

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

2 Assumptions

All the rules in the following sections are implicitly parameterized over a *program* that is well-formed.

2.0.1 Well-formed program (*program* OK)

$$\frac{\overline{cls_i} \text{ OK}}{(\overline{cls_i} \ \overline{s}) \text{ OK}} \text{ OKPROGRAM}$$

2.0.2 Well-formed class (*cls* OK)

$$\frac{\text{unique field-names} \quad \text{unique method-names} \quad \overline{method_i \text{ OK in } C}}{(\text{class } C \ \{\overline{field_i} \ \overline{method_i}\}) \text{ OK}} \text{ OKCLASS}$$

2.0.3 Well-formed method (*method* OK in *C*)

$$\frac{\begin{array}{c} FV(\phi_1) \subseteq \{x, \text{this}\} \quad FV(\phi_2) \subseteq \{x, \text{this}, \text{result}\} \\ \vdash \{x : T_x * \text{this} : C * \phi_1\} \overline{s} \{x : T_x * \text{this} : C * \text{result} : T_m * \phi_2\} \\ \emptyset \vdash_{\text{sfrm}} \phi_1 \quad \emptyset \vdash_{\text{sfrm}} \phi_2 \quad \overline{\neg \text{writesTo}(s_i, x)} \end{array}}{(T_m \ m(T_x \ x) \ \text{requires } \phi_1; \ \text{ensures } \phi_2; \ \{\overline{s}\}) \text{ OK in } C} \text{ OKMETHOD}$$

3 Static semantics

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

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

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

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

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

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

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

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

$$\frac{A \vdash_{\text{sfrm}} e}{A \vdash_{\text{sfrm}} \text{acc}(e.f)} \text{WFAcc}$$

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

$$\frac{A_s \vdash_{\text{sfrm}} \phi_1 \quad A_s \cup [\phi_1] \vdash_{\text{sfrm}} \phi_2}{A_s \vdash_{\text{sfrm}} \phi_1 * \phi_2} \text{WFSEPOP}$$

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

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

3.3 Footprint ($\lfloor \phi \rfloor = A_s$)

| | |
|-------------------------------------|--------------------------------------------------------|
| $\lfloor \mathbf{true} \rfloor$ | $= \emptyset$ |
| $\lfloor e_1 = e_2 \rfloor$ | $= \emptyset$ |
| $\lfloor e_1 \neq e_2 \rfloor$ | $= \emptyset$ |
| $\lfloor \mathbf{acc}(e.f) \rfloor$ | $= \{(e, f)\}$ |
| $\lfloor \phi_1 * \phi_2 \rfloor$ | $= \lfloor \phi_1 \rfloor \cup \lfloor \phi_2 \rfloor$ |

3.4 Type ($\phi \vdash e : T$)

$$\frac{}{\phi \vdash n : \mathbf{int}} \text{STVALNUM}$$

$$\frac{}{\phi \vdash \mathbf{null} : T} \text{STVALNULL}$$

$$\frac{\phi \Rightarrow (x : T)}{\phi \vdash x : T} \text{STVAR}$$

$$\frac{\phi \vdash e : C \quad \vdash C.f : T}{\phi \vdash e.f : T} \text{STFIELD}$$

3.5 Hoare ($\vdash \{\phi\} \bar{s} \{\phi\}$)

$$\frac{\vdash \{\phi_p\} s_1 \{\phi_{q1}\} \quad \phi_{q1} \Rightarrow \phi_{q2} \quad \emptyset \vdash_{\mathbf{sfrm}} \phi_{q2} \quad \vdash \{\phi_{q2}\} s_2 \{\phi_r\}}{\vdash \{\phi_p\} s_1; s_2 \{\phi_r\}} \text{HSEC}$$

$$\frac{\phi \Rightarrow \phi' \quad \emptyset \vdash_{\mathbf{sfrm}} \phi' \quad x \notin FV(\phi') \quad \phi \vdash x : C \quad \mathbf{fields}(C) = \bar{f}}{\vdash \{\phi\} x := \mathbf{new } C \{ \mathbf{acc}(x, f_i) * x : C * (x \neq \mathbf{null}) * \phi' \}} \text{HNEWOBJ}$$

