Precondition Strengthening

\[ (P \Rightarrow P') \quad (P') \quad C \{Q\} \]
\[ \{P\} \quad C \{Q\} \]

- Meaning: If we can show that \( P \) implies \( P' \) (i.e. \( P \Rightarrow P' \)) and we can show that \( \{P\} \quad C \{Q\} \), then we know that \( \{P\} \quad C \{Q\} \)
- \( P \) is stronger than \( P' \) means \( P \Rightarrow P' \)

\[ (x > 0 \land x < 5) \quad x := x \times x \quad \{x < 25\} \]
\[ (x = 3) \quad x := x \times x \quad \{x < 25\} \]

\[ (x = 3) \quad x := x \times x \quad \{x < 25\} \]
\[ (x > 0 \land x < 5) \quad x := x \times x \quad \{x < 25\} \]

\[ (x > 0 \land x < 5) \quad x := x \times x \quad \{x < 25\} \]
\[ (x = 3) \quad x := x \times x \quad \{x < 25\} \]

\[ (x = 3) \quad x := x \times x \quad \{x < 25\} \]
\[ (x > 0 \land x < 5) \quad x := x \times x \quad \{x < 25\} \]

\[ (x > 0 \land x < 5) \quad x := x \times x \quad \{x < 25\} \]
\[ (x = 3) \quad x := x \times x \quad \{x < 25\} \]

\[ (x > 0 \land x < 5) \quad x := x \times x \quad \{x < 25\} \]
\[ (x = 3) \quad x := x \times x \quad \{x < 25\} \]

\[ (x > 0 \land x < 5) \quad x := x \times x \quad \{x < 25\} \]
\[ (x = 3) \quad x := x \times x \quad \{x < 25\} \]

\[ (x > 0 \land x < 5) \quad x := x \times x \quad \{x < 25\} \]
\[ (x = 3) \quad x := x \times x \quad \{x < 25\} \]

\[ (x > 0 \land x < 5) \quad x := x \times x \quad \{x < 25\} \]
\[ (x = 3) \quad x := x \times x \quad \{x < 25\} \]
Which Inferences Are Correct?

\[
\begin{align*}
{x > 0 \land x < 5} & \quad x := x \times x \quad \{x < 25\} \\
{x = 3} & \quad x := x \times x \quad \{x < 25\}
\end{align*}
\]
- YES

\[
\begin{align*}
{x = 3} & \quad x := x \times x \quad \{x < 25\} \\
{x > 0 \land x < 5} & \quad x := x \times x \quad \{x < 25\}
\end{align*}
\]
- NO

Post Condition Weakening

\[
\begin{align*}
\{P\} & \quad C \quad \{Q'\} \\
Q' & \Rightarrow Q
\end{align*}
\]
- Example:

\[
\begin{align*}
{x + y = 5} & \quad x := x + y \quad \{x = 5\} \quad (x = 5) \Rightarrow (x < 10) \\
{x + y = 5} & \quad x := x + y \quad \{x < 10\}
\end{align*}
\]

Rule of Consequence

\[
P \Rightarrow P' \quad \{P'\} \quad C \quad \{Q'\} \\
Q' \Rightarrow Q \quad \{P\} \quad C \quad \{Q\}
\]
- Logically equivalent to the combination of Precondition Strengthening and Postcondition Weakening
- Uses \( P \Rightarrow P \) and \( Q \Rightarrow Q \)

Sequencing

\[
\begin{align*}
\{P\} & \quad C_1 \quad \{Q\} \quad C_2 \quad \{R\}
\end{align*}
\]
- Example:

\[
\begin{align*}
\{z = z \land z = z\} & \quad x := z \quad \{x = z \land z = z\} \\
\{x = z \land z = z\} & \quad y := z \quad \{x = z \land y = z\} \\
\{z = z \land z = z\} & \quad x := z \quad y := z \quad \{x = z \land y = z\}
\end{align*}
\]

If Then Else

\[
\begin{align*}
\{P \land B\} & \quad C_1 \quad \{Q\} \\
\{P \land \neg B\} & \quad C_2 \quad \{Q\}
\end{align*}
\]
- Example:

\[
\begin{align*}
\{y = a\} & \quad \text{if } x < 0 \text{ then } y := y - x \text{ else } y := y + x \quad \{y = a + |x|\}
\end{align*}
\]
- By If,Then,Else Rule suffices to show:
  - (1) \( \{y = a \land x < 0\} \quad y := y - x \quad \{y = a + |x|\} \) and
  - (2) \( \{y = a \land x < 0\} \quad y := y + x \quad \{y = a + |x|\} \)
We need a rule to be able to make assertions about while loops.

- Inference rule because we can only draw conclusions if we know something about the body
- Lets start with:
  \[
  \{ \ ? \} \text{C} \ \{ \ ? \} \\
  \{ \ ? \} \text{while B do C} \ \{ P \}
  \]

- (4) reduces to (5) and (6) by Precondition Strengthening
- (5) Follows from Assignment Axiom
- (6) since \( \neg(x < 0) \Rightarrow |x| = x \)

**While**

- Loop may never execute
- To know \( P \) holds after, it had better hold before
- Second approximation:
  \[
  \{ P \text{while B do C} \ \{ P \}
  \]

**While**

- Always know \( \neg B \) when while loop finishes
- Final While rule:
  \[
  \{ P \text{while B do C} \ \{ P \}
  \]

