The number of array element pairs whose product is positive

Problem

We must derive a solution to the following :

$|[$ **con** N : int $\{1 \le N\}$; A :**array**$[0..N)$**of** int;

  var r : int;

    S

  $\{(0): \quad r = \langle \#p, q:\ 0 \le p < q < N:\ 0 \le A.p * A.q \rangle\}$

$]|$

Solution

As A is an arbitrary function the only way we have to establish (0) is the repetitive construct. For the invariant of the repetition we generalise (0) by the (misnamed) technique of replacing constant N by fresh variable n thus obtaining the conjunction of

(1) $\quad r = \langle \#p, q:\ 0 \le p < q < n:\ 0 \le A.p * A.q \rangle$

(2) $\quad 0 \le n \le N$

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

As is standard with our chosen technique we are heading for an S of the form

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

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

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

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

    $n\ :=\ n+1$

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

$\{(0)\}$

$]|$

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

*   *   *

Assuming $(1)\ \wedge\ (2)\ \wedge\ n \ne N$ we investigate an increase of $n\ :=\ n+1$:

  $\langle \#p, q:\ 0 \le p < q < n+1:\ 0 \le A.p * A.q \rangle$

$=$ { split off $q = n$, $n < N$; (1) }

  $r + \langle \#p:\ 0 \le p < n:\ 0 \le A.p * A.n \rangle$

$=$ { case analysis }

$$\begin{cases} r + \langle \# p:\ 0 \le p < n:\ 0 \le A.p \rangle, & \text{if } 0 < A.n \\ r + n, & \text{if } 0 = A.n \\ r + \langle \# p:\ 0 \le p < n:\ A.p \le 0 \rangle, & \text{if } A.n < 0 \end{cases}$$

= { (3) and (4) }

$$\begin{cases} r + s, & \text{if } 0 < A.n \\ r + n, & \text{if } 0 = A.n \\ r + t, & \text{if } A.n < 0 \end{cases}$$

where (3) and (4) are obtained via the standard step of strengthening the invariant with

(3) $s = \langle \# p:\ 0 \le p < n:\ 0 \le A.p \rangle$

(4) $t = \langle \# p:\ 0 \le p < n:\ A.p \le 0 \rangle$

which we establish with $n, s, t\ :=\ 0, 0, 0$ and so our next version of S is then

|[**var** n, s, t : int;

  $n, r, s, t\ :=\ 0, 0, 0, 0$ $\{(1) \wedge (2) \wedge (3) \wedge (4)\}$

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

    if $0 < A.n \rightarrow r\ :=\ r + s$

     [] $0 = A.n \rightarrow r\ :=\ r + n$

     [] $A.n < 0 \rightarrow r\ :=\ r + t$

    fi

    $\{(n\ :=\ n + 1).(1)\}$ $\{?(n\ :=\ n + 1).(3)\}$ $\{?(n\ :=\ n + 1).(4)\}$

    ;$n\ :=\ n + 1$

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

$\{(0)\}$

]|

* * *

It remains to address the queried assertions. Assuming (2) $\wedge$ (3) $\wedge$ $n \neq N$ we observe

$\langle \# p:\ 0 \le p < n + 1:\ 0 \le A.p \rangle$

= { split off $p = n$, $n < N$; (3) }

$s + \#.(0 \le A.n)$

= { case analysis }

$$\begin{cases} s, & \text{if } A.n < 0 \\ s + 1, & \text{if } 0 \le A.n \end{cases}$$

and assuming (2) $\wedge$ (4) $\wedge$ $n \neq N$

$\langle \# p:\ 0 \le p < n + 1:\ A.p \le 0 \rangle$

$= \quad$ { split off $p = n$, $n < N$; (4) }

$t + \#.(A.n \leq 0)$

$= \quad$ { case analysis }

$$\begin{cases} t, & \text{if } 0 < A.n \\ t+1, & \text{if } A.n \leq 0 \end{cases}$$

and so we arrive at our final version for S

|[**var** n, s, t : int;

$n, r, s, t \ := \ 0, 0, 0, 0$ $\{(1) \wedge (2) \wedge (3) \wedge (4)\}$

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

$\{(1) \ \wedge \ (2) \ \wedge \ (3) \ \wedge \ (4) \ \wedge \ n \neq N\}$

if $0 < A.n \quad \rightarrow \quad r, s \quad := \quad r + s, \ s + 1$

[] $0 = A.n \quad \rightarrow \quad r, s, t \quad := \quad r + n, \ s + 1, \ t + 1$

[] $A.n < 0 \quad \rightarrow \quad r, t \quad := \quad r + t, \ t + 1$

fi

$\{(n \ := \ n+1).(1)\} \quad \{(n \ := \ n+1).(3)\} \quad \{(n \ := \ n+1).(4)\}$

;$n \ := \ n + 1$

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

$\{(0)\}$

]|

Acknowledgements

This note was written under the close supervison of Apurva Mehta and Jeremy Weissmann. Their guidance has been invaluable.

Birmingham, 12 October 2006