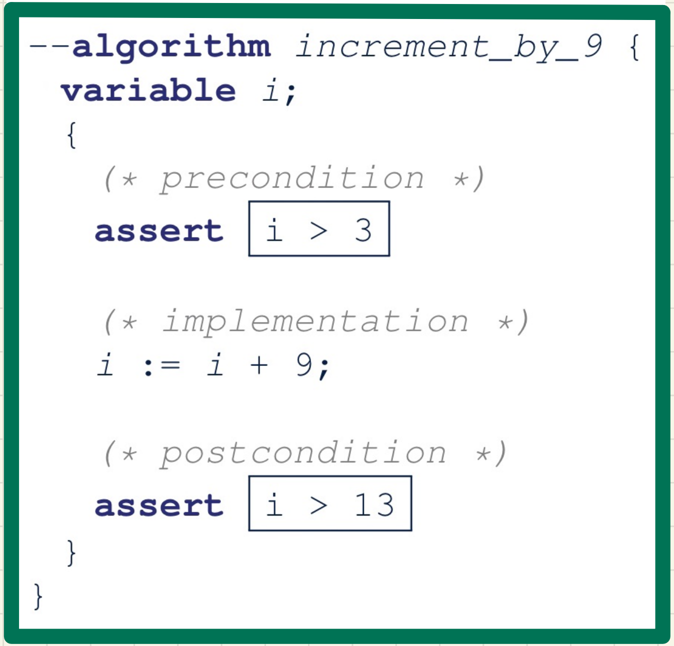
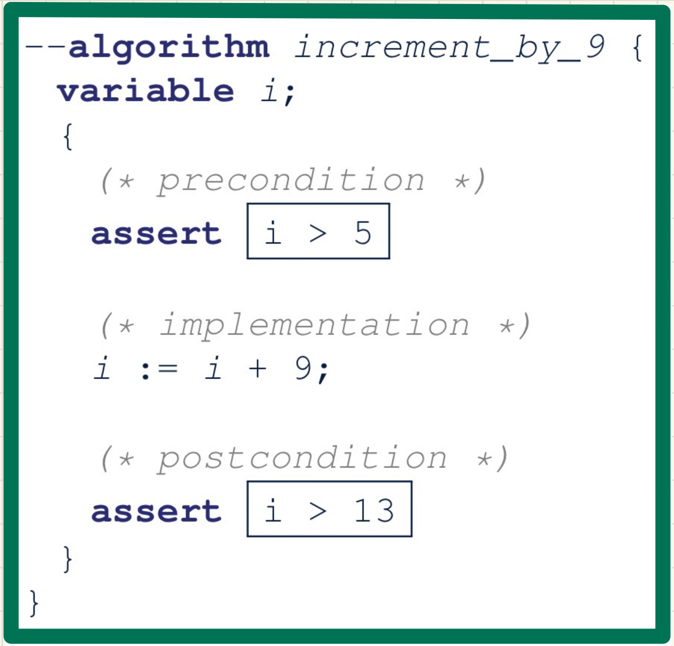
# Stronger vs. Weaker Assertions: Pre- vs. Post-Conditions

# Program Correctness: Example (1)



```
--algorithm increment_by_9 {
  variable i;
  {
    (* precondition *)
    assert i > 3

    (* implementation *)
    i := i + 9;

    (* postcondition *)
    assert i > 13
  }
}
```

