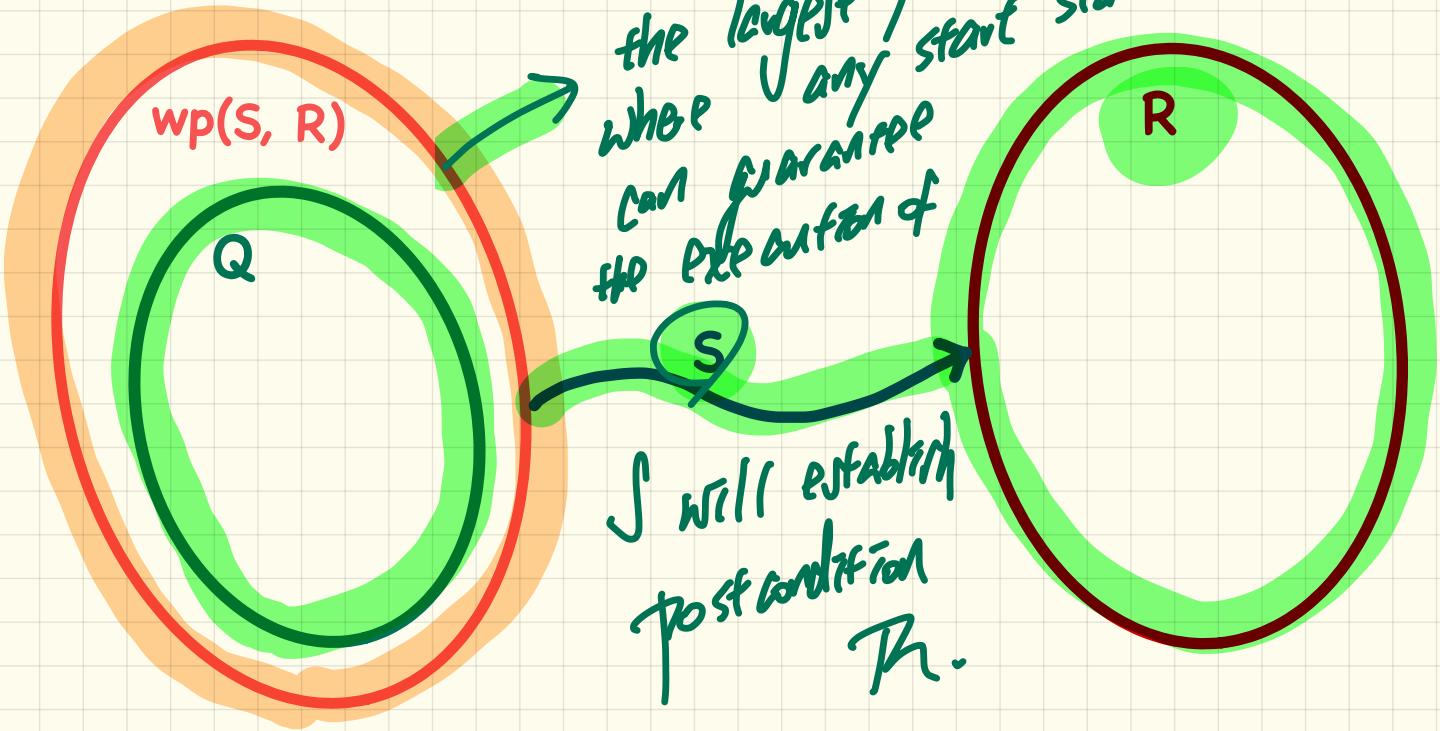