$$\frac{\phi \Rightarrow \mathbf{acc}(x.f) * (x \neq \mathbf{null}) * \phi' \quad \emptyset \vdash_{\mathbf{sfrm}} \phi' \quad \phi \vdash x : C \quad \phi \vdash y : T \quad \vdash C.f : T}{\vdash \{\phi\} x.f := y \{ x : C * \mathbf{acc}(x.f) * (x \neq \mathbf{null}) * (x.f = y) * \phi' \}} \text{HFIELDASSIGN}$$

$$\frac{\emptyset \vdash_{\mathbf{sfrm}} \phi' \quad x \notin FV(\phi') \quad \phi \Rightarrow \phi' \quad x \notin FVe(e) \quad \phi \vdash x : T \quad \phi \vdash e : T \quad \lfloor \phi' \rfloor \vdash_{\mathbf{sfrm}} e}{\vdash \{\phi\} x := e \{ \phi' * (x = e) \}} \text{HVARASSIGN}$$

$$\frac{\phi \Rightarrow \phi' \quad \emptyset \vdash_{\mathbf{sfrm}} \phi' \quad \mathbf{result} \notin FV(\phi') \quad \phi \vdash x : T \quad \phi \vdash \mathbf{result} : T}{\vdash \{\phi\} \mathbf{return } x \{ \mathbf{result} : T * (\mathbf{result} = x) * \phi' \}} \text{HRETURN}$$

$$\frac{\phi \vdash y : C \quad \text{mmethod}(C, m) = T_r \ m(T_p \ z) \ \text{requires } \phi_{pre}; \ \text{ensures } \phi_{post}; \ \{_\} \\
\phi \vdash x : T_r \quad \phi \vdash z' : T_p \quad \phi \implies (y \neq \text{null}) * \phi_p * \phi_r \\
\emptyset \vdash_{\text{sfrm}} \phi_r \quad x \notin FV(\phi_r) \quad @listDistinct(x, x \cdot y \cdot z' \cdot \emptyset) \\
\phi_p = \phi_{pre}[y, z' / \text{this}, z] \quad \phi_q = \phi_{post}[y, z', x / \text{this}, z, \text{result}]}{\vdash \{\phi\} x := y.m(z') \{\phi_q * \phi_r\}} \text{HAPP}$$

$$\frac{\phi_1 \implies \phi_2}{\vdash \{\phi_1\} \text{assert } \phi_2 \{\phi_1\}} \text{HASSERT}$$

$$\frac{\phi_1 \implies \phi_2 * \phi_r \quad \emptyset \vdash_{\text{sfrm}} \phi_r}{\vdash \{\phi_1\} \text{release } \phi_2 \{\phi_r\}} \text{HRELEASE}$$

$$\frac{\phi \implies \phi' \quad \emptyset \vdash_{\text{sfrm}} \phi' \quad x \notin FV(\phi')}{\vdash \{\phi\} T \ x \{x : T * (x = \text{defaultValue}(T)) * \phi'\}} \text{HDECLARE}$$

Note: issue with HApp and z' in the post-condition: the substitution reflects **any changes** made to z onto z' which is wrong in general (except we make z' a by-ref parameter in the small-step semantics)

4 Dynamic semantics

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

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

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

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

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

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

$$\frac{H, \rho \vdash e_1 \Downarrow v_1 \quad H, \rho \vdash e_2 \Downarrow v_2 \quad v_1 = v_2}{H, \rho, A \models (e_1 = e_2)} \text{EAEQUAL}$$

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

$$\frac{H, \rho \vdash e \Downarrow o \quad (o, f) \in A}{H, \rho, A \models \text{acc}(e.f)} \text{EAAcc}$$

$$\frac{\rho(x) = v \quad H \vdash v : T}{H, \rho, A \models x : T} \text{EATYPE}$$

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

We give a denotational semantics of formulas as $\llbracket \phi \rrbracket = \{ (H, \rho, A) \mid H, \rho, A \models \phi \}$
 Note: ϕ satisfiable $\iff \llbracket \phi \rrbracket \neq \emptyset$

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

$$\phi_1 \implies \phi_2 \iff \llbracket \phi_1 \rrbracket \subseteq \llbracket \phi_2 \rrbracket$$

