CS477 Formal Software Development Methods

Elsa L Gunter
2112 SC, UIUC
egunter@illinois.edu
http://courses.engr.illinois.edu/cs477

Slides based in part on previous lectures by Mahesh Vishwanathan, and by Gul Agha

February 15, 2013

Precondition Strengthening

$$\frac{(P \Rightarrow P')\{P'\}\ C\ \{Q\}}{\{P\}\ C\ \{Q\}}$$

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

Precondition Strengthening

- Examples:

$$\frac{x = 3 \Rightarrow x < 7 \quad \{x < 7\}\ x\ :=\ x + 3\ \{x < 10\}}{\{x = 3\}\ x\ :=\ x + 3\ \{x < 10\}}$$

$$\frac{\mathit{True} \Rightarrow (2 = 2) \quad \{2 = 2\}\ x\ :=\ 2\ \{x = 2\}}{\{\mathit{True}\}\ x\ :=\ 2\ \{x = 2\}}$$

$$\frac{x = n \Rightarrow x + 1 = n + 1 \quad \{x + 1 = n + 1\}\ x\ :=\ x + 1\ \{x = n + 1\}}{\{x = n\}\ x\ :=\ x + 1\ \{x = n + 1\}}$$

Which Inferences Are Correct?

$$\frac{\{x > 0 \wedge x < 5\}\ x\ := \ x * x\ \{x < 25\}}{\{x = 3\}\ x\ := \ x * x\ \{x < 25\}}$$

$$\frac{\{x = 3\}\ x\ := \ x * x\ \{x < 25\}}{\{x > 0 \wedge x < 5\}\ x\ := \ x * x\ \{x < 25\}}$$

$$\frac{\{x * x < 25\}\ x\ := \ x * x\ \{x < 25\}}{\{x > 0 \wedge x < 5\}\ x\ := \ x * x\ \{x < 25\}}$$

Which Inferences Are Correct?

$$\frac{\{x > 0 \wedge x < 5\}\ x\ :=\ x * x\ \{x < 25\}}{\{x = 3\}\ x\ :=\ x * x\ \{x < 25\}}\ \mathit{YES}$$

$$\frac{\{x = 3\}\ x\ :=\ x * x\ \{x < 25\}}{\{x > 0 \wedge x < 5\}\ x\ :=\ x * x\ \{x < 25\}}$$

$$\frac{\{x * x < 25\}\ x\ :=\ x * x\ \{x < 25\}}{\{x > 0 \wedge x < 5\}\ x\ :=\ x * x\ \{x < 25\}}$$

Which Inferences Are Correct?

$$\frac{\{x > 0 \land x < 5\}\ x\ := \ x * x\ \{x < 25\}}{\{x = 3\}\ x\ := \ x * x\ \{x < 25\}}\ \textit{YES}$$

$$\frac{\{x = 3\}\ x\ := \ x * x\ \{x < 25\}}{\{x > 0 \land x < 5\}\ x\ := \ x * x\ \{x < 25\}}\ \textit{NO}$$

$$\frac{\{x * x < 25\}\ x\ := \ x * x\ \{x < 25\}}{\{x > 0 \land x < 5\}\ x\ := \ x * x\ \{x < 25\}}$$

Which Inferences Are Correct?

$$\frac{\{x > 0 \wedge x < 5\}\ x\ := \ x * x\ \{x < 25\}}{\{x = 3\}\ x\ := \ x * x\ \{x < 25\}}\ \textit{YES}$$

$$\frac{\{x = 3\}\ x\ := \ x * x\ \{x < 25\}}{\{x > 0 \wedge x < 5\}\ x\ := \ x * x\ \{x < 25\}}\ \textit{NO}$$

$$\frac{\{x * x < 25\}\ x\ := \ x * x\ \{x < 25\}}{\{x > 0 \wedge x < 5\}\ x\ := \ x * x\ \{x < 25\}}\ \textit{YES}$$

