

The number of array element pairs whose product is positive

Problem

We must derive a solution to the following :

```
[[ con  $N : \text{int } \{1 \leq N\}$ ;  $A : \text{array}[0..N]$  of  $\text{int}$ ;  
   var  $r : \text{int}$ ;  
    $S$   
    $\{(0) : r = \langle \#p, q : 0 \leq p < q < N : 0 \leq A.p * A.q \rangle\}$   
]]
```

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

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

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

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  $n : \text{int}$ ;  
    $n, r := 0, 0 \{(1) \wedge (2)\}$   
   do  $n \neq N \rightarrow$   
     “Maintain (1) under  $n := n + 1$ ”  
      $n := n + 1$   
   od  $\{(1) \wedge n = N \text{ hence}\}$   
    $\{(0)\}$   
]]
```

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

* * *

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

$$\begin{aligned} & \langle \#p, q : 0 \leq p < q < n + 1 : 0 \leq A.p * A.q \rangle \\ = & \quad \{ \text{split off } q = n, n < N; (1) \} \\ & r + \langle \#p : 0 \leq p < n : 0 \leq A.p * A.n \rangle \\ = & \quad \{ \text{case analysis } \} \end{aligned}$$

$$\begin{aligned}
& \begin{cases} r + \langle \#p : 0 \leq p < n : 0 \leq A.p \rangle, & \text{if } 0 < A.n \\ r + n, & \text{if } 0 = A.n \\ r + \langle \#p : 0 \leq p < n : A.p \leq 0 \rangle, & \text{if } A.n < 0 \end{cases} \\
= & \{ (3) \text{ and } (4) \} \\
& \begin{cases} r + s, & \text{if } 0 < A.n \\ r + n, & \text{if } 0 = A.n \\ r + t, & \text{if } A.n < 0 \end{cases}
\end{aligned}$$

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

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

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

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) ∧ (2) ∧ (3) ∧ (4) }
  ;do  n ≠ N →
      if 0 < A.n → r := r + s
      [] 0 = A.n → r := r + n
      [] A.n < 0 → r := r + t
      fi
      { (n := n + 1).(1) } {?(n := n + 1).(3)} {?(n := n + 1).(4)}
      ;n := n + 1
      od { (1) ∧ n = N hence }
  {(0)}
]]

```

* * *

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

$$\begin{aligned}
& \langle \#p : 0 \leq p < n + 1 : 0 \leq A.p \rangle \\
= & \{ \text{split off } p = n, n < N; (3) \} \\
& s + \#.(0 \leq A.n) \\
= & \{ \text{case analysis} \} \\
& \begin{cases} s, & \text{if } A.n < 0 \\ s + 1, & \text{if } 0 \leq A.n \end{cases}
\end{aligned}$$

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

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

$$\begin{aligned}
&= \{ \text{split off } p = n, n < N; (4) \} \\
&\quad t + \#.(A.n \leq 0) \\
&= \{ \text{case analysis} \} \\
&\quad \begin{cases} t, & \text{if } 0 < A.n \\ t + 1, & \text{if } A.n \leq 0 \end{cases}
\end{aligned}$$

and so we arrive at our final version for S

```

[[ var n, s, t : int;
   n, r, s, t := 0, 0, 0, 0 {(1) ∧ (2) ∧ (3) ∧ (4)}
  ;do n ≠ N →
     {(1) ∧ (2) ∧ (3) ∧ (4) ∧ n ≠ N}
     if 0 < A.n → r, s := r + s, s + 1
       [] 0 = A.n → r, s, t := r + n, s + 1, t + 1
       [] A.n < 0 → r, t := r + t, t + 1
     fi
     {(n := n + 1).(1)} {(n := n + 1).(3)} {(n := n + 1).(4)}
     ;n := n + 1
   od {(1) ∧ n = N hence}
  {(0)}
]]

```

Acknowledgements

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

Birmingham, 12 October 2006