**If Then Else**

- (1) \( \{ y = a \wedge x < 0 \} \ y := y - x \ \{ y = a + |x| \} \)
- (4) \( \{ y = a \wedge \neg (x < 0) \} y := y + x \ \{ y = a + |x| \} \)

\( \{ y = a \} \text{if x < 0 then y := y - x else y := y + x} \ \{ y = a + |x| \} \)

by the If,Then,Else Rule

**While**

- Loop may never execute
- To know \( P \) holds after, it had better hold before
- Second approximation:

\[
\{ P \text{while B do C} \ \{ P \}
\]

- Third approximation:

\[
\{ P \wedge B \} \text{C} \ \{ P \}
\]

\[
\{ P \text{while B do C} \ \{ P \}
\]
While

\{(P \land B) \land C \land \{P\}\}

\{P\} while B do C \{P \land \neg B\}

- P satisfying this rule is called a loop invariant
- Must hold before and after the each iteration of the loop

Example

Prove:

\{n \geq 0\}
x := 0; y := 0;
while x < n do
(y := y + ((2 \times x) + 1);
x := x + 1)
\{y = n \times n\}

Example

First attempt:

\[ y = x \times x \]

Motivation:
- Want \( y = n \times n \)
- \( x \) counts up to \( n \)
- \textbf{Guess}: Each pass of loop calculates next square

Example

By Post-condition Weakening, suffices to show:

1. \{n \geq 0\}
x := 0; y := 0;
while x < n do
(y := y + ((2 \times x) + 1);
x := x + 1)
\{y = x \times x \land \neg(x < n)\}

and

2. \( y = x \times x \land \neg(x < n) \Rightarrow (y = n \times n) \)
Proof of (2)

- \((x < n)\) \Rightarrow (x \geq n)
- \((x \geq n) \land (x \leq n)\) \Rightarrow (x = n)
- \((x = n) \land (y = x \times x)\) \Rightarrow (y = n \times n)

Proof of (4)

By While Rule

\[ (5) \{ (y = x \times x) \land (x \leq n) \land (x < n) \} \]
\[ y := y + ((2 \times x) + 1); \ x := x + 1 \]
\[ \{ (y = x \times x) \land (x \leq n) \} \]

while \(x < n\) do
\[ y := y + ((2 \times x) + 1); \ x := x + 1 \]
\[ \{ (y = x \times x) \land (x \leq n) \land (x < n) \} \]

Example

Second attempt:

\[ P = \{ (y = x \times x) \land (x \leq n) \} \]

Again by Post-condition Weakening, suffices to show:

(1) \(\{ n \geq 0 \} x := 0; \ y := 0; \)

\(\text{while } x < n \text{ do} \)
\(y := y + ((2 \times x) + 1); \ x := x + 1 \)
\(\{ (y = x \times x) \land (x \leq n) \land (x < n) \} \)

and

(2) \((y = x \times x) \land (x \leq n) \land (x < n)\) \Rightarrow (y = n \times n)

Problem with (2)

Want (2) \((y = x \times x) \land (x < n)\) \Rightarrow (y = n \times n)

- From \(\neg(x < n)\) have \(x \geq n\)
- Need \(x = n\)
- Don’t know this; from this could have \(x > n\)
- Need stronger invariant
- Try adding \(x \leq n\)
- Then have \((x \leq n) \land \neg(x < n)\) \Rightarrow (x = n)
- Then have \(x = n\) when loop done

Proof of (5)

By Sequencing Rule

\[ (6) \{ (y = x \times x) \land (x \leq n) \} \]
\[ y := y + ((2 \times x) + 1); \ x := x + 1 \]
\[ \{ (y = x \times x) \land (x \leq n) \land (x < n) \} \]

(7) holds by Assignment Axiom
Proof of (6)

By Precondition Strengthening

(8) \((y = x \times x) \land (x \leq n) \Rightarrow ((y + ((2 \times x) + 1)) \land (x \leq n))\)

(9) \((y \times x) = ((x + 1) \times (x + 1)) \land (x \leq n)\)

Have (9) by Assignment Axiom

Proof of (8)

- (Assuming \(x\) integer) \((x < n) \Rightarrow ((x + 1) \leq n)\)
- \(y = x \times x \Rightarrow ((y + ((2 \times x) + 1)) = ((x \times x) + ((2 \times x) + 1)) = ((x + 1) \times (x + 1))\)

That finishes (8), and thus (6) and thus (5) and thus (4) (while)

Need (3) \((n \geq 0)\ x := 0; \ y := 0 \ ((y = x \times x) \land (x \leq n))\)

Proof of (3)

By Sequencing

(10) \(n \geq 0\)

\(x := 0\)

\(\{(0 = x \times x) \land (x \leq n)\}\)

(11) \(y := 0\)

\(\{(y = x \times x) \land (x \leq n)\}\)

\(\{n \geq 0\} x := 0; \ y := 0 \ ((y = x \times x) \land (x \leq n))\)

Have (11) by Assignment Axiom

Proof of (10)

By Precondition Strengthening

(13) \(\{(0 = 0 \times 0) \land (0 \leq n)\}\)

\(x := 0\)

(12) \(n \geq 0\)

\(\{(0 = 0 \times 0) \land (0 \leq n)\}\)

\(x := 0; \ y := 0 \ ((0 = x \times x) \land (x \leq n))\)

- For (12), \(0 = 0 \times 0\) and \((n \geq 0) \Rightarrow (0 \leq n)\)
- Have (13) by Assignment Axiom
- Finishes (10), thus (3), thus (1)