1 Syntax

$$
\begin{array}{lll}
program & ::= \overline{cls}\ \overline{s} \\
cls & ::= \texttt{class}\ C\ \{\overline{field}\ \overline{method}\} \\
field & ::= T\ f; \\
method & ::= T\ m(T\ x)\ contract\ \{\overline{s}\} \\
contract & ::= \texttt{requires}\ \phi;\ \texttt{ensures}\ \phi; \\
T & ::= \texttt{int}\ |\ C \\
s & ::= x.f := y;\ |\ x := e;\ |\ x := \texttt{new}\ C;\ |\ x := y.m(z);\ |\ \texttt{return}\ x;\ |\ \texttt{assert}\ \phi;\ |\ \texttt{release}\ \phi; \\
\phi & ::= \texttt{true}\ |\ e = e\ |\ e \neq e\ |\ \texttt{acc}(x.f)\ |\ \phi * \phi \\
e & ::= v\ |\ x\ |\ e.f \\
x & ::= \texttt{this}\ |\ \texttt{result}\ |\ \langle other \rangle \\
\\
\Gamma & ::= (x \mapsto T) \\
H & ::= (o \mapsto (C, \overline{(f \mapsto v)})) \\
\rho & ::= (x \mapsto v) \\
A_s & ::= \overline{(x, f)} \\
A_d & ::= \overline{(o, f)} \\
S & ::= (\rho, A_d, \overline{s}) \cdot S\ |\ nil
\end{array}
$$

2 Static semantics

2.1 Expressions ($A_s \vdash_{\texttt{sfrm}} e$)

$$
\frac{}{A \vdash_{\texttt{sfrm}} x}\ \text{WFVar}
$$

$$
\frac{}{A \vdash_{\texttt{sfrm}} v}\ \text{WFValue}
$$

$$
\frac{(x, f) \in A}{A \vdash_{\texttt{sfrm}} x.f}\ \text{WFField}
$$

2.2 Formulas ($A_s \vdash_{\texttt{sfrm}} \phi$)

$$
\frac{}{A \vdash_{\texttt{sfrm}} \texttt{true}}\ \text{WFTrue}
$$

$$
\frac{A \vdash_{\texttt{sfrm}} e_1 \qquad A \vdash_{\texttt{sfrm}} e_2}{A \vdash_{\texttt{sfrm}} e_1 = e_2}\ \text{WFEqual}
$$

$$\frac{A \vdash_{\mathtt{sfrm}} e_1 \qquad A \vdash_{\mathtt{sfrm}} e_2}{A \vdash_{\mathtt{sfrm}} e_1 \neq e_2} \ \text{WFNEQUAL}$$

$$\frac{}{A \vdash_{\mathtt{sfrm}} \mathtt{acc}(x,f)} \ \text{WFAcc}$$

$$\frac{}{A \vdash_{\mathtt{sfrm}} x : T} \ \text{WFTYPE}$$

$$\frac{A_s \vdash_{\mathtt{sfrm}} \phi_1 \qquad A_s \cup \mathtt{static\text{-}footprint}(\phi_1) \vdash_{\mathtt{sfrm}} \phi_2}{A_s \vdash_{\mathtt{sfrm}} \phi_1 * \phi_2} \ \text{WFSEPOP}$$

2.2.1 Implication ($\phi_1 \overset{.}{\Longrightarrow} \phi_2$)

Conservative approx. of $\phi_1 \implies \phi_2$.

2.3 Footprint ($\mathtt{static\text{-}footprint}(\phi) = A_s$)

$$
\begin{aligned}
\mathtt{static\text{-}footprint}(\mathtt{true}) \quad &= \emptyset \\
\mathtt{static\text{-}footprint}(e_1 = e_2) \quad &= \emptyset \\
\mathtt{static\text{-}footprint}(e_1 \neq e_2) \quad &= \emptyset \\
\mathtt{static\text{-}footprint}(\mathtt{acc}(x.f)) \quad &= \{(x,f)\} \\
\mathtt{static\text{-}footprint}(\phi_1 * \phi_2) \quad &= \mathtt{static\text{-}footprint}(\phi_1) \cup \mathtt{static\text{-}footprint}(\phi_2)
\end{aligned}
$$

2.4 Hoare ($\vdash \{\phi\}\overline{s}\{\phi\}$)

$$\frac{\vdash \{\phi_p\}s_1\{\phi_{q1}\} \qquad \phi_{q1} \implies \phi_{q2} \qquad \vdash \{\phi_{q2}\}s_2\{\phi_r\}}{\vdash \{\phi_p\}s_1; s_2\{\phi_r\}} \ \text{HSEC}$$

$$\frac{\phi(x) = C \qquad \mathtt{fields}(C) = fs}{\vdash \{\phi\}x := \mathtt{new} \ C\{(\mathtt{acc}(x,\overline{fs_i}) * (x \neq \mathtt{null} * \phi))\}} \ \text{HNEWOBJ}$$

$$\frac{\phi(x) = C \qquad \mathtt{fieldType}(C,f) = T \qquad \phi(y) = T \qquad \mathtt{acc}(x,f) \in \phi \qquad x \neq \mathtt{null} \in \phi}{\vdash \{\phi\}x.f := y\{\phi * x.f = y\}} \ \text{HFIELDASSIGN}$$

