Hoare Triples

Correctness triples AKA Hoare triples

Sir Charles Antony Richard Hoare
Also known for: Quicksort
Nullpointers
ALGOL
1980 Turing Award
Dining philosophers

$\{p\}\ s\ \{q\}$

precondition — what we assume is true before

postcondition — what should be true after

Note: Brackets are not part of conditions

$\sigma \models \{p\}\ s\ \{q\}$ – σ "satisfies" triple
if $\sigma \models p$ — p is true in σ
and $\langle s, \sigma\rangle \to^* \langle skip, \sigma'\rangle$ — we run s to termination
then $\sigma' \models q$ — q is true afterward

Note: Says nothing if p is false.
e.g. $\{x \geq 0\}\ y := sqrt(x)\ \{y^2 \leq x < (y+1)^2\}$
$\sigma = \{x = -1\}$
$\sigma \not\models x \geq 0$, so triple tells us nothing.
OTOH, if $\sigma = \{x = 1\}$ and $\langle y := sqrt(x), \sigma\rangle \to \langle skip, \sigma'\rangle$
and $\sigma' \not\models y^2 \leq x < (y+1)^2$, then our triple is wrong (has a bug)

$\models \{p\}\ s\ \{q\}$ – triple valid (satisfied in all states)

Remenber factorial prog from the other week:

$S =$ $r=1;\ i=n;$
$\quad$ while $(i>0)$ $\{r:=r*i;\ i:=-1\}$

$\models \{n\geq 0\}\ S\ \{i=0 \wedge r=i!\}$

$\not\models \{T\}\ S\ \{i=0 \wedge r=i!\}$

bc. $\langle S, \{x=-1\}\rangle \to^* \langle skip, \{x=-1, r=1\}\rangle$

$\not\models \{x>0\}\ x:=x-1\ \{x>0\}$

bc. $\langle x:=x-1, \{x=1\}\rangle \to \langle skip, \{x=0\}\rangle$

What to do?

1. Make the precondition stronger (more restrictive)
   $\models \{x>1\}\ x:=x-1\ \{x>0\}$
2. Make the postcondition weaker (less restrictive)
   $\models \{x>0\}\ x:=x-1\ \{x\geq 0\}$
3. Fix the program
   $\models \{x>0\}\ x:= x>1\ ?\ x-1 : 1\ \{x>0\}$

——— Got here 2/7

Consider: $\{x\geq 0\}\ y:=sqrt(x)\ \{y^2=x\}$

Unsat: $\{x=2\}$

Make precondition stronger:

$\{K^2=x\}\ y:=sqrt(x)\ \{y=|K|\}$

logical variable: variable that appears in conditions
"ghost" but not program

Conditions can be based on program vars. that change

$\models \{s=1+2+\ldots+k\}\ s:=s+k+1;\ k:=k+1\ \{s=1+2+\ldots+k\}$

now bigger

Invariant: true before + after

What if s errors or doesn't terminate?

$\models \{T\}$ while (T) {skip} $\{x<1 \wedge x>1\}$

<u>partial correctness</u> : q holds in σ' <u>if</u> s terminates in σ'

<u>total correctness</u> : $[p]\ s\ [q]$

if $\sigma \models p$ then $\langle s, \sigma\rangle \rightarrow^* \langle skip, \sigma'\rangle$ <u>and</u> $\sigma' \models q$

$\not\models [T]$ while (T) {skip} $[x<1 \wedge x>1]$

$\not\models [T]$ sqrt(-1) $[T]$

<u>3 extreme cases</u>

p is a contradiction : $\models \{F\}\ s\ \{q\}$ for all s, q

(remember: triple only unsatisfied in states where precondition is true) (same for $\models [F]\ s\ [q]$)

s always diverges or errors: $\models \{p\}$ while (T) {skip} $\{q\}$ for all p, q

$\models \{p\}$ sqrt(-1) $\{q\}$

(triple only unsatisfied if s terminates)

But: $\not\models [p]$ while(T){skip} $[q]$

(indeed unsat for all states, so not very informative)

q is a tautology : $\models \{p\}\ s\ \{T\}$

(postcondition requires nothing)

However: $\models [p]\ s\ [T]$ <u>does</u> tell us something:

$\langle s, \sigma\rangle$ always terminates if $\sigma \models p$

(useful)

A form of program verification

$\models \{n \geq 0\}\ s\ \{r := n!\} \Rightarrow$ <u>s is a correct factorial program</u>

specification

Getting spec right is important.

e.g. this says <u>nothing</u> if $n<0$. May need to consider that...

Equivalent:

$\models \{p\}\ s\ \{q\}$ means that if $\sigma \models p$
and $\sigma' \in M(s,\sigma)$ $(\sigma' \neq \bot)$
then $\sigma' \models q$

$\models [p]\ s\ [q]$ if $\sigma \models p$
then $\bot \notin M(s,\sigma)$
and for all $\sigma' \in M(s,\sigma)$, $\sigma' \models q$

When is it not satisfied?

$\not\models \{p\}\ s\ \{q\}$ if $\exists\, \sigma$ s.t. $\sigma \models p$
and $\sigma' \in M(s,\sigma)$ (or $\langle s,\sigma\rangle \to^* \langle \text{skip}, \sigma'\rangle$)
and $\sigma' \not\models q$

$\not\models [p]\ s\ [q]$ if $\exists\, \sigma$ s.t. $\sigma \models p$
and $\bot \in M(s,\sigma)$
or $\sigma' \neq \bot \in M(s,\sigma)$ and $\sigma' \not\models q$

Conditions can have quantifiers

$s = i := 0;$ while $(i < \text{size}(a))\ \{n := n + \text{sqrt}(a[i])\}$

Need all $a[i] \geq 0$

$[\forall j = [0, |a|).\ j \geq 0]\ \ s\ \ [T]$