Formalise Java Typestate

No Institute Given

1 Syntax

Syntax:

$$
\begin{array}{lrcl}
 & D & ::= & \texttt{class}\ C\{S; \tilde{F}; \tilde{M}\} \mid \texttt{enum}\ E\{\boldsymbol{l}\} \\
\text{(Types)} & T & ::= & \texttt{Null} \mid C[S] \\
\text{(Fields)} & F & ::= & T\ f \\
\text{(Local)} & V & ::= & T\ x \\
\text{(Methods)} & M & ::= & T\ m(Tx)\{e\} \\
\text{(Values)} & v & ::= & \texttt{null} \mid l \\
\text{(Paths)} & r & ::= & \texttt{this} \mid \texttt{this}.f \mid x \\
\text{(Expressions)} & e & ::= & V \mid v \mid r \mid r.m(e) \mid e; e \mid r = e \\
 & & \mid & \texttt{new}\ C() \mid \texttt{return}\ e \mid \texttt{switch}(e)\{l : e_l\}_{l \in E} \\
 & & \mid & \texttt{break}\ \lambda \mid \texttt{continue}\ \lambda \mid \lambda : \texttt{while}(e_1)\{e_2\} \\
 & & \mid & \texttt{if}\ e\ \texttt{then}\ e\ \texttt{else}\ e
\end{array}
$$

Runtime Syntax:

$$
\begin{array}{lrcl}
 & T & ::= & C[\{T_i\ f_i\}_{i \in I}] \\
 & v & ::= & \ldots \mid o \\
 & r & ::= & o \mid x \mid r.f \\
 & S & ::= & \mathsf{init}; S^i \mid S^i \\
 & S^i & ::= & \texttt{end} \mid T_1\ m(T_2\ x); S \mid \{S_i\}_{i \in I} \mid \langle S_i \rangle_{i \in I} \\
\text{(Context)} & \mathcal{E} & ::= & - \mid \mathcal{E}; e \mid r.m(\mathcal{E}) \mid r = \mathcal{E} \mid \texttt{return}\ \mathcal{E} \\
 & & \mid & \texttt{switch}(\mathcal{E})\{l : e\}_{l \in E} \mid \texttt{if}\ \mathcal{E}\ \texttt{then}\ e\ \texttt{else}\ e
\end{array}
$$

Operational Semantics:

$$
\begin{array}{lcl}
h & ::= & h \cdot o = C[\tilde{f} = \texttt{null}] \mid \epsilon \\
\sigma & ::= & \sigma \cdot \phi \mid \phi \\
\phi & ::= & \{\widetilde{x = r}\}
\end{array}
$$

$$\frac{o \text{ fresh} \quad C.\mathsf{fields} = \tilde{f}}{(h;\sigma;\texttt{new } C()) \longrightarrow (h \cdot o = C[\tilde{f} = \tilde{\texttt{null}}];\sigma;o)}$$

$$\frac{}{(h;\sigma \cdot \phi;T\ x) \longrightarrow (h;\sigma \cdot \phi \cup \{x = \texttt{null}\};\texttt{null})}$$

$$\frac{\phi(x) = r \qquad h(r) = v}{(h;\sigma \cdot \phi;x) \longrightarrow (h\{r = \texttt{null}\};\sigma \cdot \phi;v)}$$

$$\frac{r \neq x \qquad h(r) = v}{(h;\sigma;r) \longrightarrow (h\{r = \texttt{null}\};\sigma;v)}$$

$$\frac{r \neq x}{(h;\sigma;r = v) \longrightarrow (h\{r = v\};\sigma;\texttt{null})}$$

$$\frac{\phi(x) = r}{(h;\sigma \cdot \phi;x = v) \longrightarrow (h\{r = v\};\sigma \cdot \phi;\texttt{null})}$$

$$\frac{T_1\ m(T_2 x)\{e\} \in h(r).\texttt{class}}{(h;\sigma;r.m(v)) \longrightarrow (h;\sigma \cdot \emptyset;e\{r/\texttt{this}\}\{v/x\})}$$

$$\frac{}{(h;\sigma;v;e) \longrightarrow (h;\sigma;e)}$$

$$\frac{(h;\sigma;e) \longrightarrow (h';\sigma';e')}{(h;\sigma;\mathcal{E}[e]) \longrightarrow (h';\sigma';\mathcal{E}[e'])}$$

$$\frac{}{(h;\sigma \cdot \phi;\texttt{return } v) \longrightarrow (h;\sigma;v)}$$

$$\frac{l_k \in E}{(h;\sigma;\texttt{switch}(l_k)\{l : e_l\}_{l \in E}) \longrightarrow (h;\sigma;e_{l_k})}$$

$$\frac{}{(h;\sigma;\texttt{if tt then } e_1 \texttt{ else } e_2) \longrightarrow (h;\sigma;e_1)}$$

$$\frac{}{(h;\sigma;\texttt{if ff then } e_1 \texttt{ else } e_2) \longrightarrow (h;\sigma;e_2)}$$

$$\frac{}{(h;\sigma;\lambda : \texttt{while}(e_1)\{e_2\}) \longrightarrow (h;\sigma;\texttt{if } e_1 \texttt{ then } e_2;\lambda : \texttt{while}(e_1)\{e_2\} \texttt{ else ff})}$$