$$\frac{\begin{array}{c}\phi_1(x) = T \qquad \mathtt{staticType}_{\phi_1}(e) = T \\ \phi_1 = \phi_2[e/x] \qquad \emptyset \vdash_{\mathtt{sfrm}} \phi_1 \qquad \mathtt{static\text{-}footprint}(\phi_1) \vdash_{\mathtt{sfrm}} e\end{array}}{\vdash \{\phi_1\}x := e\{\phi_2\}} \ \text{HVARASSIGN}$$

$$\frac{\phi(x) = T \qquad \phi(\texttt{result}) = T}{\vdash \{\phi\}\texttt{return }x\{\phi * \texttt{result} = x\}} \text{ HRETURN}$$

$$\frac{\begin{array}{c} \phi(y) = C \qquad \phi(x) = T_r \qquad \phi(z') = T_p \qquad y \neq \texttt{null} \in \phi \qquad \phi \implies (\phi_p * \phi_r) \\ \texttt{mpre}(C, m) = \phi_{pre} \qquad \texttt{mpost}(C, m) = \phi_{post} \qquad \texttt{mparam}(C, m) = (T_p, z) \\ mrettypeCm = T_r \qquad \phi_p = \phi_{pre}[y, z'/\texttt{this}, z] \qquad \phi_q = \phi_{post}[y, z', x/\texttt{this}, z, \texttt{result}] \end{array}}{\vdash \{\phi\}x := y.m(z')\{(\phi_q * \phi_r)\}} \text{ HAPP}$$

$$\frac{\phi_2 \in \phi_1}{\vdash \{\phi_1\}\texttt{assert }\phi_2\{\phi_1\}} \text{ HASSERT}$$

$$\frac{\phi_1 \implies (\phi_2 * \phi_r) \qquad \emptyset \vdash_{\texttt{sfrm}} \phi_r}{\vdash \{\phi_1\}\texttt{release }\phi_2\{\phi_r\}} \text{ HRELEASE}$$

$$\frac{\phi_1(x) = \bot \qquad \phi_2 = \phi_1 * x : T}{\vdash \{\phi_1\}T\ x\{\phi_2\}} \text{ HDECLARE}$$

3   Dynamic semantics

3.1   Expressions $(H, \rho \vdash e \Downarrow v)$

$$\frac{}{H, \rho \vdash x \Downarrow \rho(x)} \text{ EEVAR}$$

$$\frac{}{H, \rho \vdash v \Downarrow v} \text{ EEVALUE}$$

$$\frac{H, \rho \vdash x \Downarrow o}{H, \rho \vdash x.f \Downarrow H(o)(f)} \text{ EEACC}$$

3.2   Formulas $(H, \rho, A \vDash \phi)$

$$\frac{}{H, \rho, A \vDash \texttt{true}} \text{ EATRUE}$$

$$\frac{H, \rho \vdash e_1 \Downarrow v_1 \qquad H, \rho \vdash e_2 \Downarrow v_2 \qquad v_1 = v_2}{H, \rho, A \vDash e_1 = e_2} \text{ EAEQUAL}$$

$$\frac{H,\rho \vdash e_1 \Downarrow v_1 \qquad H,\rho \vdash e_2 \Downarrow v_2 \qquad v_1 \neq v_2}{H,\rho,A \models e_1 \neq e_2} \text{ EANEQUAL}$$

$$\frac{\rho(x) = o \qquad (o,f) \in A}{H,\rho,A \models \mathtt{acc}(x,f)} \text{ EAAcc}$$

$$\frac{\rho(x) = T}{H,\rho,A \models x : T} \text{ EAType}$$

$$\frac{A_1 = A\backslash A_2 \qquad H,\rho,A_1 \models \phi_1 \qquad H,\rho,A_2 \models \phi_2}{H,\rho,A \models \phi_1 * \phi_2} \text{ EASepOp}$$

3.2.1 Implication ($\phi_1 \implies \phi_2$)

$$\phi_1 \implies \phi_2 \qquad \Longleftrightarrow \qquad \forall H,\rho,A : H,\rho,A \models \phi_1 \implies H,\rho,A \models \phi_2$$

Drawn from def. of entailment in "A Formal Semantics for Isorecursive and Equirecursive State Abstractions".