4.3 Footprint ($\lfloor \phi \rfloor_{H, \rho} = A_d$)

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

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

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

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

$$\frac{\begin{array}{c} o \notin \text{dom}(H) \quad \text{fields}(C) = \bar{T} \bar{f} \\ \rho' = \rho[x \mapsto o] \quad A' = A * \overline{(o, f_i)} \quad H' = H[o \mapsto [f \mapsto \text{defaultValue}(T)]] \end{array}}{(H, (\rho, A, x := \text{new } C; \bar{s}) \cdot S) \rightarrow (H', (\rho', A', \bar{s}) \cdot S)} \text{ESNEWOBJ}$$

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

$$\frac{\begin{array}{c} H(o) = (C, _) \quad \text{mmethod}(C, m) = T_r \ m(T \ w) \ \text{requires } \phi; \ \text{ensures } _; \ \{\bar{r}\} \\ \rho' = [\mathbf{result} \mapsto \mathbf{defaultValue}(T_r), \mathbf{this} \mapsto o, w \mapsto v] \quad H, \rho', A \models \phi \quad A' = \lfloor \phi \rfloor_{H, \rho'} \end{array}}{(H, (\rho, A, x := y.m(z); \bar{s}) \cdot S) \rightarrow (H, (\rho', A', \bar{r}) \cdot (\rho, A \setminus A', x := y.m(z); \bar{s}) \cdot S))} \text{ESAPP}$$

$$\frac{\begin{array}{c} \text{mpost}(C, m) = \phi \quad H, \rho \vdash y \Downarrow o \quad H(o) = (C, _) \\ H, \rho', A' \models \phi \quad A'' = \lfloor \phi \rfloor_{H, \rho'} \quad H, \rho' \vdash \mathbf{result} \Downarrow v_r \end{array}}{(H, (\rho', A', \emptyset) \cdot (\rho, A, x := y.m(z); \bar{s}) \cdot S) \rightarrow (H, (\rho[x \mapsto v_r], A * A'', \bar{s}) \cdot S)} \text{ESAPPFINISH}$$

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

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

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

5 Gradualization

5.1 Syntax

$$\tilde{\phi} ::= \phi \mid ? * \phi$$

Note: consider $?$ in other positions as “self-framing delimiter”, but with semantically identical meaning.

5.2 Concretization

Syntax $\hat{\phi} :=$ self-framed and satisfiable ϕ

$$\begin{array}{ll} \gamma(\hat{\phi}) & = \{ \hat{\phi} \} \\ \gamma(? * \phi') & = \{ \hat{\phi} \mid \hat{\phi} \implies \phi' \} \text{ if } \phi' \text{ satisfiable} \\ \gamma(\phi) & \text{undefined otherwise} \end{array}$$

5.3 Abstraction

$$\begin{aligned}
\alpha(\emptyset) & \text{ undefined} \\
\alpha(\{ \phi \}) & = \phi \\
\alpha(\bar{\phi} \text{ with maximum element } \phi) & = ? * \phi \\
\alpha(\bar{\phi}) & = ? \text{ otherwise}
\end{aligned}$$

5.4 Gradual Lifting

5.4.1 Self framing

$$\frac{A \vdash_{\text{sfrm}} \phi}{A \vdash_{\text{sfrm}} \phi} \text{GSFRMNONGRAD}$$

$$\frac{}{A \vdash_{\text{sfrm}} ? * \phi} \text{GSFRMGRAD}$$

5.4.2 Implication

$$\frac{\phi_1 \implies \phi_2}{\phi_1 \widetilde{\implies} \phi_2} \text{GIMPLNONGRAD}$$

$$\frac{\hat{\phi}_m \implies \phi_2 \quad \hat{\phi}_m \implies \phi_1}{? * \phi_1 \widetilde{\implies} \phi_2} \text{GIMPLGRAD}$$

$\hat{\phi}_m$ is evidence!

Consistent transitivity

While \implies is transitive, $\widetilde{\implies}$ is generally not.

But maybe not even necessary with smarter hoare rules?