# Program Correctness: Example (2)



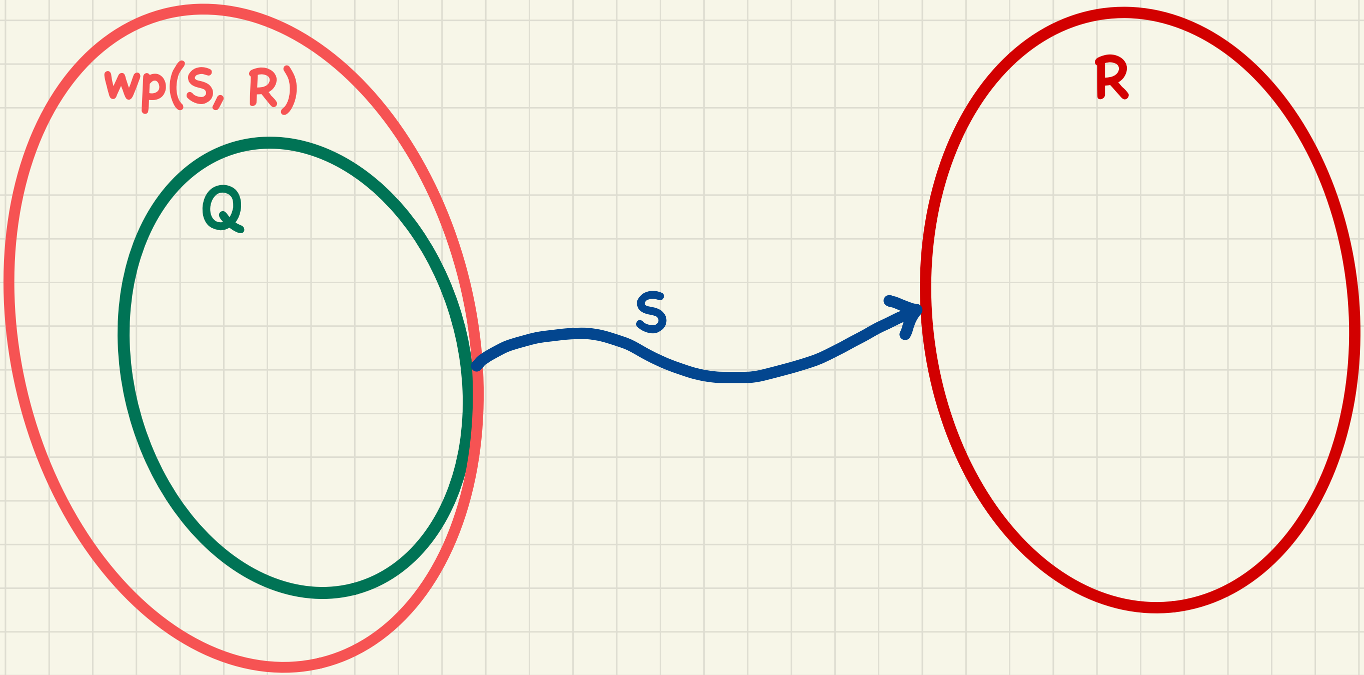
```
--algorithm increment_by_9 {
  variable i;
  {
    (* precondition *)
    assert  i > 5

    (* implementation *)
    i := i + 9;

    (* postcondition *)
    assert  i > 13
  }
}
```