Post Condition Weakening

$$\frac{\{P\}\ C\ \{Q'\} \quad Q' \Rightarrow Q}{\{P\}\ C\ \{Q\}}$$

- Example:

$$\frac{\{x + y = 5\}\ x := x + y\ \{x = 5\} \quad (x = 5) \Rightarrow (x < 10)}{\{x + y = 5\}\ x := x + y\ \{x < 10\}}$$

Rule of Consequence

$$\frac{P \Rightarrow P' \quad \{P'\}\ C\ \{Q'\} \quad Q' \Rightarrow Q}{\{P\}\ C\ \{Q\}}$$

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

Sequencing

$$\frac{\{P\}\ C_1\ \{Q\} \quad \{Q\}\ C_2\ \{R\}}{\{P\}\ C_1;\ C_2\ \{R\}}$$

- Example:

$$\frac{\begin{array}{c}\{z = z \wedge z = z\}\ x := z\ \{x = z \wedge z = z\} \\ \{x = z \wedge z = z\}\ y := z\ \{x = z \wedge y = z\}\end{array}}{\{z = z \wedge z = z\}\ x := z;\ y := z\ \{x = z \wedge y = z\}}$$

If Then Else

$$\frac{\{P \wedge B\}\ C_1\ \{Q\} \quad \{P \wedge \neg B\}\ C_2\ \{Q\}}{\{P\}\ if\ \ B\ \ then\ \ C_1\ \ else\ \ C - 2\ \{Q\}}$$

- Example:

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

  By If_Then_Else Rule suffices to show:
  - $(1)\ \{y = a \wedge x < 0\}\ y := y - x\ \{y = a + |x|\}$ and
  - $(4)\ \{y = a \wedge \neg(x < 0)\}\ y := y + x\ \{y = a + |x|\}$

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

$$\frac{\begin{array}{c}(3)\quad (y = a \wedge x < 0) \Rightarrow (y = a + |x|) \\ (2)\quad \{y - x = a + |x|\}\ y := y - x\ \{y = a + |x|\}\end{array}}{(1)\quad \{y = a \wedge x < 0\}\ y := y - x\ \{y = a + |x|\}}$$

- (1) reduces to (2) and (3) by Precondition Strengthening
- (2) instance of Assignment Axiom
- (3) holds since $x < 0 \Rightarrow |x| = -x$

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

$$\frac{\begin{array}{c}(6)\quad (y = a \land \neg(x < 0)) \Rightarrow (y + x = a + |x|) \\ (5)\quad \{y + x = a + |x|\}\ y := y + x\ \{y = a + |x\}\end{array}}{(4)\quad \{y = a \land \neg(x < 0)\}\ y := y + x\ \{y = a + |x|\}}$$

- (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

$$\frac{\begin{array}{c}(1)\ \ \{y = a \land x < 0\}\ y := y - x\ \{y = a + |x|\} \\ (4)\ \ \{y = a \land \neg(x < 0)\}\ y := y + x\ \{y = a + |x|\}\end{array}}{\{y = a\}\ \mathit{if}\ \ x < 0\ \mathit{then}\ y := y - x\ \mathit{else}\ y := y + x\ \{y = a + |x|\}}$$

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
- Lets start with:

$$\frac{\{\ \ ?\ \ \}\ C\ \{\ \ ?\ \ \}}{\{\ \ ?\ \ \}\ while\ B\ do\ C\ \{P\}}$$