5.4.3 Hoare and evidence

Discussion/Considerations:

- The post-condition- ϕ seems to inherit its gradual-ness from implication, which itself does not care about whether its second argument is gradual or not...
- Gradual

Example:

$$\frac{x \notin FV(\tilde{\phi}') \quad x \notin FV(e) \quad \epsilon \vdash \tilde{\phi} \widetilde{\implies} \tilde{\phi}' \quad \emptyset \vdash_{\text{sfrm}} \tilde{\phi}' \quad \epsilon \vdash \tilde{\phi} \vdash x : T \quad \epsilon \vdash \tilde{\phi} \vdash e : T \quad \epsilon \vdash [\tilde{\phi}'] \vdash_{\text{sfrm}} e}{\vdash \{ \tilde{\phi} \} x := e \{ \tilde{\phi}' * (x = e) \}} \text{GHVARASSIGN}$$

Collapsing (hidden) gradual implications into a single one:

$$\frac{\begin{array}{c} \epsilon \vdash \tilde{\phi} \widetilde{\Rightarrow} (x : T) * \llbracket e \rrbracket_{acc} * [e : T] * \tilde{\phi}' \\ \emptyset \vdash_{\text{sfrm}} \tilde{\phi}' \quad x \notin FV(\tilde{\phi}') \quad x \notin FV(e) \quad [e : T] \end{array}}{\vdash \{\tilde{\phi}\}x := e\{\llbracket e \rrbracket_{acc} * \tilde{\phi}' * (x = e)\}} \text{GHVARASSIGN}$$

When shifting implication responsibility to GHSec:

$$\frac{x \notin FV(\tilde{\phi}') \quad x \notin FV(e) \quad [e : T]}{\vdash \{(x : T) * \llbracket e \rrbracket_{acc} * [e : T] * \tilde{\phi}'\}x := e\{\llbracket e \rrbracket_{acc} * \tilde{\phi}' * (x = e)\}} \text{GHVARASSIGN}$$

Worth noting: the free variable part must prevent $\tilde{\phi}'$ getting instantiated into something containing x (at least that's what the mechanical gradual lifting rules dictate). Does this force an extended syntax like $?_x$ for wildcards with side conditions? Or is this solved by evidence, consequently: evidence := “coarsest” witness of implication together with variable taboos

Or does may gradual hoare rule not be gradual lifting of hoare rule? (Like TApp in AGT!)
Example derivation:

$$\begin{array}{l} \{(x : T) * \text{acc}(y.a) * \text{acc}(y.a.b) * \text{acc}(y.a.b.c) * (y : C_y) * (y.a.b \neq \text{null}) * \tilde{\phi}'\} \\ \{(x : T) * \llbracket y.a.b.c \rrbracket_{acc} * \llbracket y.a.b.c : T \rrbracket * \tilde{\phi}'\} \\ x := y.a.b.c; \quad \begin{array}{l} x \notin FV(\tilde{\phi}') \\ x \notin FV(y.a.b.c) \\ \vdash C_{y.a} : C_a \\ \vdash C_{a.b} : C_b \\ \vdash C_{b.c} : T \end{array} \\ \{\llbracket y.a.b.c \rrbracket_{acc} * \tilde{\phi}' * (x = y.a.b.c)\} \\ \{\text{acc}(y.a) * \text{acc}(y.a.b) * \text{acc}(y.a.b.c) * \tilde{\phi}' * (x = y.a.b.c)\} \end{array}$$

5.5 Theorems

5.5.1 Soundness of α

$$\forall \bar{\phi} : \bar{\phi} \subseteq \gamma(\alpha(\bar{\phi}))$$

5.5.2 Optimality of α

$$\forall \bar{\phi}, \tilde{\phi} : \bar{\phi} \subseteq \gamma(\tilde{\phi}) \implies \gamma(\alpha(\bar{\phi})) \subseteq \gamma(\tilde{\phi})$$

6 Theorems

6.1 Invariant $\text{invariant}(H, \rho, A_d, \phi)$

6.1.1 Phi valid

$$\vdash_{\text{sfrm}} \phi$$

6.1.2 Phi holds

$$H, \rho, A_d \models \phi$$

6.1.3 Types preserved

$$\begin{aligned} & \forall e, T : \phi \vdash e : T \\ \implies & H, \rho \vdash e : T \end{aligned}$$

6.1.4 Heap consistent

$$\begin{aligned} & \forall o, C, \mu, f, T : H(o) = (C, \mu) \\ \implies & \text{fieldType}(C, f) = T \\ \implies & H, \rho \vdash \mu(f) : T \end{aligned}$$

6.1.5 Heap not total

$$\begin{aligned} & \exists o_{min} : \\ & \forall o \geq o_{min} : o \notin \text{dom}(H) \\ & \quad \wedge \forall f, (o, f) \notin A \end{aligned}$$

6.2 Soundness

6.2.1 Progress

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

6.2.2 Preservation

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