_1$	(combinety-app1) *given
---------------------------------------	----------------------------

2:	$\Pi; \Gamma \vdash e_1 : t_2 \rightarrow t_1$	$\downarrow$ ty-app: 1
3:	$e_1 e_2 = \mathcal{E} e_2 [e_1]$	*given
4:	$\mathcal{E} e_2 [e_3] = e_3 e_2$	*given
5:	$\Pi; \Gamma \vdash e_3 : t_2 \rightarrow t_1$	*given
6:	$\Pi; \Gamma \vdash e_2 : t_2$	$\downarrow$ ty-app: 1
7:	$\Pi; \Gamma \vdash e_3 e_2 : t_1$	ty-app: 5,6

1:	$\Pi; \Gamma \vdash e_1 e_2 : t_1$	(combinety-app2)
2:	$\Pi; \Gamma \vdash e_2 : t_2$	*given
3:	$e_1 e_2 = e_1 \mathcal{E} [e_2]$	$\downarrow$ ty-app: 1
4:	$e_1 \mathcal{E} [e_3] = e_1 e_3$	*given
5:	$\Pi; \Gamma \vdash e_1 : t_2 \rightarrow t_1$	*given
6:	$\Pi; \Gamma \vdash e_3 : t_2$	$\downarrow$ ty-app: 1
7:	$\Pi; \Gamma \vdash e_1 e_3 : t_1$	*given
		ty-app: 5,6

1:	$\Pi; \Gamma \vdash [\ell_1 \sqsubseteq \ell_2] e_1 : \text{bool}_{\ell_2}$	(combinety-tag)
2:	$\Pi; \Gamma \vdash e_1 : \text{bool}_{\ell_1}$	*given
3:	$[\ell_1 \sqsubseteq \ell_2] e_1 = [\ell_1 \sqsubseteq \ell_2] \mathcal{E} [e_1]$	$\downarrow$ ty-tag: 1
4:	$[\ell_1 \sqsubseteq \ell_2] \mathcal{E} [e_2] = [\ell_1 \sqsubseteq \ell_2] e_2$	*given
5:	$\Pi \vdash \ell_1 \sqsubseteq \ell_2$	*given
6:	$\Pi; \Gamma \vdash e_2 : \text{bool}_{\ell_1}$	$\downarrow$ ty-tag: 1
7:	$\Pi; \Gamma \vdash [\ell_1 \sqsubseteq \ell_2] e_2 : \text{bool}_{\ell_2}$	*given
		ty-tag: 5,6

## 5 Theorems

### 5.1 Preservation

$\frac{\Pi; \Gamma \vdash e : t \quad \text{val } e}{\cdot; \vdash e : t}$	valty
<ol style="list-style-type: none"> <li>1: <math>\Pi; \Gamma \vdash \text{true}_\ell : \text{bool}_\ell</math></li> <li>2: <math>\text{val true}_\ell</math></li> <li>3: <math>\cdot; \vdash \text{true}_\ell : \text{bool}_\ell</math></li> </ol>	(valty-true) *given *given ty-true
<ol style="list-style-type: none"> <li>1: <math>\Pi; \Gamma \vdash \text{false}_\ell : \text{bool}_\ell</math></li> <li>2: <math>\text{val false}_\ell</math></li> <li>3: <math>\cdot; \vdash \text{false}_\ell : \text{bool}_\ell</math></li> </ol>	(valty-false) *given *given ty-false
<ol style="list-style-type: none"> <li>1: <math>\cdot; \vdash \lambda[\Pi]x:t_1. e : t_1 \rightarrow t_2</math></li> <li>2: <math>\cdot \leq \Pi</math></li> <li>3: <math>\Pi; \cdot, x:t_1 \vdash e : t_2</math></li> <li>4: <math>\text{val } (\lambda[\Pi]x:t_1. e)</math></li> </ol>	(valty-fun) *given $\downarrow$ ty-fun: 1 $\downarrow$ ty-fun: 1 *given
$\frac{\Pi; \cdot \vdash e_1 : t \quad \Pi \vdash e_1 \longrightarrow e_2}{\Pi; \cdot \vdash e_2 : t}$	ps
<ol style="list-style-type: none"> <li>1: <math>\Pi; \cdot \vdash (\lambda[\Pi]x:t_1. e_1) e_2 : t_2</math></li> <li>2: <math>\Pi; \cdot \vdash \lambda[\Pi]x:t_1. e_1 : t_1 \rightarrow t_2</math></li> <li>3: <math>\Pi \leq \Pi</math></li> <li>4: <math>\Pi; \cdot, x:t_1 \vdash e_1 : t_2</math></li> <li>5: <math>\Pi; \cdot \vdash e_2 : t_1</math></li> <li>6: <math>\Pi \vdash (\lambda[\Pi]x:t_1. e_1) e_2 \longrightarrow e_3</math></li> <li>7: <math>\text{val } e_2</math></li> <li>8: <math>\cdot; \vdash e_2 : t_1</math></li> <li>9: <math>e_1\{e_2/x\} = e_3</math></li> <li>10: <math>\Pi; \cdot \vdash e_3 : t_2</math></li> </ol>	(ps-app) *given $\downarrow$ ty-app: 1 $\downarrow$ ty-fun: 2 $\downarrow$ ty-fun: 2 $\downarrow$ ty-app: 1 *given $\downarrow$ ev-app: 6 valty: 5,7 $\downarrow$ ev-app: 6 subty: 4,8,9
<ol style="list-style-type: none"> <li>1: <math>\Pi; \cdot \vdash \text{if true}_{\ell_1} e_1 e_2 : t</math></li> <li>2: <math>\Pi; \cdot \vdash \text{true}_{\ell_1} : \text{bool}_{\ell_2}</math></li> <li>3: <math>\Pi; \cdot \vdash e_2 : t</math></li> <li>4: <math>\text{lab}(t) = \ell_2</math></li> <li>5: <math>\Pi \vdash \text{if true}_{\ell_1} e_1 e_2 \longrightarrow e_1</math></li> <li>6: <math>\Pi; \cdot \vdash e_1 : t</math></li> </ol>	(ps-ifb1) *given $\downarrow$ ty-ifb: 1 $\downarrow$ ty-ifb: 1 $\downarrow$ ty-ifb: 1 *given $\downarrow$ ty-ifb: 1
<ol style="list-style-type: none"> <li>1: <math>\Pi; \cdot \vdash \text{if false}_{\ell_1} e_1 e_2 : t</math></li> <li>2: <math>\Pi; \cdot \vdash \text{false}_{\ell_1} : \text{bool}_{\ell_2}</math></li> <li>3: <math>\Pi; \cdot \vdash e_1 : t</math></li> <li>4: <math>\text{lab}(t) = \ell_2</math></li> <li>5: <math>\Pi \vdash \text{if false}_{\ell_1} e_1 e_2 \longrightarrow e_2</math></li> <li>6: <math>\Pi; \cdot \vdash e_2 : t</math></li> </ol>	(ps-ifb2) *given $\downarrow$ ty-ifb: 1 $\downarrow$ ty-ifb: 1 $\downarrow$ ty-ifb: 1 *given $\downarrow$ ty-ifb: 1
<ol style="list-style-type: none"> <li>1: <math>\Pi; \cdot \vdash \text{if } (p_1 \leq p_2) e_1 e_2 : t</math></li> <li>2: <math>\Pi; \cdot \vdash e_2 : t</math></li> </ol>	(ps-ifp1) *given $\downarrow$ ty-ifp: 1