While

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

$$\frac{\{\ \ ?\ \ \}\ C\ \{\ \ ?\ \ \}}{\{P\}\ while\ B\ do\ C\ \{P\}}$$

While

- Loop may execute C; enf 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 $P \wedge B$ holds at start of C
- Third approximation:

$$\frac{\{P \wedge B\}\ C\ \{P\}}{\{P\}\ while\ B\ do\ C\ \{P\}}$$

While

- Always know $\neg B$ when *while* loop finishes
- Final While rule:

$$\frac{\{P \wedge B\}\ C\ \{P\}}{\{P\}\ while\ B\ do\ C\ \{P \wedge \neg B\}}$$

While

$$\frac{\{P \wedge B\}\ C\ \{P\}}{\{P\}\ while\ B\ do\ C\ \{P \wedge \neg B\}}$$

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

While

- 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

Example

Prove:

$$
\begin{array}{l}
\{n \geq 0\} \\
x := 0;\ \ y := 0; \\
while\ x < n\ do \\
(y := y + ((2 * x) + 1); \\
\ x := x + 1) \\
\{y = n * n\}
\end{array}
$$

Example

- Need to find P that is true before and after loop is executed, such that

$$(P \wedge \neg(x < n)) \Rightarrow y = n * n$$

Example

- First attempt:

$$y = x * x$$

- Motivation:
- Want $y = n * n$
- x counts up to n
- **Guess:** Each pass of loop calcuates next square

Example

By Post-condition Weakening, suffices to show:

$$
\begin{array}{ll}
(1) & \{n \geq 0\} \\
 & x := 0;\ \ y := 0; \\
 & \mathit{while}\ x < n\ \mathit{do} \\
 & (y := y + ((2 * x) + 1);\ \ x := x + 1) \\
 & \{y = x * x \wedge \neg(x < n)\}
\end{array}
$$

and

$$(2)\ \ (y = x * x \wedge \neg(x < n)) \Rightarrow (y = n * n)$$

Problem with (2)

- Want (2) $(y = x * x \land \neg(x < n)) \Rightarrow (y = n * n)$
- 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 ading $x \leq n$
- Then have $((x \leq n) \land \neg(x < n)) \Rightarrow (x = n)$
- Then have $x = n$ when loop done

Example

Second attempt:

$$P = ((y = x * x) \wedge (x \leq n))$$

Again by Post-condition Weakening, sufices to show:

(1) $\{n \geq 0\}$
$x := 0;\ y := 0;$
$\mathit{while}\ x < n\ \mathit{do}$
$(y := y + ((2 * x) + 1);\ x := x + 1)$
$\{(y = x * x) \wedge (x \leq n) \wedge \neg(x < n)\}$

and

(2) $((y = x * x) \wedge (x \leq n) \wedge \neg(x < n)) \Rightarrow (y = n * n)$

Proof of (2)

- $(\neg(x < n)) \Rightarrow (x \geq n)$
- $((x \geq n) \wedge (x \leq n)) \Rightarrow (x = n)$
- $((x = n) \wedge (y = x * x)) \Rightarrow (y = n * n)$

Example

- For (1), set up While Rule using Sequencing Rule
- By Sequencing Rule, suffices to show

(3) $\{n \geq 0\}\ x := 0;\ y := 0\ \{(y = x * x) \wedge (x \leq n)\}$

and

(4)
$$\begin{array}{l}\{(y = x * x) \wedge (x \leq n)\} \\ \mathit{while}\ x < n\ \mathit{do} \\ (y := y + ((2 * x) + 1);\ x := x + 1) \\ \{(y = x * x) \wedge (x \leq n) \wedge \neg(x < n)\}\end{array}$$

Proof of (4)

By While Rule

$$\frac{\begin{array}{ll}(5) & \{(y = x * x) \wedge (x \leq n) \wedge (x < n)\} \\ & y := y + ((2 * x) + 1);\ x := x + 1 \\ & \{(y = x * x) \wedge (x \leq n)\}\end{array}}{\begin{array}{l}\{(y = x * x) \wedge (x \leq n)\} \\ \mathit{while}\ x < n\ \mathit{do} \\ (y := y + ((2 * x) + 1);\ x := x + 1) \\ \{(y = x * x) \wedge (x \leq n) \wedge \neg(x < n)\}\end{array}}$$

