A nice little program

For fixed $N : N \geq 0$ and A we present a program for the computation of $(\underline{S} i : 0 \leq i < N : A^i)$. The time complexity of this program is $\mathcal{O}(\log N)$. As addition and multiplication are the only operations that are applied to values of A's type, A may be any value for which such operations are defined ; A may, for instance, be a matrix.

The derivation of the program is, once one starts looking for it, quite standard.

Let, for $k : k \geq 0$, $\quad s(k) = (\underline{S} i : 0 \leq i < k : A^i)$,

then: $\quad s(0) = 0$, and

for $k : k \geq 0$: $\quad s(k+1) = s(k) + A^k$, and

for $k : k \geq 0$: $\quad s(2*k) = (1 + A^k) * s(k)$.

The program is:

```
{ N ≥ 0 }
 x, y, c, r := 0, 1, 1, N ; do c ≤ r → c := c*2 od
{ invariant:   x = s(n) ∧ y = A^n ∧ N = n*c+r ∧
  0 ≤ r < c ∧ (E i: 0 ≤ i : c = 2^i) ; variant function : c }
; do c ≠ 1 → x, y, c := (1+y)*x, y*y, c/2
             ; do c ≤ r → x, y, r := x+y, A*y, r-c od
 od
{ x = s(N) }.
```

Note that the variable n in the invariant is an auxiliary variable only.

Eindhoven, 1985.11.19
Rob Hoogerwoord.