# Hoare Triple: Syntax and Semantics

# Proving Algorithm Correctness via Hoare Triple

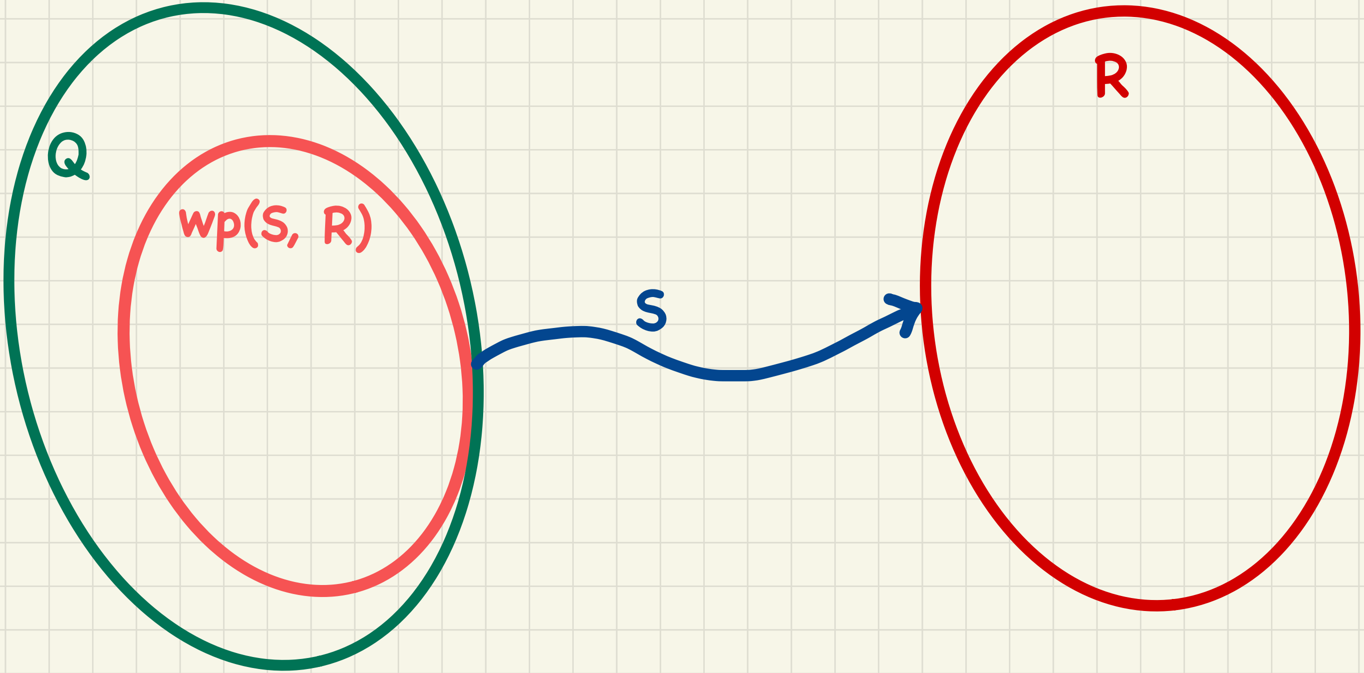
# Hoare Triple as a Predicate

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



# Hoare Triple: Incorrect Program

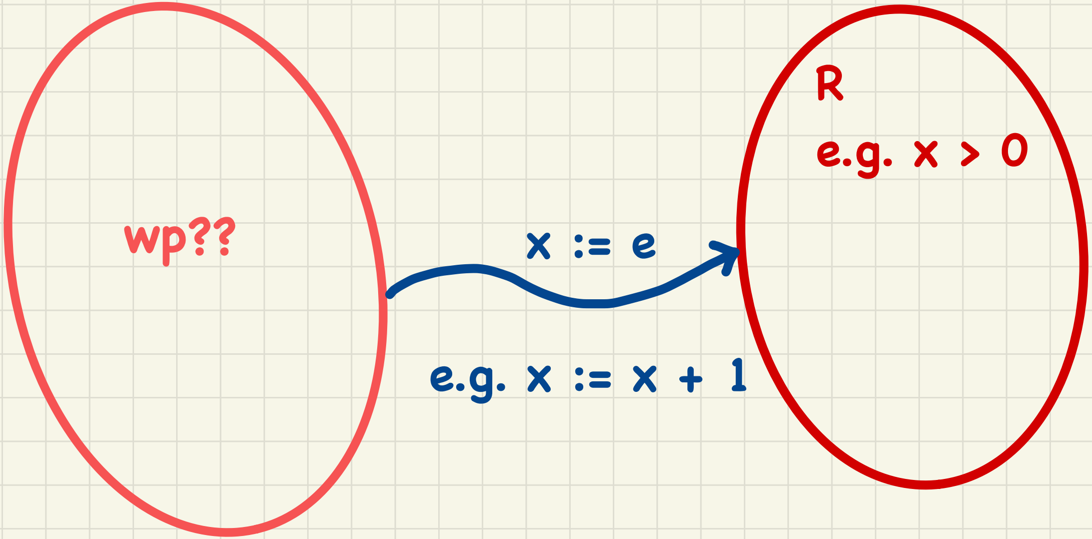
$$\boxed{\{Q\}\ \mathrm{S}\ \{R\} \equiv Q \Rightarrow wp(S, R)}$$



