A Brief Introduction to LFSR and NLFSR

Xiaolin Tang   Ziheng Zhu   Nannan Xu   Cen Wang
Capital Normal University

Contents

Chapter 1

The periodicity of LFSR sequences

1.1 Concepts

Definition 1.1.1. *In $\mathbb{F}_q$, a infinite sequence $a = (a_0, a_1, a_2, \cdots)$ is periodic if $\exists l, s.t. a_{l+k} = a_k, \forall k \geq 0$. The period of a is denoted by $p(a)$.*

Lemma 1.1.2. *$a = (a_0, a_1, a_2, \cdots)$. If $\exists l, s.t. a_{l+k} = a_k$, then $p(a)|l$.*

Lemma 1.1.3. *$f = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$ $(c_0 c_n \neq 0)$, $a \in G(f). a = (a_0, a_1, \cdots)$.*
1.$S_0 T^{p(a)} = S_0$
2.$S_0, S_0 T, S_0 T^2, \cdots, S_0 T^{p(a)-1}$ are distinct.
3.l is the minimal positive integer s.t. $S_0 T^l = S_0$, then $p(n) = l$.

Theorem 1.1.4. *$f = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n (c_0 c_n \neq 0)$. $a \in G(f)$. a is periodic, and $p(a) \leq q^n - 1$.*

Proof. Suppose $a = (a_0, a_1, a_2, \cdots)$.The states are

$$S_0, S_1 = S_0 T, S_2 = S_0 T^2, \cdots$$

If $\exists S_i = (0, 0, \cdots, 0)$, then all the states of a are zero. $a = (0, 0, \cdots)$, thus $p(a) = 1$.
If $a \neq (0, 0, \cdots)$,then $\forall S_i \neq (0, 0, \cdots, 0)$. In $\mathbb{F}_q$, there are $q^n - 1$ non-zero n-dimensional row vectors. Thus in the first q^n states, there must be at least two are the same. *i.e.* $\exists i, j, 0 \leq i \leq j \leq q^n - 1$, $S_0 T^i = S_0 T^j$. $\Rightarrow S_0 T^{j-i} = S_0$. Let$l = j - i$, we have $a_{l+k} = a_k, \forall k \geq 0 \Rightarrow a$ is periodic and $p(a) \leq l \leq q^n - 1$ $\square$

Note:
1.If $p(a) = q^n - 1, a$ is called **q-ary m-sequence.**
2. $a \in G(f)$ is periodic, $\exists f$, s.t. $a \in G(f)$?. The answer is yes, because we have $a_k - a_{k-l} = 0, k \geq l$. Thus $f(x) = 1 - x^l$.
3.No matter what the initial sate S_0 is, f generates periodic sequence.

1.2 Minimal Polynomials

Theorem 1.2.1. *a is a periodic sequence over $\mathbb{F}_q$, $\exists! f(x) \in \mathbb{F}_q$, s.t. $a \in G(h)$ if and only if $f(x)|h(x)$*

$(I = \{h(x) \in \mathbb{F}_q | a \in G(h)\}$. Only need to prove $I \lhd \mathbb{F}_q$, because $a \in G(h) \Leftrightarrow h \in I \Leftrightarrow f|h)$

Proof. $1^\circ p(a) = l \Rightarrow a_k - a_{k-l} = 0 \Rightarrow 1 - x^l \in I, I$ is non-zero.

$2^\circ g(x), h(x) \in I$. Suppose $a \in G(g), a \in G(h)$. It's easy to conclude that $a \in G(g - h)$. Thus we have $\Rightarrow g - h \in I$. Hence,I is a additive subgroup of $\mathbb{F}_q$

$3^\circ \forall h(x) \in \mathbb{F}_q$, if $g(x) \in I$, $a \in G(g) \Rightarrow a \in G(hg) \Rightarrow hg \in I$. I is closed under multiplication.

Therefore,$I \lhd \mathbb{F}_q \Rightarrow \exists f(x)$ s.t. $I = (f(x))$. Naturally, we can suppose the coefficicent of zero-order term of $f(x)$ is 1. If $f_1(x)$ satisfies the same property as $f(x)$, then $f(x)|f_1(x), f_1(x)|f(x) \Rightarrow f(x) = cf_1(x) \Rightarrow c = 1$. Therefore, the polynomial is unique. ☐

Definition 1.2.2. *f is the minimal polynomial of a.*

Theorem 1.2.3. *$f(x) \in \mathbb{F}_q, c_0 = 1$, $\exists$ a periodic sequence whose minimal polynomial is $f(x)$.*

Proof. $deg f(x) = n.(1) n = 0$, zero sequence have $f(x) = 1$ as minimal polynomial.
$(2) n > 0$, suppose $f(x) = 1 + c_1x + c_2x^2 + \cdots + c_nx^n$. Let $S_0 = (0, 0, \cdots, 0, 1)$. Let $a \in G(f)$ whose initial state is S_0 satisfying

$$a_k + c_1a_{k-1} + c_2a_{k-2} + \cdots + c_na_{k-n} = 0, k \geq n$$

$a = (a_0, a_1, a_2, \cdots)$. $a_0 = a_1 = a_2 = \cdots = a_{n-2} = 0, a_{n-1} = 1$. If $h(x)$ is a minimal polynomial of a, then $h|f$.

