At least one zero element

We define, for $0 \le n \le N$:

$$G.n \equiv \langle \exists i : \quad n \le i < N : \quad f.i = 0 \rangle$$

and our task is to derive a program which computes $G.0$.

*   *   *

We first derive a recurrence relation for G . We have

$G.n \equiv false \qquad \text{if} \quad n = N$

Moreover we observe

$$
\begin{array}{ll}
 & G.n \\
= & \{ \text{ definition of } G \ \} \\
 & \langle \exists i : \quad n \le i < N : \quad f.i = 0 \rangle \\
= & \{ \text{ split off } \ i = n \ \text{; requires } \ n < N \ \} \\
 & f.n = 0 \quad \vee \quad \langle \exists i : \quad n+1 \le i < N : \quad f.i = 0 \rangle \\
= & \{ \text{ definition of } G \ \} \\
 & f.n = 0 \quad \vee \quad G.(n+1)
\end{array}
$$

*   *   *

The postcondition of our program is

$R : \qquad G.0 \equiv r$

We choose as invariant P which is the conjunction of

$Pn : \qquad 0 \le n \le N$

$Pr : \qquad G.0 \equiv r \vee G.n$

which we establish initially with $r, n \ := \ false, 0$.

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

$$
\begin{array}{ll}
 & r \equiv r \vee G.n \\
= & \{ \text{ predicate calculus } \} \\
 & G.n \Rightarrow r \\
\Leftarrow & \{ \text{ property of } G \ \}
\end{array}
$$

$n = N$

hence $n \neq N$ is an acceptable guard. We are heading for a program of the form

$r, n \quad := \quad false, \quad 0$
; **do** $n \neq N \quad \rightarrow$
"Increase n under invariance of P "
od

* * *

We observe
$|[$ *Context:* $P \wedge n \neq N$

$r \vee G.n$
$= \quad \{$ property of G , $n < N$ $\}$
$r \vee f.n = 0 \vee G.(n+1)$

$]|$

hence our solution:

$r, n \quad := \quad false, \quad 0$
; **do** $n \neq N \quad \rightarrow$
$r, n \quad := \quad r \vee f.n = 0, \quad n+1$
od

The proofs of termination and maintenance of Pn under $n := n+1$ are standard hence we omit them.

E. Emmanuel Macaulay
eric@mathmeth.com
25 January 2007