1 Language

1.1 Syntax

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

- $\texttt{Bool} \in T$, $i_{\texttt{Bool}} = 2$
- $\texttt{True} \equiv D_1^{\texttt{Bool}}, \texttt{False} \equiv D_2^{\texttt{Bool}}$
- $$\text{if } e \text{ then } e_1 \text{ else } e_2 \doteq \text{case}_{\texttt{Bool}}\ e\ x \text{ of } \{\texttt{True} \Rightarrow e_1; \texttt{False} \Rightarrow e_2\}$$

1.2 Operational Semantics

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

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

2 Undecidable System

2.1 Erasing

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

$$
\begin{aligned}
\lfloor \emptyset \rfloor &= \emptyset \\
\lfloor x{:}\tau, \Gamma \rfloor &= x{:}\lfloor \tau \rfloor, \lfloor \Gamma \rfloor
\end{aligned}
$$

2.2 Substitutions

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

2.3 Interpretations

Definition 1. *Let Valid$_i$ ($\star$) be predicates on expressions such that*

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

2. *For any e_1, e_2,*

$$Valid_i\ (e_1) \wedge Valid_i\ (e_2) \Rightarrow Valid_i\ (e_1 \wedge e_2)$$

3. $$Valid_i\ (true)$$

$$
\begin{array}{lll}
[|\,\{v{:}b' \mid e_v\}\,|] & = \{e \mid & \vdash e : b \wedge (\forall i.\exists v.e \hookrightarrow^\star v \Rightarrow \mathrm{Valid}_i\ (e_v\,[e/v]))\} \\
[|\,\{v{:}T \mid e_T\}\,|] & = \{e \mid & \vdash e : T \wedge (\forall i.\exists v.e \hookrightarrow^\star v \Rightarrow \mathrm{Valid}_i\ (e_T\,[e/v])) \\
 & & \wedge\ e \hookrightarrow^\star v_e \Rightarrow \{v_e = D_i^T\ \overline{e_{y_i}} \wedge D_i^T \in [|\overline{x{:}\tau_{D_i^T}} \to \{v{:}T \mid e'_T\}\,|] \\
 & & \wedge\ \theta = [e_{y_i}/x] \wedge e_{y_i} \in [|\theta\ t_{D_i^T}|] \wedge e \in [|\,\{v{:}T \mid \theta e'_T\}\,|]\}\} \\
[|x{:}\tau_x \to \tau|] & = \{e \mid & \vdash e : \lfloor \tau_x \rfloor \to \lfloor \tau \rfloor \wedge \forall e_x \in [|\tau_x|].\ e\ e_x \in [|\tau\,[e_x/x]\,|]\}
\end{array}
$$

2.4 Typing

$$\Gamma \vdash e : \tau$$

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

$$\frac{(x, \{v{:}b \mid e\}) \in \Gamma}{\Gamma \vdash x : \{v{:}b \mid v =_b x\}}\ \textsc{T-Var-Base} \qquad \frac{(x, \tau) \in \Gamma \qquad \tau \neq (x, \{v{:}b \mid e\})}{\Gamma \vdash x : \tau}\ \textsc{T-Var}$$

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

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

$$\frac{\Gamma \vdash e_x : \tau_x \qquad \Gamma, x{:}\tau_x \vdash e_2 : \tau \qquad \Gamma \vdash \tau}{\Gamma \vdash \mathrm{let}\ x = e_x\ \mathrm{in}\ e : \tau}\ \textsc{T-Let}$$

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

$$\Gamma \vdash \tau$$

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

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

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

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

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

$$\vdash \Gamma$$

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

$$\Gamma \vdash \theta$$

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

2.5 Constants and Data Constructors

Definition 2. `crash`*is an untyped constant.*

For each constant or data constructor $w \neq$ `crash`

1. $\emptyset \vdash w : \mathit{ty}(w)$ *and* $\vdash \mathit{ty}(w)$
2. *If* $\mathit{ty}(w) = x{:}\tau_x \to \tau$*, then for each* v $[|w|](v)$ *is defined and if* $\emptyset \vdash v : \tau_x$ *then* $\vdash [|w|](v) : \tau\,[v/x]$*, otherwise* $[|w|](v) =$ `crash`
3. *If* $\mathit{ty}(w) = \{v{:}b \mid e\}$*, then* $\mathit{Valid}_i\ (e\,[w/v])$ *and* $\forall w'\ w' \neq w.\neg(\mathit{Valid}_i\ (e\,[w'/v]))$