3:  $\Pi, p_1 \leq p_2; \cdot \vdash e_1 : t$  ↓ty-ifp: 1  
4:  $\Pi \vdash \text{if } (p_1 \leq p_2) e_1 e_2 \longrightarrow e_1$  \*given  
5:  $\Pi \vdash p_1 \leq p_2$  ↓ev-ifp1: 4  
6:  $\Pi; \cdot \vdash e_1 : t$  pstty: 3,5

(ps-ifp2)

1:  $\Pi; \cdot \vdash \text{if } (p_1 \leq p_2) e_1 e_2 : t$  \*given  
2:  $\Pi, p_1 \leq p_2; \cdot \vdash e_1 : t$  ↓ty-ifp: 1  
3:  $\Pi \vdash \text{if } (p_1 \leq p_2) e_1 e_2 \longrightarrow e_2$  \*given  
4:  $\Pi \not\vdash p_1 \leq p_2$  ↓ev-ifp2: 3  
5:  $\Pi; \cdot \vdash e_2 : t$  ↓ty-ifp: 1

(ps-tag1)

1:  $\Pi; \cdot \vdash [l_1 \sqsubseteq l_2] \text{true}_{\ell_1} : \text{bool}_{\ell_2}$  \*given  
2:  $\Pi \vdash l_1 \sqsubseteq l_2$  ↓ty-tag: 1  
3:  $\Pi; \cdot \vdash \text{true}_{\ell_1} : \text{bool}_{\ell_1}$  ↓ty-tag: 1  
4:  $\Pi \vdash [l_1 \sqsubseteq l_2] \text{true}_{\ell_1} \longrightarrow \text{true}_{\ell_2}$  \*given  
5:  $\Pi; \cdot \vdash \text{true}_{\ell_2} : \text{bool}_{\ell_2}$  ty-true

(ps-tag2)

1:  $\Pi; \cdot \vdash [l_1 \sqsubseteq l_2] \text{false}_{\ell_1} : \text{bool}_{\ell_2}$  \*given  
2:  $\Pi \vdash l_1 \sqsubseteq l_2$  ↓ty-tag: 1  
3:  $\Pi; \cdot \vdash \text{false}_{\ell_1} : \text{bool}_{\ell_1}$  ↓ty-tag: 1  
4:  $\Pi \vdash [l_1 \sqsubseteq l_2] \text{false}_{\ell_1} \longrightarrow \text{false}_{\ell_2}$  \*given  
5:  $\Pi; \cdot \vdash \text{false}_{\ell_2} : \text{bool}_{\ell_2}$  ty-false

(ps-hole)