2 Typing

$$\begin{array}{rcl} \Gamma & ::= & r : C[\{S_i\}_{i \in I}] \cdot \Gamma \ \mid \ \emptyset \\ \Delta & ::= & r : T \cdot \Delta \ ::= \ \emptyset \end{array}$$

$$\begin{aligned}\Delta_1 \uplus \Delta_2 &= \{r : C[S_1, S_2] \mid r : C[S_1] \in \Delta_1, r : C[S_2] \in \Delta_2\} \\ &\quad \cup \Delta_1 \backslash \Delta_2 \cup \Delta_2 \backslash \Delta_1 \\ \Gamma_1 \uplus \Gamma_2 &= \{r : C[\{S\}_{i \in I} \cup \{S\}_{j \in J}] \mid r : C[\{S\}_{i \in I}] \in \Delta_1, r : C[\{S\}_{j \in J}] \in \Delta_2\} \\ &\quad \cup \Gamma_1 \backslash \Gamma_2 \cup \Gamma_2 \backslash \Gamma_1\end{aligned}$$

$$\frac{\Gamma(x) = C[\{S_i\}]_{i \in I}}{\Gamma; \Delta \vdash C[S]\ x : C[\texttt{end}] \dashv \Gamma; \Delta \cdot x : C[\texttt{end}]}\ [\text{Scope}]$$

$$\frac{}{\Gamma; \Delta \vdash \texttt{null} : \texttt{Null} \dashv \Gamma; \Delta}\ [\text{Null}]$$

$$\frac{l \in E}{\Gamma; \Delta \vdash l : E \dashv \Gamma; \Delta}\ [\text{Enum}]$$

$$\frac{}{\Gamma; \Delta \cdot r : \texttt{end} \vdash r : T \dashv \Gamma; \Delta \cdot r : T}\ [\text{Path}]$$

$$\frac{\Gamma; \Delta \cdot r : T \vdash e : T' \dashv \Gamma''; \Delta'' \cdot r : C[m(T_x\ x); S] \qquad T_m\ m(T_x\ x)\{e'\} \in C.\texttt{class} \qquad \text{stack frame}}{\Gamma; \Delta \cdot r : T \vdash r.m(e) : T \dashv \Gamma'; \Delta' \cdot r : C[S]}\ [\text{Call}]$$

$$\frac{\Gamma; \Delta \vdash e_1 \dashv \Gamma''; \Delta'' \qquad \Gamma''; \Delta'' \vdash e_2 \dashv \Gamma'; \Delta'}{\Gamma; \Delta \vdash e_1; e_2 : T \dashv \Gamma'; \Delta'}\ [\text{Seq}]$$

$$\frac{\Gamma \cdot r : C[\{S\}_{i \in I}]; \Delta \cdot r : C[S] \vdash e : C[S] \dashv \Gamma' \cdot r : C[\{S\}_{i \in I}]; \Delta' \cdot r : C[S']}{\Gamma \cdot r : C[\{S\}_{i \in I} \cup \{S\}]; \Delta \cdot r : C[\texttt{end}] \vdash r = e : C[\texttt{end}] \dashv \Gamma' \cdot r : C[\{S\}_{i \in I}]; \Delta' \cdot r : C[S']}\ [\text{Assign}]$$

$$\frac{o??? \qquad \text{o should be assignable}}{\Gamma; \Delta \cdot o : C[\mathsf{init}; S] \vdash \texttt{new}\ C() : C[\mathsf{init}; S] \dashv \Gamma; \Delta \cdot o : C[S]}\ [\text{New}]$$

$$\frac{\Gamma; \Delta \vdash e \dashv \Gamma'; \Delta' \qquad \text{stack frame}}{\Gamma; \Delta \cdot \tilde{x} : \tilde{T} \vdash \texttt{return}\ e \dashv \Gamma'; \Delta'}\ [\text{Return}]$$

$$\frac{\begin{array}{l}\Gamma; \Delta \cdot r : T \vdash r.m(e) : E \dashv \Gamma''; \Delta'' \cdot r : C[\langle S_l \rangle_{i \in E}] \\ \forall l \in E, \Gamma''; \Delta'' \cdot r : C[S_l] \vdash e_l : C[S_l] \dashv \Gamma'; \Delta' \cdot r : C[S]\end{array}}{\Gamma; \Delta \cdot r : T \vdash \texttt{switch}(r.m(e))\{l : e_l\}_{l \in E} \dashv \Gamma'; \Delta \cdot r : C[S]}$$

$$\frac{\begin{array}{ll}\Gamma_1; \Delta_1 \vdash e_1 \dashv \Gamma'; \Delta' & \Gamma_2; \Delta_2 \vdash e_1; e_2 \dashv \Gamma''; \Delta'' \\ \Delta = \Delta' \uplus \Delta'' & \Gamma = \Gamma' \uplus \Gamma''\end{array}}{\Gamma; \Delta \cdot r : T \vdash \lambda : \texttt{while}(e_1)\{e_2\} \dashv \Gamma'; \Delta'}$$

$$\frac{\begin{array}{ll}\Gamma_1; \Delta_1 \vdash e; e_1 \dashv \Gamma'; \Delta' & \Gamma_2; \Delta_2 \vdash e; e_2 \dashv \Gamma''; \Delta'' \\ \Delta = \Delta' \uplus \Delta'' & \Gamma = \Gamma' \uplus \Gamma''\end{array}}{\Gamma; \Delta \cdot r : T \vdash \lambda : \texttt{if}\ e_1\ \texttt{then}\ e_2\ \texttt{else}\ \dashv \Gamma'; \Delta'}$$