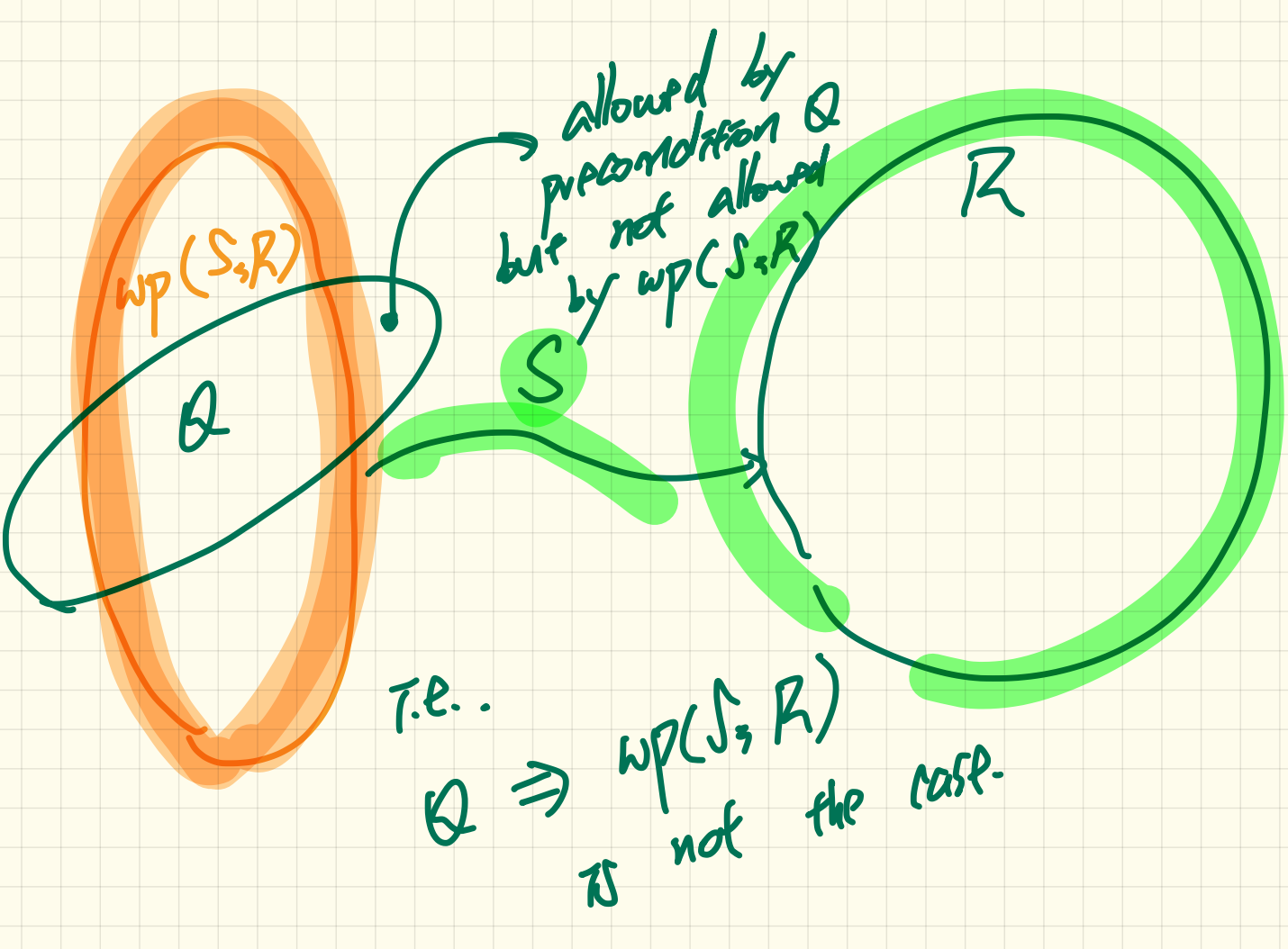
Lecture 23

