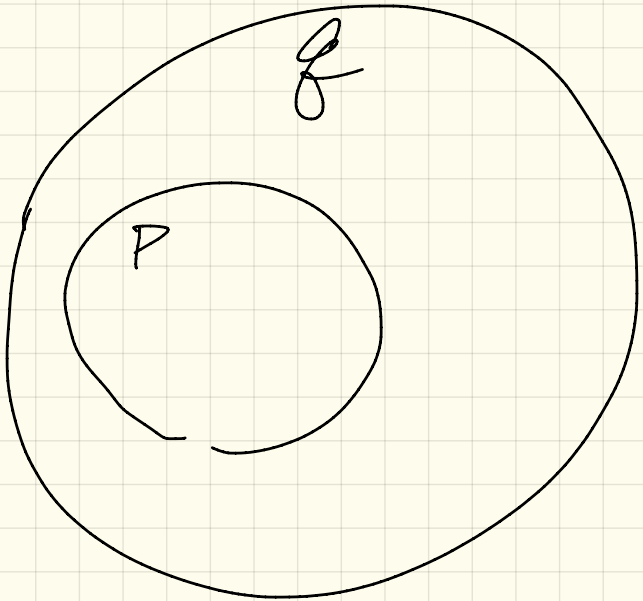
Tuesday Nov. 27

Lecture 22

$P \Rightarrow q$

P ↓ Stronger

q ↓ weaker



Program Correctness : Example (1)

```
class FOO
  i: INTEGER
  increment_by_9
    require
      i > 3
    do
      i := i + 9
    ensure
      i > 13
    end
end
```

Q

S

R

$\{Q\}\ S\ \{R\}$

$\{i > 3\}\ i := i + 9\ \{i > 13\}$

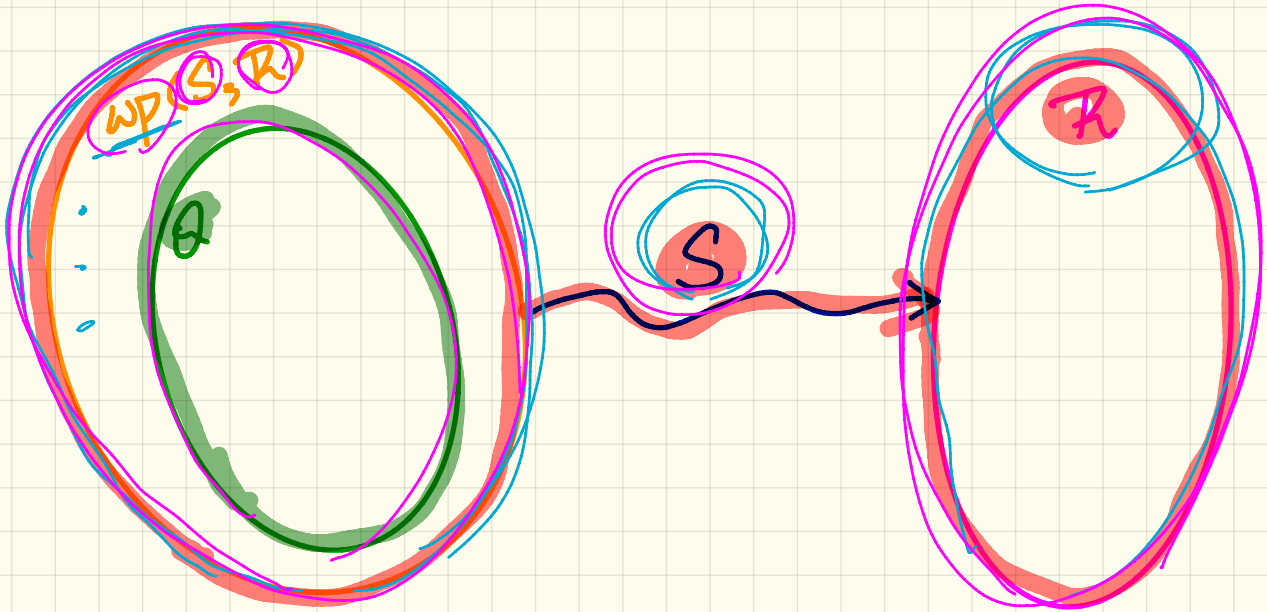
predicate (true or false)

Program Correctness : Example (2)

```
class FOO
  i: INTEGER
  increment_by_9
    require
      i > 5
    do
      i := i + 9
    ensure
      i > 13
    end
end
```