1:  $\Pi; \cdot \vdash e_1 : t_1$  \*given  
2:  $\Pi \vdash e_1 \longrightarrow e_4$  \*given  
3:  $e_1 = \mathcal{E}[e_2]$  ↓ev-hole: 2  
4:  $\Pi; \cdot \vdash e_2 : t_2$  splitty: 1,3  
5:  $\Pi \vdash e_2 \longrightarrow e_3$  ↓ev-hole: 2  
6:  $\Pi; \cdot \vdash e_3 : t_2$  ps: 4,5  
7:  $\mathcal{E}[e_3] = e_4$  ↓ev-hole: 2  
8:  $\Pi; \cdot \vdash e_4 : t_1$  combinety: 1,3,4,6,7

$$\frac{\Pi_1; \cdot \vdash e_1 : t \quad (\Pi_1; e_1) | \Pi^\bullet \longrightarrow (\Pi_2; e_2)}{\Pi_2; \cdot \vdash e_2 : t}$$

topps

(topps-ev)

1:  $\Pi; \cdot \vdash e_1 : t$  \*given  
2:  $(\Pi; e_1) | \Pi \longrightarrow (\Pi; e_2)$  \*given  
3:  $\Pi \vdash e_1 \longrightarrow e_2$  ↓topev-ev: 2  
4:  $\Pi; \cdot \vdash e_2 : t$  ps: 1,3

(topps-upd)

1:  $\Pi_1; \cdot \vdash e : t$  \*given  
2:  $(\Pi_1; e) | \Pi_2 \longrightarrow (\Pi_2; e)$  \*given  
3:  $\Pi_2 \vdash e$  ↓topev-upd: 2  
4:  $\Pi_2; \cdot \vdash e : t$  aety: 1,3

## 5.2 Progress

$$\boxed{\Pi \vdash \text{ve } e}$$

ve

$$\frac{\text{val } e}{\Pi \vdash \text{ve } e}$$

(ve-v)

$\frac{\Pi \vdash e_1 \longrightarrow e_2}{\Pi \vdash ve e_1}$	(ve-e)
<div style="border: 1px solid black; padding: 5px; display: inline-block;"> <math display="block">\frac{\Pi; \cdot \vdash e : t}{\Pi \vdash ve e}</math> </div>	<div style="border: 1px solid black; padding: 2px 5px; display: inline-block;">pg</div>
1: $\Pi; \cdot \vdash true_{\ell} : bool_{\ell}$ 2: $val\ true_{\ell}$ 3: $\Pi \vdash ve\ true_{\ell}$	(pg-true) *given val-true ve-v: 2
1: $\Pi; \cdot \vdash false_{\ell} : bool_{\ell}$ 2: $val\ false_{\ell}$ 3: $\Pi \vdash ve\ false_{\ell}$	(pg-false) *given val-false ve-v: 2
1: $\Pi; \cdot \vdash if\ e_1\ e_3\ e_4 : t$ 2: $\Pi; \cdot \vdash e_3 : t$ 3: $\Pi; \cdot \vdash e_4 : t$ 4: $lab(t) = \ell$ 5: $if\ e_1\ e_3\ e_4 = if\ \mathcal{E}\ e_3\ e_4[e_1]$ 6: $\Pi; \cdot \vdash e_1 : bool_{\ell}$ 7: $\Pi \vdash ve\ e_1$ 8: $\Pi \vdash e_1 \longrightarrow e_2$ 9: $if\ \mathcal{E}\ e_3\ e_4[e_2] = if\ e_2\ e_3\ e_4$ 10: $\Pi \vdash if\ e_1\ e_3\ e_4 \longrightarrow if\ e_2\ e_3\ e_4$ 11: $\Pi \vdash ve\ (if\ e_1\ e_3\ e_4)$	(pg-ifb1) *given $\downarrow ty$ -ifb: 1 $\downarrow ty$ -ifb: 1 $\downarrow ty$ -ifb: 1 split-ifb $\downarrow ty$ -ifb: 1 pg: 6 $\downarrow ve$ -e: 7 combine-ifb ev-hole: 5,8,9 ve-e: 10
1: $\Pi; \cdot \vdash if\ true_{\ell_1}\ e_1\ e_2 : t$ 2: $\Pi; \cdot \vdash true_{\ell_1} : bool_{\ell_2}$ 3: $\Pi; \cdot \vdash e_1 : t$ 4: $\Pi; \cdot \vdash e_2 : t$ 5: $lab(t) = \ell_2$ 6: $\Pi \vdash ve\ true_{\ell_1}$ 7: $val\ true_{\ell_1}$ 8: $\Pi \vdash if\ true_{\ell_1}\ e_1\ e_2 \longrightarrow e_1$ 9: $\Pi \vdash ve\ (if\ true_{\ell_1}\ e_1\ e_2)$	(pg-ifb2) *given $\downarrow ty$ -ifb: 1 $\downarrow ty$ -ifb: 1 $\downarrow ty$ -ifb: 1 $\downarrow ty$ -ifb: 1 pg: 2 $\downarrow ve$ -v: 6 ev-ifb1 ve-e: 8
1: $\Pi; \cdot \vdash if\ false_{\ell_1}\ e_1\ e_2 : t$ 2: $\Pi; \cdot \vdash false_{\ell_1} : bool_{\ell_2}$ 3: $\Pi; \cdot \vdash e_1 : t$ 4: $\Pi; \cdot \vdash e_2 : t$ 5: $lab(t) = \ell_2$ 6: $\Pi \vdash ve\ false_{\ell_1}$ 7: $val\ false_{\ell_1}$ 8: $\Pi \vdash if\ false_{\ell_1}\ e_1\ e_2 \longrightarrow e_2$ 9: $\Pi \vdash ve\ (if\ false_{\ell_1}\ e_1\ e_2)$	(pg-ifb3) *given $\downarrow ty$ -ifb: 1 $\downarrow ty$ -ifb: 1 $\downarrow ty$ -ifb: 1 $\downarrow ty$ -ifb: 1 pg: 2 $\downarrow ve$ -v: 6 ev-ifb2 ve-e: 8
1: $\Pi_1; \cdot \vdash \lambda[\Pi_2]x:t_1. e : t_1 \rightarrow t_2$ 2: $\Pi_1 \leq \Pi_2$ 3: $\Pi_2; \cdot, x:t_1 \vdash e : t_2$ 4: $val\ (\lambda[\Pi_2]x:t_1. e)$ 5: $\Pi_1 \vdash ve\ (\lambda[\Pi_2]x:t_1. e)$	(pg-fun) *given $\downarrow ty$ -fun: 1 $\downarrow ty$ -fun: 1 val-fun ve-v: 4

