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

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

Typing

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

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

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

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

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

$$\Gamma \vdash \tau$$

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

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

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

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

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

$$\vdash \Gamma$$

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

$$\Gamma \vdash \theta$$

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

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

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

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

`proved`

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

`proved`

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

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

Lemma 5 (Preservation)**.** *If* $\emptyset \vdash e{:}\tau$ *and* $e \hookrightarrow e'$ *then* $\emptyset \vdash e'{:}\tau$.

`proved`

Lemma 6 (Progress)**.** *If* $\emptyset \vdash e{:}\tau$ *and* $e \neq v$ *then there exists an* e' *such that* $e \hookrightarrow e'$.

`proved`

Interpretations

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

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

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.

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