### Precondition Strengthening

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

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

Examples:

\[
x = 3 \Rightarrow x < 7 \quad \{x < 7\} \quad x := x + 3 \quad \{x < 10\}
\]

\[
\{x = 3\} \quad x := x + 3 \quad \{x < 10\}
\]

\[
\text{True} \Rightarrow (2 = 2) \quad \{2 = 2\} \quad x := 2 \quad \{x = 2\}
\]

\[
\{\text{True}\} \quad x := 2 \quad \{x = 2\}
\]

\[
x = n \Rightarrow x + 1 = n + 1 \quad \{x + 1 = n + 1\} \quad x := x + 1 \quad \{x = n + 1\}
\]

\[
\{x = n\} \quad x := x + 1 \quad \{x = n + 1\}
\]
Which Inferences Are Correct?

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

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

\[
\begin{align*}
\{x \times x < 25\} & \quad \text{\(x := x \times x\)} \quad \{x < 25\} \\
\{x > 0 \land x < 5\} & \quad \text{\(x := x \times x\)} \quad \{x < 25\}
\end{align*}
\]
Which Inferences Are Correct?

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

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

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

\[
\begin{align*}
\{x > 0 \land x < 5\} & \quad x := x \times x \quad \{x < 25\} \quad \text{YES} \\
\{x = 3\} & \quad x := x \times x \quad \{x < 25\} \\
\{x > 0 \land x < 5\} & \quad x := x \times x \quad \{x < 25\} \quad \text{NO} \\
\{x < 25\} & \quad x := x \times x \quad \{x < 25\} \\
\{x > 0 \land x < 5\} & \quad x := x \times x \quad \{x < 25\} 
\end{align*}
\]
Which Inferences Are Correct?

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

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

\[
\begin{align*}
\{ x \times x < 25 \} & \quad x := x \times x \quad \{ x < 25 \} & \quad \text{YES} \\
\{ x > 0 \land x < 5 \} & \quad x := x \times x \quad \{ x < 25 \}
\end{align*}
\]
Post Condition Weakening

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

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

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

\[
\{P\} \quad C \quad \{Q\}
\]

- Logically equivalent to the combination of Precondition Strengthening and Postcondition Weakening
- Uses \( P \Rightarrow P \) and \( Q \Rightarrow Q \)
Sequencing

\[
\{P\} \ C_1 \ \{Q\} \quad \{Q\} \ C_2 \ \{R\}
\]

\[
\{P\} \ C_1 ; \ C_2 \ \{R\}
\]

- Example:

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

\[
\{z = z \land z = z\} \quad x := z; \ y := z \quad \{x = z \land y = z\}
\]
If Then Else

\[
\begin{align*}
\{P \land B\} & \quad C_1 \quad \{Q\} \\
\{P \land \neg B\} & \quad C_2 \quad \{Q\} \\
\{P\} & \quad \text{if } B \text{ then } C_1 \text{ else } C_2 \quad \{Q\}
\end{align*}
\]

- Example:

\[
\{y = a\} \quad \text{if } x < 0 \text{ then } y := y - x \text{ else } y := y + x \quad \{y = a + |x|\}
\]

By If Then Else Rule suffices to show:

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

(3) \((y = a \land x < 0) \Rightarrow (y = a + |x|)\)

(2) \( \{ y - x = a + |x| \} \ y := y - x \ \{ y = a + |x| \} \)

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

- (1) reduces to (2) and (3) by Precondition Strengthening
- (2) instance of Assignment Axiom
- (3) holds since \( x < 0 \Rightarrow |x| = -x \)
(4) \( \{ y = a \land \neg (x < 0) \} \ y := y + x \ \{ y = a + |x| \} \)

(6) \( (y = a \land \neg (x < 0)) \Rightarrow (y + x = a + |x|) \)

(5) \( \{ y + x = a + |x| \} \ y := y + x \ \{ y = a + |x| \} \)

(4) reduces to (5) and (6) by Precondition Strengthening

(5) Follows from Assignment Axiom

(6) since \( \neg (x < 0) \Rightarrow |x| = x \)
If Then Else

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

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

by the If_Then_Else Rule
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
- Let's start with:

\[
\{ \ ? \ \} \ C \ \{ \ ? \ \}
\]

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

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

$$\{ ? \} \quad \text{C} \quad \{ ? \}$$

$$\{P\} \quad \text{while } B \text{ do } C \quad \{P\}$$
Loop may execute $C$; end of loop is of $C$

