Syntax

$$
\begin{array}{rrcl}
\textbf{\textit{Value}} & v & ::= & c \;|\; \lambda x.e \\
\textbf{\textit{Expressions}} & e & ::= & v \;|\; x \;|\; e\ e \\
\textbf{\textit{Basic Types}} & b & ::= & \text{int} \;|\; \text{bool} \\
\textbf{\textit{Types}} & \tau & ::= & \{v{:}b \mid e\} \;|\; x{:}\tau \to \tau \\
\textbf{\textit{Environment}} & \Gamma & ::= & \emptyset \;|\; x{:}\tau, \Gamma
\end{array}
$$

Erasing

$$
\begin{aligned}
\lfloor \{v{:}b \mid e\} \rfloor &= b \\
\lfloor x{:}\tau_x \to \tau \rfloor &= \lfloor \tau_x \rfloor \to \lfloor \tau \rfloor
\end{aligned}
$$

$$
\begin{aligned}
\lfloor \emptyset \rfloor &= \emptyset \\
\lfloor x{:}\tau, \Gamma \rfloor &= x{:}\lfloor \tau \rfloor, \lfloor \Gamma \rfloor
\end{aligned}
$$

Substitutions

$$
\begin{aligned}
(\{v{:}b \mid e\})\,[e_y/y] &= \{v{:}b \mid e\,[e_y/y]\} \\
(x{:}\tau_x \to \tau)\,[e_y/y] &= x{:}(\tau_x\,[e_y/y]) \to (\tau\,[e_y/y])
\end{aligned}
$$

Interpretations

$$
\begin{aligned}
[|\,\{v{:}b \mid e_v\}\,|] &= \{e \mid \vdash e{:}b \wedge (\forall i.\mathrm{Fin}_i\ (e) \Rightarrow \mathrm{Valid}_i\ (e_v\,[e/v]))\} \\
[|x{:}\tau_x \to \tau|] &= \{e \mid \vdash e{:}\lfloor \tau_x \rfloor \to \lfloor \tau \rfloor \wedge \forall e_x \in [|\tau_x|].\ e\ e_x \in [|\tau\,[e_x/x]\,|]\}
\end{aligned}
$$

Typing

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

$$\frac{\Gamma \vdash e{:}\,\{v{:}b \mid e'\}}{\Gamma \vdash e{:}\,\{v{:}b \mid v =_b e\}}\ \textsc{T-Ex}$$

$$\frac{(x, \{v{:}b \mid e\}) \in \Gamma}{\Gamma \vdash x{:}\,\{v{:}b \mid v =_b x\}}\ \textsc{T-Var-Base} \qquad \frac{(x, \tau) \in \Gamma \quad \tau \equiv x'{:}\tau'_x \to \tau'}{\Gamma \vdash x{:}\tau}\ \textsc{T-Var}$$

$$\frac{}{\Gamma \vdash c{:}\mathrm{ty}(c)}\ \textsc{T-Const} \qquad \frac{\Gamma \vdash e{:}\tau' \quad \Gamma \vdash \tau' \preceq \tau \quad \Gamma \vdash \tau}{\Gamma \vdash e{:}\tau}\ \textsc{T-Sub}$$

$$\frac{\Gamma, x{:}\tau_x \vdash e{:}\tau \quad \Gamma \vdash \tau_x}{\Gamma \vdash \lambda x.e{:}(x{:}\tau_x \to \tau)}\ \textsc{T-Fun} \qquad \frac{\Gamma \vdash e_1{:}(x{:}\tau_x \to \tau) \quad \Gamma \vdash e_2{:}\tau_x}{\Gamma \vdash e_1\ e_2{:}\tau\,[e_2/x]}\ \textsc{T-App}$$

$$\Gamma \vdash \tau$$

$$\frac{\lfloor\Gamma\rfloor, v{:}b \vdash_B e{:}\text{bool}}{\Gamma \vdash \{v{:}b \mid e\}}\ \textsc{WF-Base} \qquad \frac{\Gamma \vdash \tau_x \qquad \Gamma, x{:}\tau_x \vdash \tau}{\Gamma \vdash x{:}\tau_x \to \tau}\ \textsc{WF-Fun}$$

$$\Gamma \vdash \tau \preceq \tau$$

$$\frac{\Gamma, v : b \vdash e_1 \Rightarrow e_2}{\Gamma \vdash \{v{:}b \mid e_1\} \preceq \{v{:}b \mid e_2\}}\ \preceq\text{-}\textsc{Base} \qquad \frac{\Gamma \vdash \tau_x' \preceq \tau_x \qquad \Gamma, x{:}\tau_x' \vdash \tau \preceq \tau'}{\Gamma \vdash x : \tau_x \to \tau \preceq x : \tau_x' \to \tau'}\ \preceq\text{-}\textsc{Fun}$$

$$\Gamma \vdash e \Rightarrow e$$

$$\frac{\forall \theta. \Gamma \vdash \theta \wedge \forall i. \text{Valid}_i\ (\theta\ e_1) \Rightarrow \text{Valid}_i\ (\theta\ e_2)}{\Gamma \vdash e_1 \Rightarrow e_2}\ \Rightarrow\text{-}\textsc{Base}$$

$$\vdash \Gamma$$

$$\frac{\vdash \Gamma \qquad \Gamma \vdash \tau}{\vdash x{:}\tau, \Gamma} \qquad \frac{}{\vdash \emptyset}$$

$$\Gamma \vdash \theta$$

$$\frac{\forall x \in \text{Dom}(\Gamma). \theta(x) \in [|\theta\ \Gamma(x)|]}{\Gamma \vdash \theta}$$

