

1 Syntax

<i>program</i>	$::= \overline{cls} \ \overline{s}$
<i>cls</i>	$::= \text{class } C \ \{\overline{field} \ \overline{method}\}$
<i>field</i>	$::= T \ f;$
<i>method</i>	$::= T \ m(\overline{T} \ x) \ \text{contract} \ \{\overline{s}\}$
<i>contract</i>	$::= \text{requires } \phi; \ \text{ensures } \phi;$
<i>T</i>	$::= \text{int} \mid C$
<i>s</i>	$::= x.f := y; \mid x := e; \mid x := \text{new} C; \mid x := y.m(\overline{z}); \mid \text{return } x; \mid \text{assert } \phi; \mid \text{release } \phi;$
ϕ	$::= \text{true} \mid e = e \mid e \neq e \mid \text{acc}(x.f) \mid \phi * \phi$
<i>e</i>	$::= v \mid x \mid e.f$
<i>x</i>	$::= \text{this} \mid \text{result} \mid \langle \text{other} \rangle$
Γ	$::= (x \mapsto T)$
<i>H</i>	$::= (o \mapsto (C, (\overline{f \mapsto v})))$
ρ	$::= (x \mapsto v)$
<i>A_s</i>	$::= \overline{(x, f)}$
<i>A_d</i>	$::= \overline{(o, f)}$
<i>S</i>	$::= (\rho, A_d, \overline{s}) \cdot S \mid \text{nil}$

2 Static semantics

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

$$\frac{}{A \vdash_{\text{sfrm}} x} \text{WFVAR}$$

$$\frac{}{A \vdash_{\text{sfrm}} v} \text{WFVALUE}$$

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

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

$$\frac{}{A \vdash_{\text{sfrm}} \text{true}} \text{WFTTRUE}$$

$$\frac{A \vdash_{\text{sfrm}} e_1 \quad A \vdash_{\text{sfrm}} e_2}{A \vdash_{\text{sfrm}} e_1 = e_2} \text{WFEQUAL}$$

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

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

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

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

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

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

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

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

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

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

$$\begin{array}{c}
\frac{}{\Gamma \vdash \{\phi\} \mathbf{return} \ x \{ \phi * \mathbf{result} = x \}} \quad \text{H-Return} \\
\\
\frac{\Gamma(y) = C \quad \phi \implies y \neq \mathbf{null} * \phi_p * \phi_r \quad \phi_p = \mathbf{mpre}(C, m)[y, \bar{z}/\mathbf{this}, \bar{X}] \quad \phi_q = \mathbf{mpost}(C, m)[y, \bar{z}, x/\mathbf{this}]}{\Gamma \vdash \{\phi\} x := y.m(\bar{z}) \{ \phi_q * \phi_r \}} \\
\\
\frac{\phi \implies \phi'}{\Gamma \vdash \{\phi\} \mathbf{assert} \ \phi' \{ \phi \}} \quad \text{H-Assert} \\
\\
\frac{\phi \implies \phi' * \phi_r \quad \emptyset \vdash_{\mathbf{sfrm}} \phi_r}{\Gamma \vdash \{\phi\} \mathbf{release} \ \phi' \{ \phi_r \}} \quad \text{H-Release}
\end{array}$$

3 Dynamic semantics

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

$$\begin{array}{c}
\frac{}{H, \rho \vdash x \Downarrow \rho(x)} \quad \text{EE-Var} \\
\\
\frac{}{H, \rho \vdash v \Downarrow v} \quad \text{EE-Value} \\
\\
\frac{H, \rho \vdash x \Downarrow o}{H, \rho \vdash x.f \Downarrow H(o)(f)} \quad \text{EE-Acc}
\end{array}$$

