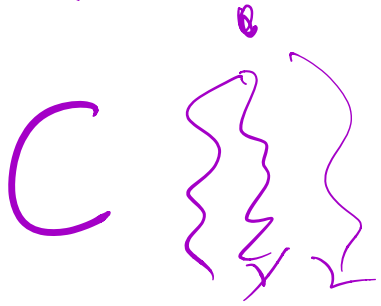
Axiomatic semantics

assume $(x \geq 0 \,\&\&\, y \geq 0)$

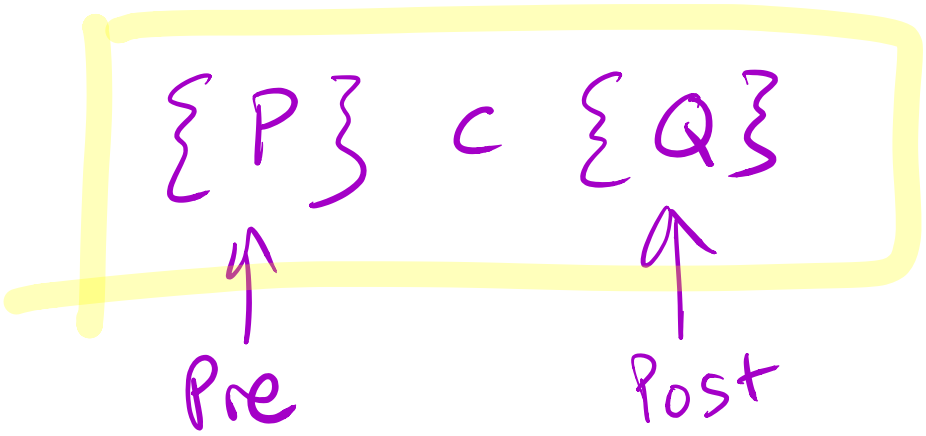


assert $(x > y)$

$\{ x \geq 0 \,\&\&\, y \geq 0 \}$ C $\{ x > y \}$

Pre — Com — Post

1. "meaning" of FHTriple
2. Rules
3. Algo




```
Legit P c Q =
  s:_ → s':_ → {bval P s}
             → BSTEP c s s'
             → {bval Q s}
```

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

$\forall s, s'.\ (\text{bval } P\ s) \to \text{BStep skip } s\ s' \to (\text{bval } P\ s')$

$\{P\}\ X := 10\ \{X \geq 0\}$

$\{Y \geq 0\}\ X := Y\ \{X \geq 0\}$

$\{10 + Y \geq 0\}\ X := 10\ \{X + Y \geq 0\}$

$\{Y = 4\}\ X := 10\ \{X + Y \geq 0\}$

$\{A + B + Y \geq 10\}\ X := A + B\ \{X + Y \geq 10\}$

$$\{Q[a/x]\}\ x := a\ \{Q\}$$

$$\{x+1 \geq 100\}\ x := x+1\ \{x \geq 100\}$$

$x \geq 99$

$$(x \geq 100)["x" \mapsto "x+1"]$$

$x+1 \geq 100$

$$\frac{\{P\}\ C_1\ \{MID\}\quad \{MID\}\ C_2\ \{Q\}}{\{P\}\ C_1\ ;\ C_2\ \{Q\}}$$

$$\frac{\{10=10\}\ x:=10\ \{x=10\} \quad \{x=10\}\ y:=10\ \{x=y\}}{\{10=10\}\ x=10;\ y:=10\ \{x=y\}}$$

C_1 C_2

- what is a "better" precond than T or F

$$\frac{\{10>1\}\ x:=10\ \{x>1\} \quad \{x>1\}\ y:=1\ \{x>y\}}{\{10>1\}\ x=10;\ y:=1\ \{x>y\}}$$

C_1 C_2

$$\frac{\{FF\}\ x := 10\ \{x = 10\} \qquad \{x = 10\}\ y := 10\ \{x = y\}}{\{FF\}\ x = 10;\ y := 10\ \{x = y\}}$$

