Syntax

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

Erasing

$$
\lfloor \{v{:}b \mid e\} \rfloor = b
$$

$$
\lfloor x{:}\tau_x \to \tau \rfloor = \lfloor \tau_x \rfloor \to \lfloor \tau \rfloor
$$

Interpretations

$$
[|\ \{v{:}b \mid e_v\}\ |] = \{e \mid \vdash e{:}b \wedge \mathrm{Fin}\ (e) \wedge (\forall i. \mathrm{Fin}_i\ (e) \Rightarrow \mathrm{Valid}_i\ (e_v\ [e/v]))\}
$$

$$
[|x{:}\tau_x \to \tau|] = \{e \mid \vdash e{:}\lfloor \tau_x \rfloor \to \lfloor \tau \rfloor \wedge \forall e_x \in [|\tau_x|].\ e\ e_x \in [|\tau\ [e_x/x]\ |]\}
$$

Typing

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

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

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

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

$$\Gamma \vdash \tau$$

$$
\frac{\Gamma, v{:}b \vdash e{:}\mathrm{bool}}{\Gamma \vdash \{v{:}b \mid e\}}
\qquad
\frac{\Gamma \vdash \tau_x \qquad \Gamma, x{:}\tau_x \vdash \tau}{\Gamma \vdash x{:}\tau_x \to \tau}
$$

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

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

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

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

$$\Gamma \vdash \theta$$

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

Constants

For each constant c,

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

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

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

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

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

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

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

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

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

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

- $\preceq$-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-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 $\tau \equiv \{v{:}b \mid v = x\}$. 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

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

which holds, as by the definition of $=$

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

- 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

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

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

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

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

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

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.

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