Thursday November 28

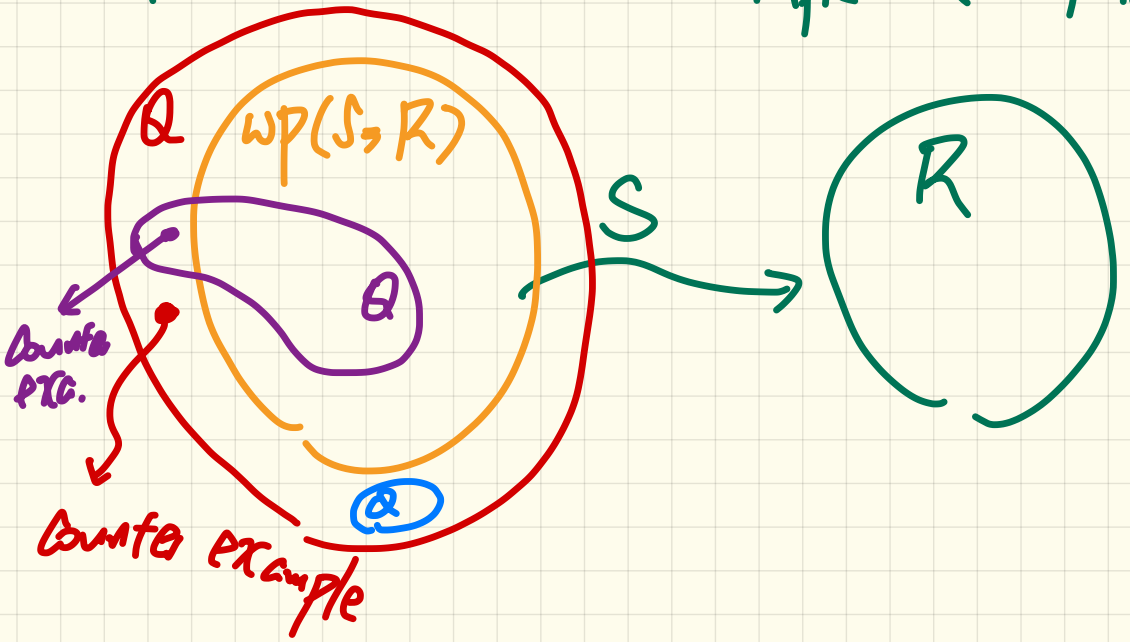
Hoare Triple as a Predicate

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




wp(S,R)
Q
allowed by precondition Q but not allowed by wp(S,R)
S
R
i.e..
Q ⇒ wp(S, R)
is not the case.

How can a Hoare Triple be false?



Program Correctness: Revisiting Example (1)

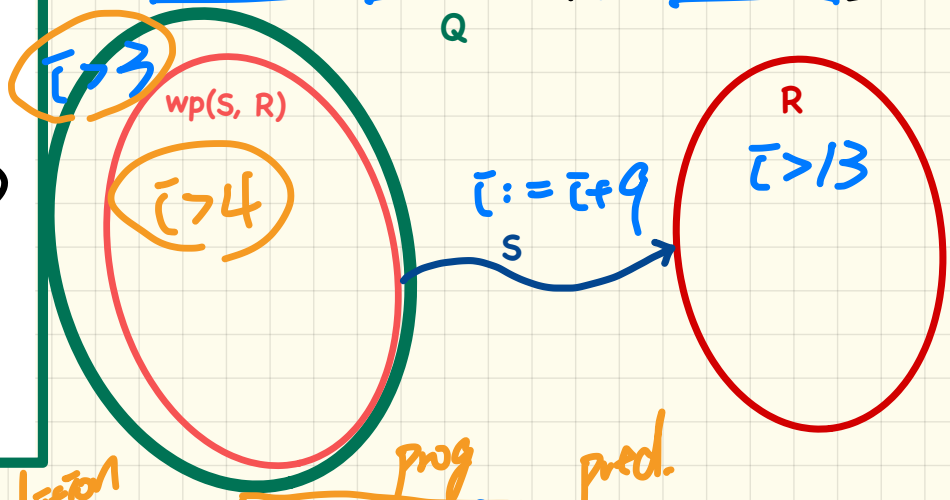
the resp. $i > 3 \Rightarrow i > 4$ is not