Proof of (5)

By Sequencing Rule

y + 2*x + 1 = (x+1)*(x+1) ∧ ((x + 1) <= n)

$$\frac{(6)\ \begin{array}{l}\{(y = x * x) \wedge (x \leq n) \\ \quad \wedge (x < n)\} \\ y := y + ((2 * x) + 1) \\ \{(y = (x+1) * (x+1)) \\ \quad \wedge ((x+1) \leq n)\}\end{array} \qquad (7)\ \begin{array}{l}\{(y = (x+1) * (x+1)) \\ \quad \wedge ((x+1) \leq n)\} \\ x := x + 1 \\ \{(y = x * x) \wedge (x \leq n)\}\end{array}}{\begin{array}{l}\{(y = x * x) \wedge (x \leq n) \wedge (x < n)\} \\ y := y + ((2 * x) + 1);\ x := x + 1 \\ \{(y = x * x) \wedge (x \leq n)\}\end{array}}$$

(7) holds by Assignment Axiom

Proof of (6)

By Precondition Strengthening

$$\frac{\begin{array}{ll} (8) & \begin{array}{l} ((y = x * x) \\ \quad \wedge (x \leq n) \wedge (x < n)) \Rightarrow \\ (((y + ((2 * x) + 1)) \\ \quad = (x + 1) * (x + 1)) \\ \quad \wedge ((x + 1) \leq n)) \end{array} \end{array} \qquad \begin{array}{ll} (9) & \begin{array}{l} \{((y + ((2 * x) + 1)) \\ \quad = ((x + 1) * (x + 1))) \\ \quad \wedge ((x + 1) \leq n)\} \\ y := y + ((2 * x) + 1) \\ \{(y = (x + 1) * (x + 1)) \\ \quad \wedge ((x + 1) \leq n)\} \end{array} \end{array}}{\begin{array}{l} \{(y = x * x) \wedge (x \leq n) \\ \quad \wedge (x < n)\} \\ y := y + ((2 * x) + 1) \\ \{(y = (x + 1) * (x + 1)) \\ \quad \wedge ((x + 1) \leq n)\} \end{array}}$$

Have (9) by Assignment Axiom

Proof of (8)

- (Assuming x integer) $(x < n) \Rightarrow ((x + 1) \leq n)$
- $$(y = x * x) \Rightarrow \begin{array}{l} ((y + ((2 * x) + 1)) \\ = ((x * x) + ((2 * x) + 1)) \\ = ((x + 1) * (x + 1))) \end{array}$$

- That finishes (8), and thus (6) and thus (5) and thus (4) (*while*)
- Need (3) $\{n \geq 0\}\ x := 0;\ \ y := 0\ \{(y = x * x) \wedge (x \leq n)\}$

Proof of (3)

By Sequencing

$$\frac{(10)\quad \begin{array}{l}\{n \geq 0\}\\ x := 0\\ \{(0 = x * x) \wedge (x \leq n)\}\end{array} \qquad (11)\quad \begin{array}{l}\{(0 = x * x) \wedge (x \leq n)\}\\ y := 0\\ \{(y = x * x) \wedge (x \leq n)\}\end{array}}{\{n \geq 0\}\ x := 0;\ \ y := 0\ \{(y = x * x) \wedge (x \leq n)\}}$$

Have (11) by Assignment Axiom

Proof of (10)

By Precondition Strengthening

$$\dfrac{(12)\ (n \geq 0) \Rightarrow ((0 = 0 * 0) \wedge (0 \leq n)) \qquad \begin{array}{ll} (13) & \{(0 = 0 * 0) \wedge (0 \leq n)\} \\ & x := 0 \\ & \{(0 = x * x) \wedge (x \leq n)\} \end{array}}{\{n \geq 0\}\ x := 0;\ \ y := 0\ \{(0 = x * x) \wedge (x \leq n)\}}$$

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