

## 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!

post condition

pre condition

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

pre condition

post condition

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

if  $P$  is true initially, and we execute  $S$ ,  
then  $Q$  is true in the final state

and  $S$   
terminates

"partial correctness"  
because of termination

---

pre/post condition

$P, Q : \text{State} \rightarrow \{\text{true}, \text{false}\}$

↑  
like last time

$\text{Var} \rightarrow \mathbb{Z}$

$P_1 \wedge P_2$  ,  $\neg P_1$  , 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

$$\frac{\{P\} S_1 \{Q\} \quad \{Q\} S_2 \{R\}}{\{P\} S_1 ; S_2 \{R\}}$$

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

$$\frac{\{P'\} S \{Q'\}}{\{P\} S \{Q\}}$$

$P \subseteq P' \quad Q' \subseteq Q$   
 $P \Rightarrow P' \quad Q' \Rightarrow Q$

make the precondition smaller  
 make the postcondition bigger

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

...aller

5th  
precond

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

bigger  
post  
cond

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

|       |                          |
|-------|--------------------------|
| while | $\{P \wedge B\} S \{P\}$ |
|-------|--------------------------|

---

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

loop  
invariant

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

eg.

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

$\Gamma := 1$

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

$i := 0$

$\{\Gamma = n^i \wedge i \leq n\}$

while ( $i < n$ )

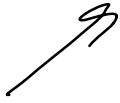
$\Gamma := \Gamma * n$

$i := i + 1$

are two same  $\rightarrow \{\Gamma = n^i \wedge i \leq n \wedge \underline{i \geq n}\} \leftarrow$   
 $\{\Gamma = n^n\}$   
 $i = n$

Loop body

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



$$r := r * n$$

loop invariant

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

$$\underline{i := i + 1}$$

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

$\{n > 0\}$

$y := 1$

$z := 0$

while ( $z \neq n$ )

$z = z + 1$

$y = y * z$

$I = z \leq n$   
 $\wedge y = z!$  ✓

$\{y = n!\}$

① initiation ✓

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

② consecution ✓

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

③ safety

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