Moreover, for any base type b*,* $=_b$ *is a constant and*

- *For any expression* e *we have*

$$\forall i.\,\mathit{Valid}_i\ (e =_b e)$$

- *For any base type* b

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

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

2.6 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. *If* e *diverges and* $\emptyset \vdash_B e : \lfloor \tau \rfloor$ *then* $\emptyset \vdash e \in \tau$

`TODO`

Lemma 2. *If* $e \hookrightarrow^\star e'$ *and* $e' \in [|\tau|]$ *then* $e \in [|\tau|]$

`TODO`

Lemma 3. *.*

1. *If* $\Gamma \vdash \tau_1 \preceq \tau_2$ *then* $\Gamma \vdash \tau_1 \subseteq \tau_2$

2. *If* $\Gamma \vdash e : \tau$ *then* $\Gamma \vdash e \in \tau$

`TODO`

Lemma 4 (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 5. *If* $\Gamma \vdash e : \tau$ *then* $\lfloor \Gamma \rfloor \vdash_B e : \lfloor \tau \rfloor$.

Lemma 6. *If* $\vdash \Gamma$ *and* $\Gamma \vdash e : \tau$ *then* $\Gamma \vdash \tau$.

`proved`

2.7 Soundness

Lemma 7. *If* $e \hookrightarrow e'$ *then* $\Gamma \vdash \tau\,[e'/x] \preceq \tau\,[e/x]$.

`proved`

Lemma 8 (Preservation)**.** *If* $\emptyset \vdash e : \tau$ *and* $e \hookrightarrow e'$ *then* $\emptyset \vdash e' : \tau$.

`proved`

Lemma 9 (Progress)**.** *If* $\emptyset \vdash e : \tau$ *and* $e \neq v$ *then there exists an* e' *such that* $e \hookrightarrow e'$.

`proved`

3 Decidable System

Typing

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

$$\frac{(x, \{v{:}b \mid e\}) \in \Gamma}{\Gamma \vdash x : \{v{:}b \mid v =_b x\}}\ \textsc{T-Var-Base} \qquad \frac{(x, \tau) \in \Gamma \quad \tau \neq (x, \{v{:}b \mid e\})}{\Gamma \vdash x : \tau}\ \textsc{T-Var}$$

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

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

$$\frac{\Gamma \vdash e_x : \tau_x \quad \Gamma, x{:}\tau_x \vdash e_2 : \tau \quad \Gamma \vdash \tau}{\Gamma \vdash \text{let } x = e_x \text{ in } e : \tau}\ \textsc{T-Let}$$

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

$$\boxed{\Gamma \vdash \tau}$$

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

$$\boxed{\Gamma \vdash \tau \preceq \tau}$$

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

$$\boxed{\Gamma \vdash e \Rightarrow e}$$

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

$$\boxed{\vdash \Gamma}$$

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

$$\boxed{\Gamma \vdash \theta}$$

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

3.1 Interpretations

$$\mathrm{Valid}(e) \Leftrightarrow e \hookrightarrow^\star v \Rightarrow e \hookrightarrow^\star \mathrm{true}$$

3.2 Constants

Now, we should prove that each constant we define respects the definition of constants.

Note that if $\mathrm{Valid}(e) \Leftrightarrow \mathrm{true}$ then each $\emptyset \vdash v : \{v{:}b \mid \mathrm{false}\}$ so `error :: {v: b | false } -> T` should be defined for each value.

With the above definition for Valid_i $(\star)$ we can show that there is no value v such that $\Gamma \vdash v : \{v{:}b \mid \mathrm{false}\}$

- ```
  prop :: Bool -> bool
  prop(True) = true
  prop(False) = false
  ```

- ```
  <=> :: bool -> bool -> bool
  true  <=> true  = true
  false <=> false = true
  true  <=> false = false
  false <=> true  = false
  ```

- $\texttt{Bool} \in T$, $i_{\texttt{Bool}} = 2$
- $\texttt{True} \equiv D_1^{\texttt{Bool}}, \texttt{False} \equiv D_2^{\texttt{Bool}}$
- $\text{ty}(\texttt{True}) = \{v{:}\texttt{Bool} \mid \texttt{prop}\ v \Leftrightarrow \text{true}\}$, and $\text{ty}(\texttt{False}) = \{v{:}\texttt{Bool} \mid \texttt{prop}\ v \Leftrightarrow \text{false}\}$
- ```
  error :: {v:b | false} -> T
  error _ = crash
  ```
  Valid as $e \hookrightarrow^\star v \Rightarrow e \notin [|\ \{v{:}b \mid \text{false}\}\ |]$
-

$$\texttt{fix}_\tau : (\tau \to \tau) \to \tau$$
$$\texttt{fix}_\tau f = f\ (\texttt{fix}_\tau\ f)$$

