Loop Invariants

Dr. Mattox Beckman

University of Illinois at Urbana-Champaign
Department of Computer Science

Objectives

You should be able to ...

- Explain the concept of well formed induction.
- Enumerate the three conditions necessary for a loop to yield the correct answer.
- Enumerate the three conditions necessary for a loop to terminate.
- Pick a good loop invariant to verify a loop.

What Is a Loop?

- Remember from our discussion of `if` that it is best to consider the `if` as one statement rather than two branches.

$$\frac{\{p \wedge B\}S_1\{q\} \qquad \{p \wedge \neg B\}S_2\{q\}}{\{p\}\mathtt{if}\ B\ \mathtt{then}\ S_1\ \mathtt{else}\ S_2\ \mathtt{fi}\ \{q\}}$$

- With loops, we have a similar problem.
- … p and q are the same thing, though!

Loop Proof

- A loop proof outline looks like this:

$$
\begin{array}{l}
\{q\} \\
S_i \\
\{inv : p\}\ \{bd : t\} \\
\textbf{while } B \textbf{ do} \\
\quad \{p \land B\} \\
\quad S \\
\quad \{p\} \\
\textbf{od} \\
\{p \land \neg B\} \\
\{r\}
\end{array}
$$

Loop Equations

- We need to solve five equations.

$\{q\}$
S_i
$\{inv : p\}$ $\{bd : t\}$
while B **do**
  $\{p \wedge B\}$
  S
  $\{p\}$
od
$\{p \wedge \neg B\}$
$\{r\}$

1. $\{q\}S_i\{p\}$
2. $\{p \wedge B\}S\{p\}$
3. $p \wedge \neg B \to r$
4. $p \to t \geq 0$
5. $\{p \wedge B \wedge t = z\}S\{t < z\}$

Example 1 – Partial Correctness

Example 1

$s := 0;$
$i := 0;$
while $(i < |A|)$ **do**
  $s := s + A[i];$
  $i := i + 1$
od

What are these equations?

- $\{q\}S_i\{p\}$
- $\{p \wedge B\}S\{p\}$
- $p \wedge \neg B \to r$

Solutions:

- $\{\mathbf{true}\}s := 0; i := 0\{i \leq |A| \wedge s = \Sigma_0^{i-1} A[i]\}$
- $\{i \leq |A| \wedge s = \Sigma_0^{i-1} A[i] \wedge i < |A|\}S\{i \leq |A| \wedge s = \Sigma_0^{i-1} A[i]\}$
- $i \leq |A| \wedge s = \Sigma_0^{i-1} A[i] \wedge i \geq |A| \to s = \Sigma_0^{|A|-1} A[i]$

Example 2 – Partial Correctness

Example 2

$$\texttt{while } (a > 0) \texttt{ do}$$
$$a, b := b \; mod \; a, a$$
$$\texttt{od}$$

What are these equations?

- $\{q\}S_i\{p\}$
- $\{p \wedge B\}S\{p\}$
- $p \wedge \neg B \rightarrow r$

Solutions:

- No initialization!
- $\{gcd(a,b) = gcd(a',b') \wedge a > 0\}S\{gcd(a,b) = gcd(a',b')\}$
- $gcd(a,b) = gcd(a',b') \wedge a = 0 \rightarrow b = gcd(a',b')$

How to Pick a Loop Invariant

- The loop invariant is a weaker version of the postcondition.
- $p \wedge \neg B \rightarrow r$
- The loop's job is to incrementally make B false.
- So, to pick a loop invariant, you need to weaken the postcondition.

Ways to Weaken

- Replace a constant with a range.
- Add a disjunct.
- Remove a conjunct.

Example 1

$$s = \Pi_{j=0}^{|A|-1} A[j]$$

Example 1

$$s = \Pi_{j=0}^{|A|-1} A[j]$$

Replace a constant with a range:

$$0 \leq n \leq |A| \wedge r = \Pi_{j=0}^{n-1} A[j]$$

Example 2

$$a = 0 \land b = gcd(a', b');$$

Example 2

$$a = 0 \land b = gcd(a', b');$$

Add a disjunct:

$$a > 0 \land gcd(a, b) = gcd(a', b') \lor a = 0 \land b = gcd(a', b');$$

Example 3

$$|f(x)| < \varepsilon \wedge \delta < \varepsilon$$

Example 3

$$|f(x)| < \varepsilon \wedge \delta < \varepsilon$$

$$|f(x)| < \varepsilon$$

Making Progress

- What does it mean to “make progress toward termination?”
- Consider a function on integers ...
- A function on lists ...
- A function on Hydras ...

The Total Correctness Formulas

- $p \to t \geq 0$
- $\{p \land B \land t = z\}S\{t < z\}$

Example 1 – Total Correctness

Example 1

$$
\begin{array}{l}
s := 0; \\
i := 0; \\
\mathbf{while}\ (i < |A|)\ \mathbf{do} \\
\quad s := s + A[i]; \\
\quad i := i + 1 \\
\mathbf{od}
\end{array}
$$

What are these equations?

- $p \rightarrow t \geq 0$
- $\{p \wedge B \wedge t = z\}S\{t < z\}$

Solution:

- $i \leq |A| \wedge s = \Sigma_0^{i-1} A[i] \rightarrow t \geq 0$
- $\{i \leq |A| \wedge s = \Sigma_0^{i-1} A[i] \wedge i < |A| \wedge t = z\}S\{t < z\}$
- Let $t = |A| - i$.

Example 2 – Total Correctness

Example 2

```
while (a > 0) do
   a, b := b mod a, a
od
```

What are these equations?

- $p \rightarrow t \geq 0$
- $\{p \wedge B \wedge t = z\}S\{t < z\}$

Solutions:

- $a > 0 \rightarrow t \geq 0$
- (Too big to fit. But notice *a* always decreases!)