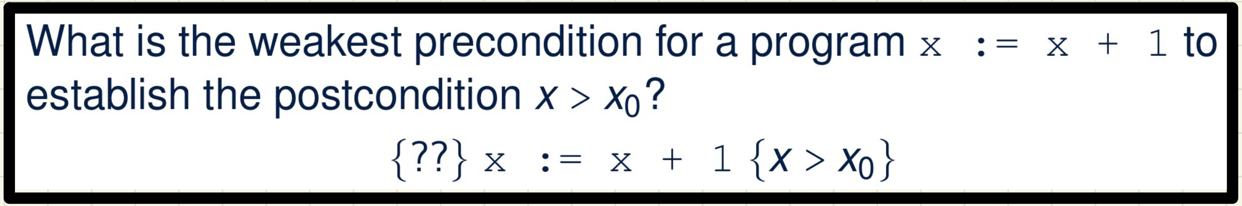
# Expressing Pre-State vs. Post-State Values

# Rules of Weakest Precondition: Assignment

$$\boxed{wp(x \;:=\; e,\; R) =}$$



# Correctness of Programs: Assignment (1)



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

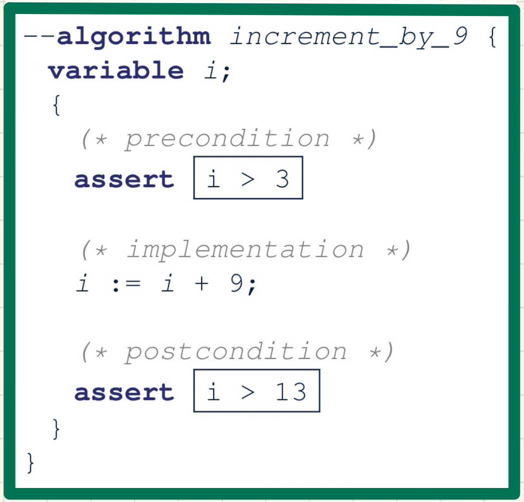
$$\{??\}\ \texttt{x := x + 1}\ \{x > x_0\}$$

# Correctness of Programs: Assignment (2)

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

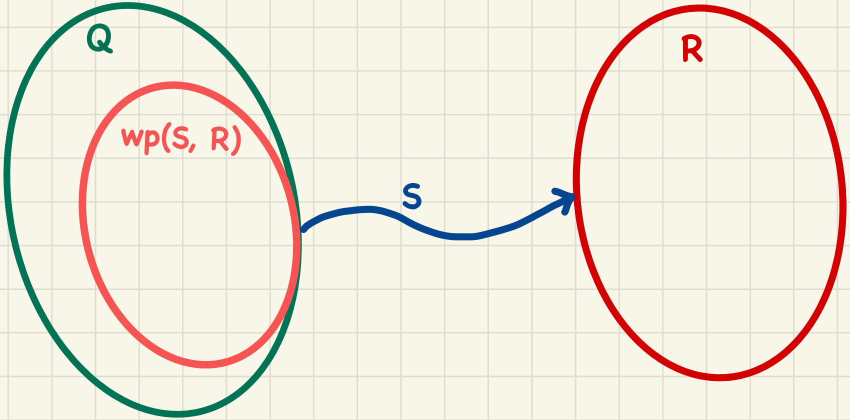
$$\{??\}\ \texttt{x := x + 1}\ \{x = 23\}$$