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

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

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

Q



weakest precondition

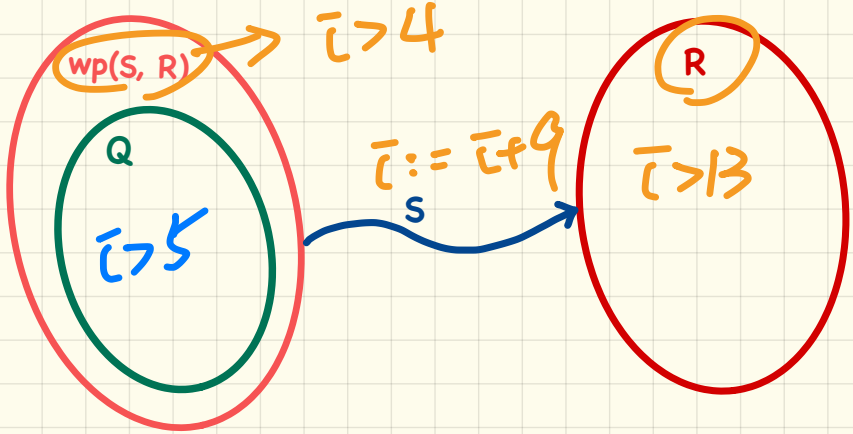
$wp(\underbrace{i := i + 9}_{\text{prog}}, \underbrace{i > 13}_{\text{pred.}}) = i > 4$

Program Correctness: Revisiting Example (2)

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

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

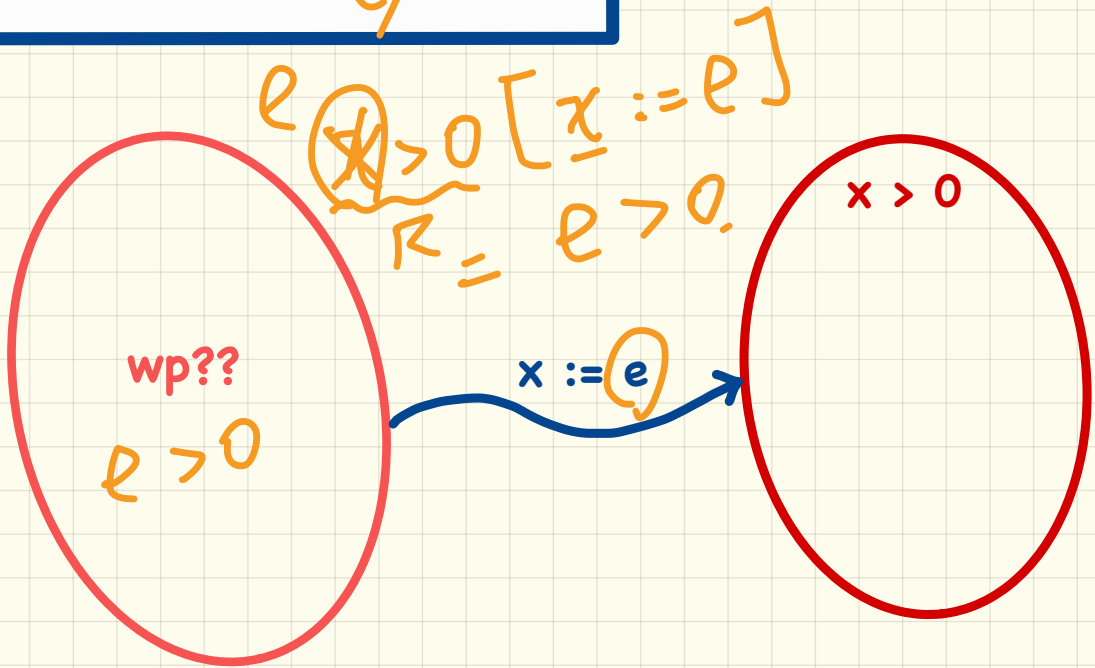
$\{i > 5\}\ i := i + 9\ \{i > 13\}$



$wp(i := i + 9, i > 13) = i > 4$

Rules of Weakest Precondition: Assignment

$$wp(x := e, R) = R[x := e]$$



Correctness of Programs: Assignment (1)