1:	$\Pi; \cdot \vdash e_1 e_3 : t_2$	(pg-app1)
2:	$\Pi; \cdot \vdash e_3 : t_1$	*given
3:	$e_1 e_3 = \mathcal{E} e_3 [e_1]$	$\downarrow$ ty-app: 1
4:	$\Pi; \cdot \vdash e_1 : t_1 \rightarrow t_2$	split-app1
5:	$\Pi \vdash ve e_1$	$\downarrow$ ty-app: 1
6:	$\Pi \vdash e_1 \rightarrow e_2$	pg: 4
7:	$\mathcal{E} e_3 [e_2] = e_2 e_3$	$\downarrow$ ve-e: 5
8:	$\Pi \vdash e_1 e_3 \rightarrow e_2 e_3$	combine-app1
9:	$\Pi \vdash ve (e_1 e_3)$	ev-hole: 3,6,7
		ve-e: 8

1:	$\Pi; \cdot \vdash e_3 e_1 : t_2$	(pg-app2)
2:	$\Pi; \cdot \vdash e_3 : t_1 \rightarrow t_2$	*given
3:	$\Pi \vdash ve e_3$	$\downarrow$ ty-app: 1
4:	val $e_3$	pg: 2
5:	$e_3 e_1 = e_3 \mathcal{E} [e_1]$	$\downarrow$ ve-v: 3
6:	$\Pi; \cdot \vdash e_1 : t_1$	split-app2
7:	$\Pi \vdash ve e_1$	$\downarrow$ ty-app: 1
8:	$\Pi \vdash e_1 \rightarrow e_2$	pg: 6
9:	$e_3 \mathcal{E} [e_2] = e_3 e_2$	$\downarrow$ ve-e: 7
10:	$\Pi \vdash e_3 e_1 \rightarrow e_3 e_2$	combine-app2
11:	$\Pi \vdash ve (e_3 e_1)$	ev-hole: 5,8,9
		ve-e: 10

1:	$\Pi_1; \cdot \vdash (\lambda[\Pi_2]x:t_2. e_1) e_2 : t_3$	(pg-app3)
2:	$\Pi_1; \cdot \vdash \lambda[\Pi_2]x:t_2. e_1 : t_1 \rightarrow t_3$	*given
3:	$\Pi_1 \vdash ve (\lambda[\Pi_2]x:t_2. e_1)$	$\downarrow$ ty-app: 1
4:	val $(\lambda[\Pi_2]x:t_2. e_1)$	pg: 2
5:	$\Pi_1; \cdot \vdash e_2 : t_1$	$\downarrow$ ve-v: 3
6:	$\Pi_1 \vdash ve e_2$	$\downarrow$ ty-app: 1
7:	val $e_2$	pg: 5
8:	$e_1 \{e_2/x\} = e_3$	$\downarrow$ ve-v: 6
9:	$\Pi_1 \vdash (\lambda[\Pi_2]x:t_2. e_1) e_2 \rightarrow e_3$	sub-total
10:	$\Pi_1 \vdash ve ((\lambda[\Pi_2]x:t_2. e_1) e_2)$	ev-app: 7,8
		ve-e: 9

1:	$\Pi; \cdot \vdash \text{if } (p_1 \leq p_2) e_1 e_2 : t$	(pg-ifp1)
2:	$\Pi, p_1 \leq p_2; \cdot \vdash e_1 : t$	*given
3:	$\Pi; \cdot \vdash e_2 : t$	$\downarrow$ ty-ifp: 1
4:	$\Pi \vdash p_1 \diamond p_2$	$\downarrow$ ty-ifp: 1
5:	$\Pi \vdash p_1 \leq p_2$	pst-total
6:	$\Pi \vdash \text{if } (p_1 \leq p_2) e_1 e_2 \rightarrow e_1$	$\downarrow$ psty-pst: 4
7:	$\Pi \vdash ve (\text{if } (p_1 \leq p_2) e_1 e_2)$	ev-ifp1: 5
		ve-e: 6