# Program Correctness: Revisiting Example (1)

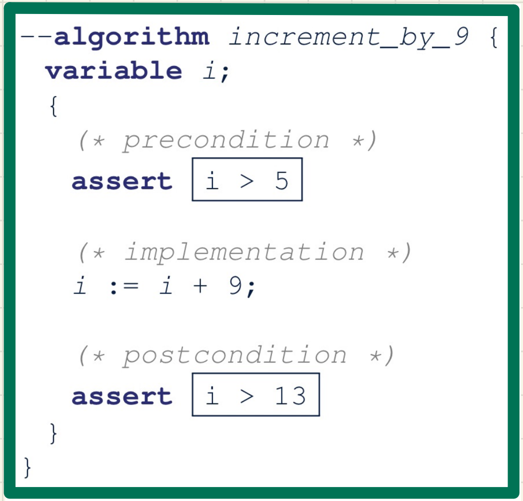


```
--algorithm increment_by_9 {
  variable i;
  {
    (* precondition *)
    assert  i > 3

    (* implementation *)
    i := i + 9;

    (* postcondition *)
    assert  i > 13
  }
}
```

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

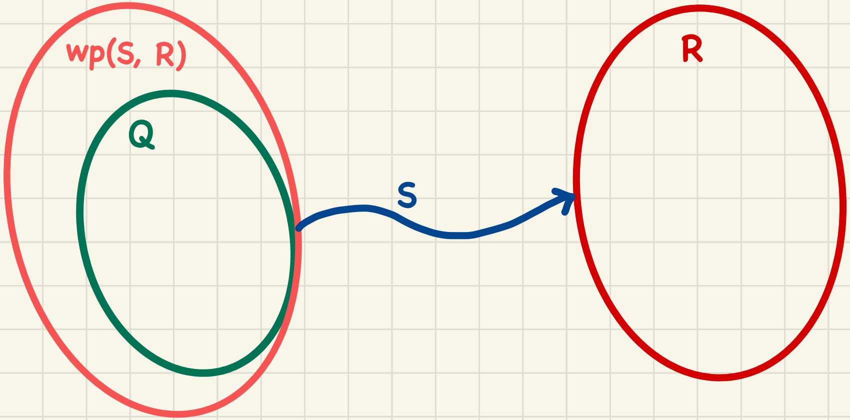


# Program Correctness: Revisiting Example (2)



```
--algorithm increment_by_9 {
  variable i;
  {
    (* precondition *)
    assert  i > 5

    (* implementation *)
    i := i + 9;

    (* postcondition *)
    assert  i > 13
  }
}
```

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

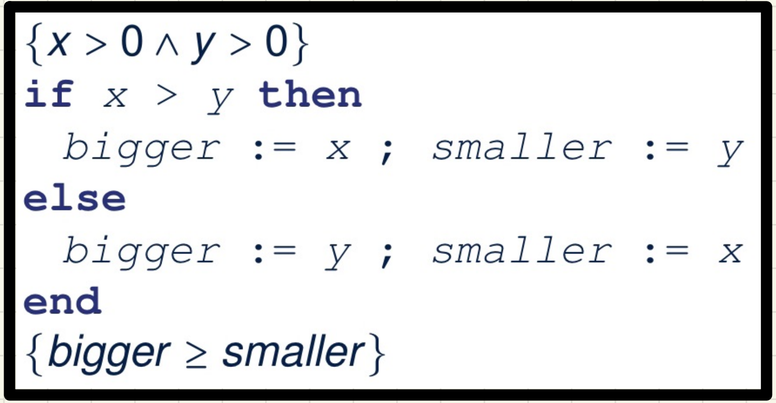


# Rules of Weakest Precondition: Conditionals

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

# Correctness of Programs: Conditionals

## Is this program correct?



```
$\{x > 0 \wedge y > 0\}$
if x > y then
  bigger := x ; smaller := y
else
  bigger := y ; smaller := x
end
$\{bigger \geq smaller\}$
```