FLOYD-HOARE LOGIC

AKA AXIOMATIC SEMANTICS

```
fact(x)
    y = 1
    while (x ≠ 1)
        y = y * x
        x = x - 1
    return y
```

Theorem for any $x > 0$, fact(x) returns $y = x!$

precondition

post condition

$$\{x > 0\}\ \text{fact}(x)\ \{y = x!\}$$

precondition

postcondition

$\{P\}\ S\ \{Q\}$

if P is true initially, and we execute S, and S terminates

then Q is true in the final state

"partial correctness" because of termination

---

pre/post conditions

$P, Q : State \longrightarrow \{true, false\}$

like last time

$Var \to \mathbb{Z}$

$P_1 \wedge P_2$, $\neg P_1$, etc.

skip $\{P\}\ \text{skip}\ \{P\}$

asn $\{P[x \mapsto a]\}\ x := a\ \{P\}$

---

e.g. $\{y \geq 10\}\ x := y\ \{x \geq 10\}$

$x \geq 10$

replace x with y

$\{\text{true}\}\ x := 5\ \{x \geq 5\}$

replace x with 5

$5 \geq 5 \equiv \text{true}$

"weakest precondition"

Sequential composition

$$\frac{\{P\}\,S_1\,\{Q\} \qquad \{Q\}\,S_2\,\{R\}}{\{P\}\,S_1 ; S_2\,\{R\}}$$

if

$$\frac{\{P \wedge B\}\,S_1\,\{Q\} \qquad \{P \wedge \neg B\}\,S_2\,\{Q\}}{\{P\}\ \text{if } B \text{ then } S_1 \text{ else } S_2\ \{Q\}}$$

$$\frac{\{P'\}\,S\,\{Q'\} \qquad P \subseteq P' \qquad Q' \subseteq Q \qquad P \Rightarrow P' \qquad Q' \Rightarrow Q}{\{P\}\,S\,\{Q\}}$$

make the precondition smaller

make the postcondition bigger

e.g. $\{x > 0\}\ fact(x)\ \{y = x!\}$

...easier

smaller precond

$\{x > 100\}\ fact(x)\ \{y = x!\}$

bigger post cond

$\{x > 100\}\ fact(x)\ \{y \geq x!\}$

---

while

$$\frac{\{P \wedge B\}\ S\ \{P\}}{\{P\}\ \text{while } B \text{ do } S\ \{\neg B \wedge P\}}$$

loop invariant

Notation $\vdash \{P\}\ S\ \{Q\}$

Eg.

$\{m \geq 0 \wedge n > 0\}$

$r := 1$

$\{m \geq 0 \wedge n > 0 \wedge r = 1\}$

$i := 0$

$\{r = n^i \wedge i \leq m\}$

while $(i < m)$

$r := r * n$

$i := i + 1$

$\{r = n^i \wedge i \leq m \wedge i \geq m\}$ $i = m$

we have same $\{r = n^m\}$

Loop body

$\{r = n^i \wedge i \leq m \wedge i < m\}$

$r := r * n$

loop invariant $\{r = n^{i+1} \wedge i \leq m \wedge i < m\}$

$i := i + 1$

$\{r = n^i \wedge i \leq m\}$

$\{n > 0\}$

$y := 1$

$z := 0$

while $(z \neq n)$

$z = z + 1$

$y = y * z$

$\{y = n!\}$

$I = z \leq n \wedge y = z!$ ✓

① initialization

$\{n > 0\}\ y := 1\ ;\ z := 0\ \{I\}$ ✓ ?

② consecution

$\{I \wedge z \neq n\}\ z := z + 1\ ;\ y := y * z\ \{I\}$

③ safety

$\{I \wedge z = n\}$ skip $\{y = n!\}$ ✓