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 $R_{n-1}, \ldots, R_1, R_0$, 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:

1. 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:

   $\begin{array}{cccc}
   s_3 & s_2 & s_1 & s_0 \\
   a) & 0 & 1 & 1 & 0 \\
   b) & 1 & 1 & 1 & 0 \\
   c) & 1 & 0 & 1 & 0 \\
   d) & 1 & 1 & 0 & 0 \\
   \end{array}$

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

2. Show that every linear feedback register defines and is defined by a recursion of the form $s_{i+n} = \sum_{j=0}^{n-1} a_j s_{i+j}$, where the $a_j$ are bits in $\mathbb{Z}/2\mathbb{Z}$; the products $a_j s_{i+j}$ 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.)
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 $s_{i+n} = \sum_{j=0}^{n-1} a_j s_{i+j}$. Define a polynomial $g(x) = \sum_{j=0}^{n-1} a_j x^{n-j} + 1$. Show that $f(x) = g(x)s(x)$ is a polynomial, that is, all of its coefficients are eventually zero. What is the polynomial $f(x)$?

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

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