Lecture 17

- assert $(x \geq 7)$;

- "Program state": Program counter / line of code
  Value of each variable

① $x := input()$

② $y := x + x$ $\leftarrow$ (③ $\{x \mapsto 3 \quad y \mapsto 6\}$)

③ while $x > 0$ $\leftarrow$ (④ $\{x \mapsto 3 \quad y \mapsto 6\}$) (④ 2 5)

④ $x := x - 1$ (④ 1 4)

⑤ $y := y - 1$ (⑥ 0 3)

⑥ fin!

$$\frac{e(\sigma) = v}{\sigma \xrightarrow[x:=e]{} \sigma[x \mapsto v]}$$

- assert $(X \geq 7)$ / "Predicate"

(② $\{X \mapsto 8, y \mapsto 16\}$) ✓

(③ $\{X \mapsto 4, y \mapsto 18\}$) ✗

"Hoare triple"

$\{\varphi\}\ P\ \{\psi\}$

$\{\varphi\}$ ← Precondition

↓

P

↓

$\{\psi\}$ ← Postcondition

"If φ holds when we start executing P, if P terminates, then ψ will hold."

The Hoare triple $\{\varphi\}\ P\ \{\psi\}$ is valid if

Ex:

$\{x \geq 8\}$

$y = x + 1;$

$\{y \geq 9\}$ ✓

$\{x = y + 2\}$

$x := x + 1$

$y := y + 3$

$\{x = y + 4\}$ ✓

$\{true\}$

if $x < y$

$z = x$

$x = y$

$y = z$

Swapping the contents of x & y

✓ $\{x \geq y\}$ ✓

$\{x \geq y\}$

if $x < y$

$y := y + 1$

$\{x < y\}$

X

Safety / Partial correctness

$\{x \geq 5\}$

while $(x > 0)$

  $x := x + 1$

$\{x < 3\}$

Valid

Liveness / Termination Checking

Checking function totality.

$\{x = 3\}$	$\{false\}$	$\{\varphi\}$
$x := 8$	$x := 8$	P
$\{x = 3\}$	$\{x = 3\}$	$\{true\}$
Invalid	Valid	Valid

$\{\varphi\}$

P

$\Rightarrow \{false\}$

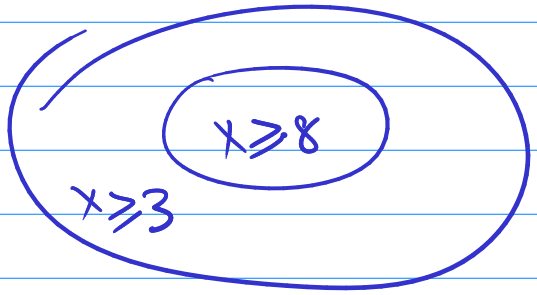
$\Leftrightarrow$ "Program P does not terminate"

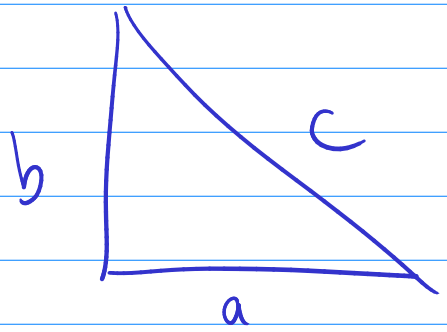
"This line of code is never reached".

assert (false)

$\{x \geq 8\} \Longrightarrow \{x \geq 3\}$

strong weak.



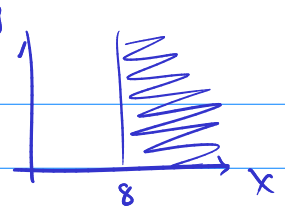


Claim 1: If a, b, c are the sides of a right triangle, then $c^2 \geq a^2 + b^2$

Claim 2: If a, b, c are the sides of a right triangle, then $c^2 \leq a^2 + b^2$

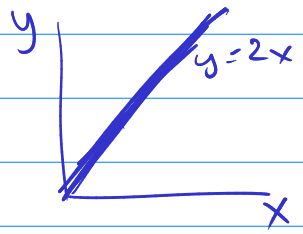
Claim 3: If a, b, c are the sides of a rt. $\triangle$ then $c^2 = a^2 + b^2$.

