

Wednesday April 3
Lecture 23

Makeup Lecture

Friday
April 5

2pm

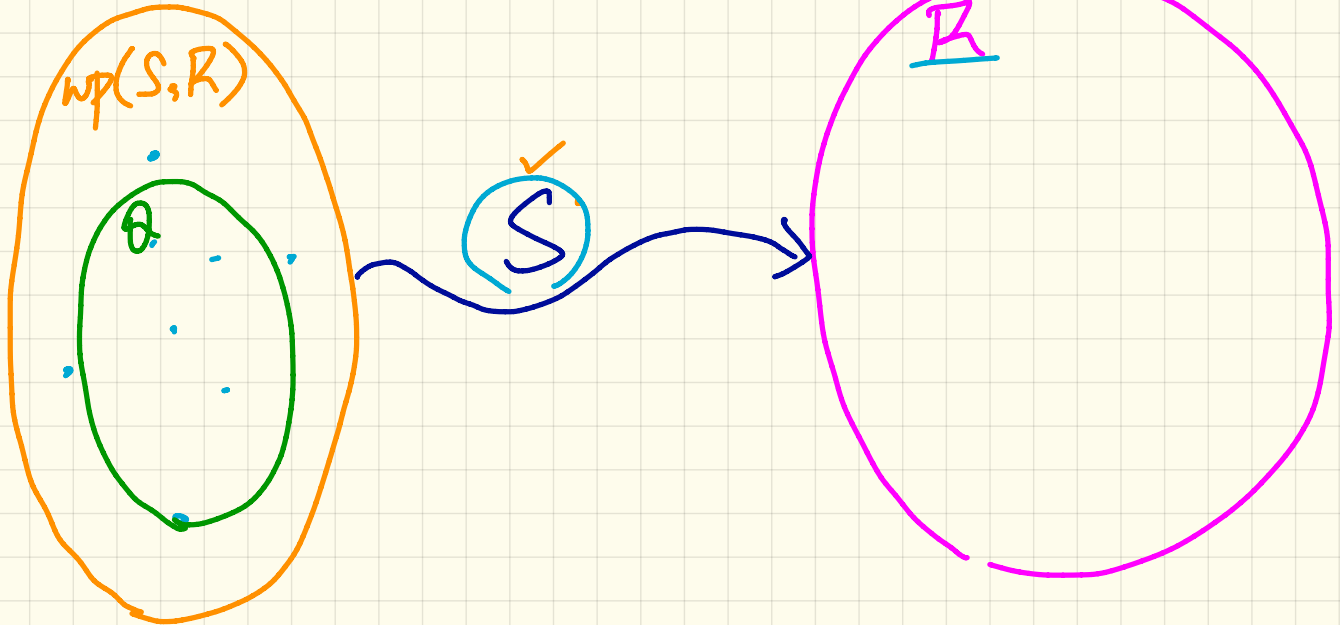
~ 4pm

CAS B

Hoare Triple as a Predicate

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

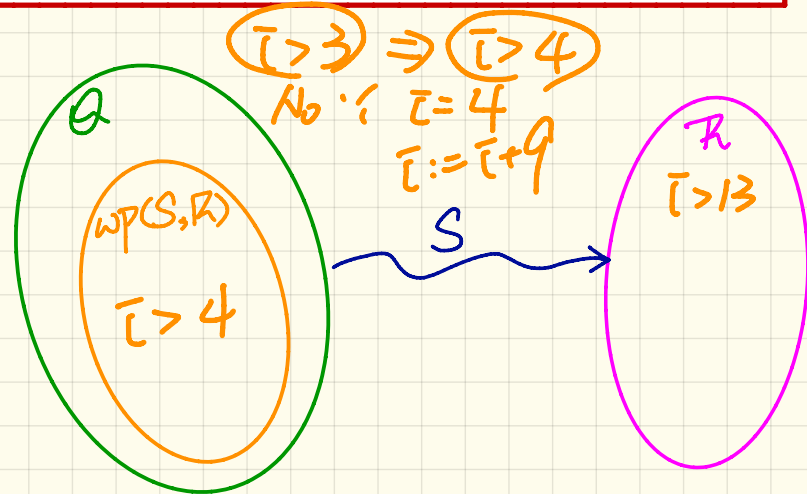
The diagram shows the Hoare triple $\{Q\} S \{R\}$ and its equivalence to the predicate $Q \Rightarrow wp(S, R)$. The components are color-coded: Q is green, S is blue, and R is pink. The entire expression is enclosed in a red box. Checkmarks are placed above Q , S , and R . A double-headed arrow indicates the equivalence between the two forms. The $wp(S, R)$ part of the second form is circled in orange.