What is the weakest precondition for a program `x := x + 1` to establish the postcondition $x > x_0$?

$$\{??\}\ \texttt{x := x + 1}\ \{x > x_0\}$$

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

$$= \{\ wp\ \text{rule for assign.}\ \}$$

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

$$= x_0 + 1 > x_0$$

$$= \text{True}$$

→ this program works for any precondition.

Correctness of Programs: Assignment (2)

What is the weakest precondition for a program `x := x + 1` to establish the postcondition $x > x_0$?

$\{Q\}$ `x := x + 1` $\{x = 23\}$

$x \geq 22$

Is this program correct?

1. Calculate $wp(x := x+1, x = 23)$

$= \{$ wp rule for assign. $\}$

$x = 23 [x := x+1] = x+1 = 23$

$x = 22$

!!!

2. Prove $x \geq 22 \Rightarrow wp(x := x+1, x = 23)$

given precond.

wp

not the case e.g. $x = 23$

Rules of Weakest Precondition: Conditionals

wp(if B then S1 else S2 end, R)

$B \Rightarrow wp(S_1, R)$

$\vee$

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

vs.

$B \Rightarrow wp(S_1, R)$

$\wedge$

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

??

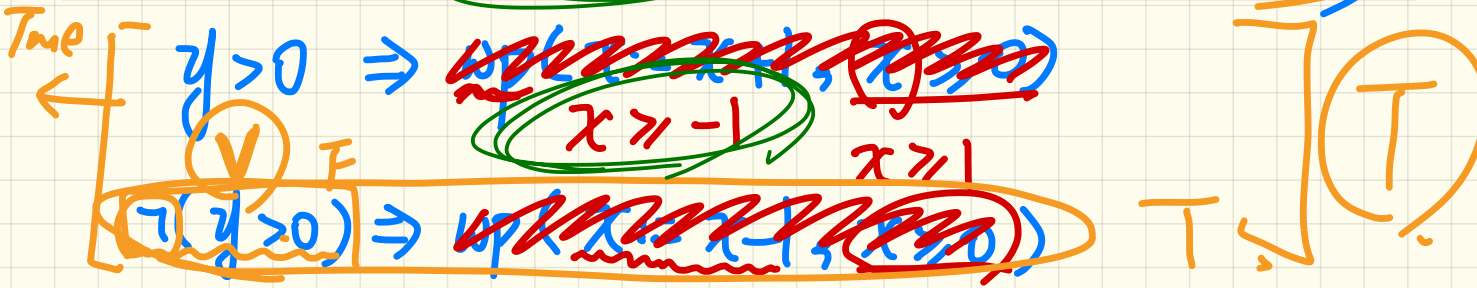
Consider:

