On the ascendingness - test and on tail invariants

One of our standard programming exercises for first-year students is the "ascendingness - test": given an integer array $f[0..N)$, $0 \leq N$, the question is to derive a programming establishing postcondition

$$R: \quad x \equiv \text{"} f[0..N) \text{ is ascending"} \quad .$$

The solution that will emerge critically depends on what formalization is taken for f's ascendingness. One —meanwhile classical— possibility is this:

$$(\forall i,j : 0 \leq i < j < N : f.i \leq f.j)$$

Based on this formulation the program is readily derived, in an absolutely standard way, by adopting as an invariant $R(N:=n)$. The resulting derivation is, however, a little bit laborious; also one may feel a little bit annoyed by the circumstance that —almost inevitably— the need arises to strengthen the invariant with the somewhat outlandish

$$y = (\underline{max}\, i : 0 \leq i < n : f.i) \quad .$$

But for the rest, a derivation along the above lines runs very smooth and does not evoke case analysis.

How different is the situation if one chooses to formalize f's ascendingness by the very traditional

$$(\forall i : 1 \le i < N : f.(i-1) \le f.i) \quad .$$

Now let us investigate our standard invariant for such problems, viz $P0 \wedge P1$ given by

$P0$: $0 \le n \le N$

$P1$: $x \equiv (\forall i : 1 \le i < n : f.(i-1) \le f.i)$

As always, we seek to increment n by 1 and carry out the corresponding calculation:

$$(\forall i : 1 \le i < n+1 : f.(i-1) \le f.i)$$
$$= \quad \{\text{splitting off the term with } i = n\}$$

However, this splitting off is only possible whenever n is in the range of the quantification, in particular whenever $1 \le n$. And here we are in trouble, because the needed condition $1 \le n$ cannot be expelled from any reasonably chosen guard nor from $P0$. The way out seems to replace $P0$ with the stronger

$P0'$: $1 \le n \le N$,

but now we are in trouble again because the initial value of N could be 0. Thus a case-distinction between $0 = N$ and $1 \le N$ is threatening. The way out seems to replace $P0'$ with

$P0''$: $1 \le n$,

and to assign $n < N$ as a conjunct to the guard. But then the demonstration that $P1 \wedge n \ge N \Rightarrow R$ becomes inconvenient because we will have to come up with benevolent thought values for $f[N..\infty)$.

In short: trouble all around.

We might suspect that the chosen formalization of f's ascendingness is the culprit, but this is not the case at all as is witnessed by the following derivation.

We define K.n for $1 \le n$ by

$$K.n \equiv (\forall i : n \le i < N : f.(i-1) \le f.i)$$

As invariant we choose $Q0 \wedge Q1$ given by

Q0: $1 \le n$

Q1: $K.1 \equiv x \wedge K.n$.

The postcondition is

R: $K.1 \equiv x$.

The repetition can terminate whenever RHS.R $\equiv$ RHS.Q1 :

$$\begin{array}{ll} & x \equiv x \wedge K.n \\ = & \quad \{\text{pred. calc.}\} \\ & \neg x \vee K.n \\ \Leftarrow & \quad \{\text{def. of } K\} \\ & \neg x \vee n \ge N \ , \end{array}$$

and therefore the negation of the last line is an acceptable guard. Thus the macroscopic structure of our program becomes

$x, n :=$ true, 1
{Inv $Q0 \wedge Q1$} {Bnd $N-n$}
; **do** $x \wedge n < N \rightarrow \ldots$ **od**
{R}

The repeatable statement will contain $n := n+1$, for termination's sake. The required adjustment of x follows from

$$
\begin{array}{ll}
 & \text{RHS. Q1} \\
= & \quad \{ \} \\
 & x \wedge K.n \\
= & \quad \{ x \equiv \text{true} \quad \text{— from the guard —} \} \\
 & K.n \\
= & \quad \{ n < N \quad \text{— from the guard —} \\
 & \quad\;\; 1 \le n \quad \text{— from Q0 —} \quad \} \\
 & f.(n-1) \le f.n \;\wedge\; K.(n+1) \\
= & \quad \{ \text{substitution} \} \\
 & (x \wedge K.n)\,(x, n := f.(n-1) \le f.n \;,\; n+1),
\end{array}
$$

and the resulting program is

$$
\begin{array}{l}
\;\; x, n := \text{true}, 1 \\
; \ \underline{\text{do}}\ \ x \wedge n < N \rightarrow x, n := f.(n-1) \le f.n \;,\; n+1 \ \ \underline{\text{od}}
\end{array}
$$

* * *

The above program can also be developed on the basis of the invariance of $P0'' \wedge P1$, the difference being that the derivation of the guard and the proof that R is established upon termination is much more cumbersome than with choice $Q0 \wedge Q1$. This note has been written to recall that tail invariants are just nicer; but as yet I don't have a satisfactory technical explanation of the phenomenon.

Sterksel, 5 November 1992,

W.H.J. Feijen