Constants

Definition 1. *For each constant c,*

1. $\emptyset \vdash c{:}ty(c)$
2. *If $ty(c) = x{:}\tau_x \to \tau$, then for each v such that $\emptyset \vdash v{:}\tau_x$ $[|c|](v)$ is defined and $\vdash [|c|](v){:}\tau\,[v/x]$*
3. *If $ty(c) = \{v{:}b \mid e\}$, then $(\forall i. Fin_i\ (c) \Rightarrow Valid_i\ (e\,[c/v]))$ and $\forall c'\ c' \neq c. \neg((\forall i. Fin_i\ (c) \Rightarrow Valid_i\ (e\,[c'/v])))$*

Moreover, for any base type b $=_b$ is a constant and

- *For any expression e we have*

$$\forall i.\, Valid_i\ (e =_b e)$$

- *For any base type b*

$$ty(=_b) \equiv x{:}b \to y{:}b \to bool$$

Semantic Typing

$$\Gamma \vdash e \in \tau \doteq \forall \theta. \Gamma \vdash \theta \Rightarrow \theta\ e \in [|\theta\ \tau|]$$
$$\Gamma \vdash \tau_1 \subseteq \tau_2 \doteq \forall \theta. \Gamma \vdash \theta \Rightarrow [|\theta\ \tau_1|] \subseteq [|\theta\ \tau_2|]$$

Lemma 1. *.*

1. *If* $\Gamma \vdash \tau_1 \preceq \tau_2$ *then* $\Gamma \vdash \tau_1 \subseteq \tau_2$
2. *If* $\Gamma \vdash e{:}\tau$ *then* $\Gamma \vdash e \in \tau$

Proof. 1. Assume $\Gamma \vdash \tau_1 \preceq \tau_2$ We will prove it by induction on the derivation tree:

- $\preceq$-Base. We have

$$\Gamma \vdash \{v{:}b \mid e_1\} \preceq \{v{:}b \mid e_2\}$$

By inversion we get

$$\Gamma, v{:}b \vdash e_1 \Rightarrow e_2$$

By inversion of $\Rightarrow$-Base we have

$$\forall \theta.\Gamma, v{:}b \vdash \theta \wedge \forall i.\text{Valid}_i\ (\theta\ e_1) \Rightarrow \text{Valid}_i\ (\theta\ e_2)(1)$$

We want to prove

$$\Gamma \vdash \{v{:}b \mid e_1\} \subseteq \{v{:}b \mid e_2\}$$

Equivalently

$$\forall \theta.\Gamma \vdash \theta \Rightarrow [|\theta\ \ \{v{:}b \mid e_1\}\,|] \subseteq [|\theta\ \ \{v{:}b \mid e_2\}\,|]$$

Equivalently

$$\begin{aligned}\forall \theta.\Gamma \vdash \theta \\ &\Rightarrow \{e \mid\vdash e{:}b \wedge (\forall i.\text{Fin}_i\ (e) \Rightarrow \text{Valid}_i\ (\theta\ e_1\,[e/v]))\} \\ &\subseteq \{e \mid\vdash e{:}b \wedge (\forall i.\text{Fin}_i\ (e) \Rightarrow \text{Valid}_i\ (\theta\ e_2\,[e/v]))\}\end{aligned}$$

Since $e \in [|b|]$, we have $\Gamma, v{:}b \vdash \theta, [e/v]$. So, from (1) for $\theta := \theta, [e/v]$ we have

$$\forall i.\text{Valid}_i\ (\theta\ e_1\,[e/v]) \Rightarrow \text{Valid}_i\ (\theta\ e_2\,[e/v])$$

- $\preceq$-Fun Assume

$$\Gamma \vdash x : \tau_x \rightarrow \tau \preceq x : \tau_x' \rightarrow \tau'$$

By inversion we have

$$\Gamma \vdash \tau_x' \preceq \tau_x \qquad \Gamma, x{:}\tau_x' \vdash \tau \preceq \tau'$$

By IH

$$\Gamma \vdash \tau_x' \subseteq \tau_x(1) \qquad \Gamma, x{:}\tau_x' \vdash \tau \subseteq \tau'(2)$$

We want to show that

$$\Gamma \vdash x : \tau_x \rightarrow \tau \subseteq x : \tau_x' \rightarrow \tau'$$

Equivalently

$$\forall \theta.\Gamma \vdash \theta \Rightarrow [|\theta\ x : \tau_x \rightarrow \tau|] \subseteq [|\theta\ x : \tau_x' \rightarrow \tau'|]$$

