Calculating the Sieve of Eratosthenes

Lambert Meertens

Kestrel Institute & Utrecht University

The Sieve, informally

- Write down the successive "plurals": 2, 3, 4, . . .
- Repeat:
  - Take the first number that is not circled or crossed out
  - Circle it
  - Cross out its proper multiples

Shown in action . . .

2	3	4	5	6	7	8	9	10	11	12	13	14	15	. . .
(2)	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~	15	. . .
(2)	(3)	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	. . .
(2)	(3)	~~4~~	(5)	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	. . .

Folklore Functional Program

There is a well-known "folklore" functional program for the Sieve

How to derive that program?

By calculation, of course!

The Essence of Sieve-hood

The Sieve produces a stream of primes,
and that stream is used

while it is being produced

to filter itself

Preliminaries: Streams

Always an *infinite* list

Codomain of final coalgebra

Corresponding anamorphism:

$$h\,x \;=\; f\,x : h\,(g\,x)$$

Notation:

$$h \;=\; [\![(f \vartriangle g)]\!]$$

Particular case

$[\!(f \vartriangle (+1))\!]$, in which $(+1)$ is the successor function on naturals

Claim:

$$[\!(f \vartriangle (+1))\!]\; n \;=\; map\; f\; [n\,..]$$

Proof:

$$\begin{aligned}
& \mathit{map}\ f\ [n\,..] \\
= & \quad \{\text{definition of `..'}\} \\
& \mathit{map}\ f\ (n : [n{+}1\,..]) \\
= & \quad \{\text{definition of } \mathit{map}\} \\
& f\ n : \mathit{map}\ f\ [n{+}1\,..]
\end{aligned}$$

Preliminaries: Primes

If $\mathit{prime}\,0 = 2$, $\mathit{prime}\,1 = 3$, $\mathit{prime}\;2 = 5$, etc.

$$\mathit{primes} \;=\; \mathit{map}\;\mathit{prime}\;[0\,..]$$

Needs characterization of function *prime*

Being Prime

> *A prime is a plural not divisible by a smaller prime*

So *prime* n is the head of the stream remaining after removing from $[2\,..]$ the multiples of *prime* 0, *prime* 1, ..., up to but not including *prime* n

In Haskell

$$\mathit{prime}\,n \;=\; \mathit{head}\,(\mathit{remvto}\,n\;[2\,..])$$

where

$$\begin{aligned}
\mathit{remvto}\;0 \quad &= \; \mathit{id} \\
\mathit{remvto}\,(n{+}1) \; &= \\
&\quad \mathit{filter}\,(\mathit{notdiv}\,(\mathit{prime}\,n)) \;\cdot\; \mathit{remvto}\,n \\
\mathit{notdiv}\,d\,n \; &= \; n \;\grave{}\mathit{mod}\grave{}\; d \;\neq\; 0
\end{aligned}$$

This is actually an effective definition

Strengthening

$$\textit{head}(\textit{remvto}\ n\ [2\,..]) \;=\; \textit{prime}\ n$$

$$\textit{tail}\ \ (\textit{remvto}\ n\ [2\,..]) \;=\; \textit{remvto}\ n\ [(\textit{prime}\ n)+1\ ..]$$

So

$$\textit{remvto}\ n\ [2\,..] \;=\; \textit{prime}\ n\ :\ \textit{remvto}\ n\ [(\textit{prime}\ n)+1\ ..]$$

Generalize

$$primes = pp\ 0$$

where

$$pp\ n = map\ prime\ [n\,..]$$

So

$$pp\ n = prime\ n : pp\,(n{+}1)$$

Calculating the solution

We want a solution in “sieve” form:

$$pp\,n \;=\; sieve\,(remvto\;n\;[2\,..])$$

for some function *sieve*

Derive *sieve* by matching to the anamorphism pattern

Abbreviate *prime n* to *p* throughout

Left-hand side

$$
\begin{array}{ll}
 & pp\; n \\
= & \qquad \{\text{sieve form}\} \\
 & sieve\,(remvto\; n\; [2\,..\,]) \\
= & \qquad \{\text{property of } remvto\} \\
 & sieve\,(p : remvto\; n\; [p{+}1\,..\,]) \\
= & \qquad \{\text{abbreviating to `}ns\text{'}\} \\
 & sieve\,(p : ns)
\end{array}
$$

Right-hand side

$$
\begin{aligned}
& p : pp\,(n{+}1) \\
= \quad & \qquad \{\text{sieve form}\} \\
& p : \mathit{sieve}\,(\mathit{remvto}\,(n{+}1)\,[2\,..\,]) \\
= \quad & \qquad \{\text{definitions}\} \\
& p : \mathit{sieve}\,(\mathit{filter}\,(\mathit{notdiv}\ p)\,(\mathit{remvto}\ n\ [2\,..\,])) \\
= \quad & \qquad \{\text{property of } \mathit{remvto}\} \\
& p : \mathit{sieve}\,(\mathit{filter}\,(\mathit{notdiv}\ p)\,(p : \mathit{remvto}\ n\ [p{+}1\,..\,])) \\
= \quad & \qquad \{\text{abbreviating as before}\} \\
& p : \mathit{sieve}\,(\mathit{filter}\,(\mathit{notdiv}\ p)\,(p : ns)) \\
= \quad & \qquad \{\mathit{notdiv}\ p\ p = \mathit{False}, \text{ definition of } \mathit{filter}\} \\
& p : \mathit{sieve}\,(\mathit{filter}\,(\mathit{notdiv}\ p)\ ns)
\end{aligned}
$$

The Solution for *sieve*

Any definition of *sieve* equating the final expressions of the last two calculations:

$$sieve\,(p : ns) \;=\; p : sieve\,(filter\,(notdiv\;p)\;ns)$$

will do

If we forget that p and ns denote abbreviations, this is a fine definition

So for *primes* ...

$$
\begin{array}{ll}
 & primes \\
= & \qquad \{\text{definition}\} \\
 & map\ prime\ [0\,..] \\
= & \qquad \{\text{definition}\} \\
 & pp\ 0 \\
= & \qquad \{\text{sieve form}\} \\
 & sieve\,(remvto\ 0\ [2\,..]) \\
= & \qquad \{\text{definitions}\} \\
 & sieve\ [2\,..]
\end{array}
$$

Wrapping it up:

$$primes = sieve\ [2\,..]$$

where

$$sieve\,(p : ns) = p : sieve\,(filter\,(notdiv\ p)\ ns)$$