1:	$\Pi; \cdot \vdash \text{if } (p_1 \leq p_2) e_1 e_2 : t$	(pg-ifp2)
2:	$\Pi, p_1 \leq p_2; \cdot \vdash e_1 : t$	*given
3:	$\Pi; \cdot \vdash e_2 : t$	$\downarrow$ ty-ifp: 1
4:	$\Pi \vdash p_1 \diamond p_2$	$\downarrow$ ty-ifp: 1
5:	$\Pi \not\vdash p_1 \leq p_2$	pst-total
6:	$\Pi \vdash \text{if } (p_1 \leq p_2) e_1 e_2 \rightarrow e_2$	$\downarrow$ psty-pnst: 4
7:	$\Pi \vdash ve (\text{if } (p_1 \leq p_2) e_1 e_2)$	ev-ifp2: 5
		ve-e: 6

1:	$\Pi; \cdot \vdash [\ell_1 \sqsubseteq \ell_2] \text{true}_{\ell_1} : \text{bool}_{\ell_2}$	(pg-tag1)
2:	$\Pi \vdash \ell_1 \sqsubseteq \ell_2$	*given
3:	$\Pi; \cdot \vdash \text{true}_{\ell_1} : \text{bool}_{\ell_1}$	$\downarrow$ ty-tag: 1
4:	$\Pi \vdash ve \text{true}_{\ell_1}$	$\downarrow$ ty-tag: 1
		pg: 3

5:  $\text{val true}_{\ell_1}$  ↓ve-v: 4  
6:  $\Pi \vdash [\ell_1 \sqsubseteq \ell_2] \text{true}_{\ell_1} \longrightarrow \text{true}_{\ell_2}$  ev-tag1  
7:  $\Pi \vdash \text{ve } ([\ell_1 \sqsubseteq \ell_2] \text{true}_{\ell_1})$  ve-e: 6

(pg-tag2)  
\*given

1:  $\Pi; \cdot \vdash [\ell_1 \sqsubseteq \ell_2] \text{false}_{\ell_1} : \text{bool}_{\ell_2}$   
2:  $\Pi \vdash \ell_1 \sqsubseteq \ell_2$  ↓ty-tag: 1  
3:  $\Pi; \cdot \vdash \text{false}_{\ell_1} : \text{bool}_{\ell_1}$  ↓ty-tag: 1  
4:  $\Pi \vdash \text{ve false}_{\ell_1}$  pg: 3  
5:  $\text{val false}_{\ell_1}$  ↓ve-v: 4  
6:  $\Pi \vdash [\ell_1 \sqsubseteq \ell_2] \text{false}_{\ell_1} \longrightarrow \text{false}_{\ell_2}$  ev-tag2  
7:  $\Pi \vdash \text{ve } ([\ell_1 \sqsubseteq \ell_2] \text{false}_{\ell_1})$  ve-e: 6

$$\boxed{\Pi \vdash \text{topve } e}$$

$$\boxed{\text{topve}}$$

$$\frac{\text{val } e}{\Pi \vdash \text{topve } e}$$

(topve-v)

$$\frac{\text{some } \Pi \quad (\Pi_1; e_1) | \Pi \longrightarrow (\Pi_2; e_2)}{\Pi_1 \vdash \text{topve } e_1}$$

(topve-e)

$$\boxed{\frac{\Pi; \cdot \vdash e : t}{\Pi \vdash \text{topve } e}}$$

$$\boxed{\text{toppg}}$$

(toppg-v)

1:  $\Pi; \cdot \vdash e : t$  \*given  
2:  $\Pi \vdash \text{ve } e$  pg: 1  
3:  $\text{val } e$  ↓ve-v: 2  
4:  $\Pi \vdash \text{topve } e$  topve-v: 3

(toppg-e)  
asome-total  
\*given

1:  $\text{some } \Pi$   
2:  $\Pi; \cdot \vdash e_1 : t$  pg: 2  
3:  $\Pi \vdash \text{ve } e_1$  ↓ve-e: 3  
4:  $\Pi \vdash e_1 \longrightarrow e_2$  topev-ev: 4  
5:  $(\Pi; e_1) | \Pi \longrightarrow (\Pi; e_2)$  topve-e: 1,5  
6:  $\Pi \vdash \text{topve } e_1$

### 5.3 Soundness

$$\boxed{\frac{\Pi_1; \cdot \vdash e_1 : t}{(\Pi_1; e_1) \Downarrow (\Pi_2; e_2)}}$$

$$\boxed{\text{snd}}$$

(snd-v)

1:  $\Pi; \cdot \vdash e : t$  \*given  
2:  $\Pi \vdash \text{topve } e$  toppg: 1  
3:  $\text{val } e$  ↓topve-v: 2  
4:  $(\Pi; e) \Downarrow (\Pi; e)$  bigev-v: 3

(snd-e)

\*given

1:  $\Pi_3; \cdot \vdash e_3 : t$  toppg: 1  
2:  $\Pi_3 \vdash \text{topve } e_3$  ↓topve-e: 2  
3:  $\text{some } \Pi_4$  ↓topve-e: 2  
4:  $(\Pi_3; e_3) | \Pi_4 \longrightarrow (\Pi_1; e_1)$  topps: 1,4  
5:  $\Pi_1; \cdot \vdash e_1 : t$  snd: 5  
6:  $(\Pi_1; e_1) \Downarrow (\Pi_2; e_2)$  bigev-e: 3,4,6  
7:  $(\Pi_3; e_3) \Downarrow (\Pi_1; e_2)$