Equivalently

$$\begin{aligned}
&\forall \theta . \Gamma \vdash \theta \\
&\quad \Rightarrow \{e \mid \vdash e{:}\lfloor \tau_x \rfloor \rightarrow \lfloor \tau \rfloor \wedge \forall e_x \in [|\tau_x|].\ e\ e_x \in [|\tau\,[e_x/x]\,|]\} \\
&\quad \subseteq \{e \mid \vdash e{:}\lfloor \tau'_x \rfloor \rightarrow \lfloor \tau' \rfloor \wedge \forall e_x \in [|\tau'_x|].\ e\ e_x \in [|\tau'\,[e_x/x]\,|]\}
\end{aligned}$$

The above holds, as for any e, e_x if $e_x \in [|\tau'|]$ then by (1) $e_x \in [|\tau|]$. Also, by (2) if $e\ e_x \in [|\tau\,[e_x/x]\,|]$ then $e\ e_x \in [|\tau'\,[e_x/x]\,|]$.

2. Assume $\Gamma \vdash e{:}\tau$. We will prove it by induction on the derivation tree.

- T-Ex Assume

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

where $\tau \equiv \{v{:}b \mid v =_b e\}$. By inversion we have

$$\Gamma \vdash e{:}\,\{v{:}b \mid e'\}$$

We need to show that

$$\forall \theta . \Gamma \vdash \theta \Rightarrow \theta\ e \in [|\theta\ \tau|]$$

Which holds, as by definition of $=_b$ $\forall i.\mathrm{Valid}_i\ ((v =_b \theta\ e)\,[\theta\ e/v])$

- T-Var Assume

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

where $e \equiv x$ By inversion we have

$$(x, \tau) \in \Gamma$$

We need to show that

$$\forall \theta . \Gamma \vdash \theta \Rightarrow \theta\ x \in [|\theta\ \tau|]$$

Which holds by the definition of well-formed substitutions

- T-Var-Base Assume

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

where $e \equiv x$ and $\tau \equiv \{v{:}b \mid v =_b x\}$. By inversion

$$(x, \{v{:}b \mid e_r\}) \in \Gamma$$

We need to show that

$$\forall \theta . \Gamma \vdash \theta \Rightarrow \theta\ x \in [|\theta\ \tau|]$$

Equivalently that

$$\forall e . e \in [|\,\{v{:}b \mid e_r\}\,|] \Rightarrow e \in [|\,\{v{:}b \mid v =_b e\}\,|]$$

which holds, as by the definition of $=_b$

$$\forall i.\mathrm{Valid}_i\ (e =_b e)$$

- T-Const Assume
$$\Gamma \vdash e{:}\tau$$
where $e \equiv c$ and $\tau \equiv \text{ty}(c)$. Then $\Gamma \vdash e \in \tau$ holds by the definition of constants.

- T-Sub Assume
$$\Gamma \vdash e{:}\tau$$
By inversion
$$\Gamma \vdash e{:}\tau' \ (1) \qquad \Gamma \vdash \tau' \preceq \tau \ (2) \qquad \Gamma \vdash \tau \ (3)$$
By IH on (1) we have
$$\Gamma \vdash e \in \tau' \ (4)$$
By 1 on (2) we have
$$\Gamma \vdash \tau' \subseteq \tau \ (5)$$
By (4) and (5) we get
$$\Gamma \vdash e \in \tau$$

- T-Fun Assume
$$\Gamma \vdash e{:}\tau$$
where $e \equiv \lambda x.e'$ and $\tau \equiv x{:}\tau'_x \to \tau'$. By inversion we get
$$\Gamma, x{:}\tau'_x \vdash e'{:}\tau' \ (1) \qquad \Gamma \vdash \tau'_x \ (2)$$
By IH on (1) we have
$$\Gamma, x{:}\tau'_x \vdash e' \in \tau' \ (3)$$
Equivalently
$$\forall \theta.(\Gamma, x{:}\tau'_x) \vdash (\theta\, [e_x/x]) \Rightarrow (\theta\, [e_x/x])\ e' \in [|(\theta\, [e_x/x])\ \tau'|]$$
Or
$$\forall \theta.\Gamma \vdash \theta \Rightarrow \forall e_x.e_x \in [|\tau'_x|] \Rightarrow \theta\ e\ e_x \in [|\theta\ (\tau'\, [e_x/x])|]$$
Moreover, $e \vdash \lfloor \tau'_x \rfloor \to \lfloor \tau \rfloor$:. So,
$$\forall \theta.\Gamma \vdash \theta\ \theta\ e \in [|\theta\ \tau|]$$
Or,
$$\Gamma \vdash e \in \tau$$

- T-App Assume
$$\Gamma \vdash e{:}\tau$$
where $e \equiv e_1\ e_2$ and $\tau \equiv \tau'\, [e_2/x]$. By inversion:
$$\Gamma \vdash e_1{:}(x{:}\tau'_x \to \tau') \ (1) \qquad \Gamma \vdash e_2{:}\tau'_x \ (2)$$
By IH we get
$$\Gamma \vdash e_1 \in (x{:}\tau'_x \to \tau') \ (3) \qquad \Gamma \vdash e_2 \in \tau'_x \ (4)$$

