Feedback Shift Register Sequences

Spring School of Algebra

Veronika Stankovianska

Department of Algebra
Faculty of Mathematics and Physics
Charles University in Prague

March 25, 2010

Feedback Shift Registers – Motivation

Motivation

- cryptography (PRNG in stream ciphers);
- digital broadcasting & communications.

Feedback Shift Registers – An Outline

An Outline

- Section 1 – **Feedback Shift Registers (FSR)**

  (Concepts, Examples, Finite Field Configuration, Periodicity, Linearity);

- Section 2 – **Linear Feedback Shift Registers (LFSR): Sequences from the Polynomial Ring**

  (Left Shift Operator).

Concepts & Examples

Definition (Boolean Function of n Variables)

Let $F = GF(2) = \{0, 1\}$ and $F^{(n)} = \{(a_0, a_1, \ldots, a_{n-1}) | a_i \in F\}$. A function $f; f : F^{(n)} \longrightarrow F$ is said to be the *Boolean Function of n Variables*.

Concepts

Each FSR consists of a *shift register* and a *feedback function (f)*.

A shift register is a device which

- shifts its contents into adjacent positions within the register or out of register (end position);
- interts a *feedback function* output into the position emptied by the shift.

Concepts & Examples

Definition (Feedback Shift Register Sequence)

An output sequence $a_0, a_1, \ldots, a_n, \ldots$ satisfying the recursive relation

$$a_{n+k} = f(a_k, a_{k+1}, \ldots, a_{k+n-1}),\ k = 0, 1, \ldots$$

is called the *Feedback Shift Register Sequence*.

If f is linear, the output sequence is called *Linear Feedback Shift Register (LSFR) Sequence*, otherwise the sequence is non-linear (NLSFR).

It is said that $\underline{a}$ is *generated* by either LSFR or NLSFR.

Concepts & Examples

Definition (Stage of the Shift Register)

We call n binary storage elements the *Stage* of the shift register.

Definition (State of the Shift Register)

Their contents (regarded either as an n-bit long binary number or binary vector) are said to be the *State* of the shift register.

Definition (Initial State of the Shift Register)

The sequence $(a_0, a_1, \ldots, a_{n-1}) \in F^{(n)}$ is called the *Initial State* of the shift register.

Concepts & Examples

Definition (Feedback Function)

A Boolean function of n variables $f(x_0, x_1, \ldots, x_{n-1}) = \sum c_{i_1 i_2 \ldots i_t} x_{i_1} x_{i_2} \ldots x_{i_t}$ is called the *Feedback Function*.

Note: The following term can be written as $a_n = f(a_0, \ldots, a_{n-1})$. Any n consecutive terms of the output sequence represent a state of the shift register.

Concepts & Examples

Examples

Example 1: A 3-stage FSR with a non-linear feedback function $f(x_0, x_1, x_2) = x_0x_1$.

Example 2: A 3-stage LFSR; $f(x_0, x_1, x_2) = x_0 + x_1$.

Example 3: A 3-stage NLFSR; $f(x_0, x_1, x_2) = x_0 + x_1x_2 + x_2 + 1$.

Example 4: A 4-stage FSR with a non-linear feedback function $f(x_0, x_1, x_2, x_3) = x_0 + x_1x_2x_3 + x_1 + 1$.

Concepts & Examples

Definition (De Bruijn Sequence)

An n-stage NLFSR output sequence with a period of 2^n having every n-tuple occurring exactly once per period is *De Bruijn*.

Remark: Examples 3 and 4 are instances of De Bruijn sequences.

Finite Field Configuration for q-ary FSR Sequences

Let $F = F(q)$. In terms of FSR, each stage is replaced by a q state storage unit and the feedback function is replaced by a function $f : F^{(n)} \longrightarrow F$:

$$f(x_0, x_1, \ldots, x_{n-1}) = \sum c_{i_0,i_1,\ldots,i_{n-1}} x_{i_0}^{i_0} x_{i_1}^{i_1} \ldots x_{i_{n-1}}^{i_{n-1}} \in F.$$

The q-ary FSR sequence and its initial state are defined analogously to binary FSR.

Finite Field Configuration for q-ary FSR Sequences

Note: The only difference between binary and q-ary FSR is that of a block diagram representation.

