Sequencing

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

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

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

Postcondition Weakening

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

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

Example:
\[
\begin{align*}
\{z = z & \land z = z\} & \ x := z ; \ y := z \{x = z & \land y = z\} \\
\{x = z & \land y = z\} & \ (x = y) \\
\{z = z & \land z = z\} & \ x := z ; \ y := z \{x = y\}
\end{align*}
\]

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 \[ Q' \Rightarrow Q \]

If Then Else

\[ \{P \text{ and } B\} \quad C_1 \{Q\} \quad \{P \text{ and } \lnot B\} \quad C_2 \{Q\} \quad \{P\} \quad \text{if } B \text{ then } C_1 \text{ else } C_2 \text{ fi } \{Q\} \]

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

Suffices to show:
\[
\begin{align*}
(1) \{y = a & \land x < 0\} & \ y := y - x \quad \{y = a + |x|\} \quad \text{and} \\
(4) \{y = a & \lnot(x < 0)\} & \ y := y + x \quad \{y = a + |x|\}
\end{align*}
\]
\{ y = a \land x < 0 \} \quad y := y - x \quad \{ y = a + |x| \}

(3) \quad (y = a \land x < 0) \implies y - x = a + |x|

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

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

(1) Reduces to (2) and (3) by Precondition Strengthening

(2) Follows from assignment axiom

(3) Because $x < 0 \implies |x| = -x$

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

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

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

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

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

(5) Follows from assignment axiom

(6) Because $\neg (x < 0) \implies |x| = x$

If then else

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

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

While

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:

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

\{ \ ? \ \} \quad \text{while} \quad B \quad \text{do} \quad C \quad \text{od} \quad \{ P \}

While

- The loop may never be executed, so if we want $P$ to hold after, it had better hold before, so let’s try:

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

\{ P \} \quad \text{while} \quad B \quad \text{do} \quad C \quad \text{od} \quad \{ P \}

While

- If all we know is $P$ when we enter the while loop, then we all we know when we enter the body is $(P \land B)$
- If we need to know $P$ when we finish the while loop, we had better know it when we finish the loop body:

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

\{ P \} \quad \text{while} \quad B \quad \text{do} \quad C \quad \text{od} \quad \{ P \}
We can strengthen the previous rule because we also know that when the loop is finished, not B also holds.

Final while rule:

\[
\{ P \text{ and } B \} \rightarrow C \rightarrow \{ P \}
\]

\[
\{ P \} \text{ while } B \text{ do } C \text{ od } \{ P \text{ and not } B \}
\]

P satisfying this rule is called a loop invariant because it must hold before and after the each iteration of the loop.

Example

We need to find a condition P that is true both before and after the loop is executed, and such that

\[(P \text{ and not } x > 0) \Rightarrow (\text{fact} = a!)}\]

First attempt:

\[a! = \text{fact} * (x!)}\]

Motivation:

- What we want to compute: a!
- What we have computed: fact
- which is the sequential product of a down through \((x + 1)\)
- What we still need to compute: x!
Example

By post-condition weakening suffices to show
1. \{x \geq 0 \text{ and } x = a\}
   
   \text{fact} := 1;
   \text{while } x > 0 \text{ do (fact := fact } \times x; x := x - 1) \text{ od}
   
   \{a! = \text{fact } \times (x!) \text{ and not } (x > 0)\}

and

2. \{a! = \text{fact } \times (x!) \text{ and not } (x > 0)\} \Rightarrow \{\text{fact } = a!\}

Example

Second try, combine the two:
\[ P = \{a! = \text{fact } \times (x!) \text{ and } x \geq 0\} \]

Again, suffices to show
1. \{x \geq 0 \text{ and } x = a\}
   
   \text{fact} := 1;
   \text{while } x > 0 \text{ do (fact := fact } \times x; x := x - 1) \text{ od}
   
   \{P \text{ and not } x > 0\}

and

2. \{P \text{ and not } x > 0\} \Rightarrow \{\text{fact } = a!\}

Example

For 2, we need
\[ \{a! = \text{fact } \times (x!) \text{ and } x \geq 0 \text{ and not } (x > 0)\} \Rightarrow \{\text{fact } = a!\} \]

But \{x \geq 0 \text{ and not } (x > 0)\} \Rightarrow \{x = 0\} \text{ so }

\text{fact } \times (x!) = \text{fact } \times (0!) = \text{fact}

Therefore
\[ \{a! = \text{fact } \times (x!) \text{ and } x \geq 0 \text{ and not } (x > 0)\} \Rightarrow \{\text{fact } = a!\} \]

