0.1 Syntax

$\langle foo \rangle \quad ::= \langle bar \rangle \; [\; \langle baz \rangle \;] \mid \langle wat \rangle$

0.2 Static rules for expressions

$$\frac{}{A \vdash_{\texttt{sfrm}} x} \quad \text{WF-Var}$$

$$\frac{}{A \vdash_{\texttt{sfrm}} v} \quad \text{WF-Value}$$

$$\frac{(x, f) \in A}{A \vdash_{\texttt{sfrm}} x.f} \quad \text{WF-Field}$$

0.3 Static rules for formulas

$$\frac{}{A \vdash_{\texttt{sfrm}} \texttt{true}} \quad \text{WF-True}$$

$$\frac{A \vdash_{\texttt{sfrm}} e_1 \qquad A \vdash_{\texttt{sfrm}} e_2}{A \vdash_{\texttt{sfrm}} e_1 = e_2} \quad \text{WF-Equal}$$

$$\frac{A \vdash_{\texttt{sfrm}} e_1 \qquad A \vdash_{\texttt{sfrm}} e_2}{A \vdash_{\texttt{sfrm}} e_1 \neq e_2} \quad \text{WF-NEqual}$$

$$\frac{}{A \vdash_{\texttt{sfrm}} \texttt{acc}(x.f)} \quad \text{WF-Acc}$$

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

0.4 Static footprint

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

0.5 Hoare

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

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

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

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

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

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

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

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

0.6 Dynamic rules for expressions

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

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

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

0.7 Dynamic rules for formulas

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

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

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

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

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

0.8 Dynamic footprint

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

0.9 Small-step semantics

TODO

0.10 Theorems

Hoare preserves self-framing

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

Hoare progress

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

Hoare preservation

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