So

$$\forall \theta . \Gamma \vdash \theta \Rightarrow \forall e_x \in [|\theta\ \tau'_x|] \Rightarrow (\theta e_1)\ e_x \in [|\theta\ \tau' [e_x/x]\,|]\ (5)$$

and

$$\forall \theta . \Gamma \vdash \theta \Rightarrow \theta\ e_2 \in [|\theta\ \tau'_x|]\ (6)$$

From (5) and (6), we get

$$\forall \theta . \Gamma \vdash \theta \Rightarrow \theta\ e \in [|\theta\ \tau|]$$

Or

$$\Gamma \vdash e \in \tau$$

□

Lemma 2 (Substitution). *If $\Gamma \vdash e_x{:}\tau_x$ and $\vdash \Gamma, x{:}\tau_x, \Gamma'$, then*

1. *If $\Gamma, x{:}\tau_x, \Gamma' \vdash \tau_1 \preceq \tau_2$ then $\Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,\tau_1 \preceq [e_x/x]\,\tau_2$*
2. *If $\Gamma, x{:}\tau_x, \Gamma' \vdash e{:}\tau$ then $\Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,e{:}\,[e_x/x]\,\tau$*
3. *If $\Gamma, x{:}\tau_x, \Gamma' \vdash \tau$ then $\Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,\tau$*

Proof. If $\Gamma \vdash e_x{:}\tau_x$ and $\Gamma, x{:}\tau_x, \Gamma' \vdash$, then

1. Assume

$$\Gamma, x{:}\tau_x, \Gamma' \vdash \tau_1 \preceq \tau_2$$

We will prove the lemma by induction on the derivation tree.

- $\preceq$-Base Assume

$$\Gamma, x{:}\tau_x, \Gamma' \vdash \tau_1 \preceq \tau_2$$

where $\tau_1 \equiv \{v{:}b \mid e_1\}$ and $\tau_2 \equiv \{v{:}b \mid e_2\}$ By inversion

$$\Gamma, x{:}\tau_x, \Gamma', v : b \vdash e_1 \Rightarrow e_2$$

By inversion

$$\begin{aligned}&\forall \theta, e'_x, \theta', e . \Gamma, x{:}\tau_x, \Gamma', v : b \vdash \theta\,[e'_x/x]\,\theta'\,[e/v]\\ &\quad \Rightarrow \forall i . \text{Valid}_i\ ((\theta\,[e'_x/x]\,\theta'\,[e/v])e_1) \Rightarrow \text{Valid}_i\ ((\theta\,[e'_x/x]\,\theta'\,[e/v])e_2)\end{aligned}$$

But $\Gamma \vdash e_x{:}\tau_x$, so $\Gamma \vdash e_x \in \tau_x$, so

$$\begin{aligned}&\forall \theta, \theta', e . \Gamma, x{:}\tau_x, \Gamma', v : b \vdash \theta\,[e_x/x]\,\theta'\,[e/v]\\ &\quad \Rightarrow \forall i . \text{Valid}_i\ ((\theta\,[e_x/x]\,\theta'\,[e/v])e_1) \Rightarrow \text{Valid}_i\ ((\theta\,[e_x/x]\,\theta'\,[e/v])e_2)\end{aligned}$$

Or $\Gamma \vdash e_x{:}\tau_x$, so $\Gamma \vdash e_x \in \tau_x$, so

$$\begin{aligned}&\forall \theta, \theta', e . \Gamma, [e_x/x]\,\Gamma', v : b \vdash \theta\theta'\,[e/v]\\ &\quad \Rightarrow \forall i . \text{Valid}_i\ ((\theta\theta'\,[e/v])(e_1\,[e_x/x])) \Rightarrow \text{Valid}_i\ ((\theta\theta'\,[e/v])(e_2\,[e_x/x]))\end{aligned}$$

So,

$$\Gamma, [e_x/x]\,\Gamma', v : b \vdash e_1\,[e_x/x] \Rightarrow e_2\,[e_x/x]$$

And

$$\Gamma, [e_x/x]\,\Gamma', v : b \vdash t_1\,[e_x/x] \preceq t_2\,[e_x/x]$$

- $\preceq$-Fun Assume
$$\Gamma, x{:}\tau_x, \Gamma' \vdash \tau_1 \preceq \tau_2$$
where $\tau_1 \equiv y{:}\tau_y \to \tau$ and $\tau_2 \equiv y{:}\tau_y' \to \tau'$ By inversion
$$\Gamma, x{:}\tau_x, \Gamma' \vdash \tau_y' \preceq \tau_y \ (1) \qquad \Gamma, x{:}\tau_x, \Gamma', y{:}\tau_y' \vdash \tau \preceq \tau' \ (2)$$
By IH
$$\Gamma, [e_x/x]\,\Gamma' \vdash \tau_y'\,[e_x/x] \preceq \tau_y\,[e_x/x] \qquad \Gamma, [e_x/x]\,\Gamma', y{:}\tau_y'\,[e_x/x] \vdash \tau\,[e_x/x] \preceq \tau'\,[e_x/x]$$
By rule $\preceq$-Fun
$$\Gamma, [e_x/x]\,\Gamma' \vdash \tau_1\,[e_x/x] \preceq \tau_2\,[e_x/x]$$

$$\frac{\Gamma, v : b \vdash e_1 \Rightarrow e_2}{\Gamma \vdash \{v{:}b \mid e_1\} \preceq \{v{:}b \mid e_2\}}\ \preceq\text{-Base} \qquad \frac{\Gamma \vdash \tau_x' \preceq \tau_x \quad \Gamma, x{:}\tau_x' \vdash \tau \preceq \tau'}{\Gamma \vdash x : \tau_x \to \tau \preceq x : \tau_x' \to \tau'}\ \preceq\text{-Fun}$$

then $\Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,\tau_1 \preceq [e_x/x]\,\tau_2$