Example

For 1, by the sequencing rule it suffices to show
3. \{x \geq 0 \text{ and } x = a\}
   
   \text{fact} := 1
   
   \{a! = \text{fact } \times (x!) \text{ and } x \geq 0\}

And

4. \{a! = \text{fact } \times (x!) \text{ and } x \geq 0\}
   \text{while } x > 0 \text{ do (fact := fact } \times x; x := x - 1) \text{ od}
   
   \{a! = \text{fact } \times (x!) \text{ and } x \geq 0 \text{ and not } (x > 0)\}

Example

Suffices to show that
\[ \{a! = \text{fact } \times (x!) \text{ and } x \geq 0\} \]
holds before the while loop is entered and that if

\[ \{(a! = \text{fact } \times (x!)) \text{ and } x \geq 0 \text{ and } x > 0\} \]
holds before we execute the body of the loop, then

\[ \{(a! = \text{fact } \times (x!)) \text{ and } x \geq 0\} \]
holds after we execute the body.
Example

By the assignment rule, we have
\{a! = 1 \times (x!) \text{ and } x \geq 0\}
\text{fact} := 1
\{a! = \text{fact} \times (x!) \text{ and } x \geq 0\}
Therefore, to show (3), by precondition strengthening, it suffices to show
\begin{align*}
(x \geq 0 \text{ and } x = a) \implies \\
(a! = 1 \times (x!) \text{ and } x \geq 0)
\end{align*}

Example

\((x \geq 0 \text{ and } x = a) \implies \\
(a! = 1 \times (x!) \text{ and } x \geq 0)\)
holds because \(x = a \implies x! = a!\)
Have that \(\{a! = \text{fact} \times (x!) \text{ and } x \geq 0\}\) holds at the start of the while loop

Example

To show (4):
\{a! = \text{fact} \times (x!) \text{ and } x \geq 0\}
while \(x > 0\) do
\begin{align*}
&\text{fact} := \text{fact} \times x; \\
&x := x - 1
\end{align*}
\{a! = \text{fact} \times (x!) \text{ and } x \geq 0 \text{ and } x > 0\}
we need to show that
\{a! = \text{fact} \times (x!) \text{ and } x \geq 0\}
is a loop invariant

Example

We need to show:
\{a! = \text{fact} \times (x!) \text{ and } x \geq 0 \text{ and } x > 0\}
\begin{align*}
\text{(fact = fact} \times x; \\
x := x - 1 )
\end{align*}
\{a! = \text{fact} \times (x!) \text{ and } x \geq 0\}
We will use assignment rule, sequencing rule and precondition strengthening

Example

By the assignment rule, we have
\{(a! = \text{fact} \times ((x-1)!) \text{ and } x - 1 \geq 0)\}
\text{x} := x - 1
\{(a! = \text{fact} \times (x!) \text{ and } x \geq 0\}
By the sequencing rule, it suffices to show
\{(a! = \text{fact} \times (x!) \text{ and } x \geq 0 \text{ and } x > 0\}
\text{fact} = \text{fact} \times x
\{(a! = \text{fact} \times ((x-1)!) \text{ and } x - 1 \geq 0)\}
By Precondition strengthening, it suffices to show that
\{(a! = \text{fact} \times (x!) \text{ and } x \geq 0 \text{ and } x > 0) \implies \\
((a! = \text{fact} \times (x!) \text{ and } x \geq 0) \text{ and } x - 1 \geq 0)\}
Example

However

\[ \text{fact} \times x \times (x - 1)! = \text{fact} \times (x!) \]

and \( (x > 0) \Rightarrow x - 1 \geq 0 \)

since x is an integer, so

\{ (a! = \text{fact} \times (x!)) \text{ and } x \geq 0 \text{ and } x > 0 \} \Rightarrow \n \{ (a! = (\text{fact} \times x) \times ((x-1)!)) \text{ and } x - 1 \geq 0 \} \]

Therefore, by precondition strengthening

\{ (a! = \text{fact} \times (x!)) \text{ and } x \geq 0 \text{ and } x > 0 \}

\text{fact} = \text{fact} \times x

\{ (a! = \text{fact} \times ((x-1)!)) \text{ and } x - 1 \geq 0 \}

This finishes the proof