If deg$h(x)$ =deg$f(x)$,$f(x)$ is the minimal polynomial of (a).

If $f(x)$ is not the minimal polynomial of a, then deg$f(x)$ >deg$h(x) = m$. $h(x) = 1 + d_1x + \cdots + d_mx^m \Rightarrow a_k + d_1a_{k-1} + \cdots + d_ma_{k-m} = 0, k \geq 1$. *i.e.* $(a_0, a_1, \cdots, a_{m-1})$ is the initial state of a. Then a is zero sequence. This leads a contradiction. ☐

Note:$\forall f[x] \in \mathbb{F}_q$, $\exists$ a periodic sequence whose minimal polynomial is $f(x)$.

Definition 1.2.4. *$f(x) \in \mathbb{F}_q[x], deg\ f \geq 1$. The period of $f(x)$ is $p(f) = min\{l \mid f(x)|x^l - 1\}$.*

Definition 1.2.5. *$p(f) = ord\ x$, in $\mathbb{F}_q[x]^*_{f(x)}$.*

Lemma 1.2.6. *$f(x)|(x^l - 1) \Rightarrow p(f)|l$.*

Lemma 1.2.7. *$p(f) = p(\widetilde{f})$.*

Proof. $p(f) = \min\ \{l : f(x)|x^l - 1\}, deg(f) = n$

Let $p(\widetilde{f}) = l$.

$$x^l - 1 = \widetilde{f}(x)g(x)$$

Substitute x with x^{-1},

$$(x^{-1})^l - 1 = \widetilde{f}(x^{-1})g(x^{-1})$$

Let $h(x) = x^{l-n}g(x^{-1})$,

$$1 - x^l = x^n\widetilde{f}(x^{-1})h(x)$$

$$f(x) = x^n\widetilde{f}(x^{-1})|(x^l - 1)$$

Thus we have

$$p(f)|p(\widetilde{f})$$

For the same reason,

$$p(\widetilde{f})|p(f)$$

Hence,

$$p(f) = p(\widetilde{f})$$

☐

Lemma 1.2.8. *$f(x) \in \mathbb{F}_q[x]$ is irreducible,$degf(x) = n$. $p(f) \mid q^n - 1$.*

Definition 1.2.9. *$A \in GL(\mathbb{F}_q)$,if $\exists l, s.t. A^l = I, p(A) \triangleq min\{l|A^l\}$.*

Lemma 1.2.10. *$A \in GL(\mathbb{F}_q), \exists l, s.t. A^l = I$, and $p(A)|l$.*

Lemma 1.2.11. $p(f) = p(T)$.

Proof. $f(x) = 1 + c_1x + \cdots + c_nx^n \in \mathbb{F}_q[x]$. T is a matrix determined by $f(x)$.
$\widetilde{f}(x)|x^{p(\widetilde{f})} - 1, \widetilde{f}(T) = 0 \Rightarrow T^{p(\widetilde{f})} = I \Rightarrow p(T)|p(\widetilde{f})$.
$T^{p(T)} = I \Rightarrow T$ satisfies $x^{p(T)} - 1 = 0$.
$\widetilde{f}(x)$ is the minimal polynomial of T. $\Rightarrow \widetilde{f}|x^{p(T)} - 1$. $\Rightarrow p(\widetilde{f})|p(T)$
$\Rightarrow p(\widetilde{f}) = p(T)$.
$p(f) = p(\widetilde{f}) \Rightarrow p(f) = p(T)$. □

Theorem 1.2.12. *a is a LFSR sequence whose minimal polynomial is $f(x)$, then $p(a) = p(f)$.*

Proof. a satisfies $a_k - a_{k-p(a)} = 0, k \geq p(a)$.

$$h(x) = 1 - x^{p(a)}, a \in G(h) \Rightarrow f|h = 1 - x^{p(a)} \Rightarrow p(f)|p(a)$$

$$T^{p(T)} = I \Rightarrow S_kT^{p(T)} = S_k \Rightarrow S_{k+p(T)} = S_k \Rightarrow a_{k+p(T)} = a_k, \forall k \geq 0 \Rightarrow p(T)|p(a)$$

$$p(f) = p(T) \Rightarrow p(f)|p(a)$$

Thus we have

$$p(a) = p(f)$$

□

Corollary 1.2.13. $f(x) \in \mathbb{F}_q[x], irreducible.$ $\forall a \in G(f), p(a) = p(f)$

