A sequel to AvG52a/WF67a

(This note is not self-contained.)

Like in AvG52a/WF67a, we address the problem of constructing a program square satisfying functional specification

$$\{h = [U]\} \text{ square } \{h = [U] \underline{m} [U]\} .$$

Like in AvG52a/WF67a, the solution consists of three steps, dealing with three different concerns: (i) the correctness of the final answer, (ii) the desired in-situity, and (iii) the implementation of the algorithm in terms of the array H.

Unlike in AvG52a/WF67a, we shall not require that h remains a ring. The resulting program will be equally efficient, much shorter in text, but require a slightly more complicated correctness argument. The existence of such a solution was first pointed out to us by Jaap van der Woude.

(i) Again we choose

P: $\quad h \underline{m} [pX] = [U] \underline{m} [U]$

as an invariant. This time we decide to shrink X by one element at a time. The first version then becomes

$\{h = [U]\}$
$p, X : pX = U \quad \{P\}$
$; \underline{do}\ X \neq \text{empty}$
$\rightarrow q, Y :\ qY = X$
{hence we have in combination with P:

$h \ \underline{m}\ [pq\,Y] = [U]\ \underline{m}\ [U]$, or
– using the one-pivot rule from ring calculus, pivot q –
$h\ \underline{m}\ [pq]\ \underline{m}\ [q\,Y] = [U]\ \underline{m}\ [U]$, so that
the statements}
; $h := h\ \underline{m}\ [pq]$
; $p, X := q, Y$
{reestablish P}

<u>od</u>
{$X = \text{empty} \wedge P$, hence
$h\ \underline{m}\ [p] = [U]\ \underline{m}\ [U]$, so that}
; $h := h\ \underline{m}\ [p]$
{establishes $h = [U]\ \underline{m}\ [U]$} .

(ii) The desired in-situity is based on the invariance of

Q: $\quad Q0 \vee Q1$

where $Q0$ and $Q1$ are given by

$Q0$: $\quad h = [FpGX]$
$Q1$: $\quad h = [Fp]\ \underline{m}\ [GX]$.

The condition Q will inherit its truth alternatingly from $Q0$ and $Q1$, to start with from $Q0$ by the initialization $F, G :=$ empty, empty . For later purposes we shall show separately how a step of the repetition transforms the truth of $Q0$ into the truth of $Q1$ and vice versa.

{$h = [U]$}
$p, X : pX = U$
; $F, G :=$ empty, empty
{$Q0$, hence Q}

; <u>do</u> $X \neq$ empty
→

{Q0}	{Q1}

q, Y : $qY = X$

{hence $h = [FpGqY]$}	{hence $h = [Fp]\ \underline{m}\ [GqY]$}

; $h := h\ \underline{m}\ [pq]$

{hence $h = [FpGqY]\ \underline{m}\ [pq]$, or —ring calculus— $h = [FpY]\ \underline{m}\ [Gq]$}	{hence $h = [Fp]\ \underline{m}\ [GqY]\ \underline{m}\ [pq]$, or —ring calculus— $h = [FpYGq]$}

; $F, G := G, Fp$

{hence $h = [GY]\ \underline{m}\ [Fq]$}	{hence $h = [GYFq]$}

; $p, X := q, Y$

{hence $h = [GX]\ \underline{m}\ [Fp]$, i.e. Q1}	{hence $h = [GXFp]$, i.e. Q0}

<u>od</u>
; $h := h\ \underline{m}\ [p]$

<u>Note</u> When Q1 is established by a Q0 - Q1 transition, sequence $G \neq$ empty, so that the expression $[GX]$ occurring in Q1 is a legal expression.
(End of Note.)

(iii) In this last step we are concerned with the elimination of the thought variables, in particular with the elimination of the guard $X \neq empty$ and the computation of q, the first element of a nonempty X.

Guided by Q0 we would propose

$$L0: \quad q = first.(XFp) \quad \wedge \quad r = first.(Fp) .$$

Guided by Q1 we would propose

$$L1: \quad q = first.(XG) \quad \wedge \quad r = first.(GX)$$

Since we are not able to abstract from the differences between the expressions L0 and L1, we choose to maintain

$$L: \quad L0 \vee L1 .$$

Like Q, L will inherit its truth alternatingly from L0 and L1, to start with from L0 by the initialization $q, r := H.p, p$ (from Q0 and the representational convention). Both in case L0 and in case L1 the guard $X \neq empty$ is expressed by $q \neq r$, and in both cases the statement $q, Y : qY = X$ is a skip.

The invariance of L is achieved by

{L0}	{L1 and $X = qY$}

$$; h := h \ \underline{m} \ [pq]$$

{$h = [FpY] \ \underline{m} \ [Gq]$, from the previous version, and $r = first.(Fp)$, from L0}	{$h = [FpYGq]$, from the previous version, and $r = first.(GX)$, from L1, i.e. $r = first.(GqY)$}

$$; \ q := H.p$$

$\{q = \mathrm{first}.(YFp) \wedge r = \mathrm{first}.(FpY)\}$ $\quad$ $\{q = \mathrm{first}.(YGq) \wedge r = \mathrm{first}.(Gq)\}$

$$; \ F, G := G, Fp$$

$\{q = \mathrm{first}.(YG) \wedge r = \mathrm{first}.(GY)\}$ $\quad$ $\{q = \mathrm{first}.(YFq) \wedge r = \mathrm{first}.(Fq)\}$

$$; \ p, X := q, Y$$

$\{L1\}$ $\quad$ $\{L0\}$.

The ultimate program text is

$\{p = \text{any element of the ring to be squared}\}$
$q, r := H.p, p$
; **do** $q \neq r$
$\rightarrow$ $H: \mathrm{swap}(p, q)$
; $q := H.p$; $p := q$
od .

Eindhoven,
24 September 1985

A.J.M. van Gasteren,
W.H.J. Feijen