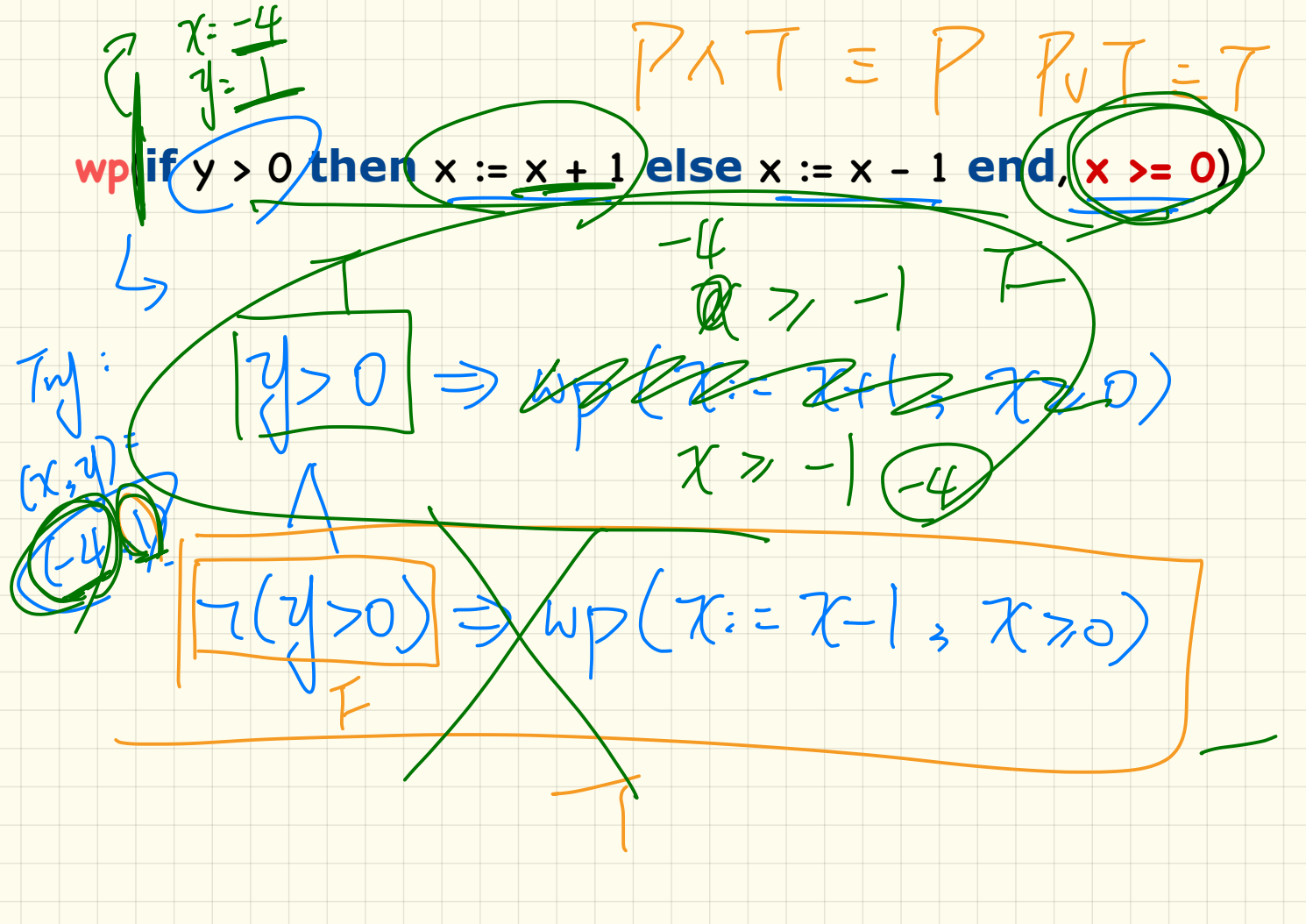
(x, y)

(-4, 1)

$x - 1 \geq 0$ $\quad x + 1 \geq 0$

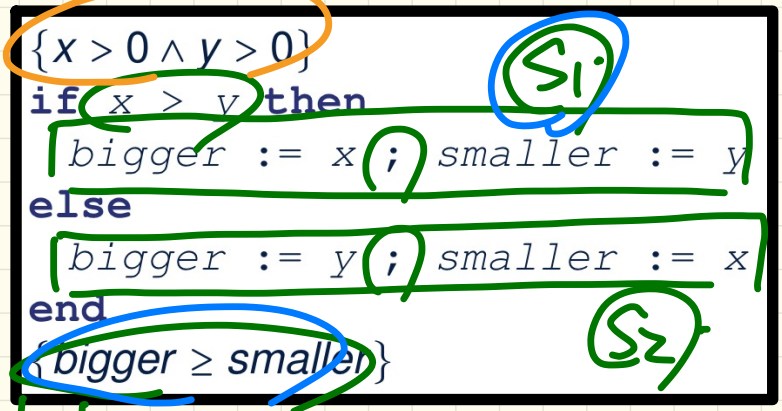
wp(if y > 0 then x := x + 1 else x := x - 1 end, x >= 0)




