Multiplication

Given G defined by

$G.x.0 = 0$

$G.x.y \quad = \quad G.(x * 2).(y \textbf{ div } 2) \qquad if \quad y \textbf{ mod } 2 \; = \; 0$

$G.x.y \quad = \quad x \; + \; G.x.(y - 1) \qquad if \quad y \textbf{ mod } 2 \; = \; 1$

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

* * *

As invariant we choose P given by

$Py : \qquad 0 \leq y$

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

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

The postcondition is

$R : \qquad r \; = \; G.A.B$

* * *

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

$$
\begin{array}{ll}
 & r \quad = \quad r \; + \; G.x.y \\
= & \qquad \{ \quad \text{arithmetic} \quad \} \\
 & 0 \; = \; G.x.y \\
\Leftarrow & \qquad \{ \quad \text{properties of} \quad G \; \} \\
 & y = 0
\end{array}
$$

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

$$
\begin{array}{l}
x, y, r \quad := \quad A, B, 0 \\
; \textbf{ do } \quad y \neq 0 \quad \rightarrow \\
\qquad \text{“Decrease } \quad y \quad \text{under invariance of } \quad P \text{ ”} \\
\textbf{ od}
\end{array}
$$

* * *

We observe

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

and

$$
\begin{array}{ll}
|[& \textit{Context:} \quad P \quad \wedge \quad y \neq 0 \quad \wedge \quad y \ \mathbf{mod}\ 2 \ = \ 1 \\
& \quad r \ + \ G.x.y \\
& = \qquad \{\ y \ \mathbf{mod}\ 2 \ = \ 1 \ \text{, property of } \ G\ \} \\
& \quad r \ + \ x \ + \ G.x.(y-1) \\
]| &
\end{array}
$$

and the resulting program is

$$
\begin{array}{l}
x, y, r \quad := \quad A, B, 0 \\
\ ; \mathbf{do} \quad y \neq 0 \quad \rightarrow \\
\quad \mathbf{if} \quad y \ \mathbf{mod}\ 2 \ = \ 0 \quad \rightarrow \quad x, y \quad := \quad x * 2,\ y \ \mathbf{div}\ 2 \\
\quad [] \quad y \ \mathbf{mod}\ 2 \ = \ 1 \quad \rightarrow \quad r, y \quad := \quad r + x,\ y - 1 \\
\quad \mathbf{fi} \\
\mathbf{od}
\end{array}
$$

The proofs of termination and maintenance of Py 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