

Multiplication

Given G defined by

$$G.x.0 = 0$$

$$G.x.y = G.(x * 2).(y \text{ div } 2) \quad \text{if } y \bmod 2 = 0$$

$$G.x.y = x + G.x.(y - 1) \quad \text{if } y \bmod 2 = 1$$

we are asked to derive, for integers A and B , a program to compute $G.A.B$.

* * *

As invariant we choose P given by

$$Py : \quad 0 \leq y$$

$$Pr : \quad G.A.B = r + G.x.y$$

which we initially establish with $x, y, r := A, B, 0$.

The postcondition is

$$R : \quad r = G.A.B$$

* * *

The repetition can terminate whenever $LHS.R = RHS.Pr$:

$$\begin{aligned} r &= r + G.x.y \\ &= \{ \text{arithmetic} \} \\ 0 &= G.x.y \\ \Leftarrow & \{ \text{properties of } G \} \\ y &= 0 \end{aligned}$$

and therefore $y \neq 0$ is an acceptable guard. Hence we are heading for a program of the form

```
x, y, r := A, B, 0
; do y ≠ 0 →
    “Decrease y under invariance of P ”
od
```

* * *

We observe

$$\begin{aligned} & [[\textit{Context}: P \wedge y \neq 0 \wedge y \bmod 2 = 0 \\ & \quad r + G.x.y \\ & = \quad \{ y \bmod 2 = 0, \textit{property of } G \} \\ & \quad r + G.(x * 2).(y \mathbf{div} 2) \\ &]] \end{aligned}$$

and

$$\begin{aligned} & [[\textit{Context}: P \wedge y \neq 0 \wedge y \bmod 2 = 1 \\ & \quad r + G.x.y \\ & = \quad \{ y \bmod 2 = 1, \textit{property of } G \} \\ & \quad r + x + G.x.(y - 1) \\ &]] \end{aligned}$$

and the resulting program is

```
x, y, r := A, B, 0
; do y ≠ 0 →
  if y mod 2 = 0 → x, y := x * 2, y div 2
  [] y mod 2 = 1 → r, y := r + x, y - 1
  fi
od
```

The proofs of termination and maintenance of P_y under $y := y - 1$ and $y := y \mathbf{div} 2$ are standard and we thus omit them.

E. Emmanuel Macaulay
eric@mathmeth.com

22 January 2007