Corollary 1.2.14. $a \in G(f), S_0 = (0, 0, \cdots, 0, 1)$ *is the initial state of a.* $p(a) = p(f)$

Corollary 1.2.15. $\forall a \in G(f), p(a)|p(f),\ f(x) \in \mathbb{F}_q[x], deg\ f(x) \geq 1$

Chapter 2

Shift Equivalent Class

2.1 Shift Equivalent Class

Definition 2.1.1. $a = (a_0, a_1, a_2, \cdots)$. *Left shifting transform L is an operator over $G(f)$:*

$$L(a) = (a_1, a_2, a_3, \cdots)$$

$$L^0(a) = a$$

$$L^t(a) = L(L^{t-1}(a)), t \geq 1$$

Definition 2.1.2. *If a and b are shift equivalent,$a \sim b$ if $\exists t \geq 0, b = L^t(a)$.*

Lemma 2.1.3. *$a \sim b$ is a equivalence relation.*

Proof. $(1)a \sim a$
$(2)a \sim b \Rightarrow b \sim a$
$(3)a \sim b, b \sim c \Rightarrow a \sim c$ □

Lemma 2.1.4. *(1)$a \sim b \Rightarrow p(a) = p(b)$*
(2)$L^{p(a)}(a) = L^0(a) = a$
(3)$\{b|b \sim a\} = a, L(a), L^2(a), \cdots, L^{p(a)-1}(a)$

Definition 2.1.5. *A set of q-ary periodic sequences is shift equivalent class(C) if $\forall a, b \in C \Rightarrow a \sim b$, and $d \sim a \Rightarrow d \in C$*

Theorem 2.1.6. *a is q-ary periodic sequence. The shift equivalent class C that contains a:*

$$C = a, L(a), L^2(a), \cdots, L^{p(a)-1}(a)$$

C_1 and C_2 are any two shift equivalent classes. $C_1 = C_2$ or $C_1 \bigcap C_2 \neq \varnothing$

Corollary 2.1.7. $|C| = p(a)$

Corollary 2.1.8. *$G(f)$ is a disjoint sum of several shift equivalent classes.*

Proof. $a \in G(f) \Rightarrow L(a) \in G(f) \Rightarrow C \subset G(f)$ □

Theorem 2.1.9. *$f(x) = f_1(x)f_2(x)\cdots f_r(x)$. deg $f_i = n_i$. gcd$(f_i, f_j) = 1, i \neq j$. Then*

$$G(f) = G(f_1) \oplus G(f_2) \oplus \cdots \oplus G(f_r)$$

Proof. If $a \in G(f_i) \Rightarrow \exists g_i$, s.t. $g_i|f_i \Rightarrow G(f_i) \subset G(f)$. i.e. $G(f_i)$ is a subspace of $G(f)$.

$deg\ f_i = n_i \Rightarrow$ suppose $(a_{i_1}, a_{i_2}, \cdots, a_{i_{n_i}})$ is a basis of $G(f_i), 1 \leq i \leq r$

First, we need to prove

$$(a_{11}, \cdots, a_{1_{n_1}}, a_{2_1}, \cdots, a_{2n_2}, \cdots, a_{r1}, \cdots, a_{rn_r}) \tag{2.1}$$

is a basis of $G(f_1) + G(f_2) + \cdots + G(f_r)$.

Assume $\exists c_i (i = 1, 2, \cdots, r, \quad j = 1, 2, \cdots, n_i)$ s.t.

$$\sum_{j=1}^{n_i} c_{ij} a_{ij} = 0$$

Let

$$a_i = \sum_{j=1}^{n_i} c_{ij} a_{ij} \in G(f_i)$$

$$a_1 = -(a_2 + \cdots + a_n) \in G(f_2) + \cdots + G(f_r)$$

Notice that

$$f_i | f_2 f_3 \cdots f_r, i = 2, 3, \cdots, r$$

Thus we have

$$G(f_2) + \cdots + G(f_r) \subset G(f_2 f_3 \cdots f_r)$$

Then

$$a_1 \subset G(f_2 f_3 \cdots f_r)$$

Suppose the minimal polynomial of a_1 is $m(x)$.

$$a_1 \in G(f_1) \Rightarrow m(x) | f_1(x)$$

$$a_1 \in G(f_2 f_3 \cdots f_r) \Rightarrow m(x) | f_2 \cdots f_r$$

Notice that $gcd\ (f_1, f_2 \cdots f_r) = 1$, then $m(x) = 1$.

