

CSC165 LOOP INVARIANTS

GARY BAUMGARTNER

The following algorithm implements multiplication using addition, doubling and halving. For numbers represented in binary, doubling and halving are fast operations.

```
// Return mn.
// Precondition: m, n are integers, m ≥ 0.
MULT(m, n)
  x := m
  y := n
  z := 0
  // Loop invariant: z = mn - xy
  while x ≠ 0
    if x is odd
      z := z + y
    x := x div 2
    y := 2y
  // z = mn when done, since x = 0
  return z
```

Let's show that an iteration of the loop preserves the loop invariant: that if $z = mn - xy$ at the beginning of an iteration then it's still true at the end of that iteration.

We need to be careful about our use of variables. The values of x , y and z actually vary during an iteration. Put another way: the symbol " x " refers to different values in different places. This is not how we've been using variables in our reasoning.

For example, in $\forall x \in D, p(x) \rightarrow q(x)$ the three " x "s refer to the same value. Imagine how much more difficult our reasoning would be if p had side-effects and changed the value of x before q used it! Would the contrapositive still be equivalent?! (By the way, this is one reason that good programming should keep the amount of varying variables to a minimum).

We handle this by naming the *values* before and after the iteration: let x' , y' and z' be the values of the variables x , y and z at the start of an iteration, and let x'' , y'' and z'' be their values after that iteration.

Now we prove that

$$z' = mn - x'y' \rightarrow z'' = mn - x''y''.$$

Proof:

Suppose $z' = mn - x'y'$.

Case: x' is odd.

Then the if body is executed, so $z'' = z' + y'$.

Since x' is odd, $x' \text{ div } 2 = (x' - 1) / 2$, so $x'' = (x' - 1) / 2$.

And $y'' = 2y'$.

So

$$\begin{aligned} mn - x''y'' &= mn - ((x' - 1) / 2) * 2y' \\ &= mn - (x' - 1) y' \\ &= mn - x'y' + y' \\ &= z' + y' \\ &= z''. \end{aligned}$$

Case: x' is even.

[Left as an exercise: easier than the first case]

Since x' is odd or x' is even, in all cases $z'' = mn - x''y''$.

Therefore $z' = mn - x'y' \rightarrow z'' = mn - x''y''$.