Lecture 22

Wednesday Nov. 29

Program:

```
inc_by_9
  require $i > 3$
          $i > 5$
  do
    $i := i + 9$
  ensure
    $i > 13$
  end
```

Is this correct? $i > 3$ No e.g. $i = 4$

4. $i > 3$

$i > 5 \Rightarrow i > 4$ □

existing Proved wp □

1. Translate Prog. into Hoare Triple

$i > 3$

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

2. Prove existing precond. $i > 5$ is no weaker than

$i > 3$

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

3. Calculate $wp(i := i + 9, i > 13)$

$wp(i := i + 9, i > 13)$ pre-state

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

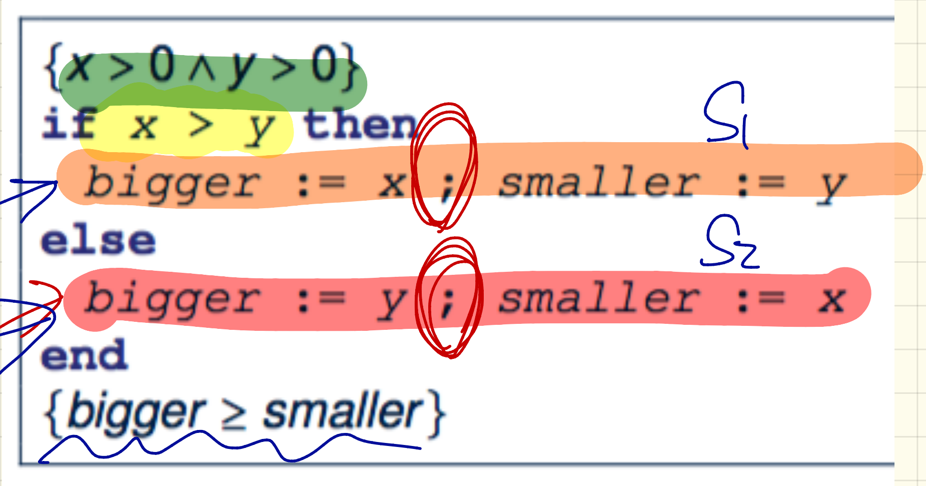
$i > 13\ [i := i_0 + 9]$ Post-state value

$= \{ \text{subs.} \}$

$i_0 + 9 > 13$

$= \{ \text{simp.} \}$

$i_0 > 4$ ← wp for $i := i + 9$ to establish $i > 13$



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

$$\{x>0 \land y>0 \land x>y\}\ S_1\ \{bigger \geq smaller\}$$

$$\land$$

$$\{x>0 \land y>0 \land \neg(x>y)\}\ S_2\ \{bigger \geq smaller\}$$

$wp(x := 3, x > 0) = T$

$x := -2$

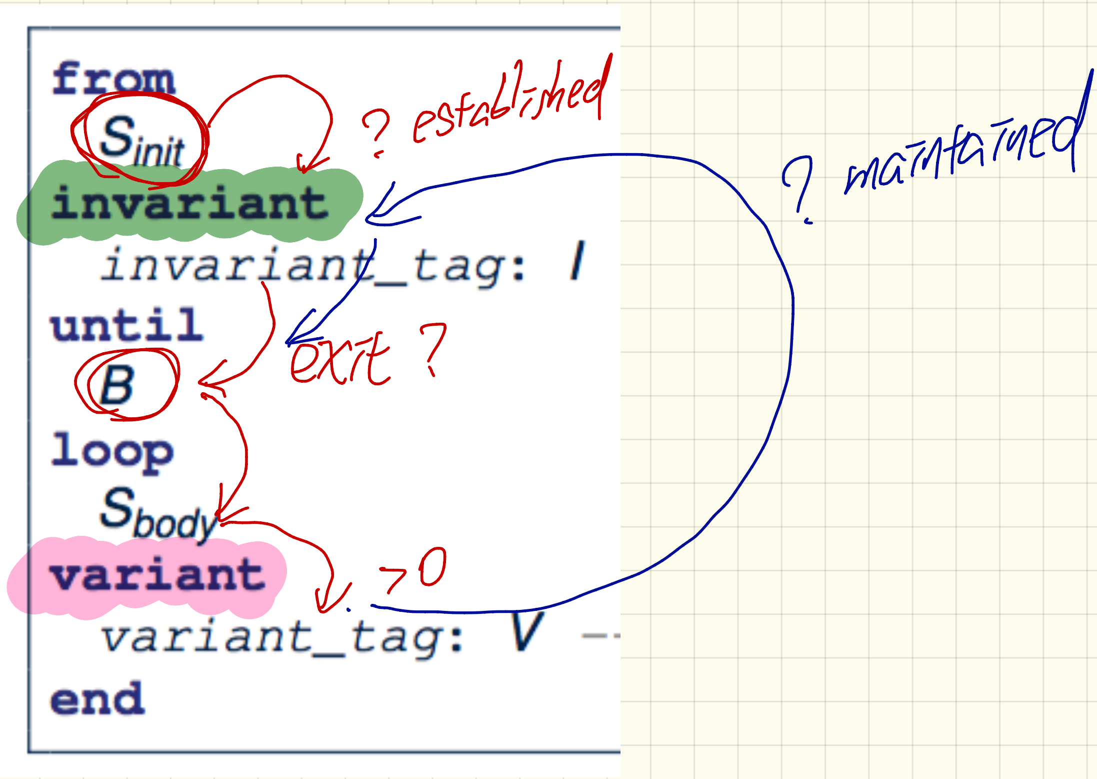
$$wp(\underbrace{\text{if } B \text{ then } S_1 \text{ else } S_2 \text{ end}}_{prog},\ R) \quad F$$

