The existence of a particular subsequence

Given integer array $A[0..N)$, $1 \leq N$, we wish to develop a program establishing postcondition

$R: \quad b \equiv G.N$

where, for $0 \leq n \leq N$:

$G.n \;\equiv\; \langle \exists p, q \;:\; 0 \leq p < q < n \;:\; A.p - A.q \quad \leq \quad 2 \rangle$

* *
*

We are heading for a program of the form

$n := 0;\; b := false;$
$\{$inv: $b \equiv G.n\}$
do $\;n \neq N \quad \rightarrow$
  "Establish $\;b \;\equiv\; G.(n+1)$"
  $;n := n+1$
od
$\{b \equiv G.N\}$

With regards to termination we appeal to the well-known

Lemma

For constant N, $0 \leq N$, the following program terminates:

$n := 0$
;**do** $\;n \neq N \quad \rightarrow \quad ... \quad n \;:=\; n+1 \quad$ **od**

where clearly ... does not contain assignments to n.

End Lemma.

* *
*

In order to refine "Establish $\;b \;\equiv\; G.(n+1)$" we try to derive a simple recurrence relation for G:

$$
\begin{array}{ll}
 & G.(n+1) \\
= & \quad \{ \; G \; \} \\
 & \langle \exists p,q \; : \; 0 \le p < q < n+1 \; : \; A.p - A.q \quad \le \quad 2 \rangle \\
= & \quad \{ \text{ split off } q = n \; \} \\
 & \langle \exists p,q \; : \; 0 \le p < q < n \; : \; A.p - A.q \quad \le \quad 2 \rangle \; \vee \; \langle \exists p \; : \; 0 \le p < n \; : \; A.p - A.n \quad \le \quad 2 \rangle \\
= & \quad \{ \; G \; \} \\
 & G.n \quad \vee \quad \langle \exists p \; : \; 0 \le p < n \; : \; A.p - A.n \quad \le \quad 2 \rangle \\
= & \quad \{ \text{ see sidebar calculation } \} \\
 & G.n \quad \vee \quad \langle \downarrow p \; : \; 0 \le p < n \; : \; A.p \rangle - A.n \quad \le \quad 2 \\
= & \quad \{ \text{ introducing } H.n = \langle \downarrow p \; : \; 0 \le p < n \; : \; A.p \rangle \; \} \\
 & G.n \quad \vee \quad H.n - A.n \; \le \; 2
\end{array}
$$

We strengthen the invariant with

$c = H.n$

and hence find for "Establish $b \equiv G.(n+1)$"

$b \quad := \quad b \quad \vee \quad c - A.n \; \le \; 2;$
"Establish $c = H.(n+1)$" .

Sidebar calculation

$$
\begin{array}{ll}
 & \langle \exists p \; : \; 0 \le p < n \; : \; A.p - A.n \quad \le \quad 2 \rangle \\
= & \quad \{ \text{ lattice theory } \} \\
 & \langle \downarrow p \; : \; 0 \le p < n \; : \; A.p - A.n \rangle \quad \le \quad 2 \\
= & \quad \{ \; + \text{ over } \downarrow \; \} \\
 & \langle \downarrow p \; : \; 0 \le p < n \; : \; A.p \rangle - A.n \quad \le \quad 2
\end{array}
$$

End of Sidebar calculation.

* *
*

With the observations

$G.0 \equiv false$

$H.0 = \infty$

$H.(n+1) \;=\; H.n \downarrow A.n$

we may collect the pieces to arrive at our solution:

$n := 0;\; b := false;\; c := \infty;$
$\{\text{inv:} \quad (b \equiv G.n) \quad \wedge \quad c = H.n\}$
do $\;n \neq N \quad \rightarrow$
$\qquad b \quad := \quad b \;\vee\; c - A.n \;\leq\; 2$
$\qquad ;c \quad := \quad c \downarrow A.n$
$\qquad ;n \quad := \quad n + 1$
od
$\{b \equiv G.N\}$

*   *
*

We can say a bit more, however. As *true* is a fixpoint of $\vee$ we may weaken the termination condition to $n = N \;\vee\; b$. Our guard is now $n \neq N \;\wedge\; \neg b$ so $b \equiv false$ holds within the loop allowing the simplification of the assignment to b. Thus we arrive at our final program

$n := 0;\; b := false;\; c := \infty;$
$\{\text{inv:} \quad (b \equiv G.n) \quad \wedge \quad c = H.n\}$
do $\;n \neq N \;\wedge\; \neg\, b \quad \rightarrow$
$\qquad b \quad := \quad c - A.n \;\leq\; 2$
$\qquad ;c \quad := \quad c \downarrow A.n$
$\qquad ;n \quad := \quad n + 1$
od
$\{b \equiv G.N\}$

12 November 2007

E. Emmanuel Macaulay
eric@mathmeth.com