The maximum squared difference

Given integer array A of length N , $1 \le N$, we are asked to compute the maximum squared difference for A . Formally, for natural numbers p and q and integer r our program establishes

$$R: \quad r \;=\; \langle \uparrow p,q: \;\; 0 \le p < q < N: \;\; (A.p - A.q)^2 \rangle$$

* * *

Jeremy Weissmann conjectures that $\langle \uparrow i :\; : \; i^2 \rangle \;=\; (\langle \uparrow i :\; : \; i \rangle)^2 \;\uparrow\; (\langle \uparrow i :\; : \; -i \rangle)^2$ and we therefore have to compute the maximum of $r0^2$ and $r1^2$ where $r0$ is defined by

$$R0: \quad r0 \;=\; \langle \uparrow p,q: \;\; 0 \le p < q < N: \;\; A.p - A.q \rangle$$

and $r1$ is

$$R1: \quad r1 \;=\; \langle \uparrow p,q: \;\; 0 \le p < q < N: \;\; A.q - A.p \rangle$$

We focus on computing $r0$ first.

* * *

We investigate our standard invariant, P , which is the conjunction of

$$Pr0: \quad r0 \;=\; \langle \uparrow p,q: \;\; 0 \le p < q < n: \;\; A.p - A.q \rangle$$

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

which we initially establish with $n, r0 \;:=\; 0, -\infty$. We are heading for a program of the form

$n, r0, \;:=\; 0, -\infty$
; **do** $n \ne N \;\rightarrow$
“Increase n by 1 under invariance of P ”
od

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

* * *

We observe

|[*Context:* $P \;\wedge\; n \ne N$

$\langle \uparrow p,q: \;\; 0 \le p < q < n+1: \;\; A.p - A.q \rangle$

$=$ { split off $q = n$ requires $n < N$ which follows from $Pn \;\wedge\; n \ne N$ }

$\langle \uparrow p,q: \;\; 0 \le p < q < n: \;\; A.p - A.q \rangle \;\uparrow\; \langle \uparrow p: \;\; 0 \le p < n: \;\; A.p - A.n \rangle$

$=$ { $Pr0$; $+$ over $\uparrow$; $Ps0$ }

$r0 \;\uparrow\; (s0 - A.n)$

]|

where we strengthen P with

$Ps0: \quad s0 = \langle \uparrow p : \; 0 \le p < n : \; A.p \rangle$

We establish $Ps0$ initially with $n, s0 := 0, -\infty$.

At this point we have

$$
\begin{array}{l}
|[\quad \textit{Context:} \quad P \quad \wedge \quad n \neq N \\
\qquad \{ \quad Pr0 \quad \wedge \quad Ps0 \quad \} \\
\qquad r0 \quad := \quad r0 \quad \uparrow \quad (s0 \; - A.n) \\
\qquad \{ \quad (n \; := \; n+1).Pr0 \quad \} \\
]|
\end{array}
$$

giving us a program of the form

$$
\begin{array}{l}
\quad n, r0, s0 \quad := \quad 0, \quad -\infty, \quad -\infty \\
; \mathbf{do} \quad n \neq N \quad \rightarrow \\
\qquad \text{“Maintain} \quad Ps0 \quad \text{under} \quad n, r0 \quad := \quad n+1, \quad r0 \; \uparrow \; (s0 \; - A.n) \text{ ”} \\
\quad \mathbf{od}
\end{array}
$$

* * *

We turn our attention to the maintenance of $Ps0$. We observe

$$
\begin{array}{l}
|[\quad \textit{Context:} \quad P \quad \wedge \quad n \neq N \\
\qquad \langle \uparrow p : \quad 0 \le p < n+1 : \quad A.p \rangle \\
\quad = \qquad \{ \quad \text{split off} \quad p = n \quad \text{, requires} \quad 0 \le n \quad \text{which follows from} \quad Pn \; \} \\
\qquad \langle \uparrow p : \quad 0 \le p < n : \quad A.p \rangle \quad \uparrow \quad A.n \\
\quad = \qquad \{ \; Ps0 \; \} \\
\qquad s \; \uparrow \; A.n \\
]|
\end{array}
$$

We now have

$$
\begin{array}{l}
|[\quad \textit{Context:} \quad P \quad \wedge \quad n \neq N \\
\qquad \{ \quad Ps0 \quad \} \quad s \quad := \quad s \; \uparrow \; A.n \quad \{ \quad (n \; := \; n+1).Ps0 \quad \} \\
]|
\end{array}
$$

giving us

$$
\begin{array}{l}
\quad n, r0, s0 \quad := \quad 0, \quad -\infty, \quad -\infty \\
;\ \mathbf{do} \quad n \neq N \quad \rightarrow \\
\qquad ;\ n, r0, s0 \quad := \quad n+1, \quad r0 \ \uparrow \ (s0 \ - A.n), \quad s \ \uparrow \ A.n \\
\quad \mathbf{od}
\end{array}
$$

The computation of $Pr1$ is similar. Strengthening P with invariants

$Pr1: \quad r1 \quad = \quad \langle \uparrow p, q: \quad 0 \ \leq \ p \ < \ q \ < \ n: \quad A.q \ - \ A.p \rangle$

$Ps1: \quad s1 \quad = \quad \langle \uparrow p: \quad 0 \ \leq \ p \ < \ n: \quad -A.p \rangle$

a solution is

$$
\begin{array}{l}
\quad n := 0 \\
;\ r0, s0 \quad := \quad -\infty,\ -\infty \\
;\ r1, s1 \quad := \quad -\infty,\ -\infty \\
;\ \mathbf{do} \quad n \neq N \quad \rightarrow \\
\qquad ;\ r0, s0 \quad := \quad r0 \ \uparrow \ (s0 \ - A.n), \quad s \ \uparrow \ A.n \\
\qquad ;\ r1, s1 \quad := \quad r1 \ \uparrow \ (s0 \ + A.n), \quad s \ \uparrow \ -A.n \\
\qquad ;\ n \quad := \quad n+1 \\
\quad \mathbf{od} \\
;\ r \quad := \quad r0^2 \ \uparrow \ r1^2
\end{array}
$$

E. Emmanuel Macaulay
eric@mathmeth.com

19th January 2007