2. Assume $\Gamma, x{:}\tau_x, \Gamma' \vdash e{:}\tau$. We will prove the lemma by induction on the derivation tree.

   - T-Ex Assume
   $$\Gamma, x{:}\tau_x, \Gamma' \vdash e{:}\tau$$
   where $\tau \equiv \{v{:}b \mid v =_b e\}$. By inversion we get
   $$\Gamma, x{:}\tau_x, \Gamma' \vdash e{:}\,\{v{:}b \mid e'\}$$
   By IH
   $$\Gamma, [e_x/x]\,\Gamma' \vdash e\,[e_x/x] : \{v{:}b \mid e'\,[e_x/x]\}$$
   By rule T-Ex
   $$\Gamma, [e_x/x]\,\Gamma' \vdash e\,[e_x/x] : \{v{:}b \mid v =_b [e_x/x]\}$$
   Or
   $$\Gamma, [e_x/x]\,\Gamma' \vdash e\,[e_x/x] : \tau\,[e_x/x]$$
   - T-Var Assume
   $$\Gamma, x{:}\tau_x, \Gamma' \vdash e{:}\tau$$
   where $e \equiv y$. By inversion
   $$(y, \tau) \in \Gamma, x{:}\tau_x, \Gamma'$$
   Assume
   $$(y, \tau) \in \Gamma$$
   By rule T-Var
   $$\Gamma, [e_x/x]\,\Gamma' \vdash e{:}\tau$$

Since $\vdash \Gamma$, x cannot appear in τ so $\tau\,[e_x/x] \equiv \tau$. Also, $x \neq y$, so $e\,[e_x/x] \equiv e$. So,

$$\Gamma, [e_x/x]\,\Gamma' \vdash e\,[e_x/x] : \tau\,[e_x/x]$$

Assume

$$(y, \tau) \equiv (x, \tau_x)$$

By lemma's assumption

$$\Gamma \vdash e_x{:}\tau_x$$

so

$$\Gamma, [e_x/x]\,\Gamma' \vdash e_x{:}\tau_x$$

Since $x = y$, $e\,[e_x/x] \equiv e_x$. Also, since $x \notin Dom(\Gamma)$ it cannot appear in τ,so $\tau\,[e_x/x] \equiv \tau \equiv \tau_x$. So,

$$\Gamma, [e_x/x]\,\Gamma' \vdash e\,[e_x/x] : \tau\,[e_x/x]$$

Otherwise, assume

$$(y, \tau) \in \Gamma'$$

So,

$$(y, [e_x/x]\,\tau) \in [e_x/x]\,\Gamma'$$

Also, $e\,[e_x/x] \equiv e \equiv y$. By which and rule T-Var, we get

$$\Gamma, [e_x/x]\,\Gamma' \vdash e\,[e_x/x] : \tau\,[e_x/x]$$

- T-Var-Base Assume

$$\Gamma, x{:}\tau_x, \Gamma' \vdash e{:}\tau$$

where $e \equiv y$ and $\tau \equiv \{v{:}b \mid v =_b y\}$. By inversion

$$(y, \{v{:}b \mid e'\}) \in \Gamma, x{:}\tau_x, \Gamma'$$

Assume

$$(y, \tau) \in \Gamma$$

By rule T-Var-Base

$$\Gamma, [e_x/x]\,\Gamma' \vdash e{:}\tau$$

Since $\vdash \Gamma$, x cannot appear in τ so $\tau\,[e_x/x] \equiv \tau$. Also, $x \neq y$, so $e\,[e_x/x] \equiv e$. So,

$$\Gamma, [e_x/x]\,\Gamma' \vdash e\,[e_x/x] : \tau\,[e_x/x]$$

Assume

$$y \equiv x$$

By lemma's assumption

$$\Gamma \vdash e_x{:}\tau_x$$

and since each expression has at most one unrefined type

$$\Gamma, [e_x/x]\,\Gamma' \vdash e_x{:}\,\{v{:}b \mid e''\}$$

By rule T-Ex we get

$$\Gamma, [e_x/x]\,\Gamma' \vdash e_x \colon \{v{:}b \mid v =_b e_x\}$$

Since $x = y$, $e\,[e_x/x] \equiv e_x$. Also, $\{v{:}b \mid v = y\}\,[e_x/x] = \{v{:}b \mid v =_b e_x\}$
So,

$$\Gamma, [e_x/x]\,\Gamma' \vdash e\,[e_x/x] : \tau\,[e_x/x]$$

Otherwise, assume

$$(y, \tau) \in \Gamma'$$

So,

$$(y, [e_x/x]\,\tau) \in [e_x/x]\,\Gamma'$$

Also, $e\,[e_x/x] \equiv e \equiv y$ and $\tau\,[e_x/x] = \tau$. By which and rule T-Var, we get

