Example proof of inductive invariant

March 1, 2011

```
private static int fi3(int x, int y)
/*: requires "x >= 0 & y >= 0"
    ensures "result = x * y" */
{
  int r = 0;
  int i = y;
  while //: inv "..."
     (i > 0) {
    i = i - 1;
    r = r + x;
  }
  return r;
}
```

The loop invariant is

```
I :  r = (y-i) * x   &   i >=0
```

To prove the three conditions, we prove that

I holds at loop entry From the precondition and the two initial assignments we have

$$x \geq 0 \quad \& \quad y \geq 0 \quad \& \quad r = 0 \quad \& \quad i = y$$

From $y \geq 0 \quad \& \quad i = y$ it follows that $i \geq 0$, which proves the second part of our invariant. Also, at loop entry,

$$r = (y - i) * x = 0 * x = 0$$

which holds as well, proving our invariant holds at loop entry.

I is maintained over loop iteration We want to prove

$$r = (y - i) * x \quad \& \quad i \geq 0 \quad \& \quad i > 0 \quad \rightarrow \quad r' = (y - i') * x \quad \& \quad i' \geq 0$$

Since $i > 0$ and $i' = i - 1$ it follows that $i' \geq 0$. The first part of the invariant holds as follows:

$$\begin{aligned} r' &= r + x \\ &= (y - i) * x + x \\ &= (y - i + 1) * x \\ &= (y - (i - 1)) * x \\ &= (y - i') * x \end{aligned}$$

Hence, the invariant is maintained across loops.

I implies postcondition after loop We need to prove that

$$r = (y - i) * x \quad \& \quad i \geq 0 \quad \& \quad \neg(i > 0) \rightarrow result = x * y$$

$$\begin{aligned} & r = (y - i) * x \quad \& \quad i \geq 0 \quad \& \quad \neg(i > 0) \\ \Leftrightarrow \quad & r = (y - i) * x \quad \& \quad i \geq 0 \quad \& \quad i \leq 0 \\ \Leftrightarrow \quad & r = (y - i) * x \quad \& \quad i = 0 \\ \Leftrightarrow \quad & r = (y - 0) * x \\ \Leftrightarrow \quad & r = y * x \end{aligned}$$

Hence, we have proven that all three conditions for the invariant hold.