Cryptography 1/09/2015

Lecture 7: LFSR I; Finite Fields

Instructor: Goutam Paul *Scribe: Procheta Sen*

1 LFSR (Linear Feedback Shift Register)

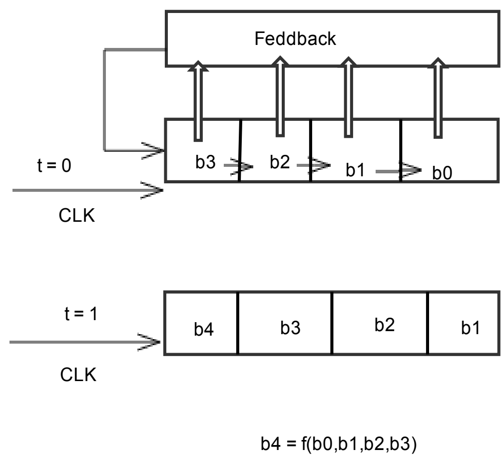

Figure 1: Digaram of a shift register with feedback

When f is a linear function then it is called linear feedback shift register.

$$b_{n+1} = C_0 b_0 + C_1 b_1 + C_2 b_2 + \ldots + C_{n-1} b_{n-1} \tag{1}$$

Hetre bits are over 0 and 1 and coefficients are over 0 and 1.
Let us assume at t = 0, $\vec{S_0}$ is the state.

$$\vec{S_0} = \begin{pmatrix} b_{n-1} \\ b_{n-2} \\ \vdots \\ b_0 \end{pmatrix}$$

At t = 1 the matrix will be following

$$\vec{S}_1 = \begin{pmatrix} b_n \\ b_{n-1} \\ \vdots \\ b_1 \end{pmatrix}$$

$$= \begin{pmatrix} C_0 b_0 + C_1 b_1 + \vdots + C_{n-1} b_{n-1} \\ b_{n-1} \\ \ldots \\ b_1 \end{pmatrix}$$

$$= \begin{pmatrix} C_{n-1} & C_{n-2} & \ldots & C_0 \\ 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & & & \\ 0 & \ldots & 1 & 0 \end{pmatrix} \times \begin{pmatrix} b_{n-1} \\ b_{n-2} \\ \vdots \\ b_0 \end{pmatrix}$$

So we can write $\vec{S}_1 = T\vec{S}_0$ Here T is the transition matrix
Similarly $\vec{S}_2 = T\vec{S}_1 = T^2\vec{S}_0$

Hence we can write $\vec{S}_t = T^t\vec{S}_0$

There should be non-zero numbers in the bit positions which are multiplied with coefficients. If the same state is repeated after t steps, it is said that LFSR has a period t.

In a n bit register the total number of possible states are $2^n - 1$. So period can be atmost $2^n - 1$. The period should be made as large as possible.

1.1 Finite Field

It is a set F with two operators $+$ and $*$. $(F, +)$ is an additive group with 0 as the identity and $(F \setminus \{0\}, *)$ is a multiplicative group with 1 as the identity.

Example of a finite group: $F_3 = \{0, 1, 2\}$, Here $+$ is modulo 3 addition and $*$ is modulo 3 multiplication.

1.1.1 Results

1. For any prime p, z_p, i.e the set of integers modulo p, forms a finite field with respect to addition and multiplication modulo p.

2. $\exists$ a finite field with n elements iff n is a prime power i.e $n = p^m$ for some prime p and $n \in N$.

3. For $m > 1$ all finite fields of size p^m are isomorphic to the set of all polynomials over z_p modulo some irreducible polynomial $g_m(x)$ of degree m with addition and multiplication defined as follows

$$(a_0+a_1x+a_2x^2+\ldots+a_{m-1}x^{m-1})+(b_0+b_1x+b_2x^2+\ldots+)b_{m-1}x^{m-1}) = (a_0+b_0)_p+(a_1+b_1)_px+\ldots \tag{2}$$

$$(a_0+a_1x+a_2x^2+\ldots+a_{m-1}x^{m-1})(b_0+b_1x+b_2x^2+\ldots+)b_{m-1}x^{m-1}) = (a_0b_0)_p+(a_0b_1+a_1b_0)_px+\ldots \tag{3}$$