Hence,

$$a_1 = (0, 0, \cdots)$$

For the same reason

$$a_2 = \cdots = a_r = 0$$

Thus

$$\sum_{j=1}^{n_i} c_{ij} a_{ij} = 0,\ i = 1, \cdots, r$$

Then

$$c_{ij} = 0, i = 1, \cdots, r,\ j = 1, \cdots, n_i$$

Therefore (3) is linearly independent.

$$f = f_1 \cdots f_r \Rightarrow n = n_1 + n_2 + \cdots + n_r$$

(3) is a basis of $\sum_{i=1}^{r} G(f_i)$. Then $\sum_{i=1}^{r} G(f_i)$ is a direct sum.

Notice that

$$dim\ G(f) = n = dim\ G(f_1) + \cdots + dim\ G(f_r)$$

Hence

$$G(f) = G(f_1) \oplus G(f_2) \oplus \cdots \oplus G(f_r)$$

□

2.2 The Decompositions of G(f)

Lemma 2.2.1. *If* $gcd(f_1(x), f_2(x)) = 1$, $a \in G(f_1), b \in G(f_2)$, *then* $p(a+b) = lcm[p(a), p(b)]$

Proof. Let $l = lcm[p(a), p(b)], l' = p(a+b)$,

$$a = (a_0, a_1, a_2, \cdots)$$

$$b = (b_0, b_1, b_2, \cdots)$$

Let s be the period of

$$(a_0, b_0), (a_1, b_1), (a_2, b_2), \cdots$$

On the one hand $a_l = a_0, b_l = b_0 \Rightarrow (a_l, b_l) = (a_0, b_0)$, then $s|l$.
$(a_s, b_s) = (a_0, b_0) \Rightarrow a_s + b_s = a_0 + b_0 \Rightarrow l'|s$. Thus we have $\Rightarrow l'|l$
On the other hand, $p(a+b) = l' \Rightarrow$

$$a_{l'+k} + b_{l'+k} = a_k + b_k, \forall k \geq 0$$

$$(a_{l'+k} - a_k) + (b_{l'+k} - b_k) = 0, \forall k \geq 0$$

$$(L^{l'}(a) - a) + (L^{l'}(b) - b) = 0$$

$$gcd(f_1, f_2) = 1 \Rightarrow G(f_1) \oplus G(f_2)$$

$$L^{l'}(a) - a \in G(f_1) \Rightarrow L^{l'}(a) = a \Rightarrow p(a)|l'$$

$$L^{l'}(b) - b \in G(f_2) \Rightarrow L^{l'}(b) = b \Rightarrow p(b)|l'$$

$\Rightarrow l = lcm[p(a), p(b)]|l'$
In conclusion, $l = l'$ □

Corollary 2.2.2. $gcd(f_i, f_j) = 1, i \neq j$, $a_i \in G(f_i), 1 \leq i \leq r$, *then* $p(a_1+a_2+\cdots+a_r) = lcm[p(a_1), p(a_2), \cdots, p(a_r)]$.

Theorem 2.2.3. $f = f_1 f_2$. $gcd(f_1, f_2) = 1, deg(f_i) = n_i$.
Suppose $G(f_1)$ *consists of two shift equivalent classes:* C_{11}, C_{12}.
Suppose $G(f_2)$ *consists of two shift equivalent classes:* C_{21}, C_{22}. $|C_{ij}| = p_{ij}$.
$G(f)$ *consists of*

$$\sum_{k_2=1}^{2} \sum_{k_1=1}^{2} p_{1k_1} p_{2k_2} / lcm[p_{1k_1} p_{2k_2}]$$

shift equivalent classes

Proof.

$$\begin{aligned} G(f) &= G(f_1) \oplus G(f_2) \\ &= (C_{11} \cup C_{12}) \oplus (C_{21} \cup C_{22}) \\ &= (C_{11} \oplus C_{21}) \cup (C_{11} \oplus C_{22}) \cup (C_{12} \oplus C_{21}) \cup (C_{12} \oplus C_{22}) \end{aligned}$$

$|C_{11} \oplus C_{21}| = p_{11} p_{21}$, then the period of every sequence in $C_{11} \oplus C_{21}$ is $lcm[p_{11}, p_{21}]$ according to **Lemma 3.2.3**. Thus $C_{11} \oplus C_{21}$ consists

$$p_{11} p_{21} / lcm[p_{11}, p_{21}]$$

shift equivalent classes.

Hence $G(f)$ consists of

$$\sum_{k_2=1}^{2} \sum_{k_1=1}^{2} p_{1k_1} p_{2k_2} / lcm[p_{1k_1} p_{2k_2}]$$

shift equivalent classes.