3.3 Footprint ($\mathtt{footprint}_{H,\rho}(\phi) = A_d$)

$$
\begin{aligned}
\mathtt{footprint}_{H,\rho}(\mathtt{true}) &= \emptyset \\
\mathtt{footprint}_{H,\rho}(e_1 = e_2) &= \emptyset \\
\mathtt{footprint}_{H,\rho}(e_1 \neq e_2) &= \emptyset \\
\mathtt{footprint}_{H,\rho}(\mathtt{acc}(e.f)) &= \{(o,f)\} \text{ where } H,\rho \vdash e \Downarrow o \\
\mathtt{footprint}_{H,\rho}(\phi_1 * \phi_2) &= \mathtt{footprint}_{H,\rho}(\phi_1) \cup \mathtt{footprint}_{H,\rho}(\phi_2)
\end{aligned}
$$

3.4 Small-step ($(H,S) \to (H,S)$)

$$\frac{H,\rho \vdash x \Downarrow o \qquad H,\rho \vdash y \Downarrow v_y \qquad (o,f) \in A \qquad H' = H[o \mapsto [f \mapsto v_y]]}{(H,(\rho,A,x.f := y;\overline{s}) \cdot S) \to (H',(\rho,A,\overline{s}) \cdot S)} \text{ ESFieldAssign}$$

$$\frac{H,\rho \vdash e \Downarrow v \qquad \rho' = \rho[x \mapsto v]}{(H,(\rho,A,x := e;\overline{s}) \cdot S) \to (H,(\rho',A,\overline{s}) \cdot S)} \text{ ESVarAssign}$$

$$\frac{\mathtt{fields}(C) = f \qquad \rho' = \rho[x \mapsto o] \qquad \overset{H(o) = \bot}{A' = A * \overline{(o,f_i)}} \qquad H' = H[o \mapsto \mathtt{new}\ C]}{(H,(\rho,A,x := \mathtt{new}\ C;\overline{s}) \cdot S) \to (H',(\rho',A',\overline{s}) \cdot S)} \text{ ESNewObj}$$

$$\frac{H, \rho \vdash x \Downarrow v_x \qquad \rho' = \rho[\texttt{result} \mapsto v_x]}{(H, (\rho, A, \texttt{return } x; \overline{s}) \cdot S) \rightarrow (H, (\rho', A, \overline{s}) \cdot S)} \text{ ESRETURN}$$

$$\frac{\begin{array}{c} H, \rho \vdash y \Downarrow o \\ H, \rho \vdash z \Downarrow v \qquad H(o) = (C, c) \qquad \texttt{mbody}(C, m) = \overline{r} \qquad \texttt{mparam}(C, m) = (T, w) \\ \texttt{mpre}(C, m) = \phi \qquad \rho' = [\texttt{this} \mapsto o, w \mapsto v] \qquad H, \rho', A \vDash \phi \qquad A' = \texttt{footprint}_{H, \rho'}(\phi) \end{array}}{(H, (\rho, A, x := y.m(z); \overline{s}) \cdot S) \rightarrow (H, (\rho', A', \overline{r}) * (\rho, A \setminus A', x := y.m(z); \overline{s}) \cdot S)} \text{ ESAPP}$$

$$\frac{\texttt{mpost}(C, m) = \phi \qquad H, \rho', A' \vDash \phi \qquad A'' = \texttt{footprint}_{H, \rho'}(\phi) \qquad H, \rho' \vdash \texttt{result} \Downarrow v_r}{(H, (\rho', A', \emptyset) * (\rho, A, x := y.m(z); \overline{s}) \cdot S) \rightarrow (H, (\rho[x \mapsto v_r], A * A'', \overline{s}) \cdot S)} \text{ ESAPPFINISH}$$

$$\frac{H, \rho, A \vDash \phi}{(H, (\rho, A, \texttt{assert } \phi; \overline{s}) \cdot S) \rightarrow (H, (\rho, A, \overline{s}) \cdot S)} \text{ ESASSERT}$$

$$\frac{H, \rho, A \vDash \phi \qquad A' = A \setminus \texttt{footprint}_{H, \rho}(\phi)}{(H, (\rho, A, \texttt{release } \phi; \overline{s}) \cdot S) \rightarrow (H, (\rho, A', \overline{s}) \cdot S)} \text{ ESRELEASE}$$

$$\frac{\rho' = \rho[x \mapsto \texttt{defaultValue}(T)]}{(H, (\rho, A, T\ x; \overline{s}) \cdot S) \rightarrow (H, (\rho', A, \overline{s}) \cdot S)} \text{ ESDECLARE}$$

4 Theorems

Hoare preserves self-framing?

$$\forall\ \Gamma, \phi_1, \phi_2, s :\vdash \{\phi_1\} s \{\phi_2\}$$
$$\implies \emptyset \vdash_{\texttt{sfrm}} \phi_1$$
$$\implies \emptyset \vdash_{\texttt{sfrm}} \phi_2$$

Hoare progress

$$\forall\ ... :\vdash \{\phi_1\} s' \{\phi_2\}$$
$$\implies H_1, \rho_1, A_1 \vDash \phi_1$$
$$\implies \exists H_2, \rho_2, A_2 : (H_1, (\rho_1, A_1, s'; \overline{s}) \cdot S) \rightarrow^* (H_2, (\rho_2, A_2, \overline{s}) \cdot S)$$

Hoare preservation

$$\forall\ ... :\vdash \{\phi_1\} s' \{\phi_2\}$$
$$\implies H_1, \rho_1, A_1 \vDash \phi_1$$
$$\implies (H_1, (\rho_1, A_1, s'; \overline{s}) \cdot S) \rightarrow^* (H_2, (\rho_2, A_2, \overline{s}) \cdot S)$$
$$\implies H_2, \rho_2, A_2 \vDash \phi_2$$