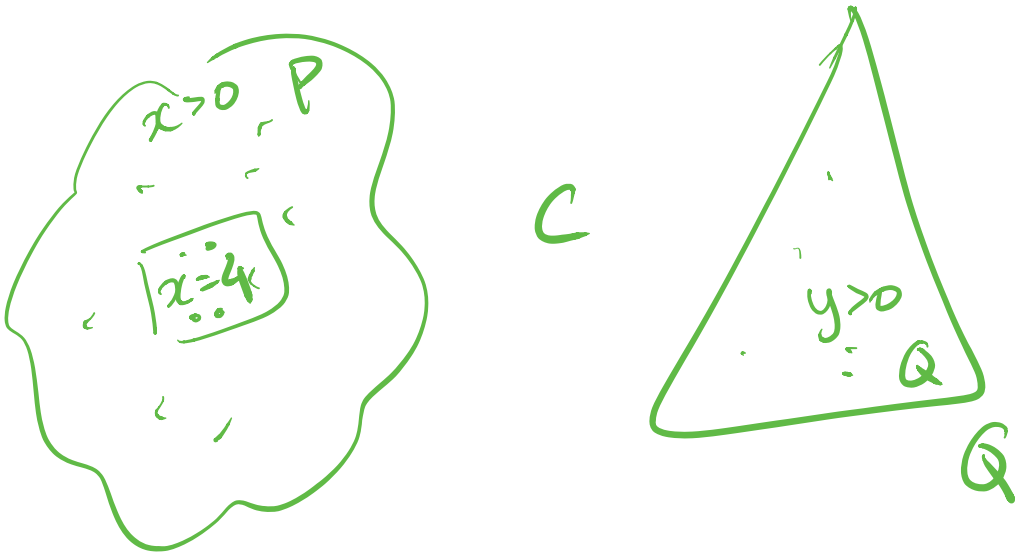
$$\{Q[x \mapsto a]\}\ x := a\ \{Q\}$$

legit

$$\{x = 4\}_{s}\quad y := x \rightsquigarrow \quad \{y > 0\}_{s'}$$

$$\forall\ s \rightsquigarrow s'$$

$$\{x > 0\}\ y := x\ \{y > 0\}$$



$x = 4 \Rightarrow x > 0$

in any state
'x=4' is true

$$\{P\}\ C\ \{Q\}$$

Legit $\{\text{TRUE}\}\ C\ \{Q\}$ ✗ ?

$\{\text{False}\}\ C\ \{Q\}$ ✓

$s*$ s'

$\{P\}\ c\ \{\text{True}\}$ ✓

or

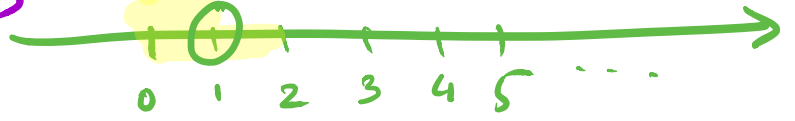
$\{P\}\ c\ \{\text{False}\}$ ×

$$\frac{\{P\}\ c\ \{Q\} \qquad Q \Rightarrow Q'}{\{P\}\ c\ \{Q'\}}$$

$Q' \geq Q$ (i.e. $x \geq 0$ vs. $x = 1$)

IF $\{\text{TRUE}\}\ c\ \{x = 1\}$

THEN $\{\text{TRUE}\}\ c\ \{x \geq 0\}$



$Q \Rightarrow Q' \doteq$ if $Q(s)$ then $Q'(s)$

$$\frac{\text{IF } \{P\}\ c\ \{Q\} \qquad P' \Rightarrow P}{\{P'\}\ c\ \{Q\}}$$

$x \geq 0$

$x = 5$

$$P' \subseteq P$$

$\forall s.$ IF $P'(s)$ THEN $P(s)$

$$\{P\}\ c\ \{Q\}$$

$\forall s, s'$ IF $P(s)$, $(\text{Bstep } c\ s\ s')$ THEN $Q(s')$

$$\frac{P \Rightarrow P' \quad \{P'\}\ c\ \{Q'\} \quad Q' \Rightarrow Q}{\{P\}\ c\ \{Q\}}\ \text{FH CONS}$$