$P$ holds at end of while means $P$ holds at end of loop $C$

$P$ holds at start of while; loop taken means $P \land B$ holds at start of $C$

Third approximation:

$$\{P \land B\} \quad C \quad \{P\}$$

$$\{P\} \quad \text{while} \quad B \quad \text{do} \quad C \quad \{P\}$$
Always know $\neg B$ when \textit{while} loop finishes

Final \textbf{While} rule:

$$\{ P \land B \} \ C \ \{ P \}$$

$$\{ P \} \ \text{while} \ B \ \text{do} \ C \ \{ P \land \neg B \}$$
While

\[ \{ P \land B \} \quad C \quad \{ P \} \]

\[ \{ P \} \quad \text{while } B \text{ do } C \quad \{ P \land \neg B \} \]

- \( P \) satisfying this rule is called a loop invariant
- Must hold before and after the each iteration of the loop
• **While** rule generally used with precondition strengthening and postcondition weakening

• **No** algorithm for computing $P$ in general

• Requires intuition and an understanding of why the program works
Prove:

\{ n \geq 0 \}
x := 0; \quad y := 0;
while x < n do
  (y := y + ((2 \times x) + 1);
  x := x + 1)
\{ y = n \times n \}
Need to find \( P \) that is true before and after loop is executed, such that

\[
(P \land \neg (x < n)) \Rightarrow y = n \ast n
\]
Example

- First attempt:
  \[ y = x \times x \]

- Motivation:
- Want \( y = n \times n \)
- \( x \) counts up to \( n \)
- **Guess:** Each pass of loop calculates next square
By Post-condition Weakening, suffices to show:

(1) \( \{ n \geq 0 \} \)

\[
\begin{align*}
    &x := 0; \ y := 0; \\
    &\text{while } x < n \text{ do} \\
    &\quad (y := y + ((2 \times x) + 1); \ x := x + 1) \\
    &\quad \{ y = x \times x \land \neg(x < n) \}
\end{align*}
\]

and

(2) \( (y = x \times x \land \neg(x < n)) \Rightarrow (y = n \times n) \)
Problem with (2)

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

Second attempt:

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

Again by Post-condition Weakening, suffices to show:

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

and

(2) \[ ((y = x \times x) \land (x \leq n) \land \neg(x < n)) \Rightarrow (y = n \times n) \]
Proof of (2)

- \(\neg(x < n) \Rightarrow (x \geq n)\)
- \(((x \geq n) \land (x \leq n)) \Rightarrow (x = n)\)
- \(((x = n) \land (y = x \times x)) \Rightarrow (y = n \times n)\)
For (1), set up While Rule using Sequencing Rule

By Sequencing Rule, suffices to show

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

and

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

while \( x \prec n \) do

\( (y := y + ((2 \times x) + 1); \ x := x + 1) \)

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

\{ (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 \neg(x < n) \}
Proof of (5)

By Sequencing Rule

\[(6) \quad \{(y = x \times x) \land (x \leq n) \land (x < n)\} \quad \text{and} \quad (7) \quad \{(y = (x + 1) \times (x + 1)) \land ((x + 1) \leq n)\}\]

\[
y := y + ((2 \times x) + 1) \quad \text{and} \quad x := x + 1
\]

\[
\{(y = (x + 1) \times (x + 1)) \land ((x + 1) \leq n)\}
\]

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

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

By Precondition Strengthening

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

(9) \{(((y + ((2 \times x) + 1)) = (x + 1) \times (x + 1)) \land ((x + 1) \leq n)}

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

\{y := y + ((2 \times x) + 1)\}

\{((y = (x + 1) \times (x + 1)) \land ((x + 1) \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 \cdot x) \land (x \leq n)\}

(11) \{ (0 = x \cdot x) \land (x \leq n) \}
    y := 0 
    \{(y = x \cdot x) \land (x \leq n)\}

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

Have (11) by Assignment Axiom
Proof of (10)

By Precondition Strengthening

\[(n \geq 0) \Rightarrow ((0 = 0 \times 0) \land (0 \leq n))\]

\[
\begin{align*}
(12) & \quad (n \geq 0) \Rightarrow ((0 = 0 \times 0) \land (0 \leq n)) \\
(13) & \quad \{ (0 = 0 \times 0) \land (0 \leq n) \} \\
\end{align*}
\]

\[
(n \geq 0) \times := 0; \quad \{ (0 = x \times x) \land (x \leq n) \}
\]

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