Syntax

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

- $\texttt{Bool} \in T$
- $\texttt{True}, \texttt{False} \in D$
- $\text{ty}(\texttt{True}) = \{v{:}\texttt{Bool} \mid v \Leftrightarrow \text{true}\}$, and $\text{ty}(\texttt{False}) = \{v{:}\texttt{Bool} \mid v \Leftrightarrow \text{false}\}$
- $$\text{if } e \text{ then } e_1 \text{ else } e_2 \doteq \text{case } e\; x \text{ of } \{\texttt{True} \Rightarrow e_1; \texttt{False} \Rightarrow e_2\}$$

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

Definition 1. *Let $Fin_i\ (\star)$ and $Valid_i\ (\star)$ be predicates on expressions such that*

1. *For $\emptyset \vdash e{:}\{v{:}b \mid e_r\}$ $(\forall i.Fin_i\ (e) \Rightarrow Valid_i\ (e_r))$ is a "meaningful" soundness predicate.*
2. *For any x, e, e_r, θ, if $e \hookrightarrow e'$ then $\forall i.Valid_i\ (\theta\ e_r\,[e'/x]) \Rightarrow Valid_i\ (\theta\ e_r\,[e/x])$ and $\forall i.Valid_i\ (\theta\ e_r\,[e/x]) \Rightarrow Valid_i\ (\theta\ e_r\,[e'/x])$.*

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

Typing

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

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

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

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

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

$$\frac{\begin{array}{c}\Gamma \vdash e{:}\,\{v{:}T \mid e_T\} \\ \forall i. \left\{\begin{array}{l} \mathrm{ty}(D_i) = \overline{x{:}\tau_D} \to \{v{:}T \mid e'_T\} \qquad \theta = [y_i/x] \\ \Gamma, \overline{y_i{:}\theta\ \tau_D}, x{:}\,\{v{:}T \mid e_T \wedge \theta e'_T\} \vdash e_i{:}\tau \end{array}\right.\end{array}}{\Gamma \vdash \mathsf{case}\ e\ x\ \mathsf{of}\ \overline{D_i\ \overline{y_i} \to e_i}{:}\tau}\ \textsc{T-Case}$$

$$\frac{}{\Gamma \vdash D{:}\mathrm{ty}(D)}\ \textsc{T-Data}$$

$$\Gamma \vdash \tau$$

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

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

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

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

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

$$\vdash \Gamma$$

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

$$\Gamma \vdash \theta$$

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

Constants

Definition 2. *For each constant c,*

1. $\emptyset \vdash c{:}ty(c)$ *and* $\vdash ty(c)$
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* $\Gamma \vdash e \in \tau$

`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* $\Gamma \vdash e{:}\tau$ *then* $\lfloor\Gamma\rfloor \vdash_B e{:}\lfloor\tau\rfloor$.

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

`proved`

Operational Semantic

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

$$\begin{array}{rcll} \text{case } e\ x \text{ of } \overline{D_i\ \overline{y} \to e_i} & \hookrightarrow & \text{case } e'\ x \text{ of } \overline{D_i\ \overline{y} \to e_i} & \text{if } e \hookrightarrow e' \\ \text{case } D_j\ \overline{e'}\ x \text{ of } \overline{D_i\ \overline{y} \to e_i} & \hookrightarrow & e_j\,[e_l'/y_l] & \end{array}$$

Soundness

Lemma 5. *If* $e \hookrightarrow e'$ *then* $\Gamma \vdash \tau\,[e'/x] \preceq \tau\,[e/x]$.

```
proved
```

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

```
proved
```

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

```
proved
```

Interpretations

$$\begin{aligned} \text{Fin } (e) &\doteq \exists v.e \hookrightarrow^{\star} v \\ \text{Valid}(e) &\Leftrightarrow e \hookrightarrow^{\star} v \Rightarrow e \hookrightarrow^{\star} \text{true} \end{aligned}$$

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

Claim 1.

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