## 6 Translations

### 6.1 Types

$u ::= \dots$	$u$
$u ::= \text{bool}_\ell$	(ubool)
$u ::= u \rightarrow u$	(ufun)

### 6.2 Terms

$m ::= \dots$	$m$
$m ::= \text{true}_\ell$	(mtrue)
$m ::= \text{false}_\ell$	(mfalse)
$m ::= x$	(mvar)
$m ::= \lambda x : u. m$	(mfun)
$m ::= m m$	(mapp)
$m ::= \text{if } m m m$	(mifb)
$m ::= \text{if } (p \preceq p) m m$	(mifl)

### 6.3 Contexts

$\Gamma ::= \dots$	$h$
$\Gamma ::= \cdot$	(hz)
$\Gamma ::= \Gamma, x : u$	(hx)

### 6.4 Type labels

$\text{lab}(u) = \ell$	$\text{ulab}$
$\text{lab}(\text{bool}_\ell) = \ell$	(ulab-bool)
$\frac{\text{lab}(u_2) = \ell}{\text{lab}(u_1 \rightarrow u_2) = \ell}$	(ulab-fun)

### 6.5 Subtypings

$\Pi \vdash u \preceq u$	$\text{ust}$
$\frac{\Pi \vdash \ell_1 \sqsubseteq \ell_2}{\Pi \vdash \text{bool}_{\ell_1} \preceq \text{bool}_{\ell_2}}$	(ust-bool)
$\frac{\Pi \vdash u_3 \preceq u_1 \quad \Pi \vdash u_2 \preceq u_4}{\Pi \vdash u_1 \rightarrow u_2 \preceq u_3 \rightarrow u_4}$	(ust-fun)

### 6.6 Typings

$\text{some } u$	$\text{usome}$
$\Pi; \Gamma \vdash m : u$	$\text{mty}$
$\Pi; \Gamma \vdash \text{true}_\ell : \text{bool}_\ell$	(mty-true)

$\Pi; \Gamma \vdash \text{false}_\ell : \text{bool}_\ell$	(mty-false)
$\frac{\Pi; \Gamma \vdash m_1 : \text{bool}_\ell \quad \Pi; \Gamma \vdash m_2 : u \quad \Pi; \Gamma \vdash m_3 : u \quad \text{lab}(u) = \ell}{\Pi; \Gamma \vdash \text{if } m_1 m_2 m_3 : u}$	(mty-iff)
$\Pi; \Gamma, x : u \vdash x : u$	(mty-var1)
$\frac{\Pi; \Gamma \vdash x_2 : u_2}{\Pi; \Gamma, x_1 : u_1 \vdash x_2 : u_2}$	(mty-var2)
$\frac{\Pi; \Gamma, x : u_1 \vdash m : u_2}{\Pi; \Gamma \vdash \lambda x : u_1 . m : u_1 \rightarrow u_2}$	(mty-fun)
$\frac{\Pi; \Gamma \vdash m_1 : u_1 \rightarrow u_2 \quad \Pi; \Gamma \vdash m_2 : u_1}{\Pi; \Gamma \vdash m_1 m_2 : u_2}$	(mty-app)
$\frac{\Pi, p_1 \leq p_2; \Gamma \vdash m_1 : u \quad \Pi; \Gamma \vdash m_2 : u}{\Pi; \Gamma \vdash \text{if } (p_1 \leq p_2) m_1 m_2 : u}$	(mty-iff)
$\frac{\Pi; \Gamma \vdash m : u_1 \quad \text{some } u_2 \quad \Pi \vdash u_1 \preceq u_2}{\Pi; \Gamma \vdash m : u_2}$	(mty-sub)