□

Corollary 2.2.4. $f = f_1 \cdot f_2 \cdots f_r$, $deg(f) = n_i \geqslant 1$, $gcd(f_i, f_j) = 1$ $(i \neq j)$

$G(f_i)$ consists of m_i shift equivalent classes, $(i = 1, 2, 3 \cdots, r)$, i.e. $\mathrm{C}_{i1}, \mathrm{C}_{i2}, \cdots, \mathrm{C}_{im_i}$

The period of sequences in C_{ij} is $p_{ij}(i = 1, 2, \cdots, r; j = 1, 2, \cdots, m_i)$. Then $G(f)$ consists of

$$\sum_{k_1=1}^{m_1}\sum_{k_2=1}^{m_2}\cdots\sum_{k_r=1}^{m_r}\frac{p_{1k_1}\cdot p_{2k_2}\cdot\cdots\cdot p_{rk_r}}{lcm[p_{1k_1}, p_{2k_2}, \cdots, p_{rk_r}]}$$

shift equivalent classes.

Lemma 2.2.5. $f(x) \in F_q[x], c_0 = 1$. *irreducible.* $m = min\{i \in Z_+ | p^i \geq e\}, (p^m \geq e > p^{m-1})$

$\Longrightarrow p(f^e) = p^m \cdot p(f)$

Proof. On the one hand,

$$f \,|\, x^{p(f)}-1 \Rightarrow f^{p^m} | (x^{p(f)} - 1)^{p^m} = x^{p^m \cdot p(f)}-1$$

Notice that $p^m \geq e \Rightarrow f^e \,|\, f^{p^m}$, thus we have

$$f^e \,|\, x^{p^m \cdot p(f)}-1 \Rightarrow p(f^e) \,|\, p^m \cdot p(f)$$

On the other hand,suppose

$$p(f) = p^j \cdot t\,, p \nmid t$$

Then we have

$$f^e \,|\, (x^{p^j t} - 1) = (x^t - 1)^{p^j}$$

$p \nmid t \Rightarrow (x^t - 1)' = t \cdot x^{t-1} \neq 0 \Longrightarrow gcd(x^t - 1, (x^t - 1)') = 1$, then $x^t - 1$ is irreducible. f is irreducible, thus

$$f \,|\, x^t - 1\,, e \leq p^j$$

Notice that m =min$\{i \in \mathbb{Z}_+ \,|\, p^j \geq e\}$, then $m \leq j$, Thus $p(f)|t \Longrightarrow p^m p(f)|p^m t \Longrightarrow p^m p(f)|p^j t = p(f^e)$ Hence, we can conclude that $p(f^e) = p^m p(f)$. □

Note: $p^m \geq e > p^{m-1} \Longrightarrow e = p^{m-1}{+}1\,, p^{m-1}{+}2\,, \cdots p^m$, then $p(f^e) = p^m \cdot p(f)$

$$p(f^2) = p(f^3) = \cdots = p(f^p) = p \cdot p(f)$$
$$p(f^{p+1}) = p(f^{p+2}) = \cdots = p(f^{p^2}) = p^2 \cdot (f)$$
$$\vdots$$
$$p(f^{p^{i-1}+1}) = p(f^{p^{i-1}+2}) = \cdots = p(f^{p^i}) = p^i \cdot p(f)$$

Theorem 2.2.6. $f(x) \in F_q[x], c_0 = 1, irreducidle, deg(f) = n.q = p^r\,, m = min\{i \in Z_+ | p^j \geq e\}$

The periods of sequences in $G(f^e)$ are

$$1, p(f), p^j p(f)(j = 1, 2, \cdots m - 1), p^m p(f)$$

Respectively, the numbers of the sequences which have the periods above are

$$1, q^n - 1, q^{np^i} - q^{np^{i-1}}(i = 1, 2, \cdots, m - 1), q^{ne} - q^{np^{m-1}}$$

Thus, the numbers of the shift equivalent class in $G(f^e)$ which have the periods aove are.

$$1, \frac{q^n - 1}{p(f)}, \frac{q^{np^i} - q^{np^{i-1}}}{p^j p(f)}\,, (i = 1, 2, \cdots, m - 1)\,, \frac{q^{ne} - q^{np^{m-1}}}{p^m p(f)}$$

Proof. f is irreducible, then $\forall a \in G(f^e)$ the minimal polynomial of a is $f(x)$. And we have

$$G(f^0) \subset G(f^1) \subset G(f^2) \subset \cdots G(f^e)$$

Let's prove the most simple cases first.

0. $G(f^0) = 0$. $|G(f^0)| = 1$ $p(0) = 1$

1. $\forall a \in G(f^1) \setminus G(f^0)$, $p(a) = p(f)$ (f is irreducible), $|G(f^1) \setminus G(f^0)| = q^n - 1$. Then $G(f^1) \setminus G(f^0)$ has $\frac{q^n-1}{p(f)}$ shift equivalent classes.

