

Syntax

Value	$v ::= c \mid \lambda x.e$
Expressions	$e ::= v \mid x \mid e e$
Basic Types	$b ::= \text{int} \mid \text{bool}$
Types	$\tau ::= \{v:b \mid e\} \mid x:\tau \rightarrow \tau$
Environment	$\Gamma ::= \emptyset \mid x:\tau, \Gamma$

Erasing

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

Substitutions

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

Interpretations

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

Typing

$$\begin{array}{c} \Gamma \vdash e:\tau \\[10pt] \frac{\Gamma \vdash e: \{v:b \mid e'\}}{\Gamma \vdash e: \{v:b \mid v = e\}} \text{ T-EX} \\[10pt] \frac{(x, \{v:b \mid e\}) \in \Gamma}{\Gamma \vdash x: \{v:b \mid v = x\}} \text{ T-VAR-BASE} \quad \frac{(x, \tau) \in \Gamma \quad \tau \equiv x':\tau'_x \rightarrow \tau'}{\Gamma \vdash x:\tau} \text{ T-VAR} \\[10pt] \frac{}{\Gamma \vdash c:\text{ty}(c)} \text{ T-CONST} \quad \frac{\Gamma \vdash e:\tau' \quad \Gamma \vdash \tau' \preceq \tau \quad \Gamma \vdash \tau}{\Gamma \vdash e:\tau} \text{ T-SUB} \\[10pt] \frac{\Gamma, x:\tau_x \vdash e:\tau \quad \Gamma \vdash \tau_x}{\Gamma \vdash \lambda x.e:(x:\tau_x \rightarrow \tau)} \text{ T-FUN} \quad \frac{\Gamma \vdash e_1:(x:\tau_x \rightarrow \tau) \quad \Gamma \vdash e_2:\tau_x}{\Gamma \vdash e_1 e_2:\tau [e_2/x]} \text{ T-APP} \\[10pt] \Gamma \vdash \tau \\[10pt] \frac{\Gamma, v:b \vdash e:\text{bool}}{\Gamma \vdash \{v:b \mid e\}} \text{ WF-BASE} \quad \frac{\Gamma \vdash \tau_x \quad \Gamma, x:\tau_x \vdash \tau}{\Gamma \vdash x:\tau_x \rightarrow \tau} \text{ WF-FUN} \\[10pt] \Gamma \vdash \tau \preceq \tau \\[10pt] \frac{\Gamma, v:b \vdash e_1 \Rightarrow e_2}{\Gamma \vdash \{v:b \mid e_1\} \preceq \{v:b \mid e_2\}} \preceq\text{-BASE} \quad \frac{\Gamma \vdash \tau'_x \preceq \tau_x \quad \Gamma, x:\tau'_x \vdash \tau \preceq \tau'}{\Gamma \vdash x:\tau_x \rightarrow \tau \preceq x:\tau'_x \rightarrow \tau'} \preceq\text{-FUN} \end{array}$$

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

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

$$\vdash \Gamma$$

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

$$\Gamma \vdash \theta$$

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

Constants

For each constant c ,

1. $\emptyset \vdash c:\text{ty}(c)$
2. If $\text{ty}(c) = x:\tau_x \rightarrow \tau$, 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 $\Gamma, [e_x/x] \Gamma' \vdash [e_x/x] \tau$

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

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

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

Operational Semantic

$$\begin{array}{ll} e_1 \ e_2 \hookrightarrow e'_1 \ e_2 & \text{if } e_1 \hookrightarrow e'_1 \\ \lambda x. e \ e_x \hookrightarrow e[e_x/x] & \\ c \ e \hookrightarrow c \ e' & \text{if } e \hookrightarrow e' \\ c \ v \hookrightarrow \llbracket c \rrbracket(v) & \end{array}$$

Interpretations

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

Claim 1.

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