$$= B \Rightarrow wp(S_1, R) \quad wp: T$$

$$\cancel{\vee} \ \wedge \quad T$$

$$\neg B \Rightarrow wp(S_2, R) \quad wp: F$$

```
if B then     T
    x := 3
else
    x := -2
end
{ x > 0 }
```



```
from
  S_init
invariant
  invariant_tag: I
until
  B
loop
  S_body
variant
  variant_tag: V --
end
```

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

what should be satisfied

(Starting precondition for S_2)

established by S_1

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

starting pointing of S_2

ending point of S_1

$$wp(S_1 \underset{\uparrow}{;} S_2 , R)$$

$$wp(S_1 ; \underbrace{wp(S_2 , R)}_{\text{starting condition for } S_2 \text{ to establish } R.})$$

$\{\mathit{True}\}\ tmp := x\ ;\ x := y\ ;\ y := tmp\ \{x > y\}$

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

$= \{\ wp \text{ for seq. comp.}\ \}$

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

$= \{\ wp \text{ for seq. comp.}\ \}$

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

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

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

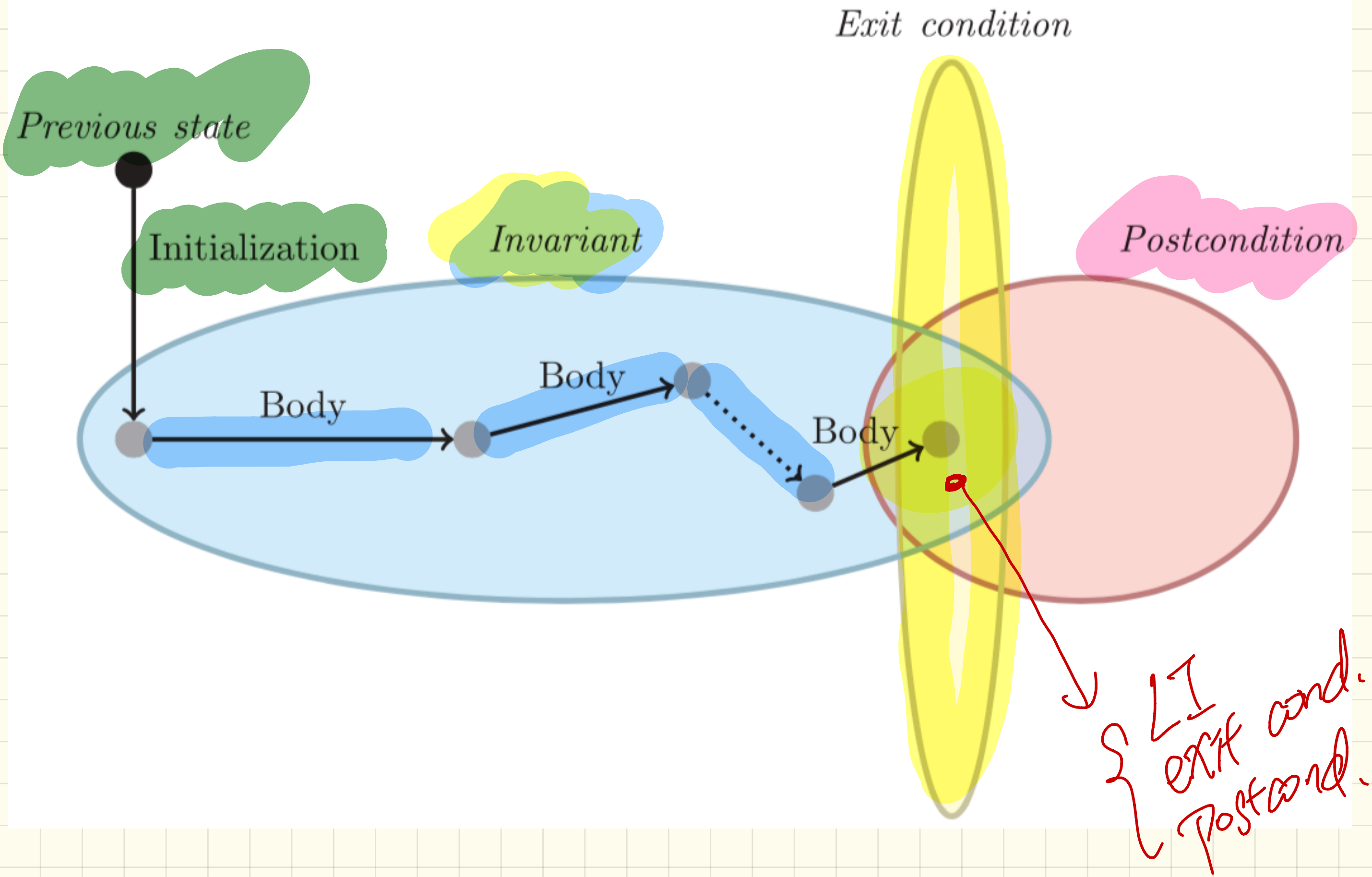
$x > tmp$

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

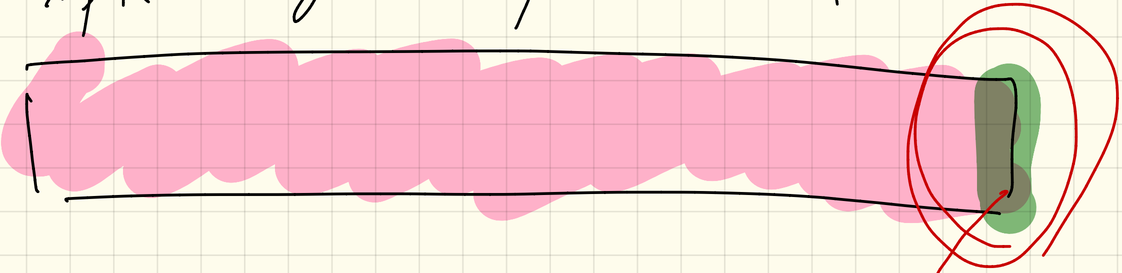
$wp(tmp := x,\ y > tmp) = y > x$

$[\mathit{True} \Rightarrow y > x$

X

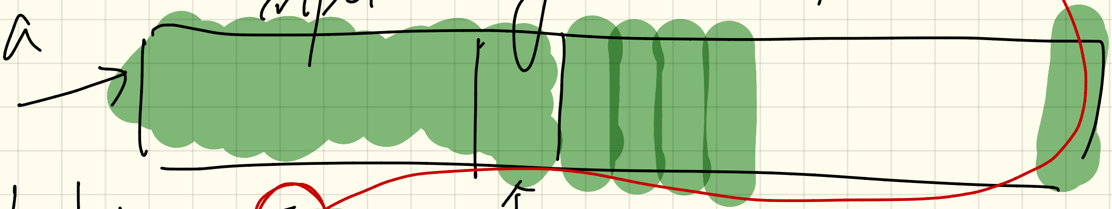

Exit condition
Previous state
Initialization
Invariant
Postcondition
Body
Body
Body
LI
exit cond.
Postcond.

input array : postcondition



Result

input array : Loop invariant



$\forall j \mid 1 \leq j < i,$

$Result \geq a[j]$ i loop counter

Result is max from $a[0], a[1], \ldots a[i]$