Hoare Triple as a Predicate

$$\{Q\}\ S\ \{R\} \equiv Q \Rightarrow wp(S, R)$$



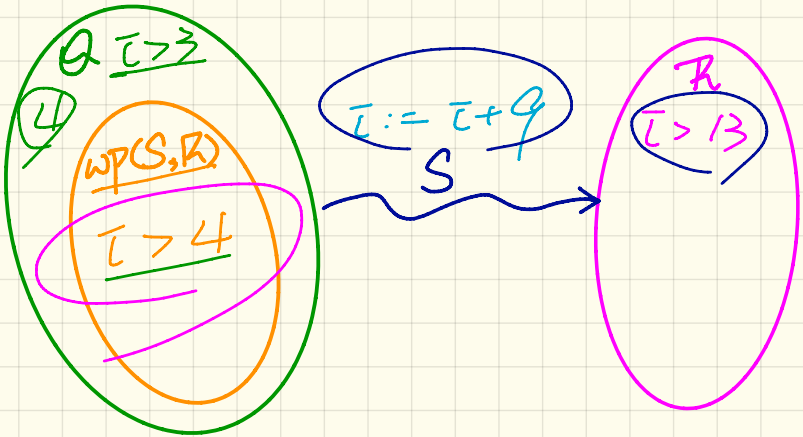
Program Correctness : Example (1)

wp(x := x + 1 , $\sum_{x=1}^{n} x + x > 10$)

bounded — free — x+1

```
class FOO
  i: INTEGER
  increment_by_9
    require
      i > 3
    do
      i := i + 9
    ensure
      i > 13
    end
end
```

$$\{Q\}\ S\ \{R\} \equiv Q \Rightarrow wp(S, R)$$



wp(i := i+9 , i > 13)

= { rule of wp for := }

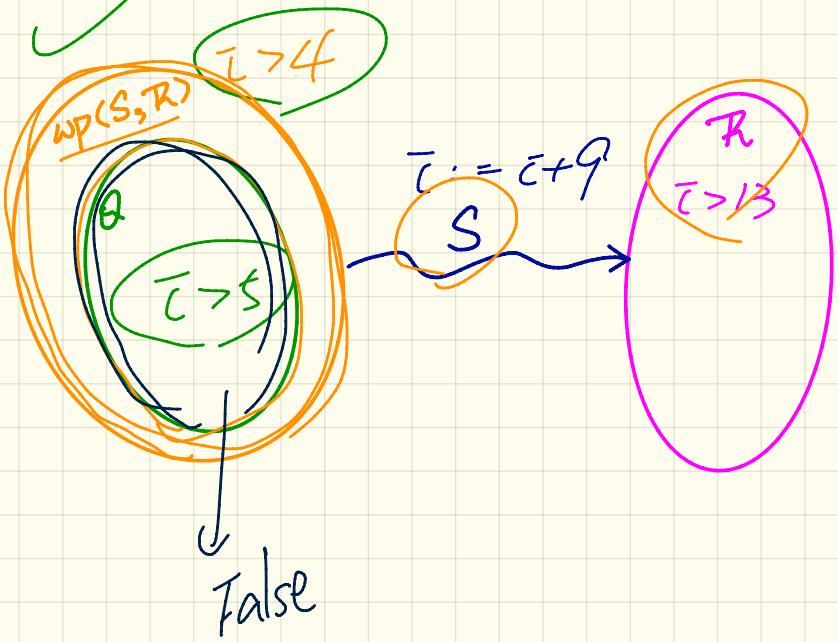
i+9 > 13 [i := i+9] = i+9 > 13

= i > 4

Program Correctness : Example (2)

```
class FOO
  i: INTEGER
  increment_by_9
    require
      i > 5
    do
      i := i + 9
    ensure
      i > 13
    end
end
```

$$\{Q\}\ S\ \{R\} \equiv Q \Rightarrow wp(S, R)$$



wp Rules

$$wp(\texttt{x := e}, R) = R[x := e]$$

$$wp(\texttt{if } B \texttt{ then } S_1 \texttt{ else } S_2 \texttt{ end}, R) = \left(\begin{array}{l} B \Rightarrow wp(S_1, R) \\ \wedge \\ \neg B \Rightarrow wp(S_2, R) \end{array} \right)$$

$$wp(S_1 \texttt{ ; } S_2, R) = wp(S_1, wp(S_2, R))$$

Proof Rules

$$\{Q\}\ S\ \{R\} \equiv Q \Rightarrow wp(S, R)$$

$$\{Q\}\ \texttt{x := e}\ \{R\} \iff Q \Rightarrow \underbrace{R[x := e]}_{wp(\texttt{x := e}, R)}$$

$$\{Q\}\ \texttt{if}\ B\ \texttt{then}\ S_1\ \texttt{else}\ S_2\ \texttt{end}\ \{R\}$$
$$\iff \begin{pmatrix} \{\ Q \wedge B\ \}\ S_1\ \{\ R\ \} \\ \wedge \\ \{\ Q \wedge \neg B\ \}\ S_2\ \{\ R\ \} \end{pmatrix} \iff \begin{pmatrix} (Q \wedge B) \Rightarrow wp(S_1, R) \\ \wedge \\ (Q \wedge \neg B) \Rightarrow wp(S_2, R) \end{pmatrix}$$

$$\{Q\}\ S_1\ ;\ S_2\ \{R\} \iff Q \Rightarrow \underbrace{wp(S_1, wp(S_2, R))}_{wp(S_1\ ;\ S_2, R)}$$

$wp(x := x+1,\ x > x_0)$

$= \{ wp \text{ rule for } := \}$

$x > x_0\ [x := x+1]$

post pre post

$= x_0 + 1 > x_0$

$= 1 > 0$

$= \text{True}$

1. To be correct, choose any Q stronger than True.
   e.g. $x > 0$, $x = 0$, $x < 0$, False
2. To be appropriate design, up to the agreement between UC and S.