## 6.7 Theorems

$\boxed{[u] = t}$	$\boxed{\text{ut}}$
$\llbracket \text{bool}_\ell \rrbracket = \text{bool}_\ell$	(ut-bool)
$\frac{\llbracket u_1 \rrbracket = t_1 \quad \llbracket u_2 \rrbracket = t_2}{\llbracket u_1 \rightarrow u_2 \rrbracket = t_1 \rightarrow t_2}$	(ut-fun)
$\boxed{\frac{\text{lab}(u) = \ell \quad \Pi; \Gamma \vdash e : t}{\text{lab}(t) = \ell}}$	$\boxed{\text{ulablab}}$
<ol style="list-style-type: none"> <li>1: <math>\text{lab}(\text{bool}_\ell) = \ell</math></li> <li>2: <math>\Pi; \Gamma \vdash e : \text{bool}_\ell</math></li> <li>3: <math>\text{lab}(\text{bool}_\ell) = \ell</math></li> </ol>	<ul style="list-style-type: none"> <li>(ulablab-bool)</li> <li>*given</li> <li>*given</li> <li>lab-bool</li> </ul>
<ol style="list-style-type: none"> <li>1: <math>\Pi_2; \Gamma \vdash \lambda[\Pi_1]x : t_1 . e : t_1 \rightarrow t_2</math></li> <li>2: <math>\Pi_2 \leq \Pi_1</math></li> <li>3: <math>\text{lab}(u_2 \rightarrow u_1) = \ell</math></li> <li>4: <math>\text{lab}(u_1) = \ell</math></li> <li>5: <math>\Pi_1; \Gamma, x : t_1 \vdash e : t_2</math></li> <li>6: <math>\text{lab}(t_2) = \ell</math></li> <li>7: <math>\text{lab}(t_1 \rightarrow t_2) = \ell</math></li> </ol>	<ul style="list-style-type: none"> <li>(ulablab-fun)</li> <li>*given</li> <li><math>\downarrow</math>ty-fun: 1</li> <li>*given</li> <li><math>\downarrow</math>ulab-fun: 3</li> <li><math>\downarrow</math>ty-fun: 1</li> <li>ulablab: 4,5</li> <li>lab-fun: 6</li> </ul>
$\boxed{\text{fresh } x}$	$\boxed{\text{fresh}}$
$\boxed{\frac{\Pi \vdash u_1 \preceq u_2}{\Pi; \Gamma \vdash e : t_1 \rightarrow t_2}}$	$\boxed{\text{ustty}}$
<ol style="list-style-type: none"> <li>1: <math>x</math></li> <li>2: <math>\Pi \leq \Pi</math></li> <li>3: <math>\Pi \vdash \text{bool}_{\ell_1} \preceq \text{bool}_{\ell_2}</math></li> <li>4: <math>\Pi \vdash \ell_1 \sqsubseteq \ell_2</math></li> <li>5: <math>\Pi; \Gamma, x : \text{bool}_{\ell_1} \vdash x : \text{bool}_{\ell_1}</math></li> </ol>	<ul style="list-style-type: none"> <li>(ustty-bool)</li> <li>fresh</li> <li>ast-z</li> <li>*given</li> <li><math>\downarrow</math>ust-bool: 3</li> <li>ty-var1</li> </ul>

6:  $\Pi; \Gamma, x : \text{bool}_{\ell_1} \vdash [\ell_1 \sqsubseteq \ell_2]x : \text{bool}_{\ell_2}$  ty-tag: 4,5  
7:  $\Pi; \Gamma \vdash \lambda[\Pi]x : \text{bool}_{\ell_1}. ([\ell_1 \sqsubseteq \ell_2]x) : \text{bool}_{\ell_1} \rightarrow \text{bool}_{\ell_2}$  ty-fun: 2,6

(ustty-fun)  
1:  $x_2$  fresh  
2:  $x_1$  fresh  
3:  $\Pi \leq \Pi$  ast-z  
4:  $\Pi \vdash u_4 \rightarrow u_1 \preceq u_3 \rightarrow u_2$  \*given  
5:  $\Pi \vdash u_1 \preceq u_2$   $\downarrow$ ust-fun: 4  
6:  $\Pi; (\Gamma, x_1 : (t_1 \rightarrow t_2)), x_2 : t_3 \vdash e_1 : t_2 \rightarrow t_4$  ustty: 5  
7:  $\Pi; \Gamma, x_1 : (t_1 \rightarrow t_2) \vdash x_1 : t_1 \rightarrow t_2$  ty-var1  
8:  $\Pi; (\Gamma, x_1 : (t_1 \rightarrow t_2)), x_2 : t_3 \vdash x_1 : t_1 \rightarrow t_2$  ty-var2: 7  
9:  $\Pi \vdash u_3 \preceq u_4$   $\downarrow$ ust-fun: 4  
10:  $\Pi; (\Gamma, x_1 : (t_1 \rightarrow t_2)), x_2 : t_3 \vdash e_2 : t_3 \rightarrow t_1$  ustty: 9  
11:  $\Pi; (\Gamma, x_1 : (t_1 \rightarrow t_2)), x_2 : t_3 \vdash x_2 : t_3$  ty-var1  
12:  $\Pi; (\Gamma, x_1 : (t_1 \rightarrow t_2)), x_2 : t_3 \vdash e_2 x_2 : t_1$  ty-app: 10,11  
13:  $\Pi; (\Gamma, x_1 : (t_1 \rightarrow t_2)), x_2 : t_3 \vdash x_1 (e_2 x_2) : t_2$  ty-app: 8,12  
14:  $\Pi; (\Gamma, x_1 : (t_1 \rightarrow t_2)), x_2 : t_3 \vdash e_1 (x_1 (e_2 x_2)) : t_4$  ty-app: 6,13  
15:  $\Pi; \Gamma, x_1 : (t_1 \rightarrow t_2) \vdash \lambda[\Pi]x_2 : t_3. (e_1 (x_1 (e_2 x_2))) : t_3 \rightarrow t_4$  ty-fun: 3,14  
16:  $\Pi; \Gamma \vdash \lambda[\Pi]x_1 : (t_1 \rightarrow t_2). (\lambda[\Pi]x_2 : t_3. (e_1 (x_1 (e_2 x_2)))) : (t_1 \rightarrow t_2) \rightarrow (t_3 \rightarrow t_4)$  ty-fun: 3,15

$\Pi; \Gamma \vdash m : u$
$\Pi; \Gamma \vdash e : t$

mtyty
-------

(mtyty-true)  
1:  $\Pi; \Gamma \vdash \text{true}_{\ell} : \text{bool}_{\ell}$  \*given  
2:  $\Pi; \Gamma \vdash \text{true}_{\ell} : \text{bool}_{\ell}$  ty-true

