Syntax

$$
\begin{array}{rrcl}
\textbf{\textit{Value}} & v & ::= & c \mid \lambda x.e \mid D_i^T\ \overline{e} \\
\textbf{\textit{Constants}} & w & ::= & c \mid D_i^T \\
\textbf{\textit{Expressions}} & e & ::= & w \mid \lambda x.e \mid x \mid e\ e \\
 & & & \text{case}_T\ e\ x \text{ of } \overline{D_i^T\ \overline{x} \to e} \\
\textbf{\textit{Basic Types}} & b' & ::= & \text{int} \mid \text{bool} \\
\textbf{\textit{Basic Types}} & b & ::= & b' \mid T \\
\textbf{\textit{Types}} & \tau & ::= & \{v{:}b \mid e\} \mid x{:}\tau \to \tau \\
\textbf{\textit{Environment}} & \Gamma & ::= & \emptyset \mid x{:}\tau, \Gamma
\end{array}
$$

- $\texttt{Bool} \in T$, $i_{\texttt{Bool}} = 2$
- $\texttt{True} \equiv D_1^{\texttt{Bool}}, \texttt{False} \equiv D_2^{\texttt{Bool}}$
- $\text{ty}(\texttt{True}) = \{v{:}\texttt{Bool} \mid v \Leftrightarrow \text{true}\}$, and $\text{ty}(\texttt{False}) = \{v{:}\texttt{Bool} \mid v \Leftrightarrow \text{false}\}$
- $$\text{if } e \text{ then } e_1 \text{ else } e_2 \doteq \text{case}_{\texttt{Bool}}\ e\ x \text{ of } \{\texttt{True} \Rightarrow e_1; \texttt{False} \Rightarrow e_2\}$$

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 $\forall i. Valid_i\ (\theta\ e_r\,[e/x]) \Rightarrow Valid_i\ (\theta\ e_r\,[e'/x])$.*

3. For any e_1, e_2,

$$\mathit{Valid}_i\ (e_1) \land \mathit{Valid}_i\ (e_2) \Rightarrow \mathit{Valid}_i\ (e_1 \land e_2)$$

$$\begin{array}{lll}
[\![\, \{v{:}b' \mid e_v\} \,]\!] & = \{e \mid & \vdash e{:}b \land (\forall i.\mathrm{Fin}_i\ (e) \Rightarrow \mathrm{Valid}_i\ (e_v\,[e/v]))\} \\
[\![\, \{v{:}T \mid e_T\} \,]\!] & = \{e \mid & \vdash e{:}b \land (\forall i.\mathrm{Fin}_i\ (e) \Rightarrow \mathrm{Valid}_i\ (e_T\,[e/v]))\} \\
 & \cap\ \{e \mid & \forall (1 \le i \le i_T) \{D_i^T \in [\![\overline{x{:}\tau_{D_i^T}} \to \{v{:}T \mid e'_T\}\,]\!] \land \theta = [e_{y_i}/x] \land \forall e_{y_i} \in [\![\theta\ t_{D_i^T}]\!] \\
 & & e \in [\![\, \{v{:}T \mid \theta e'_T\} \,]\!] \Rightarrow e_i\,[e/x]\,[e_{y_i}/y_i] \in [\![\tau]\!]\} \\
 & & \Rightarrow \mathrm{case}_T\ e\ x\ \mathrm{of}\ \overline{D_i^T\ \overline{y_i} \to e_i} \in [\![\tau]\!]\} \\
[\![x{:}\tau_x \to \tau]\!] & = \{e \mid & \vdash e{:}\lfloor \tau_x \rfloor \to \lfloor \tau \rfloor \land \forall e_x \in [\![\tau_x]\!].\ e\ e_x \in [\![\tau\,[e_x/x]\,]\!]\}
\end{array}$$

Typing

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

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

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

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

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

$$\frac{\begin{array}{cc} \Gamma \vdash e{:}\,\{v{:}T \mid e_T\} & \Gamma \vdash \tau \\ \multicolumn{2}{c}{\forall (1 \le i \le i_T). \left\{ \begin{array}{l} \mathrm{ty}(D_i^T) = \overline{x{:}\tau_{D_i^T}} \to \{v{:}T \mid e'_T\} \qquad \theta = [y_i/x] \\ \Gamma, \overline{y_i{:}\theta\ \tau_{D_i^T}}, x{:}\,\{v{:}T \mid e_T \land \theta e'_T\} \vdash e_i{:}\tau \end{array} \right.} \end{array}}{\Gamma \vdash \mathrm{case}_T\ e\ x\ \mathrm{of}\ \overline{D_i^T\ \overline{y}_i \to e_i}{:}\tau}\ \textsc{T-Case}$$

$$\Gamma \vdash \tau$$

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

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

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

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

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

$$\vdash \Gamma$$

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

$$\Gamma \vdash \theta$$

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

Constants and Data Constructors

Definition 2. *For each constant or data constructor w*

1. $\emptyset \vdash w{:}ty(w)$ *and* $\vdash ty(w)$
2. *If* $ty(w) = x{:}\tau_x \to \tau$*, then for each* v *such that* $\emptyset \vdash v{:}\tau_x$ $[|w|](v)$ *is defined and* $\vdash [|w|](v){:}\tau\,[v/x]$

   Also, for all $e \in [|\tau_x|]$*, we have* $w\ e \in [|\tau\,[e/x]\,|]$
3. *If* $ty(w) = \{v{:}b \mid e\}$*, then* $(\forall i.Fin_i\ (w) \Rightarrow Valid_i\ (e\,[w/v]))$ *and* $\forall w'\ w' \neq w.\neg((\forall i.Fin_i\ (w) \Rightarrow Valid_i\ (e\,[w'/v])))$

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

$$ty(=_b) \equiv x{:}b \to y{:}b \to bool$$

For each T *there are exactly* i_T *constants with result type* $\{v{:}T \mid e_T\}$*, namely* D_i^T*,* $\forall 1 \leq i \leq i_T$*.*

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* $\Gamma \vdash e_x \in \tau_x$ *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

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

$$\begin{array}{rcll} \text{case}_T\ e\ x \text{ of } \overline{D_i^T\ \overline{y} \to e_i} & \hookrightarrow & \text{case}_T\ e'\ x \text{ of } \overline{D_i^T\ \overline{y} \to e_i} & \text{if } e \hookrightarrow e' \\ \text{case}_T\ D_j^T\ \overline{e'}\ x \text{ of } \overline{D_i^T\ \overline{y} \to e_i} & \hookrightarrow & e_j\,[e_l'/y_l]\left[D_j^T\ \overline{e'}/x\right] & \end{array}$$

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

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

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

Claim 1.

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