Binary FSR provides a model at the gate level; q-ary FSR is only a finite field configuration diagram. (There are more circuits needed to implement the finite field arithmetics – feedback function computation.)

Nevertheless, the output sequences of an arbitrary FSR are completely determined by its initial state and its feedback function.

Periodic Property

Definition (q-ary Sequence)

Let q be a prime or a power of a prime. A sequence $\underline{a} = a_0, a_1, \cdots = \{a_i\};\ a_i \in F = GF(q)$ is called the *q-ary Sequence*.

Definition (Ultimately Periodic Sequence)

A q-ary sequence $\underline{a}$ is *Ultimately Periodic* if there exists $r > 0$ and $i_0 \geq 0$ such that

$$a_{i+r} = a_i \text{ for } \forall\ i \geq i_0.$$

The number r is called the length/period of the sequence.

Periodic Property

Theorem

A q-ary FSR sequence is ultimately periodic with a period $r \leq q^n$. If $q = 2$, then $r \leq 2^n$; n is the number of the stages.

Proof.

There are at maximum q^n states for a q-ary FSR sequence. Hence, there are q different times $t_1, \ldots, t_q$ where the register is in the same state S. At $t_1 + 1, \ldots, t_q + 1$, the register shifts to S' (the following state is generated unambiguously). As a result, periodicity of $\underline{a}$ is established. □

Linear Feedback Shift Register Sequences

Consider linear feedback function:

$$f(x_0, x_1, \ldots, x_{n-1}) = c_0 x_0 + c_1 x_1 + \cdots + c_{n-1} x_{n-1};\ c_i \in GF(q).$$

The recursive relation then becomes linear:

$$a_{n+k} = \sum_{i=0}^{n-1} c_i a_{i+k};\ k = 0, 1, \ldots.$$

Note: LFSR are also referred to as of linear recursive sequences over F; $F = GF(2)$ or $GF(q)$.

Linear Feedback Shift Register Sequences

Theorem

Let $\underline{a}$ be the sequence generated by an n-stage LFSR over F, then the period of $\underline{a} \leq q^n - 1$.

Proof.

There are q^n different possible states of the LFSR. Zero sequence is always followed by a zero sequence, thus $r \leq q^n - 1$. □

The focus of the following section is shifted to LFSR on which the majority of methods used to obtain NLFSR with designed properties are based.

Left Shift Operator

Let $F = GF(q)$, $V(F) = \{\underline{a} = (a_0, a_1, \dots) | a_i \in F\}$ be the set of all infinite sequences over F.

We define addition and product multiplication on $V(F)$ as follows: For $\underline{a}$, $\underline{b} \in V(F)$, $c \in F$:

$$\underline{a} + \underline{b} = (a_0 + b_0, a_1 + b_1, \dots);$$

$$c\underline{a} = (ca_0, ca_1, \dots).$$

Note: $V(F)$ is a linear space over F. The *zero sequence* $(0, 0, \dots)$ is denoted by 0.

Left Shift Operator

Definition (LFRS Sequence)

We call $\underline{a} = (a_0, a_1, \dots) \in V(F)$ the Linear Feedback Shift Register Sequence if it satisfies the linear recursive relation

$$a_{n+k} = \sum_{i=0}^{n-1} c_i a_{i+k}; \;\; k = 0, 1, \dots .$$

Left Shift Operator

Definition (Left Shift Operator)

Let $\underline{a} = (a_0, a_1, \dots) \in V(F)$. We define the Left Shift Operator L as

$$L\underline{a} = (a_1, a_2, a_3, \dots).$$

Note: L is a linear transformation of $V(F)$. Thus, $L^{i+1} = L(L^i)$ and $L^i\underline{a} = (a_i, a_{i+1}, a_{i+2}, \dots)$ for any positive integer i.
We write $L^0\underline{a} = I\underline{a} = \underline{a}$, where I is the Identity Transformation of $V(F)$.

