All array elements positive?

Problem

Derive a solution to the following :

$|[$ **con** N : int $\{0 \leq N\}$; A :**array**$[0..N)$ **of** int;

var r : bool;

S

$\{(0): \quad r = \langle \forall i : \ 0 \leq i < N : \ 0 \leq f.i \rangle\}$

$]|$.

Solution

The only way we have to establish the postcondition is the repetitive construct. For the invariant of the repetition we generalize (0) by introducing a fresh variable n, thus obtaining the conjunction of

(1) $\quad r \equiv \langle \forall i : \ 0 \leq i < n : \ 0 \leq f.i \rangle \qquad ,$

(2) $\quad 0 \leq n \leq N \qquad ,$

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

As is customary given our chosen technique we are heading for an S of the form

$|[$ **var** n : int;

$n, r \ := \ 0, true \ \{(1) \wedge (2)\}$

; **do** $\quad n \neq N \quad \rightarrow$

"Maintain (1) under $n \ := \ n + 1$"

$n \ := \ n + 1$

od $\quad \{(1) \ \wedge \ n = N$ hence$\}$

$\{(0)\}$

$]|$.

As both the proofs of termination and maintenance of (2) under $n \ := n + 1$ are standard and trivial we omit them.

* * *

We refine "Maintain (1) under $n \ := \ n + 1$" by observing

$|[\ (1) \ \wedge \ (2) \ \wedge \ n \neq N$

$\triangleright$

$\langle \forall i : \ 0 \leq i < n + 1 : \ 0 \leq f.i \rangle$

$=$ $\qquad \{$ split off $i = n, \ n < N$; (1) $\}$

$r \ \wedge \ 0 \leq f.n$

]|.

As our program scheme ensures that $0 \leq n < N$ holds within the body of the loop $r \ := \ r \ \wedge \ 0 \leq f.n$ is a suitable refinement for "Maintain (1) under $n \ := \ n + 1$". Hence the final program

|[**var** n : int;

$n, r \ := \ 0, true \ \{(1) \wedge (2)\}$

; **do** $n \neq N \quad \rightarrow$

$r \ := \ r \ \wedge \ 0 \leq f.n$

; $n \ := \ n + 1$

od $\{(1) \ \wedge \ n = N$ hence$\}$

$\{(0)\}$

]|

Birmingham, 16 October 2006