$$\frac{}{\vdash \{P\}\ \text{SKIP}\ \{P\}}\ \text{FH SKIP}$$

R}

P	Q	P⇒Q
0	0	1
0	1	1
1	0	0
1	1	1

{False} SKIP {False} ✓

{False} SKIP {TRUE} ✓

{TRUE} SKIP {False} ×

{TRUE} SKIP {TRUE} ✓

IF P, Q

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

THEN

$P \Rightarrow Q$

$$\frac{\text{False} \Rightarrow \text{TRUE} \qquad \{\text{TRUE}\}\ \text{SKIP}\ \{\text{TRUE}\}}{\{\text{False}\}\ \text{SKIP}\ \{\text{TRUE}\}}\ \begin{matrix}\text{FH SKIP}\\ \text{FH CONS}\end{matrix}$$

$$\frac{P \Rightarrow P' \qquad \{P'\}\ C\ \{Q'\} \qquad Q' \Rightarrow Q}{\{P\}\ C\ \{Q\}}\ \text{FH CONS}$$

✓

$P = \text{False}$

$P' = \text{TRUE}$

$Q, Q' = \text{TRUE}$

$$\frac{\text{TRU} \Rightarrow 10 = 10 \qquad \{10 = 10\}\ x := 10\ \{x = 10\}}{\{\text{TRUE}\}\ x := 10\ \{x = 10\}}\ \text{CONS} \qquad \frac{}{\{x = 10\}\ y := x\ \{y = 10\}}\ \text{Asg} \qquad y = 10 \Rightarrow y \geq 0$$

$$\frac{\{\text{TRUE}\}\ x := 10\ \{x = 10\} \qquad \{x = 10\}\ y := x\ \{y \geq 0\}}{\{\text{TRUE}\}\ x := 10;\ y := x\ \{y \geq 0\}}$$

$$\frac{}{\{Q[a/x]\}\ x := a\ \{Q\}}$$

$$\dfrac{\dfrac{}{\{10 \geq 0\}\ x := 10\ \{x \geq 0\}}\ \text{ASGN} \qquad \dfrac{}{\{x \geq 0\}\ y := x\ \{y \geq 0\}}\ \text{ASGN}}{\{\text{TRUE}\}\ x := 10\ \{x \geq 0\}}\ \text{CONS} \qquad \text{TRUE} \Rightarrow 10 \geq 0$$

$$\dfrac{\{\text{TRUE}\}\ x := 10\ \{x \geq 0\} \qquad \{x \geq 0\}\ y := x\ \{y \geq 0\}}{\{\text{TRUE}\}\ x := 10;\ y := x\ \{y \geq 0\}}$$

CONSEQ,
SKIP
ASSIGN
SEQ
IF
WHILE

$$\dfrac{\{P\}\ C_1\ \{Mid\} \qquad \{Mid\}\ C_2\ \{Q\}}{\{P\}\ C_1; C_2\ \{Q\}}$$

$$\frac{\{P \wedge b\}\, c_1\, \{Q\} \qquad \{P \wedge \neg b\}\, c_2\, \{Q\}}{\{P\}\ \text{IF } b\ c_1\ c_2\ \{Q\}}$$

$$\frac{\{P\}\ c_1\ \{Q\}}{\{P\}\ \text{IF } b\ c_1\ c_2\ \{Q\}} \qquad \frac{\{P\}\ c_2\ \{Q\}}{\{P\}\ \text{IF } b\ c_1\ c_2\ \{Q\}}$$

$$\frac{\{P\}\ x := A\ \{x \geq 0\} \qquad \{P\}\ x := B\ \{x \geq 0\}}{\{P\}\ \text{IF } (z = 8)\ \text{THEN } x := A\ \text{ELSE } x := B\ \{x \geq 0\}}$$

