1 Syntax

$$
\begin{array}{ll}
\mathit{program} & ::= \overline{\mathit{cls}}\ \overline{s} \\
\mathit{cls} & ::= \texttt{class}\ C\ \{\overline{\mathit{field}}\ \overline{\mathit{method}}\} \\
\mathit{field} & ::= T\ f; \\
\mathit{method} & ::= T\ m(\overline{T\ x})\ \mathit{contract}\ \{\overline{s}\} \\
\mathit{contract} & ::= \texttt{requires}\ \phi;\ \texttt{ensures}\ \phi; \\
T & ::= \texttt{int} \mid C \\
s & ::= x.f := y; \mid x := e; \mid x := \mathit{new}C; \mid x := y.m(\overline{z}); \mid \texttt{return}\ x; \mid \texttt{assert}\ \phi; \mid \texttt{release}\ \phi; \\
\phi & ::= \texttt{true} \mid e = e \mid e \neq e \mid \texttt{acc}(x.f) \mid \phi * \phi \\
e & ::= v \mid x \mid e.f \\
x & ::= \texttt{this} \mid \texttt{result} \mid \langle \mathit{other} \rangle
\end{array}
$$

$$
\begin{array}{ll}
\Gamma & ::= (x \mapsto T) \\
H & ::= (o \mapsto (C, \overline{(f \mapsto v)})) \\
\rho & ::= (x \mapsto v) \\
A_s & ::= \overline{(x, f)} \\
A_d & ::= \overline{(o, f)} \\
S & ::= (\rho, A_d, \overline{s}) \cdot S \mid \mathit{nil}
\end{array}
$$

2 Static semantics

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

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

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

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

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

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

$$\frac{A \vdash_{\texttt{sfrm}} e_1 \qquad A \vdash_{\texttt{sfrm}} e_2}{A \vdash_{\texttt{sfrm}} e_1 = e_2} \text{ WFE{\scriptsize QUAL}}$$

$$\frac{A \vdash_{\texttt{sfrm}} e_1 \qquad A \vdash_{\texttt{sfrm}} e_2}{A \vdash_{\texttt{sfrm}} e_1 \neq e_2} \text{ WFNE{\scriptsize QUAL}}$$

$$\frac{}{A \vdash_{\texttt{sfrm}} \texttt{acc}(x, f)} \text{ WFA{\scriptsize CC}}$$

$$\frac{A_s \vdash_{\texttt{sfrm}} \phi_1 \qquad A_s \cup \texttt{static-footprint}(\phi_1) \vdash_{\texttt{sfrm}} \phi_2}{A_s \vdash_{\texttt{sfrm}} \phi_1 * \phi_2} \quad \text{WF-SepOp}$$

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

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

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

$$\frac{\Gamma \vdash \{\phi_p\}s_1\{\phi_{q1}\} \qquad \phi_{q1} \implies \phi_{q2} \qquad \Gamma \vdash \{\phi_{q2}\}s_2\{\phi_r\}}{\Gamma \vdash \{\phi_p\}s_1; s_2\{\phi_r\}} \quad \text{H-Sec}$$

$$\frac{\Gamma(x') = C' \qquad \texttt{fields}(C') = fs}{Gamma \vdash \{p\}x' := \texttt{ new } C'\{\overline{(\texttt{acc}(x', fs) :: (x' \neq \texttt{null} :: p))}\}} \text{ HN{\scriptsize EW}O{\scriptsize BJ}}$$

$$\frac{\texttt{acc}(x', f') \in p \qquad x' \neq \texttt{null} \in p \qquad y' = e' \in p}{Gamma \vdash \{p\}x' := f'.y'\{p * x'.f' = y'\}} \text{ HF{\scriptsize IELD}A{\scriptsize SSIGN}}$$

$$\frac{p' = p[x'/e'] \qquad e' = e2' \in p' \qquad sfrmphi[]p' \qquad (staticFootprintp') \vdash_{\texttt{sfrm}} e'}{Gamma \vdash \{p'\}(sAssignx'e')\{p\}} \text{ HVarAssign}$$

$$\frac{}{Gamma \vdash \{p\}\texttt{return } x'\{p * \texttt{result} = x'\}} \text{ HReturn}$$

$$\frac{(sndpr)))Xz'), \Gamma(y') = C' \qquad y' \neq \texttt{null} \in p \qquad p \implies (pp + +pr) \qquad pp = option_m ap(phiSubsts((\texttt{this}, y'}{Gamma \vdash \{p\}(sCallx'y'}$$

$$\frac{p2 \in p1}{Gamma \vdash \{p1\}\texttt{assert } p2\{p1\}} \text{ HAssert}$$