$$\Gamma, [e_x/x]\,\Gamma' \vdash e\,[e_x/x] : \tau\,[e_x/x]$$

- T-Const Assume

$$\Gamma, x{:}\tau_x, \Gamma' \vdash e{:}\tau$$

where $e \equiv c$ and $\tau \equiv \text{ty}(c)$. Since $e\,[e_x/x] \equiv e$ and $\tau\,[e_x/x] \equiv \tau$

$$\Gamma, [e_x/x]\,\Gamma' \vdash e\,[e_x/x] : \tau\,[e_x/x]$$

- T-Sub Assume

$$\Gamma, x{:}\tau_x, \Gamma' \vdash e{:}\tau$$

By inversion

$$\Gamma, x{:}\tau_x, \Gamma' \vdash e{:}\tau' \;(1) \qquad \Gamma, x{:}\tau_x, \Gamma' \vdash \tau' \preceq \tau \;(2) \qquad \Gamma, x{:}\tau_x, \Gamma' \vdash \tau \;(3)$$

By IH, 1 and 3

$$\Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,e \colon [e_x/x]\,\tau' \qquad \Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,\tau' \preceq [e_x/x]\,\tau$$

$$\Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,\tau$$

By rule T-Sub

$$\Gamma, [e_x/x]\,\Gamma' \vdash e\,[e_x/x] : \tau\,[e_x/x]$$

- T-Fun Assume

$$\Gamma, x{:}\tau_x, \Gamma' \vdash e{:}\tau$$

where $e \equiv \lambda y.e'$ and $\tau \equiv y{:}\tau'_y \to \tau'$. By inversion

$$\Gamma, x{:}\tau_x, \Gamma', y{:}\tau'_y \vdash e'{:}\tau' \;(1) \qquad \Gamma, x{:}\tau_x, \Gamma' \vdash \tau'_y \;(2)$$

By IH and 3

$$\Gamma, [e_x/x]\,\Gamma', y\colon [e_x/x]\,\tau'_y \vdash [e_x/x]\,e' \colon [e_x/x]\,\tau' \qquad \Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,\tau'_y$$

By rule T-Fun

$$\Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,e \colon [e_x/x]\,\tau$$

- T-App Assume
$$\Gamma, x{:}\tau_x, \Gamma' \vdash e{:}\tau$$
where $e \equiv e_1\ e_2$ and $\tau \equiv \tau'\,[e_2/y]$. By inversion
$$\Gamma, x{:}\tau_x, \Gamma' \vdash e_1{:}y{:}\tau'_y \rightarrow \tau'\ (1) \qquad \Gamma, x{:}\tau_x, \Gamma' \vdash e_2{:}\tau'_y\ (2)$$
By IH
$$\Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,e_1{:}\,[e_x/x]\,y{:}\tau'_y \rightarrow \tau' \qquad \Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,e_2{:}\,[e_x/x]\,\tau'_y$$
By rule T-App
$$\Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,e{:}\,[e_x/x]\,\tau$$

3. Assume $\Gamma, x{:}\tau_x, \Gamma' \vdash \tau$. We will prove it by induction on the derivation.
   - WF-Base Assume
   $$\Gamma, x{:}\tau_x, \Gamma' \vdash \tau$$
   where $\tau \equiv \{v{:}b \mid e\}$. By inversion
   $$\lfloor \Gamma, x{:}\tau_x, \Gamma' \rfloor, v{:}b \vdash_B e{:}\text{bool}$$
   So,
   $$\lfloor \Gamma, [e_x/x]\,\Gamma' \rfloor, v{:}b \vdash_B e\,[e_x/x]\,{:}\text{bool}$$
   By rule WF-Base
   $$\Gamma, [e_x/x]\,\Gamma' \vdash \{v{:}b \mid e\,[e_x/x]\}$$
   Or
   $$\Gamma, [e_x/x]\,\Gamma' \vdash \tau\,[e_x/x]$$
   - WF-Fun Assume
   $$\Gamma, x{:}\tau_x, \Gamma' \vdash \tau$$
   where $\tau \equiv y{:}\tau'_y \rightarrow \tau'$. By inversion, we get
   $$\Gamma, x{:}\tau_x, \Gamma' \vdash \tau_x \qquad \Gamma, x{:}\tau_x, \Gamma', y{:}\tau'_y \vdash \tau'$$
   By IH
   $$\Gamma, [e_x/x]\,\Gamma' \vdash \tau_x\,[e_x/x] \qquad \Gamma, [e_x/x]\,(\Gamma', y{:}\tau'_y) \vdash \tau'\,[e_x/x]$$
   Due to α-renaming, $x \neq y$, so
   $$\Gamma, [e_x/x]\,\Gamma' \vdash \tau'_y\,[e_x/x] \qquad \Gamma, [e_x/x]\,\Gamma', y{:}\,[e_x/x]\,\tau'_y \vdash \tau'\,[e_x/x]$$
   By WF-Fun
   $$\Gamma, [e_x/x]\,\Gamma' \vdash y{:}\tau'_y\,[e_x/x] \rightarrow \tau'\,[e_x/x]$$
   Or
   $$\Gamma, [e_x/x]\,\Gamma' \vdash \tau\,[e_x/x]$$

   then $\Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,\tau$

$\square$

Lemma 3. *If $e \hookrightarrow e'$ then $\Gamma \vdash \tau\,[e'/x] \preceq \tau\,[e/x]$.*