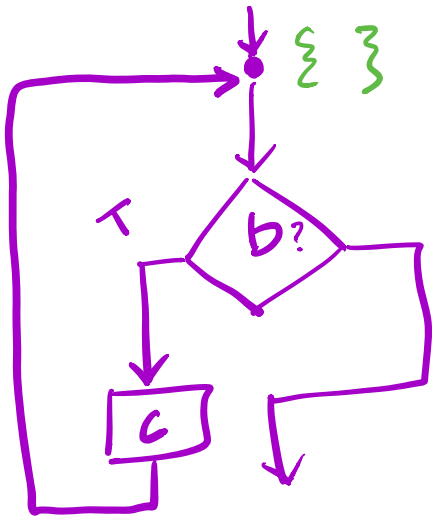
$$\frac{\dfrac{x < 0 \Rightarrow \{0 - x \geq 0\}\, y := x\, \{y \geq 0\}}{x < 0} \qquad \{\text{TRUE}\}\ y := 0 - x\ \{y \geq 0\}}{\{\text{TRUE}\}\ \text{if } (x \geq 0)\ \text{THEN } y := x\ \text{ELSE } y := 0 - x\ \{y \geq 0\}}$$

$\{\text{TRUE}\}\ y := x\ \{y \geq 0\}$ (since $x \geq 0$)

$$\frac{\{\text{TRUE}\}\ R := x\ \{R \geq 0\} \qquad \{\text{TRUE}\}\ R := 0 - x\ \{R \geq 0\}}{\{\text{TRUE}\}\ \text{IF}\ (x \geq 0)\ R := x\ \text{ELSE}\ R := 0 - x\ \{R \geq 0\}}$$

$$\frac{\{P \wedge b\}\ c_1\ \{Q\} \qquad \{P \wedge \neg b\}\ c_2\ \{Q\}}{\{P\}\ \text{IF}\ b\ c_1\ c_2\ \{Q\}}$$

$$\frac{\{I \wedge b\}\ c\ \{I\} \qquad I \wedge \neg b \Rightarrow Q}{\{I\}\ \underset{\text{Inv}}{\text{WHILE}\ b\ c}\ \{I \wedge \neg b\}}$$



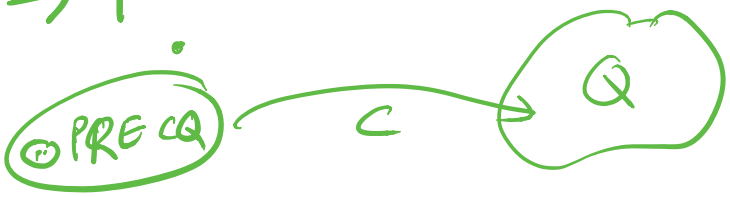
$\boxed{Pre\ c\ Q} = P$

P is "best" assertion

s.t. $\{P\}\ c\ \{Q\}$

if some other $\{P'\}\ c\ \{Q\}$

THEN $P' \Rightarrow P$.



$\{TRUE\}$
while TRUE
SKIP

$\{x \geq 0\}$

legit!

$$\frac{T \wedge T \Rightarrow \{T\}\ SKIP\ \{T\} \qquad \{T\}\ WHILE\ TRUE\ SKIP\ \{T \wedge \neg T\} \Rightarrow \{x \geq 0\}}{\{T\}\ while\ TR\ SKIP\ \{x \geq 0\}}$$