$$\frac{p1 \implies (p2 :: pr) \qquad sfrmphi[]pr}{Gamma \vdash \{p1\}\texttt{release } p2\{pr\}} \text{ HRelease}$$

$$\frac{\Gamma(x) = C \qquad \texttt{fields}(C) = \{\overline{f_i}\}}{\Gamma \vdash \{\phi\}x := \texttt{new } C\{\overline{\texttt{acc}(x.f_i)} * x \neq \texttt{null} * \phi\}} \quad \text{H-NewObj}$$

$$\frac{\phi \implies \texttt{acc}(x.f) * x \neq \texttt{null}}{\Gamma \vdash \{\phi\}x.f := y\{\phi * x.f = y\}} \quad \text{H-FieldAssign}$$

$$\frac{\phi' = \phi[e/x] \qquad \emptyset \vdash_{\texttt{sfrm}} \phi' \qquad \texttt{static-footprint}(\phi') \vdash_{\texttt{sfrm}} e}{\Gamma \vdash \{\phi'\}x := e\{\phi\}} \quad \text{H-VarAssign}$$

$$\frac{}{\Gamma \vdash \{\phi\}\texttt{return } x\{\phi * \texttt{result} = x\}} \quad \text{H-Return}$$

$$\frac{\Gamma(y) = C \qquad \phi \implies y \neq null * \phi_p * \phi_r \qquad \phi_p = \texttt{mpre}(C, m)[y, \overline{z}/\texttt{this}, \overline{X}] \qquad \phi_q = \texttt{mpost}(C, m)[y, \overline{z}, x/\texttt{th}}{\Gamma \vdash \{\phi\}x := y.m(\overline{z})\{\phi_q * \phi_r\}}$$

$$\frac{\phi \implies \phi'}{\Gamma \vdash \{\phi\}\texttt{assert } \phi'\{\phi\}} \quad \text{H-Assert}$$

$$\frac{\phi \implies \phi' * \phi_r \qquad \emptyset \vdash_{\texttt{sfrm}} \phi_r}{\Gamma \vdash \{\phi\}\texttt{release } \phi'\{\phi_r\}} \quad \text{H-Release}$$

3 Dynamic semantics

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

$$\frac{}{H, \rho \vdash x \Downarrow \rho(x)} \quad \text{EE-Var}$$

$$\frac{}{H, \rho \vdash v \Downarrow v} \quad \text{EE-Value}$$

$$\frac{H, \rho \vdash x \Downarrow o}{H, \rho \vdash x.f \Downarrow H(o)(f)} \quad \text{EE-Acc}$$

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

$$\frac{}{H, \rho, A \vDash \mathtt{true}} \quad \text{EA-True}$$

$$\frac{H, \rho \vdash e_1 \Downarrow v_1 \qquad H, \rho \vdash e_2 \Downarrow v_2 \qquad v_1 = v_2}{H, \rho, A \vDash e_1 = e_2} \quad \text{EA-Equal}$$

$$\frac{H, \rho \vdash e_1 \Downarrow v_1 \qquad H, \rho \vdash e_2 \Downarrow v_2 \qquad v_1 = v_2}{H, \rho, A \vDash e_1 = e_2} \quad \text{EA-NEqual}$$

$$\frac{H, \rho \vdash x \Downarrow o \qquad (o, f) \in A}{H, \rho, A \vDash \mathtt{acc}(x.f)} \quad \text{EA-Acc}$$

$$\frac{A_1 = A \backslash A_2 \qquad H, \rho, A_1 \vDash \phi_1 \qquad H, \rho, A_2 \vDash \phi_2}{H, \rho, A \vDash \phi_1 * \phi_2} \quad \text{EA-SepOp}$$

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 $((H, S) \rightarrow (H, S))$

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

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

$$\frac{H, \rho \vdash e \Downarrow v \qquad H, \rho \vdash e \Downarrow v \qquad H, \rho \vdash e \Downarrow v \qquad H, \rho \vdash e \Downarrow v \qquad H, \rho \vdash e \Downarrow v}{(H, (\rho, A, x := \texttt{new}\ C;\ \overline{s}) \cdot S) \rightarrow (H, (\rho, A, \overline{s}) \cdot S)} \text{ ES-NewObj}$$

4 Theorems

Hoare preserves self-framing

$$\begin{aligned} &\forall\ \Gamma, \phi_1, \phi_2, s : \Gamma \vdash \{\phi_1\} s \{\phi_2\} \\ &\qquad \implies \texttt{static-footprint}(\phi_1) \vdash_{\texttt{sfrm}} \phi_1 \\ &\qquad \implies \texttt{static-footprint}(\phi_2) \vdash_{\texttt{sfrm}} \phi_2 \end{aligned}$$

Hoare progress

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

Hoare preservation

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