Left Shift Operator

Alternative definition of LSFR Sequence

Having defined L, we can rewrite the linear recursive relation

$$a_{n+k} = \sum_{i=0}^{n-1} c_i a_{i+k}; \;\; k = 0, 1, \ldots$$

as

$$L^n \underline{a} = \sum_{i=0}^{n-1} c_i L^i \underline{a}.$$

$$L^n \underline{a} = L(a_{n-1}, a_{n-2}, \dots) = L^n(a_0, a_1, \dots) = (a_n, a_{n+1}, \dots)$$

$$a_n = c_0 a_0 + c_1 a_1 + c_2 a_2 + \cdots + c_{n-1} a_{n-1}$$
$$a_{n+1} = c_0 a_1 + c_1 a_2 + c_2 a_3 + \cdots + c_{n-1} a_n$$
$$a_{n+2} = c_0 a_2 + c_1 a_3 + c_2 a_4 + \cdots + c_{n-1} a_{n+1}$$
$$\dots$$
$$(a_n, a_{n+1}, \dots) = (c_0 a_0 + \cdots + c_{n-1} a_{n-1}, c_0 a_1 + \cdots + c_{n-1} a_n, \dots)$$
$$= c_0 L\underline{a} + (c_1 a_1 + \cdots + c_{n-1} a_{n-1}, c_1 a_2 + \cdots + c_{n-1} a_n, \dots)$$
$$= c_0 I + c_1 L\underline{a} + (c_2 a_2 + \cdots + c_{n-1} a_{n-1}, c_2 a_3 + \cdots + c_{n-1} a_n, \dots)$$

Eventually, we obtain:

$$L^n \underline{a} = \sum_{i=0}^{n-1} c_i L^i \underline{a}.$$

Let $f(x) \in F[x]$, then

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0;$$
$$f(L) = c_n L^n + c_{n-1} L^{n-1} + \cdots + c_0 I.$$

The following holds:

$$L^n \underline{a} = \sum_{i=0}^{n-1} c_i L^i \underline{a} \quad \Leftrightarrow \quad \left(L^n - \sum_{i=0}^{n-1} c_i L^i \right) \underline{a} = 0.$$

Definition (LFRS Sequence)

An infinite sequence $\underline{a} \in V(F)$ is a *LFSR sequence* if there exists a non-zero polynomial $f(x) \in F[x]$ such that $f(L)\underline{a} = 0$.

Definition (Characteristic Polynomial of a LFRS Sequence)

A polynomial $f(x)$ is called the *Characteristic Polynomial* of $\underline{a}$ over F.

An instance of a subspace of V(F)

If we define $G(f)$ as

$$G(f) = \{\underline{a} \in V(f) | f(L)\underline{a} = 0;\ 0 \neq f(x) \in F[x]\},$$

$G(f)$ is a subspace of $V(f)$ since $f(L)$ is a linear transformation.

Note: The constant polynomial $f(x) = 1$ is a characteristic polynomial of $0 = (0, 0, \dots)$, the zero sequence.

Theorem

Let $f(x) \in F[x]$ be a polynomial of degree n, then $G(f)$ is a linear space of dimension n. Hence it contains q^n different sequences. If $q = 2$, $G(f)$ contains 2^n binary sequences.

Proof.

The degree of the polynomial $deg(f) = n$ determines the number of components needed to generate the rest of the sequence $\underline{a} = (a_0, a_1, \ldots, a_{n-1}, a_n, \ldots) \in G(f)$ (the initial state $(a_0, a_1, \ldots, a_{n-1})$). The rest of the components starting from a_n is derived from $\left(L^n - \sum_{i=0}^{n-1} c_i L^i\right) \underline{a} = 0$.

There are q^n different ways to choose an n-tuple $(a_0, a_1, \ldots, a_{n-1})$ over F. Therefore, $|G(f)| = q^n$.

□

Application

A sequence $\underline{a} = (00010011010111)$ is generated by a LFSR with the feedback function $f(x_0, x_1, x_2, x_3) = x_0 + x_1$.

The sequence $\underline{a} = (a_0, a_1, \dots)$

1. satisfies the linear recursive relation
   $a_{k+4} = a_k + a_{k+1};\ k = 0, 1, \dots;$
2. has the characteristic polynomial $f(x) = x^4 + x + 1$;
3. is an element of $G(f)$ & $f(L)\underline{a} = (L^4 + L + I)\underline{a} = 0$.

The space $G(f)$ has $2^4 = 16$ different sequences.