SKIP

$\{?\}\ x=y$

SKIP

$\{x=y\}$

$\{pre\ c\ Q\}$

SKIP

$\{Q\}$ ✓

Assign

$\{?\}\ x=b+1$

$y := b+1$

$\{x=y\}$

$\{Q[a/x]\}$ ✓

$x := a$

$\{Q\}$ ✓

Seq

$\{?\}\ a+1=b+1$

$x := a+1;$

$\{x=b+1\}$

$y := b+1$

$\{x=y\}$

$pre\ c_1\ (pre\ c_2\ Q)$

$c_1; c_2$

$\{Q\}$

BRANCH

$\{pre\ c\ Q\}$

c

$\{Q\}$

$\{\text{TRUE}\ ?\}$

if $x \geq 0$

$r := x$

else

$r := 0 - x$

$\{r \geq 0\}$

$\{?\}$

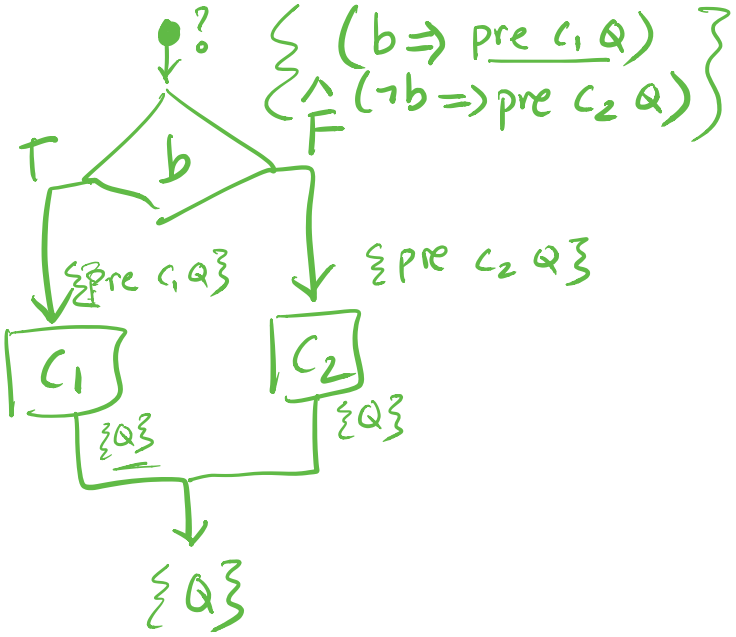
IF b

c_1

ELSE

c_2

$\{Q\}$


?
{ (b ⇒ pre c1 Q)
∧ (¬b ⇒ pre c2 Q) }
T
b
F
{pre c1 Q}
{pre c2 Q}
c1
c2
{Q}
{Q}
{Q}

LOOP

$\{?\}$ $x=0 \wedge y=0$ ✓ $x=y$ $x \geq 0$

while $(x \neq 0)$

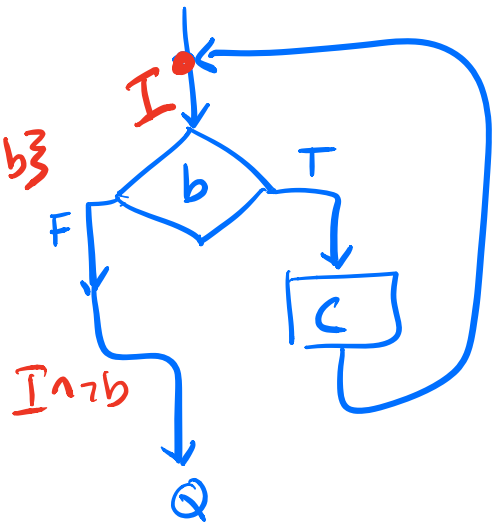
I $\{?\}$ $x=y$ $x \neq 0$ ×

$x := x-1$ $x \neq -1$

$y := y-1$

$\{y=0\}$

$$\frac{\{I \wedge b\}\ c\ \{I\}}{\{I\}\ \text{while } b\ c\ \{I \wedge \neg b\}}$$



$\{P\}\ c\ \{Q\}$

↳ "VC"

VC is valid $\Rightarrow$ Legit $P\ c\ Q$

$\{pre\ c\ q\}\ c\ \{Q\}$

$$\frac{\boxed{P \Rightarrow (pre\ c\ Q)} \quad \{(pre\ c\ Q)\}\ c\ \{Q\}}{\{P\}\ c\ \{Q\}}$$

SKIP

$X := a$

$\{pre\ c_1;c_2\ Q\}\ c\ \{Q\}$

c_1 ; c_2 $\{prec_2 Q\}$ $\{Q\}$

$vc\ c_1\ (pre\ c_2\ Q)$

$\wedge$

$vc\ c_2\ Q$