$wp(x := x+1,\ x = 22)$

$= [x = 22]$

$x \neq 22$

22 23

wp(if B then S_1 else S_2 end, R)

→ [B S_1] $B \Rightarrow wp(S_1, R)$

$\neg B$ S_2 $\neg B \Rightarrow wp(S_2, R)$

Rule of wp: Conditionals

$wp(\text{if } B \text{ then } S_1 \text{ else } S_2 \text{ end}, R)$

$(B \Rightarrow wp(S_1, R)) \vee (\neg B \Rightarrow wp(S_2, R))$

vs.

$(B \Rightarrow wp(S_1, R)) \wedge (\neg B \Rightarrow wp(S_2, R))$

??

choose $x = -1$

$x \geq -1$

$\vee$

Consider: $x \geq 1$

$\equiv x \geq -1$

$x \geq -1$

$\wedge$

$x \geq 1$

$\equiv x \geq 1$

$wp(\text{if } y > 0 \text{ then } x := x + 1 \text{ else } x := x - 1 \text{ end}, x \geq 0)$

$y > 0 \Rightarrow wp(x := x + 1, x \geq 0)$ $\quad x \geq -1$

$y \leq 0 \Rightarrow wp(x := x - 1, x \geq 0)$ $\quad x \geq 1$

{Q}

if B_1 then

S_1

elseif B_2 then

S_2

else

S_3

end

{R}

$B_1 \Rightarrow wp(S_1, R)$

$\wedge$

$\neg B_1 \wedge B_2 \Rightarrow wp(S_2, R)$

$\wedge$

$\neg(B_1 \vee B_2) \Rightarrow wp(S_3, R)$

$\{Q\}$ if B then S_1 else S_2 end $\{R\}$

$\equiv$

$Q \Rightarrow \left(\begin{array}{l} \neg B \Rightarrow wp(S_1, R) \\ \wedge \\ \neg B \Rightarrow wp(S_2, R) \end{array} \right)$

shunting

$p \Rightarrow (q \Rightarrow r)$

$\equiv$

$(p \wedge q) \Rightarrow r$

Correctness of Program: Conditionals

Is this program correct?

```
{x > 0 ∧ y > 0}
if x > y then
  bigger := x ; smaller := y
else
  bigger := y ; smaller := x
end
{bigger ≥ smaller}
```

1. Calculate the wp

wp (if $x > y$ then b := x ; s := y else b := y ; s := x end , $b \geq s$)

= $x > y \Rightarrow$ wp([ ] , $b \geq s$)

$\neg(x > y) \Rightarrow$ wp([ ] , $b \geq s$)

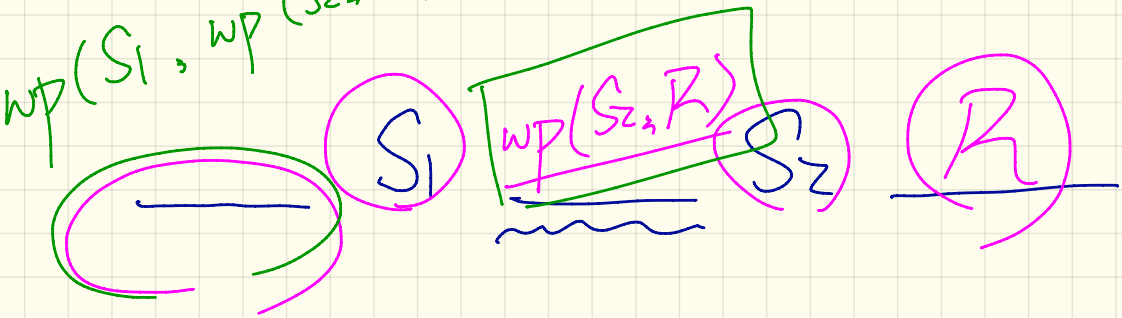
2. Prove or disprove

$x > 0 \wedge y > 0 \Rightarrow$ wp

$$wp(S_1 ; S_2, R)$$

$$= wp(S_1, wp(S_2, R))$$

$wp(S_1, wp(S_2, R))$



Correctness of Program : Sequental Composition

Is { ***True*** } `tmp := x; x := y; y := tmp` { $x > y$ } correct?

Q: Swap x and y without using a temp variable.

$x = x + y - x$

$y =$