Base X to decimal conversion

We define, for $0 \leq n \leq N$:

$$G.n = \langle \Sigma\, i : \quad n \leq i < N : \quad f.i * X^{i-n} \rangle$$

and our task is to derive a program which computes $G.0$.

* * *

We first derive a recurrence relation for G . We have

$G.n = 0 \qquad \text{if} \quad n = N$

Moreover we observe

$$\begin{array}{ll} & G.n \\ = & \{ \text{ definition of } G \} \\ & \langle \Sigma\, i : \quad n \leq i < N : \quad f.i * X^{i-n} \rangle \\ = & \{ \text{ split off } i = n \text{ , requires } n < N \} \\ & f.n + \langle \Sigma\, i : \quad n+1 \leq i < N : \quad f.i * X^{i-n} \rangle \\ = & \{ \text{ algebra } \} \\ & f.n + \langle \Sigma\, i : \quad n+1 \leq i < N : \quad f.i * X^{i-n-1} * X \rangle \\ = & \{ * \text{ over } \Sigma \text{ ; arithmetic } \} \\ & f.n \quad + \quad X * \langle \Sigma\, i : \quad n+1 \leq i < N : \quad f.i * X^{i-(n+1)} \rangle \\ = & \{ \text{ definition of } G \} \\ & f.n \quad + \quad X * G.(n+1) \end{array}$$

* * *

The postcondition of our program is

$R : \qquad G.0 = r$

We choose as invariant P , which is the conjunction of

$Pn : \qquad 0 \leq n \leq N$

$Pr : \qquad G.0 \quad = \quad r \quad + \quad X^n * G.n$

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

The repetition can terminate whenever $RHS.R \ = \ RHS.Pr$:

$$\begin{array}{ll} & r \ = \ r + X^n * G.n \\ = & \{ \text{ algebra } \} \\ & 0 \ = \ X^n * G.n \\ \Leftarrow & \{ \text{ property of } G \} \\ & n = N \end{array}$$

and hence $n \neq N$ is an acceptable guide. We are heading for a program of the form

$r, n \ := \ 0, 0$
; **do** $n \neq N \ \rightarrow$
  "Increase n under invariance of P "
  od

* * *

We observe

$$\begin{array}{ll} |[& \textit{Context:} \quad P \ \wedge \ n \neq N \\ & r + X^n * G.n \\ = & \{ \text{ property of } G \ , \ n < N \} \\ & r + X^n * (f.n + X * G.(n+1)) \\ = & \{ \text{ algebra } \} \\ & r + X^n * f.n + X^{n+1} * G.(n+1) \\ ]| & \end{array}$$

hence our solution is

$r, n \ := \ 0, 0$
; **do** $n \neq N \ \rightarrow$
  $r, n \ := \ r + X^n * f.n, \ \ n+1$
  od

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

E. Emmanuel Macaulay
eric@mathmeth.com

24 January 2007