How to Find an Invariant

Brandon Ronald
COMP SCI 3EA3 - Software Specification and Correctness

March 3rd, 2017

1 Two Methods

1. Delete a conjunct.
2. Replace a constant(Expr) with a variable.

2 Example 1: Division Algorithm

Given

$$x \geq 0 \land y \geq 0$$

and post-condition R:

$$R : q = x \div y \land r = x \,\mathsf{mod}\, y$$

We wish to eliminate mod and $\div$ in favour of simpler arithmetical operations, therefore we rewrite R as

$$R : x = q \times y + r \;\land\; 0 \leq r < y$$

For quotient q and remainder r. We can establish our invariant by deleting the second conjunct from R to arrive at our invariant P. In order to truthify P initially, we declare:

$$q := 0 \tag{1}$$
$$r := x \tag{2}$$
$$0 \leq x \tag{3}$$

We need to find our bound function *bf*. When does the program terminate? When the remainder r is less than y! Thus,

$$P \land \neg(r < y) \rightarrow bf > 0$$

From this we take $bf : r + 1$, and decrease the bound by increasing r.

3 Example 2: Linear Search

Given

$$F \leq -ordered \wedge 1 \leq N \wedge F\ 1 \leq x \leq F\ N\ (F[1..N]\ in\ \mathbf{R}\ and\ N\ in\ \mathbf{Z}_{)}$$

and post-condition R:

$$R : 1 \leq i \leq N \wedge F\ i \leq x \leq F\ (i+1)$$

Since the condition

$$x \leq F(i+1)$$

is not necessarily true at every iteration, we replace 1 with the variable j. This maintains the notion that our element x is 'still ahead' in F.

This gives us the invariant

$$P : 1 \leq i \leq N \wedge F\ i \leq x \wedge x < F(i+j) \wedge i+j \leq N \wedge 0 \leq j$$

of course we can choose an even simpler invariant by replacing the expression 'i+1' in 'R' with 'j' to obtain

$$P : 1 \leq i \leq j < N \wedge F\ i \leq x \wedge x < F(j) \wedge i+1 \leq j \wedge 0 \leq j$$