2.
$$\forall a \in \left\{ \begin{array}{ll} G(f^2) \setminus G(f^1) & p(a) = p(f^2) \\ G(f^3) \setminus G(f^2) & p(a) = p(f^3) \\ \cdots & \cdots \\ G(f^{i+1}) \setminus G(f^i) & p(a) = p(f^{i+1}) \\ \cdots & \cdots \\ G(f^p) \setminus G(f^{p-1}) & p(a) = p(f^p) \end{array} \right\} \Longrightarrow p(a) = p(f^2) = \cdots = p(f^p) = p \cdot f(p)$$

$|G(f^p) \setminus G(f^1)| = q^{np} - q^n$,$G(f^p) \setminus G(f^1)$ has $\frac{q^{np}-q^n}{p \cdot p(f)}$ shit equivalent classes.

And so on,

$\forall a \in G(f^{p^i}) \setminus G(f^{p^{i-1}}), p(a) = p(f^{p^{i-1}+1}) = \cdots = p(f^{p^i}) = p^i \cdot p(f)$

$|G(f^{p^i}) \setminus G(f^{p^{i-1}})| = q^{np^i} - q^{np^{i-1}}$, thus $G(f^{p^i}) \setminus G(f^{p^{i-1}})$ has $\frac{q^{np^i}-q^{np^{i-1}}}{p^i \cdot p(f)}$ shift equivalent classes. $(i = 1, 2, \cdots, m-1)$

$\forall a \in G(f^{p^e}) \setminus G(f^{p^m-1}), p(a) = p^m \cdot p(f)$

$|G(f^{p^e}) \setminus G(f^{p^m-1})| = q^{np^i} - q^{np^{i-1}}$, thus $G(f^{p^e}) \setminus G(f^{p^m-1})$ has $\frac{q^{ne}-q^{np^{m-1}}}{p^m \cdot p(f)}$ shift equivalent classes.

□

Definition 2.2.7. *All the states of LFSR compose of a set. We denote it by* $V_n(\mathbb{F}_q)$.

$$V_n(\mathbb{F}_q) = \{(a_1, a_2, \cdots, a_n) | a_1, a_2, \cdots, a_n \in F_q\}$$

While running LFSR, there is a transform acting in such set. We call it State-transition transform, denoted by T_f.

$$\begin{aligned} T_f: \quad V_n(\mathbb{F}_q) &\longrightarrow V_n(\mathbb{F}_q) \\ S_k &\longmapsto S_k T (= S_{k+1}) \end{aligned}$$

Chapter 3

m-sequence and its sampling

3.1 m-sequence

Definition 3.1.1. *$a = (a_0, a_1, a_2, \cdots)$ is a q-ary n-level LFSR sequence, satisfying*

$$a_k + c_1 a_{k-1} + c_2 a_{k-2} + \cdots + c_n a_{k-n} = 0 \quad (k \geq n, c_n \neq 0)$$

*If $p(a) = q^n - 1$, then a is called **m-sequence**.*

Theorem 3.1.2. *$f(x) \in \mathbb{F}_q[x], f(x) = 1 + c_1 x + c_2 x^2 + \cdots + c_n x^n \quad (c_n \neq 0)$, a is a nonzero sequence in G(f) . If a is a m-sequence , then*

(1)$L^k(a)$ is m-sequence, for $k = 0, 1, 2, \cdots$

(2)$a, L(a), l^2(a), \cdots L^{q^n-2}(a)$ are all nonzero sequence in $G(f)$. and $L^{q^n-1}(a) = a$.

(3)$S_0, S_1, \cdots, S_{q^n-2} \in V_n(\mathbb{F}_q)$ distinct nonzero $q^n - 1$ and $S_{q^n-1} = S_0$

Proof. (1)(2) can be concluded from Lemma 3.4

(3) If $\exists S_i = S_j, (0 \leq i \leq j < q^n - 1)$, then $L^i(a) = L^j(a) \Longrightarrow i = j$.

□

Corollary 3.1.3. *$f(x) \in \mathbb{F}_q[x], f(x) = 1 + c_1 x + c_2 x^2 + \cdots + c_n \, (c_n \neq 0)$, $a(\neq 0) \in G(f)$. Suppose $t_1 > t_2 > 0$,. If a is a m-sequence,*

$$L^{t_1}(a) + L^{t_2}(a) \in G(f)$$

is a m-sequence when $(q^n - 1) \nmid (t_1 - t_2)$.

Theorem 3.1.4. *In $\mathbb{F}_2$, a is a periodic sequence. $\forall i, j (0 \leq i, j \leq p(a) - 1), L^i(a) + L^j(a) = 0$ or $L^k(a)(0 \leq 1 \leq \cdots \leq p(a) - 1)$,then*

$\exists n$, s.t.a is a m-sequence with $p(a) = 2^n - 1$.

