

0.1 Syntax

$\langle foo \rangle ::= \langle bar \rangle [\langle baz \rangle] | \langle wat \rangle$

0.2 Static rules for expressions

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

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

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

0.3 Static rules for formulas

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

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

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

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

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

0.4 Static footprint

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

0.5 Hoare

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

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

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

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

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

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

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

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

0.6 Dynamic rules for expressions

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

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

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

0.7 Dynamic rules for formulas

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

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

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

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

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

0.8 Dynamic footprint

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

0.9 Small-step semantics

TODO

0.10 Theorems

Hoare preserves self-framing

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

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

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