Lemma 4. *If $\Gamma \vdash e{:}\tau$ then $\lfloor\Gamma\rfloor \vdash_B e{:}\lfloor\tau\rfloor$.*

Lemma 5. *If $\vdash \Gamma$ and $\Gamma \vdash e{:}\tau$ then $\Gamma \vdash \tau$.*

Proof. Assume $\vdash \Gamma$ and $\Gamma \vdash e{:}\tau$. We will prove the Lemma by induction on the derivation tree.

- Case T-Ex. Assume

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

  where $\tau \equiv \{v{:}b \mid v = e\}$. By inversion

  $$\Gamma \vdash e{:}\,\{v{:}b \mid e'\}$$

  By Lemma 4

  $$\lfloor\Gamma\rfloor \vdash_B e{:}b$$

  By Definition 1

  $$\lfloor\Gamma\rfloor, v{:}b \vdash_B v = e{:}\mathrm{bool}$$

$$\frac{}{\Gamma \vdash e{:}\,\{v{:}b \mid v = e\}}\ \textsc{T-Ex}$$

$$\frac{(x, \{v{:}b \mid e\}) \in \Gamma}{\Gamma \vdash x{:}\,\{v{:}b \mid v = x\}}\ \textsc{T-Var-Base} \qquad \frac{(x,\tau) \in \Gamma \qquad \tau \equiv x'{:}\tau'_x \to \tau'}{\Gamma \vdash x{:}\tau}\ \textsc{T-Var}$$

$$\frac{}{\Gamma \vdash c{:}\mathrm{ty}(c)}\ \textsc{T-Const} \qquad \frac{\Gamma \vdash e{:}\tau' \qquad \Gamma \vdash \tau' \preceq \tau \qquad \Gamma \vdash \tau}{\Gamma \vdash e{:}\tau}\ \textsc{T-Sub}$$

$$\frac{\Gamma, x{:}\tau_x \vdash e{:}\tau \qquad \Gamma \vdash \tau_x}{\Gamma \vdash \lambda x.e{:}(x{:}\tau_x \to \tau)}\ \textsc{T-Fun} \qquad \frac{\Gamma \vdash e_1{:}(x{:}\tau_x \to \tau) \qquad \Gamma \vdash e_2{:}\tau_x}{\Gamma \vdash e_1\ e_2{:}\tau\,[e_2/x]}\ \textsc{T-App}$$

then $\Gamma \vdash \tau$. $\square$

Lemma 6 (Preservation)**.** *If $\emptyset \vdash e{:}\tau$ and $e \hookrightarrow e'$ then $\emptyset \vdash e'{:}\tau$.*

Proof. Assume $\emptyset \vdash e{:}\tau$ and $e \hookrightarrow e'$. We will prove the lemma by induction on the derivation tree.

- Case T-Ex. Assume

  $$\emptyset \vdash e{:}\tau \ (1)$$

  where $\tau \equiv \{v{:}b \mid v =_b e\}$.

  By inversion

  $$\emptyset \vdash e{:}\,\{v{:}b \mid e_v\}$$

  By IH

  $$\emptyset \vdash e'{:}\,\{v{:}b \mid e_v\}$$

  By rule T-Ex

  $$\emptyset \vdash e'{:}\,\{v{:}b \mid v =_b e'\} \ \ (2)$$

  By Lemma 3

  $$\emptyset \vdash \{v{:}b \mid v =_b e'\} \preceq \{v{:}b \mid v =_b e\} \ \ (3)$$

By Lemma 5 on (1) (since $\vdash \emptyset$)

$$\emptyset \vdash \{v{:}b \mid v =_b e\} \;\; (4)$$

By $(2), (3), (4)$ and rule T-Sub:

$$\emptyset \vdash e' \colon \{v{:}b \mid v =_b e\}$$

- Cases T-Var-Base, T-Var, T-Const and T-Fun trivially hold as there is no e' such that $e \hookrightarrow e'$.
- Case T-Sub. Assume

  $$\emptyset \vdash e{:}\tau$$

  By inversion

  $$\emptyset \vdash e{:}\tau' \;(1) \qquad \emptyset \vdash \tau' \preceq \tau \;(2) \qquad \emptyset \vdash \tau \;(3)$$

  By IH on (1)

  $$\emptyset \vdash e'{:}\tau'$$

  By which, $(2), (3)$ and T-Sub

  $$\emptyset \vdash e'{:}\tau$$

- Case T-App. Assume

  $$\emptyset \vdash e{:}\tau \;(1)$$

  where $e \equiv e_1\ e_2$, and $\tau \equiv \tau'\,[e_2/x]$
  By inversion

  $$\emptyset \vdash e_1{:}(x{:}\tau_x \rightarrow \tau') \;(2) \qquad \emptyset \vdash e_2{:}\tau_x \;(3)$$

  We split cases on the structure of e.