x := -4
y := 1
P ∧ T ≡ P
P ∨ T ≡ T
wp(if y > 0 then x := x + 1 else x := x - 1 end, x >= 0)
-4
x >= -1
T
Try:
y > 0 ⇒ wp(x := x+1, x >= 0)
x >= -1
-4
(x, y) =
(-4, 1)
A
¬(y > 0) ⇒ wp(x := x-1, x >= 0)
F
T

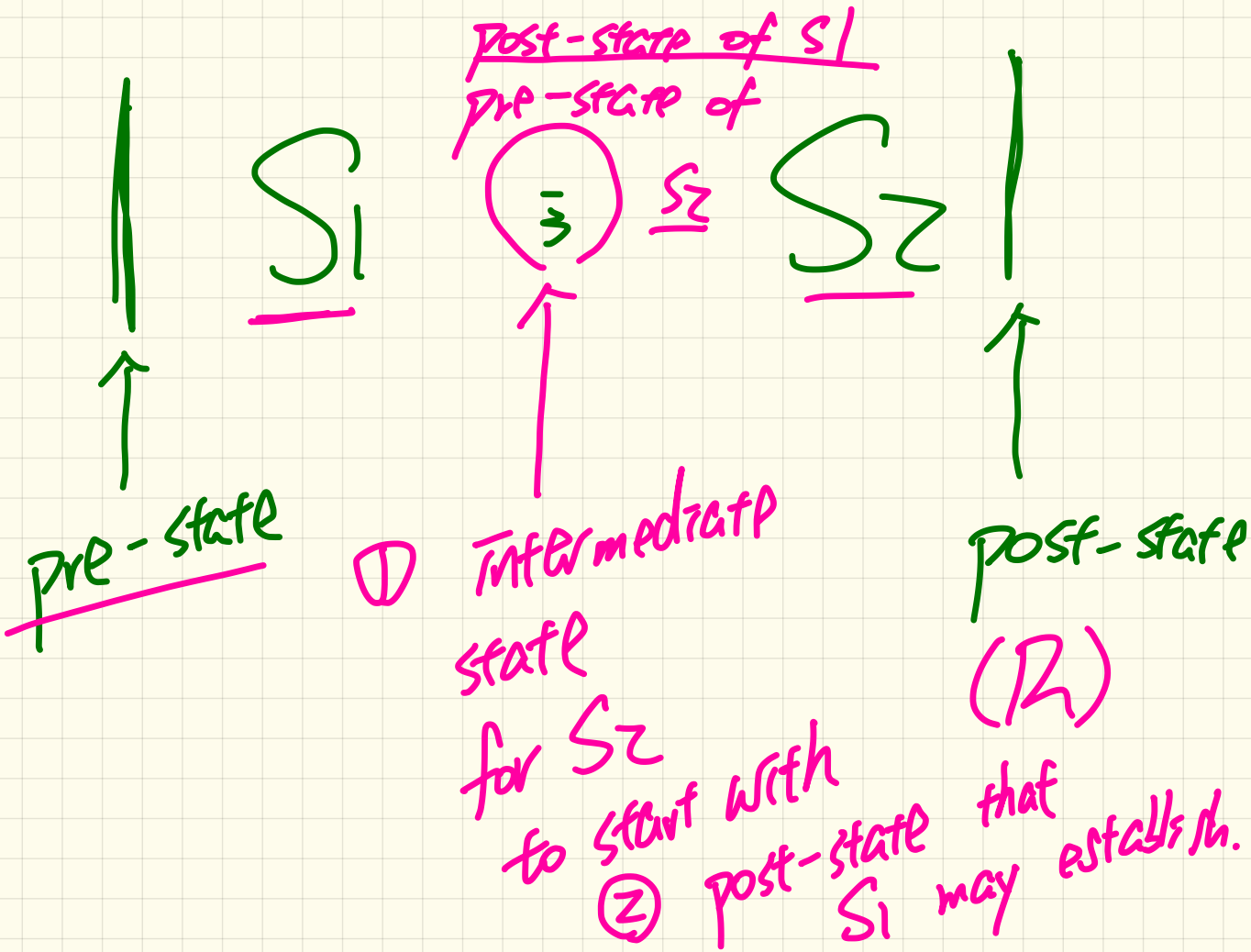
Correctness of Programs: Conditionals

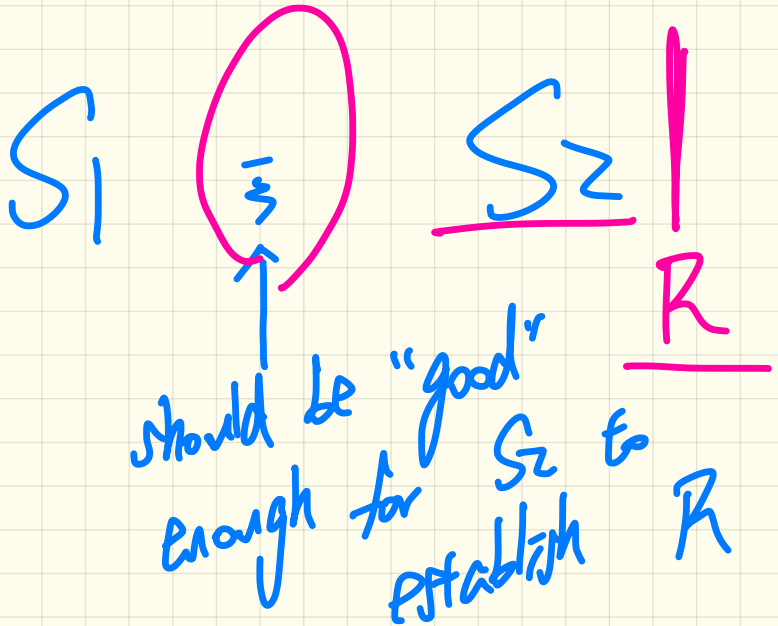
Is this program correct?



2. Prove or disprove:
$x>0 \wedge y>0 \Rightarrow wp.$

1. Calculate
$wp(\text{if } x>y \text{ then } S_1 \text{ else } S_2 \text{ end}, b \geq s)$
= { wp rule for conditionals }
$x>y \Rightarrow wp(S_1, b \geq s)$
$\wedge$
$\neg(x>y) \Rightarrow wp(S_2, b \geq s)$


Post-state of S1
pre-state of
S1
S2
S2
pre-state
① Intermediate state for S2 to start with
② post-state that S1 may establish.
post-state
(R)



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

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

$$wp(S_1 ; \underline{S_2} ; S_3, R)$$

$$= wp(S_1, wp(S_2, wp(S_3, R)))$$

Correctness of Programs: Sequential Composition

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

① Calculate $wp(tmp := x;\ x := y;\ y := tmp,\ x > y)$

$= \{$ wp rule of ; $\}$

$wp(tmp := x,\ wp(x := y;\ y := tmp,\ x > y))$

$= \{$ wp rule of ; $\}$

$wp(tmp := x,\ wp(x := y,\ wp(y := tmp,\ x > y)))$

Numbers

Swap x and y

without using an intermediate variable.