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

$$\begin{array}{c}
\frac{}{H, \rho, A \models \mathbf{true}} \quad \text{EA-True} \\
\\
\frac{H, \rho \vdash e_1 \Downarrow v_1 \quad H, \rho \vdash e_2 \Downarrow v_2 \quad v_1 = v_2}{H, \rho, A \models e_1 = e_2} \quad \text{EA-Equal} \\
\\
\frac{H, \rho \vdash e_1 \Downarrow v_1 \quad H, \rho \vdash e_2 \Downarrow v_2 \quad v_1 = v_2}{H, \rho, A \models e_1 = e_2} \quad \text{EA-NEqual} \\
\\
\frac{H, \rho \vdash x \Downarrow o \quad (o, f) \in A}{H, \rho, A \models \mathbf{acc}(x.f)} \quad \text{EA-Acc} \\
\\
\frac{A_1 = A \setminus A_2 \quad H, \rho, A_1 \models \phi_1 \quad H, \rho, A_2 \models \phi_2}{H, \rho, A \models \phi_1 * \phi_2} \quad \text{EA-SepOp}
\end{array}$$

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

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

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

$$\frac{H, \rho \vdash x \Downarrow o \quad H, \rho \vdash y \Downarrow v_y \quad (o, f) \in A \quad H' = H[o \mapsto [f \mapsto v_y]]}{(H, (\rho, A, x := f.y; \bar{s}) \cdot S) \rightarrow (H', (\rho, A, \bar{s}) \cdot S)} \text{ESFIELDASSIGN}$$

$$\frac{H, \rho \vdash e \Downarrow v \quad \rho' = \rho[x \mapsto v]}{(H, (\rho, A, x := e; \bar{s}) \cdot S) \rightarrow (H, (\rho', A, \bar{s}) \cdot S)} \text{ESVARASSIGN}$$

$$\frac{
\begin{array}{l}
H(o) = \perp \quad \text{fields}(C) = Cf' \\
\rho' = \rho[x \mapsto o] \quad A' = A * \text{map}(funcf' \Rightarrow (o, sndcf'))Cf' \\
H' = HSubstso(\text{map}(funcf' \Rightarrow (sndcf', vnull))Cf')Heap
\end{array}
}{(H, (\rho, A, x := \text{new } C; \bar{s}) \cdot S) \rightarrow (H', (\rho', A', \bar{s}) \cdot S)} \text{ESNEWOBJ}$$

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

$$\frac{
\begin{array}{l}
h, r \vdash y' \Downarrow o' \quad h, r \vdash z' \Downarrow v' \quad ho' = (C', fvf) \\
mbodyC'm' = rs \quad mparamC'm' = (T, w') \quad mpre(C', m') = pre \\
r' = (\text{fun } rx \Rightarrow \text{if } x_{decbr}x \text{ then } \text{Some}(voo') \text{ else } (\text{if } x_{decbr}x' \text{ then } \text{Some } v' \text{ else } \text{None})) \\
h, r', A \models pre \quad A' = \text{footprint}_{h,r'}(pre)
\end{array}
}{(h, (r, A, x' := y'.m'(z') * s') \cdot S') \rightarrow (h, (r', A', rs) * (r, A \text{ except } AA', x' := y'.m'(z') * s') \cdot S')} \text{ESAPP}$$

$$\frac{
\begin{array}{l}
m\text{post}(C, m) = \phi \\
H, \rho', A' \models \phi \quad A'' = \text{footprint}_{H,\rho'}(\phi) \quad H, \rho' \vdash \text{result} \Downarrow v_r
\end{array}
}{(H, (\rho', A', \emptyset) * (\rho, A, x := y.m(zs'); \bar{s}) \cdot S) \rightarrow (H, (\rho[x \mapsto v_r], A * A'', \bar{s}) \cdot S)} \text{ESAPPFINISH}$$

$$\frac{H, \rho, A \models \phi}{(H, (\rho, A, \mathbf{assert} \ \phi; \bar{s}) \cdot S) \rightarrow (H, (\rho, A, \bar{s}) \cdot S)} \text{ESAssert}$$

$$\frac{H, \rho, A \models \phi \quad A' = A \text{except} A(\text{footprint}' \text{Heaprhophi})}{(H, (\rho, A, \mathbf{release} \ \phi; \bar{s}) \cdot S) \rightarrow (H, (\rho, A', \bar{s}) \cdot S)} \text{ESRELEASE}$$

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

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

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

4 Theorems

Hoare preserves self-framing

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

Hoare progress

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

Hoare preservation

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