Inference Rules for Hoare Triples

Last week: talked about when $\{p\}\ s\ \{q\}$ is true
($[p]\ s\ [q]$)

Now: When is it <u>provable</u>?
How do we even prove that $\{p\}\ s\ \{q\}$ is true?
We need a <u>proof system</u>: a set of axioms and rules for deriving facts

Not everything true is provable (Gödel's Incompleteness Thms)
Also, proving things about loops gives us trouble
We'll have to approximate

Remember inference rules:

Axiom: $\dfrac{}{\text{axiom}}$ Rule: $\dfrac{\text{premise 1} \quad \text{premise 2}}{\text{conclusion}}$

$\vdash \{p\}\ s\ \{q\}$ - Can prove $\{p\}\ s\ \{q\}$

As w/ semantics, need an axiom/rule for each type of stmt
$s ::= skip \mid s;s \mid x := e \mid a[e] := e \mid \text{if } e \text{ then } \{s\} \text{ else } \{s\} \mid \text{while } e\ \{s\}$

Skip $\dfrac{}{\vdash \{p\}\ skip\ \{p\}}$ Anything true before is true after

sequence $\dfrac{\vdash \{p\}\ s_1\ \{q_1\} \quad \vdash \{q_1\}\ s_2\ \{q_2\}}{\vdash \{p\}\ s_1 ; s_2\ \{q_2\}}$

We need to make sure the precond. of s_2 is true after running s_1.

If $\dfrac{\vdash \{p \wedge e\}\ s_1\ \{q_1\} \qquad \vdash \{p \wedge \neg e\}\ s_2\ \{q_2\}}{\vdash \{p\}\ \text{if } e \text{ then } \{s_1\} \text{ else } \{s_2\}\ \{q_1 \vee q_2\}}$

If we execute s_1: we know p, know $\sigma(e) = T$
" " s_2: " " " F

Know we executed one, so one post cond. is true.

While: Wait until after spring break

Assignment (Idea) $\dfrac{}{\vdash \{\ \}\ x := e\ \{q\}}$

q, but everything we want to know about x after, we need to know about e

$x \geq 0$

$\{x - 1 > 0\}\ x := x - 1\ \{x > 0\}$

$\{(sqrt(y))^2 \leq y \wedge y < (sqrt(y)+1)^2\}\ x := sqrt(y)\ \{x^2 \leq y \wedge y < (x+1)^2\}$

T

Need a more formal way of saying "q, but with x replaced by e"

$[e/x]q$ - "substitution"

Defined recursively on q

$[e/x]\,x = e$

$[e/x]\,y = y \quad x \neq y \qquad [e/x]\,c = c$ (T, F)

$[e/x](p \wedge q) = [e/x]p \wedge [e/x]q$

$\vee, \leftrightarrow, \rightarrow, \ldots$

$[e/x]\,P(e_1, \ldots, e_n) = P([e/x]e_1, \ldots, [e/x]e_n)$

Ex. $[y-1/x](x * 5 \geq 2) = [y-1/x](x*5) \geq 2$
$= [y-1/x]x * [y-1/x]5 \geq [y-1/x]2$
$= (y-1) * 5 \geq 2$

Formally, substituting into expressions

$[e/x](e_1 \text{ op } e_2) = [e/x]e_1 \text{ op } [e/x]e_2$

$[e/x](e_1 ? e_2 : e_3) = [e/x]e_1 \; ? \; [e/x]e_2 : [e/x]e_3.$

$[e/x](a[e_1]) = a[[e/x]e_1]$

$[e/x](\text{size}(a)) = \text{size}(a)$

In general, if x doesn't appear in p (e_1),

$[e/x]p = p \quad [e/x]e_1 = e_1$

Predicates w/ quantifiers

$[e/x](\underset{(\exists)}{\forall} y.\ p) = \forall y.\ [e/x]p \qquad y \neq x$

$[e/x]\ \underset{(\exists)}{\forall} x.\ p = \forall x.\ p \neq \cancel{\forall e.\ [e/x]\ p}$

quantifying on an exp doesn't make sense

Subbing for wrong x

$[e/x]\ \forall x.\ x > y$

not the x we're replacing

$\cancel{[\forall 0 \le 5 < |a|.\ a[5] > 0]}$??? $\qquad x := 5\ [\forall 0 \le x < |a|.\ a[x] > 0]$

Replace all <u>free</u> occurences of x with e.

$[e/x]((\forall y.\ y > x \to (\exists x.\ y > x)) \wedge x \neq 0)$

$= (\forall y.\ y > e \to (\exists x.\ y > x)) \wedge e \neq 0$

Assign $\overline{\vdash \{[e/x]\,q\}\ x := e\ \{q\}}$