  - $e \equiv c\ v_2$. Then, $e' \equiv [|c|](v_2)$. By Definition 1,

    $$\emptyset \vdash e'{:}\tau$$

  - $e \equiv c\, e_2$ where e_2 is not a value, Then, by (3) and Lemma 7, $e_2 \hookrightarrow e_2'$, and $e' \equiv e_1\ e_2'$ By IH on (2)

    $$\emptyset \vdash e_2'{:}\tau_x$$

    By which, (1) and rule T-App we get

    $$\emptyset \vdash e'{:}\tau'\,[e_2'/x] \;\; (4)$$

    By Lemma 3

    $$\emptyset \vdash \tau'\,[e_2'/x] \preceq \tau'\,[e_2/x] \;\; (5)$$

    By (1) and Lemma 5, since $\vdash \emptyset$

    $$\emptyset \vdash \tau'\,[e_2/x] \;\; (6)$$

    By $(4), (5), (6)$ and rule T-Sub

    $$\emptyset \vdash e'{:}\tau$$

– $e \equiv \lambda x.e_x\ e_2$. Then, $e' \equiv e_x\,[e_2/x]$.
  By inversion on (2)
$$x{:}\tau_x \vdash e_x{:}\tau'$$
  By which, (3) and Lemma 2 (since $\vdash x{:}\tau_x$)
$$\emptyset \vdash e'{:}\tau'$$
– $e \equiv e_1\ e_2$, where e_1 is not a value. Then, by (2) and Lemma 7, $e_1 \hookrightarrow e_1'$ and $e' \equiv e_1'\ e_2$ By IH on (2)
$$\emptyset \vdash e_1'{:}(x{:}\tau_x \rightarrow \tau')$$
  By which, (3) and rule T-App we get
$$\emptyset \vdash e'{:}\tau$$

□

Lemma 7 (Progress)**.** *If $\emptyset \vdash e{:}\tau$ and $e \neq v$ then there exists an e' such that $e \hookrightarrow e'$.*

Proof. Assume $\emptyset \vdash e{:}\tau$. We will prove the Lemma by induction on the derivation tree.

- Case T-Ex. Assume
$$\emptyset \vdash e{:}\,\{v{:}b \mid v =_b e\}$$
  where $\tau \equiv \{v{:}b \mid v =_b e\}$. By inversion
$$\emptyset \vdash e{:}\,\{v{:}b \mid e'\}$$
  By IH either $e \equiv v$ or there exists an e' such that $e \hookrightarrow e'$.
- Cases T-Var-Base, T-Var cannot occur, as $\Gamma = \emptyset$
- Cases T-Const and T-Fun are trivial, as e is a value
- Case T-Sub. Assume
$$\emptyset \vdash e{:}\tau$$
  By inversion
$$\emptyset \vdash e{:}\tau'$$
  By IH either $e \equiv v$ or there exists an e' such that $e \hookrightarrow e'$.
- Case T-App. Assume
$$\emptyset \vdash e{:}\tau\ (1)$$
  where $e \equiv e_1\ e_2$ and $\tau \equiv \tau'\,[e_2/x]$ By inversion
$$\emptyset \vdash e_1{:}(x{:}\tau_x \rightarrow \tau)\ (2) \qquad \emptyset \vdash e_2{:}\tau_x\ (3)$$
  We split cases on the structure of e.
  – $e \equiv c\ v_2$. Then, $e' \equiv [|c|](v_2)$.
  – $e \equiv c\ e_2$ where e_2 is not a value, By IH on (3) $e_2 \hookrightarrow e_2'$ and $e' \equiv e_1\ e_2'$
  – $e \equiv \lambda x.e_x\ e_2$. Then, $e' \equiv e_x\,[e_2/x]$.
  – $e \equiv e_1\ e_2$, where e_1 is not a value. Then, by IH on (2) $e_1 \hookrightarrow e_1'$ and $e' \equiv e_1'\ e_2$.

□

Interpretations

$$\text{Fin }(e) \doteq \exists v.e \hookrightarrow^\star v$$

$$\begin{aligned}[|x|] &= x & [|\lambda x.e|] &= f\\ [|c|] &= c & [|e_1\ e_2|] &= [|e_1|]([|e_2|])\end{aligned}$$

Operational Semantic

$$\begin{array}{ll} e_1\ e_2 \hookrightarrow e_1'\ e_2 & \text{if } e_1 \hookrightarrow e_1' \\ \lambda x.e\ e_x \hookrightarrow e\,[e_x/x] & \\ c\ e \hookrightarrow c\ e' & \text{if } e \hookrightarrow e' \\ c\ v \hookrightarrow [|c|](v) & \end{array}$$

Interpretations

$$\text{Valid}(e) \Leftrightarrow e \hookrightarrow^\star v \Rightarrow e \hookrightarrow^\star \text{true}$$

Claim 1.

$$\left\{ \bigwedge_{(x,\{b:v|e\})\in\Gamma} (\mathit{Fin}\ (x) \Rightarrow [|e\,[x/v]\,|]) \Rightarrow [|e_1|] \Rightarrow [|e_2|] \right\} \Rightarrow \{\Gamma \vdash e_1 \Rightarrow e_2\}$$