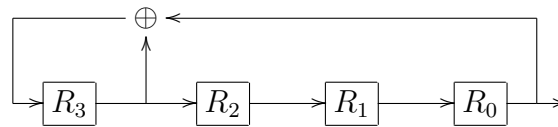


## Linear Feedback Shift Registers

Linear feedback shift registers (LFSR's) are an efficient way of describing and generating certain sequences in hardware implementations. We derive and work with equivalent mathematical descriptions of the sequences produced by a LFSR, along with some generalized sequences which do not arise in this way.

A linear feedback shift register is composed of a shift register  $R$  which contains a sequence of bits and a feedback function  $f$  which is the bit sum (**xor**) of a subset of the entries of the shift register. The shift register contains  $n$  memory cells, or stages, labelled  $R_{n-1}, \dots, R_1, R_0$ , each holding one bit. Each time a bit is needed the entry in stage  $R_0$  is output while the entry in cell  $R_i$  is passed to cell  $R_{i-1}$  and the top stage  $R_{n-1}$  is updated with the value  $f(R)$ .

The following is a schematic of a linear feedback shift register:



- In the above LFSR, let the initial entries of stages  $R_i$  be  $s_i$ , for  $0 \leq i \leq n$ . For each of the following initial entries below:

	$s_3$	$s_2$	$s_1$	$s_0$
a)	0	1	1	0
b)	1	1	1	0
c)	1	0	1	0
d)	1	1	0	0

compute the first 16 bits in the output sequence. Show that the output sequence is defined by the initial entries and the recursion  $s_{i+4} = s_{i+3} + s_i$ .

*Solution* The recursion  $s_{i+4} = s_{i+3} + s_i$  is immediately apparent as that specified by the diagram of the LFSR. From this recursion, the given initial states expand to the following sequences:

- (a) 0110010001111010...
- (b) 1110101100100011...
- (c) 1010110010001111...
- (d) 1100100011110101...

2. Show that every linear feedback register defines and is defined by a recursion of the form  $s_{i+n} = \sum_{j=0}^{n-1} c_j s_{i+j}$ , where the  $c_j$  are bits in  $\mathbb{Z}/2\mathbb{Z}$ ; the products  $c_j s_{i+j}$  and the summation are operations in  $\mathbb{Z}/2\mathbb{Z}$ .

N.B. The ring  $\mathbb{Z}/2\mathbb{Z}$  is also referred to as  $\mathbb{F}_2$ , the unique finite field of two elements. Note that the addition operation is the same **xor** that we have been using and the multiplication operation is the logical **and** operation.)

*Solution* The data of a LFSR diagram, of a linear recurrences relation, and of a connection polynomial are equivalent — they express the same information. The connection polynomial  $g(x) = \sum_j c_j x^j$  encodes the wiring of a LFSR which implements a recurrence relation. Thinking of  $x^j$  as a shift operator acting on the sequence  $s_0, s_1, s_2, \dots$ , the behaviour of  $g(x)$  in the product  $g(x)s(x)$  (below) is precisely this recurrence relation.

3. For a linear feedback register of length  $n$ , define a power series

$$s(x) = \sum_{i=1}^{\infty} s_i x^i$$

from the output sequence  $s_i$ . Suppose that the linear feedback register defines the recursion  $s_{i+n} = \sum_{j=0}^{n-1} c_{n-j} s_{i+j}$ . Define a polynomial  $g(x) = \sum_{j=0}^{n-1} c_j x^j + 1$ . Show that  $f(x) = g(x)s(x)$  is a polynomial, that is, all of its coefficients are eventually zero. What is the polynomial  $f(x)$ ?

*Solution* The expression  $f(x) = s(x)g(x)$  for a polynomial  $f(x)$  of degree less than  $n = \deg(g(x))$  is another equivalent formulation of the recurrence relation. The initial  $n$  coefficients of  $s(x)$  are the entries of the shift register, and the  $n$  coefficients of  $f(x)$  is a linear combination of these coefficients. Although the coefficients of  $f(x)$  are not equal to the initial state, for a nonsingular LFSR, the initial states are in bijection with the numerator polynomials  $f(x)$ .

4. In the previous exercise we showed that the power series  $s(x)$  has the form  $f(x)/g(x)$  in the power series ring  $\mathbb{F}_2[[x]]$ . In **Magma** it is possible to form power series rings in the following way

```
> F2 := FiniteField(2);
> PS<x> := PowerSeriesRing(F2);
> f := x^2 + x;
> g := x^3 + x + 1;
> f/g + 0(x^16);
x + x^4 + x^5 + x^6 + x^8 + x^11 + x^12 + x^13 + x^15 + 0(x^16)
```

Consider the linear feedback shift register at the beginning of the worksheet. Construct the corresponding power series and verify that these are the same of the output sequences that you computed.

*Solution* The power series expansions of the first question are:

$$\begin{aligned}s(x) &= x + x^2 + x^5 + x^9 + x^{10} + x^{11} + x^{12} + x^{14} + \dots \\s(x) &= 1 + x + x^2 + x^4 + x^6 + x^7 + x^{10} + x^{14} + x^{15} + \dots \\s(x) &= 1 + x^2 + x^4 + x^5 + x^8 + x^{12} + x^{13} + x^{14} + x^{15} + \dots \\s(x) &= 1 + x + x^4 + x^8 + x^9 + x^{10} + x^{11} + x^{13} + x^{15} + \dots\end{aligned}$$

Multiplying each through by the connection polynomial  $g(x) = x^4 + x + 1$ , we find the numerator polynomials for each of the sequences:

$$\begin{aligned}f(x) &= x + x^3 \\f(x) &= 1 + x^3 \\f(x) &= 1 + x + x^2 + x^3 \\f(x) &= 1 + x^2\end{aligned}$$

This verifies that the sequences output are consistent with their expected structure as coefficients of a rational power series.