LAST TIME

operational semantics

TODAY

axiomatic semantics / Hoare logic

Floyd-Hoare logic

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

Theorem

for any $x > 0$ (precondition) $x > 1000$

fact(x) returns $x!$ $> x$ (postcondition)

Hoare triple

code/program

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

precondition — postcondition

Hoare triple

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

if P is true initially, and we execute S,

then if S terminates, it is in a state in Q

possible

pre / postcodition

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

Equivalently $P, Q \subseteq State$

a state is $Var \to \underbrace{\mathbb{Z}}_{int}$

$P \wedge Q$

$\neg P$

$P \vee Q$

etc.

$P \Rightarrow Q$

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

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

weakest precondition

e.g.

$\{y \geq 10\}\ x := y\ \{x \geq 10\}$

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

$\{y \geq 0\}\ x := y\ \{x \geq 10\}$ X

$\{false\}\ x := 4\ \{x \geq 5\}$

sequential composition

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

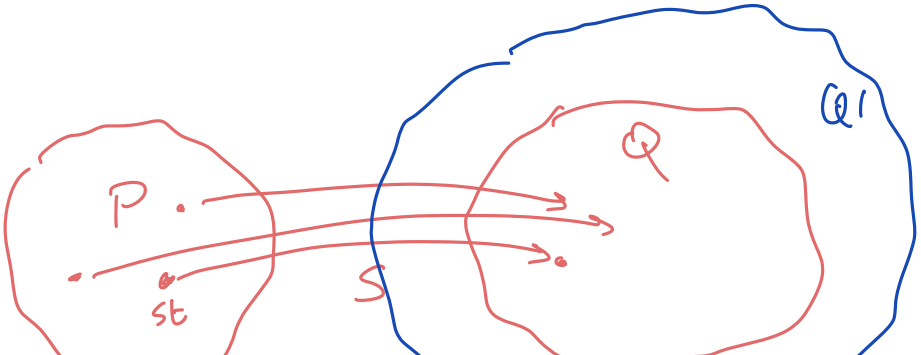
if

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

weakening strengthening

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

$$\frac{\{P\}\ S\ \{Q\} \qquad Q' \Leftarrow Q \quad (Q' \supseteq Q)}{\{P\}\ S\ \{Q'\}}$$



while

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

loop invariant

$$\frac{\vdash \{P\}\ S\ \{Q\} \qquad \vdash \{P\}\ S\ \{Q\}}{\vdash \{P\}\ S\ \{Q\}}$$

\vdash

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

$r := 1$

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

$i := 0$

$\{m \geq 0 \wedge n > 0 \wedge r = 1 \wedge i = 0\} \Rightarrow \{r = n^i \wedge i \leq m\}$

while $(i < m)$

$r := r * n$

$i := i + 1$

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

$\{r = n^m\}$

---

loop condition

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

$r := r * n$

$\{r = n^{i+1} \wedge i \leq m \wedge \underbrace{i < m}_{i+1 < m \;==\; i \leq m}\}$

$i := i + 1$

(i: x, $i + 1$: a)

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

$\{r = n^{i+1} \wedge \underline{i+1 \leq m}\}$

$\Vert\Vert$

$\{r = n^{i+1} \wedge \underline{i \leq m}\}$

$\{n>0\}$

$y := 1$

$z := 0$

while $(z \neq n)$

$z := z+1$

$y := y * z$

$\{y = z! \wedge z = n\}$

$\{y = n!\}$

$\{y = z!\}$

$y := 1 \quad z := 0$

$y = 0! = 1$ ✓

$y := 1 \quad z := 1$

$y = 1! = 1$

$y := 2 \quad z := 2$

$y = 2! = 2$

$y := 6 \quad z := 3$

$y = 3! = 6$

loop inv

initialization

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

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

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