Let Ω_τ be an expression defined by induction on τ:

$$\Omega_b = \texttt{fix}_b\ \lambda x.x \qquad\qquad \Omega_{x:\tau_x \to \tau} = \lambda x.\Omega_\tau$$

By using Ω_τ we define $\texttt{fix}^i_\tau$, for $i \in \mathbb{N}$ as

$$\texttt{fix}^0_\tau = \Omega_{(\tau\to\tau)\to\tau} \qquad\qquad \texttt{fix}^{i+1}_\tau = \lambda x.x\ \texttt{fix}^i_\tau$$

Lemma 10 (Fix Lemma)**.** *Let $e_0, \dots, e_m$ be expressions with $m \geq 0$, then*

1. *Let $e \equiv \Omega_\tau\ e_0\ \dots\ e_m$. If $\emptyset \vdash_B e : \tau'$ then e diverges.*
2. $\texttt{fix}_\tau\ e_0\ \dots\ e_m \hookrightarrow^\star v \iff \texttt{fix}^k_\tau\ e_0\ \dots\ e_m \hookrightarrow^\star v$*, for some $k \in \mathbb{N}$*

Proof. **??** By induction on m. For $m = 0$, then $\tau \equiv b$ and $\Omega_b = \texttt{fix}_b\ \lambda x.x$. Assume a derivation $\Omega_b\ e_0 \hookrightarrow^\star v$ with i evaluation rules. Since $\Omega_b\ e_0 \equiv \texttt{fix}_b\ \lambda x.x \hookrightarrow \lambda x.x\ (\texttt{fix}_b\ \lambda x.x) \hookrightarrow \texttt{fix}_b\ \lambda x.x$ the remaining derivation should still evaluate to v in $i-2$ evaluation rules; which is a contradiction.

For $m+1$ we have $e \equiv \Omega_{\tau_x\to\tau}\ e_0\ e_1\ \dots\ e_m\ e_{m+1}$, so $\Omega_{\tau_x\to\tau}\ e_0\ e_1\ \dots\ e_m\ e_{m+1} \equiv (\lambda x.\Omega_\tau)\ e_0\ e_1\ \dots\ e_m\ e_{m+1} \hookrightarrow \Omega_\tau\ e_1\ \dots\ e_m\ e_{m+1}$ which diverges by inductive hypothesis.

?? We will prove both directions by induction on the length of the derivation of the hypothesis: Assume $e \equiv \texttt{fix}_\tau\ e_0\ \dots\ e_m \hookrightarrow^i v$. The lemma trivially holds for $i = 0$, as e is not a value. So,

$$\texttt{fix}_\tau\ e_0\ e_1\ \dots\ e_m \hookrightarrow e_0\ (\texttt{fix}_\tau\ e_0)\ e_1\ \dots\ e_m$$

By inductive hypothesis, for some k, $e_0\ (\texttt{fix}^k_\tau\ e_0)\ e_1\ \dots\ e_m \hookrightarrow^\star v$ So, the lemma holds for $k+1$.

Assume $e \equiv \texttt{fix}^k_\tau\ e_0\ \dots\ e_m \hookrightarrow^i v$. The lemma trivially holds for $i = 0$, as e is not a value. So,

$$\texttt{fix}^k_\tau\ e_0\ e_1\ \dots\ e_m \hookrightarrow e_0\ (\texttt{fix}^{k-1}_\tau\ e_0)\ e_1\ \dots\ e_m$$

By inductive hypothesis, $e_0\ (\texttt{fix}_\tau\ e_0)\ e_1\ \dots\ e_m \hookrightarrow^\star v$ So, the lemma holds. □

By induction we can prove that $\forall i.\texttt{fix}^i_T \in [|(T \to T) \to T|]$
  ```

3.3 Logic

$$\mathcal{C}_0 = \{\text{true}, \text{false}, 0, 1, \dots\}$$
$$\mathcal{C}_i = \{f, +, -, =, >, \neg, \wedge, \dots\}$$

$$\Gamma \vdash_{\text{pure}} e$$

$$\frac{(x, b) \in \Gamma}{\Gamma \vdash_{\text{pure}} x} \qquad \frac{c_n \in \mathcal{C}_n \quad \forall i. 1 \leq i \leq n \Rightarrow \Gamma \vdash_{\text{pure}} e_i}{\Gamma \vdash_{\text{pure}} c_n\ e_1\ \dots e_n}$$