(mtyty-false)  
1:  $\Pi; \Gamma \vdash \text{false}_{\ell} : \text{bool}_{\ell}$  \*given  
2:  $\Pi; \Gamma \vdash \text{false}_{\ell} : \text{bool}_{\ell}$  ty-false

(mtyty-if)  
1:  $\Pi; \Gamma \vdash \text{if } m_3 \ m_2 \ m_1 : u$  \*given  
2:  $\Pi; \Gamma \vdash m_3 : \text{bool}_{\ell}$   $\downarrow$ mty-afb: 1  
3:  $\Pi; \Gamma \vdash e_1 : \text{bool}_{\ell}$  mtyty: 2  
4:  $\Pi; \Gamma \vdash m_2 : u$   $\downarrow$ mty-afb: 1  
5:  $\Pi; \Gamma \vdash e_3 : \text{bool}_{\ell}$  mtyty: 4  
6:  $\Pi; \Gamma \vdash m_1 : u$   $\downarrow$ mty-afb: 1  
7:  $\Pi; \Gamma \vdash e_2 : \text{bool}_{\ell}$  mtyty: 6  
8:  $\text{lab}(u) = \ell$   $\downarrow$ mty-afb: 1  
9:  $\text{lab}(\text{bool}_{\ell}) = \ell$  ulablab: 8,3  
10:  $\Pi; \Gamma \vdash \text{if } e_1 \ e_3 \ e_2 : \text{bool}_{\ell}$  ty-afb: 3,5,7,9

(mtyty-var1)  
1:  $\Pi; \Gamma, x : u \vdash x : u$  \*given  
2:  $\Pi; \Gamma, x : t \vdash x : t$  ty-var1

(mtyty-var2)  
1:  $\Pi; \Gamma, x_1 : u_1 \vdash x_2 : u_2$  \*given  
2:  $\Pi; \Gamma \vdash x_2 : u_2$   $\downarrow$ mty-var2: 1  
3:  $\Pi; \Gamma \vdash x_2 : t_2$  mtyty: 2  
4:  $\Pi; \Gamma, x_1 : t_1 \vdash x_2 : t_2$  ty-var2: 3

(mtyty-fun)  
1:  $\llbracket u_1 \rrbracket = t_1$  ut  
2:  $\Pi \leq \Pi$  ast-z

3:	$\Pi; \Gamma \vdash \lambda x:u_1. m : u_1 \rightarrow u_2$	*given
4:	$\Pi; \Gamma, x:u_1 \vdash m : u_2$	$\downarrow$ mty-fun: 3
5:	$\Pi; \Gamma, x:t_1 \vdash e : t_2$	mtyty: 4
6:	$\Pi; \Gamma \vdash \lambda[\Pi]x:t_1. e : t_1 \rightarrow t_2$	ty-fun: 2,5
(mtyty-app)		
1:	$\Pi; \Gamma \vdash m_2 m_1 : u_2$	*given
2:	$\Pi; \Gamma \vdash m_2 : u_1 \rightarrow u_2$	$\downarrow$ mty-app: 1
3:	$\Pi; \Gamma \vdash e_2 : t_1 \rightarrow t_2$	mtyty: 2
4:	$\Pi; \Gamma \vdash m_1 : u_1$	$\downarrow$ mty-app: 1
5:	$\Pi; \Gamma \vdash e_1 : t_1$	mtyty: 4
6:	$\Pi; \Gamma \vdash e_2 e_1 : t_2$	ty-app: 3,5
(mtyty-ifp)		
1:	$\Pi; \Gamma \vdash \text{if } (p_1 \preceq p_2) m_2 m_1 : u$	*given
2:	$\Pi, p_1 \leq p_2; \Gamma \vdash m_2 : u$	$\downarrow$ mty-ifp: 1
3:	$\Pi, p_1 \leq p_2; \Gamma \vdash e_2 : t$	mtyty: 2
4:	$\Pi; \Gamma \vdash m_1 : u$	$\downarrow$ mty-ifp: 1
5:	$\Pi; \Gamma \vdash e_1 : t$	mtyty: 4
6:	$\Pi; \Gamma \vdash \text{if } (p_1 \leq p_2) e_2 e_1 : t$	ty-ifp: 3,5
(mtyty-sub)		
1:	$\Pi; \Gamma \vdash m : u_2$	*given
2:	some $u_2$	$\downarrow$ mty-sub: 1
3:	$\llbracket u_2 \rrbracket = t_2$	ut
4:	$\llbracket u_1 \rrbracket = t_1$	ut
5:	$\Pi \vdash u_1 \preceq u_2$	$\downarrow$ mty-sub: 1
6:	$\Pi; \Gamma \vdash e_2 : t_1 \rightarrow t_2$	ustty: 5
7:	$\Pi; \Gamma \vdash m : u_1$	$\downarrow$ mty-sub: 1
8:	$\Pi; \Gamma \vdash e_1 : t_1$	mtyty: 7
9:	$\Pi; \Gamma \vdash e_2 e_1 : t_2$	ty-app: 6,8