Proof. Let $L^i(a)$ denote a consecutive sequence in a with $p(a)$ elements $(0 \leq i \leq p(a) - 1)$

$$L^i(a) = (a_i, a_{i+1}, \cdots, a_{p(a)-1}, a_0, a_1, \cdots, a_{i-1})$$

It's easy to verify that

$$V \triangleq 0 \cup \{L^i(a) | 0 \leq i \leq p(a) - 1\}$$

is a multiplicative group.

Define operations on V.

$$0(c_0, c_1, \cdots, c_{p(a)-1}) = (0, 0, \cdots, 0)$$

$$1(c_0, c_1, \cdots, c_p(a) - 1) = (c_0, c_1, \cdots, c_p(a) - 1)$$

The V is a vector space over $\mathbb{F}_2$. Suppose $p(a) = 2^n - 1$.

$\dim(V) = n$. Thus we can assume $L^0(a), L^1(a), L^2(a), \cdots, L^{r-1}(a)$ is linearly independent over $\mathbb{F}_2$ while $L^0(a), L^1(a), L^2(a), \cdots, L^{r-1}(a), L^r(a)$ is linearly dependent over $\mathbb{F}_2$. Then we have for $r \le n$

$$L^r(a) = c_1 L^{r-1}(a) + c_2 L^{r-2}(a) + \cdots + c_{r-1} L^1(a) + c_r L^0(a), c_i \in \mathbb{F}_2$$

Let $L^{k-r}(k \ge r)$ act over two sides of the equation.

$$L^k(a) = c_1 L^{k-1}(a) + c_2 L^{k-2}(a) + \cdots + c_1 L^{k-r+1}(a) + c_r L^{k-r}(a), c_i \in \mathbb{F}_2$$

$\Longrightarrow$

$$a_k = c_1 a_{k-1} + c_2 a_{k-2} + \cdots + c_{r-1} a_{k-r+1} + c_r a_{k-r}, k \ge r$$

then, $a \in G(f)$, and $f = 1 + c_1 x + c_2 x^2 + \cdots + c_r x^r$

$L^k(a) \in G(f), \forall k \ge 0$, thus $V \subset G(f), |G(f)| = 2^r \ge 2^n \Longrightarrow r \ge n$

Hence r=n, i.e. $deg(f) = n$, $p(a) = 2^n - 1$ so a is a m-sequence with $p(a) = 2^n - 1$. □

3.2 Polynomials of m-sequences

Theorem 3.2.1. *$f(x) \in \mathbb{F}_q[x], f(x) = 1 + c_1 x + c_2 x^2 + \cdots + c_n x^n$ $(c_n \ne 0)$, $a(\ne 0) \in G(f)$*

a is a m-sequence $\Longrightarrow$ f(x) is irreducible.

In fact, we have more strong theorem.

Theorem 3.2.2. *$f(x) \in \mathbb{F}_q[x], f(x) = 1 + c_1 x + c_2 x^2 + \cdots + c^n x^n$ $(c_n \ne 0)$, $a(\ne 0) \in G(f)$*

a is a m-sequence $\Longleftrightarrow$ f(x) is a primitive polynomial.

Definition 3.2.3. *a is a periodic sequence $\mathbb{F}_q$. $a = (a_0, a_1, a_2, \cdots)$. $s \in \mathbb{Z}^+$,*

$$a^{(s)} \triangleq (a_0, a_s, a_{2s}, \cdots)$$

is a sampling sequence of a with s as its period.

Lemma 3.2.4. *a is a periodic sequence $\mathbb{F}_q$, $s \equiv s_1 \pmod{p(a)}$, then*

$$a^{(s)} = a^{(s_1)}$$

Lemma 3.2.5. *a is a periodic sequence $\mathbb{F}_q$,$s \in \mathbb{Z}^+, a^{(s)}$ is periodic, then*

$$p(a^{(s)}) | \frac{p(a)}{gcd(s, p(a))}$$

Lemma 3.2.6. *a is a periodic sequence $\mathbb{F}_q$,$s \in \mathbb{Z}^+, gcd(s, p(a)) = 1$, then $a^{(s)}$ is aslo periodic,*

$$p(a^{(s)}) = p(a)$$

Definition 3.2.7. *(the Trace Represatation of m-sequence) $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\xi) = \xi + \xi^q + \xi^{q^2} + \cdots + \xi^{q^{n-1}}$ is the trace of ξ.*

