Syntax

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

Erasing

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

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

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

Typing

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

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

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

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

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

$$\Gamma \vdash \tau$$

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

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

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

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

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

$$\vdash \Gamma$$

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

$$\Gamma \vdash \theta$$

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

Constants

For each constant c,

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

Moreover, $=$ is a constant and for any expression e we have

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

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

Lemma 2 (Substitution)**.** *If* $\Gamma \vdash e_x{:}\tau_x$ *and* $\Gamma, x{:}\tau_x, \Gamma' \vdash$, *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 $\tau \equiv \{v{:}b \mid v = e\}$. 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
$$\Gamma, [e_x/x]\,\Gamma' \vdash e\,[e_x/x] : \{v{:}b \mid v = [e_x/x]\}$$
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 $x \notin \mathit{Dom}(\Gamma)$ 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 $\tau \equiv \{v{:}b \mid v = y\}$. 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
$$\Gamma, [e_x/x]\,\Gamma' \vdash e_x{:}\,\{v{:}b \mid v = e_x\}$$
Since $x = y$, $e\,[e_x/x] \equiv e_x$. Also, $\{v{:}b \mid v = y\}\,[e_x/x] = \{v{:}b \mid v = e_x\}$ 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 $\tau \equiv \mathrm{ty}(c)$. 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
$$\Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,e{:}\,[e_x/x]\,\tau' \qquad \Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,\tau' \preceq [e_x/x]\,\tau$$
$$\Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,\tau$$
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
$$\Gamma, [e_x/x]\,\Gamma', y{:}\,[e_x/x]\,\tau'_y \vdash [e_x/x]\,e'{:}\,[e_x/x]\,\tau' \qquad \Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,\tau'_y$$
By rule T-Fun
$$\Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,e{:}\,[e_x/x]\,\tau$$

- 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
$$\Gamma, x{:}\tau_x, \Gamma' \vdash e_1{:}y{:}\tau'_y \to \tau' \ (1) \qquad \Gamma, x{:}\tau_x, \Gamma' \vdash e_2{:}\tau'_y \ (2)$$
By IH
$$\Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,e_1{:}\,[e_x/x]\,y{:}\tau'_y \to \tau' \qquad \Gamma, [e_x/x]\,\Gamma' \vdash [e_x/x]\,e_2{:}\,[e_x/x]\,\tau'_y$$
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
   $$\Gamma, x{:}\tau_x, \Gamma', v{:}b \vdash e{:}\mathrm{bool}$$

By 2
$$\Gamma, [e_x/x]\,(\Gamma', v{:}b) \vdash e\,[e_x/x] : \mathrm{bool}\,[e_x/x]$$
Equivalently
$$\Gamma, [e_x/x]\,\Gamma', v{:}b \vdash e\,[e_x/x] : \mathrm{bool}$$
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 $\tau \equiv y{:}\tau'_y \to \tau'$. 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
$$\Gamma, [e_x/x]\,\Gamma' \vdash y{:}\tau'_y\,[e_x/x] \to \tau'\,[e_x/x]$$
Or
$$\Gamma, [e_x/x]\,\Gamma' \vdash \tau\,[e_x/x]$$

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

□

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

Lemma 4 (Preservation)**.** *If $\Gamma \vdash e{:}\tau$ and $e \hookrightarrow e'$ then $\Gamma \vdash e'{:}\tau$.*

Lemma 5 (Progress)**.** *If $\emptyset \vdash e{:}\tau$ and $e \neq v$ then there exists an e' such that $e \hookrightarrow e'$.*

Interpretations

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

$$[|x|] = x \qquad [|\lambda x.e|] = f$$
$$[|c|] = c \qquad [|e_1\ e_2|] = [|e_1|]([|e_2|])$$

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.

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