Computing the prime divisors of a number

(a bagatelle for the files)

• For positive integer n, we define $\mathcal{B}.n$ as

$\mathcal{B}.n$ = the bag of all prime divisors of n.

Its most prominent properties are

(0a) $\mathcal{B}.1 = [\,]$ (the empty bag)

(0b) $\mathcal{B}.(d*n) = [d] + \mathcal{B}.n$, for prime d

• From number theory we import the theorem that, for $2 \leq n$, the smallest d, $2 \leq d$, that divides n is a prime. In formula:

(1) $\langle \forall i : 2 \leq i < d : \neg\, i \mid n \rangle \wedge d \mid n \wedge 2 \leq d$

$\Rightarrow$

d is a prime $\qquad (2 \leq n)$

• We are requested to design a program to compute $\mathcal{B}.N$, for a given N, $1 \leq N$, more precisely, to establish postcondition

R: $\quad x = \mathcal{B}.N$

* * *

We shall establish R via a repetition

with invariants

$P0$: $\quad 1 \leq n \leq N \quad$ and

$P1$: $\quad x + \textcircled{B}.n = \textcircled{B}.N$.

Then, by (0a),

$$P1 \wedge n = 1 \Rightarrow R .$$

Thus, we find ourselves heading for a program of the form

$$x, n := \lfloor\!\rfloor . N$$
$$; \{ \text{inv } P0 \wedge P1 \} \{ \text{bnd } n \}$$
$$\underline{\text{do}}\ n \neq 1 \rightarrow \text{"squeeze } n\text{"}\ \underline{\text{od}}$$
$$\{R\}$$

* * *

We can squeeze n and maintain $P1$ whenever we can find a value of d such that

(2) $\quad d$ is a prime $\wedge\ d|n \wedge 2 \leq d$,

because then, by (0b) with $n := n/d$, statement

$$\{ (2) \}\ \ x, n := x + \lfloor d \rfloor , n/d$$

does the job. And we are left with establishing pre-assertion (2).

* * *

By (1), (2) follows from

(3) $\langle \forall i : 2 \le i < d : \neg\, i \mid n \rangle \;\wedge\; d \mid n \;\wedge\; 2 \le d$,

and we shall establish the two outer conjuncts of (3) by adding them to the invariant:

P_2: $\langle \forall i : 2 \le i < d : \neg\, i \mid n \rangle \;\wedge\; 2 \le d$.

Thus, our program becomes

$x, n, d := \lfloor\rfloor, N, 2$

; {inv $P_0 \wedge P_1 \wedge P_2$} {bnd n}

do $n \neq 1 \;\rightarrow$

{inv P_2}

do $\neg\, d \mid n \;\rightarrow\; d := d + 1$ od

; { $P_2 \wedge d \mid n$, hence (3), hence (2) }

$x, n := x + \lfloor d \rfloor,\; n/d$ { P_2, see below }

od

{R} .

Finally, we have to show that

- the inner repetition terminates, which it does because
  $2 \le n \;\wedge\; n \mid n$ is a precondition of this repetition, so that P_2 implies $d \le n$
- statement $n := n/d$ maintains P_2, which it does because

$$\neg\ c|n \quad \Rightarrow \quad \neg\ c|(n/d)\ ,$$

or, writing this more positively, because

$$c\,|\,(n/d) \quad \Rightarrow \quad c|n\ .$$

* * *

This note has been written for my colleague Rudolf Mak, with his permission to mention his name. Rudolf had quite an awkward a-posteriori proof for a slightly twisted program to solve the above problem. The awkwardness came in via expressions of the form

$$(*) \qquad p_0^{i_0}\, p_1^{i_1} \cdots p_k^{i_k}\ ,$$

which then, by too many invariants, diffused through most of the calculations.

I would like to say to Rudolf and to some other colleagues: abstain from verification and focus on derivation, and try to remove overspecificities from your formulae so that they will become as sober as possible. (In expression (*) above, the order of the factors is absolutely irrelevant.) And ... think of our students: we should help them in loving formalism, not in hating it.

Yours,

W.H.J. Feijen
27 October 1997