Program Correctness: Example (1)

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

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

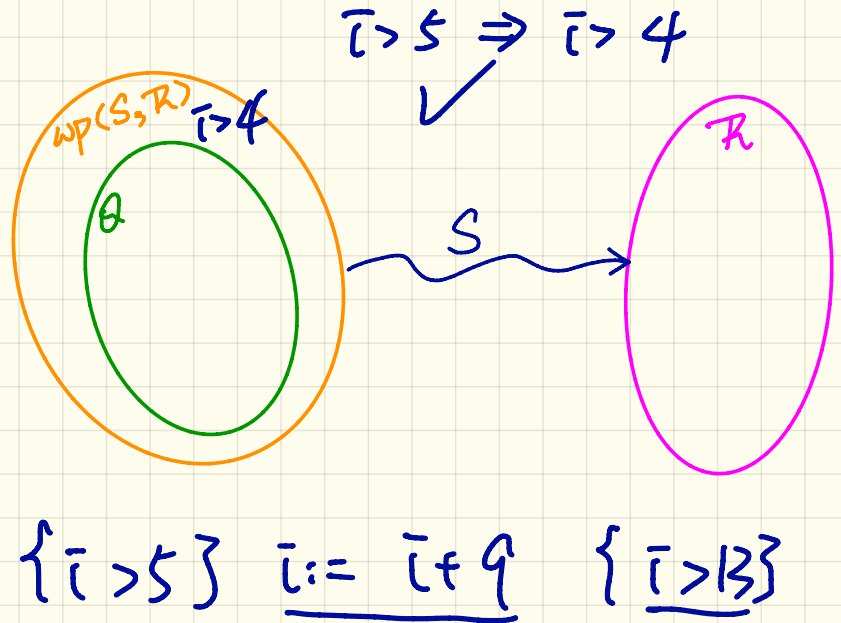


$$\{i > 3\} \quad i := i + 9 \quad \{i > 13\}$$

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 (S , R)

① :=

② if then else

③ — → —

↓
④ from · until · loop · end

post-condition
predicate

1. pre-state

2. post-state

Precondition

pre-state
 $x_0 > 4$

$$\text{WP} \left(\underbrace{x}_{\text{pre-state}} := \underbrace{x}_{\text{pre-state}} + 9 \rightarrow \underbrace{x > 13}_{\text{post-state}} \right)$$

$$\cancel{x} > 13$$

$$\underline{x_0 + 9}$$

$$\underline{x_0 > 4}$$

$$\text{wp} (x := \overset{-1}{2} x + \overset{0}{3}, x > x_0)$$

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

$$\underline{x} > x_0 [x := \underline{x_0 + 1}]$$

$$= \{ \text{substitution} \}$$

$$\cancel{x_0} + 1 > \cancel{x_0} =$$

True

any x being incremented
- will become larger

$$\text{wp} (x := x + 1, x < x_0)$$

$$= \{ \dots \}$$

$$\underline{x} < x_0 \left[x := \underline{x_0 + 1} \right]$$

$$x_0 + 1 < x_0$$

$$1 < 0$$

False.

When wp is true,

any precondition ^Q would be correct

$\therefore Q \Rightarrow \text{true} \equiv \text{true}$

When wp is false

only precondition false is correct *but useless*

$\therefore \text{false} \Rightarrow \text{false} \equiv \text{true}$

$$\{x \geq 22\} \quad x := x + 1 \quad \{x = 23\}$$

$$\text{wp}(x := x + 1, x = 23)$$
$$= \boxed{x = 22}$$

$$\{x \geq 22\} \Rightarrow x = 22$$

$$x = 23$$

$$P \Rightarrow Q$$

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

$$\rightarrow B \Rightarrow \text{wp}(S_1, R)$$

$$\neg V \quad \times$$

$$\neg B \Rightarrow \text{wp}(S_2, R)$$

Rule of wp: Conditionals

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

$$\begin{aligned}
 & B \Rightarrow \text{wp}(S_1, R) \\
 & \vee \\
 & \neg B \Rightarrow \text{wp}(S_2, R)
 \end{aligned}$$

$$\begin{aligned}
 & B \Rightarrow \text{wp}(S_1, R) \\
 & \wedge \\
 & \neg B \Rightarrow \text{wp}(S_2, R)
 \end{aligned}$$

vs.

??

$$\begin{aligned}
 x &= -1 \\
 y &= -1
 \end{aligned}$$

$$x + 1 > 0$$

Consider:

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

Counter example
 $\begin{aligned} & \bar{y} \\ & \bar{x} = -1 \end{aligned}$

$$y > 0 \Rightarrow \text{wp}(x := x + 1, x \geq 0)$$

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

$$\begin{aligned}
 x &= -1 \\
 \downarrow x := x - 1 \\
 x &= -2
 \end{aligned}$$

Correctness of Program: Conditionals

Is this program correct?

```
{x > 0 ∧ y > 0} → B  
if x > y then S1  
  bigger := x; smaller := y  
else S2  
  bigger := y; smaller := x  
end  
{bigger ≥ smaller}
```

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

$$\begin{aligned} & wp(\text{if } B \text{ then } S_1 \text{ else } S_2 \text{ end}, \text{bigger} \geq \text{smaller}) \\ &= \{ wp \text{ w.r.t. for alternation} \} \end{aligned}$$

$$x > y \Rightarrow wp(S_1, \text{bigger} \geq \text{smaller})$$

$$\wedge x \leq y \Rightarrow wp(S_2, \text{bigger} \geq \text{smaller})$$

$\cdot S_1 \circ S_2 \circ R$

$WP(S_1 \rightarrow \underline{S_2}, \underline{R})$

=

$WP(S_1 \rightarrow \underline{WP(S_2, R)})$