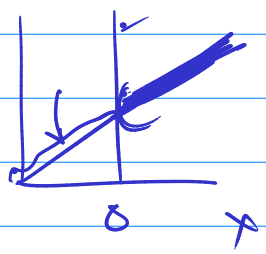
$\{x \geq 8\}$



$y = x + x$

$\{ \quad \}$





Q1 Does it make sense to speak of $\{x \geq 8 \text{ and } y = 2x\}$ the strongest post condition? ← Yes, $\{y = 2x\}$

[weakest post condition? ← Yes, $\{\text{true}\}$]

Ex · $\{z = 3x \text{ and } y = 2x\}$

$x = w$

$\{ \quad \}$

What is the strongest post condition?

$x = w$ and $z = 1.5y$

$x = w$ and $\exists x_0 \cdot z = 3x_0$ and $y = 2x_0$

Q2: What about strongest preconditions?
weakest preconditions?

$\{ \_\_\_ \}$

$y = x + 8$

$\{ y \geq 16 \}$

Proposal 1: Weakest precondition = true

$\{ true \}$

$y = x + 8$ ✗

$\{ y \geq 16 \}$

Proposal 2 Weakest precondition = false

Proposal 3

Strongest precondition

//

false

↑

False is actually the strongest claim one can make about the world

Proposal 4:

$\{x \geq 8\}$ ← Weakest precondition.

$y = x + 8$

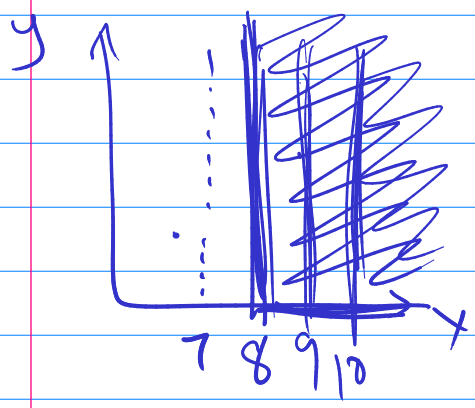
$\{y \geq 16\}$

Proposal 5:

$\{y \geq 16\}$ ← Weakest precondition

$y = x + 8$

$\{y \geq 16\}$



$\{x + 8 \geq 16\}$

$y = x + 8$

$\{y \geq 16\}$

Claim: The weakest precondition of ψ wrt the assignment $x := e$ is the predicate $\psi[e/x]$.

In ψ, replace every occurrence of x with e

Axiomatic Semantics

Claim: $\{\varphi[e/x]\}$

$x := e$

$\{\varphi\}$

is always a valid Hoare triple.

$\{z+2 \geq x+3\}$ $\quad \varphi[e/x]$

$x := y := z+2$ ~ e

$\varphi = \{y \geq x+3\}$

$\varphi[z+2/y]$

$= \{z+2 \geq x+3\}$

Where I see y in φ, I substitute $z+2$

Ex: 2 years from now twice of Xavier's age will be four more than his age. How old is he now?

$\{2(x+2) = (x+2)+4\}$

$x := x+2$

$\{2x = x+4\}$

$\Longleftrightarrow$

$\{2x+4 = x+6\}$

$\Longleftrightarrow$

$\{x = 2\}$

Claim 2: If Xavier is 2 years old today, then the problem constraints are satisfied

Claim 1: If the problem constraints are satisfied, then Xavier is 2 years old today.

Assuming P always terminates.

Claim: φ is the w.pre of ψ wrt P

iff

ψ is the s.post of φ wrt P

Ex: $\{x \geq 3\}$ $\{x \geq 4\}$

$x = 2x$ $x = 2x$

$\{x \geq 6\}$ $\{x \geq 8\}$

The strongest post c is always dependent on the pre c chosen.

The weakest pre c is always dependent on the post c chosen.

"The weakest precondition of ψ wrt P is φ if $\{\varphi\}\ P\ \{\psi\}$ holds & $\forall$ all valid triples $\{\varphi'\}\ P\ \{\psi\}$

$\varphi' \Rightarrow \varphi$"

The strongest post condition of φ wrt P is ψ if $\{\varphi\}\ P\ \{\psi\}$ is a valid triple & $\forall$ valid triples $\{\varphi\}\ P\ \{\psi'\}$

$$\psi \Rightarrow \psi'.$$

Claim: Say $\varphi' \Rightarrow \varphi$ & $\{\varphi\}\ P\ \{\psi\}$ is valid

Then $\{\varphi'\}\ P\ \{\psi\}$ is also valid

Claim: Say $\{\varphi\}\ P\ \{\psi\}$ is valid & $\psi \Rightarrow \psi'$

Then $\{\varphi\}\ P\ \{\psi'\}$ is also valid.