Lemma 3.2.8. *$\forall \xi \in \mathbb{F}_{p^n}$, $Tr(\xi) \in \mathbb{F}_q$*

3.3 Trace representations

Theorem 3.3.1. *a is m-sequence over $\mathbb{F}_q$, $a = (a_0, a_1, a_2, \cdots), p(a) = q^n - 1$. The minimal polynomial of a, $f(x) = 1 + c_1 x + c_2 x^2 + \cdots + c_n x^n$, is a primitive polynomial. α is a root of $\widetilde{f}(x)$, $\exists \beta \in \mathbb{F}^*_{q^n}$, s.t.*

$$a = (Tr(\beta), Tr(\beta\alpha).Tr(\beta\alpha^2), \cdots)$$

On the other hand, suppose $f(x) \in \mathbb{F}[x], f(x) = 1 + c_1 x + \cdots + c_n x^n$ is primitive polynomial.Let α is a root of $\widetilde{f}(x)$,$\beta \in \mathbb{F}^*_{q^n}$,

$$(Tr(\beta), Tr(\beta\alpha), Tr(\beta\alpha^2), \cdots) \in G(f)$$

is m-sequence.

Proof. $f(x) = 1 + c_1x + c_2x^2 + \cdots + c_nx^n$. $\widetilde{f}(x) = x^n + c_1x^{n-1} + \cdots + c_n$.

$\widetilde{f}(\alpha) = \alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0 \Longrightarrow \alpha^k + c_1\alpha^{k-1} + \cdots + c_n\alpha^{k-n}, k \geq n$

Then $(1, \alpha, \alpha^2, \cdots) \in G(f) \Longrightarrow (\beta, \beta\alpha, \beta\alpha^2, \cdots) \in G(f), \forall\beta \in \mathbb{F}_{q^n}$

For the same reason,

$$(\beta^{q^j}, (\beta\alpha)^{q^j}, \cdots) \in G(f)\,, \forall j\,, 0 \leq j \leq n-1$$

Add the corresponding items, then we have

$$(Tr(\beta), Tr(\beta\alpha), Tr(\beta\alpha^2, \cdots)) \in G(f)$$

It's not difficult to prove that, let $\beta = 0, 1, \cdots, q^n - 1$, we can get q^n distinct sequences, which are all of the sequences in $G(f)$.

Hence,$\forall\alpha, \exists\beta\,, s.t.\, a = (Tr(\beta), Tr(\beta\alpha), Tr(\beta\alpha^2), \cdots)$ ☐

Theorem 3.3.2. *a is m-sequence over $(F)_q$. $p(a) = q^n - 1, gcd(s, q^n - 1) = 1$. $a^{(s)}$ is m-sequence, and $p(a^{(s)}) = q^n - 1$*

Proof. Lemma4.10 $\Longrightarrow a^{(s)}$ is periodic, and $p(a) = q^n - 1$.

Assume the minimal polynomial of α is $f(x)$, $\forall\alpha$ is a root of $\widetilde{f}(x)$, $\exists\beta \in \mathbb{F}^*_{q^n}, s.t.$

$$a = (Tr(\beta), Tr(\beta\alpha), Tr(\beta\alpha^2))$$

Thus,

$$a^{(s)} = (Tr(\beta), Tr(\beta\alpha^s), Tr(\beta\alpha^{2s}), \cdots)$$

$$a^{(s)} = (Tr(\beta), Tr(\beta\alpha^s), Tr(\beta\alpha^{2s}), \cdots)$$

$\widetilde{f}(x)$ is a primitive polynomial, thus α is a primitive element. $gcd(s, q^n - 1) = 1$, hence $\alpha^{(s)}$ is also a primitive element.

Assume the minimal polynomial of $\alpha^{(s)}$ is $\widetilde{f_s}(x)$, which is a primitive polynomial. $f_x(s)$ is a primitive polynomial. According to **Theorem 4.5**, $\alpha^{(s)}$ is a m-sequence and $p(a) = q^n - 1$. ☐

Corollary 3.3.3. *a is a m-sequence in $\mathbb{F}_q, p(a) = q^n - 1, \forall$m-sequence in $\mathbb{F}_q$ is shifting equivalent to a sampling sequence of a.*

Proof. Assume the min.poly. of a is f(x),$\gamma \in \mathbb{F}_{q^n}$ is a root of f(x),and b is a m-sequence in $\mathbb{F}, p(b) = q^n - 1$ and assume γ^s is a root of the minimal polynomial of b,

$gcd(s, q^n - 1) = 1, \xRightarrow{Thm4.14} a^{(s)}$is a m-sequence,$p(a^{(s)}) = q^n - 1.\gamma^s$ is a root min.poly. of $a^{(s)}$.
$\gamma^s$is a root of the minimal polynomial of b.

b and $a^{(s)}$ have the same minimal polynomial $\xRightarrow{Thm4.2} b \sim a^{(s)}$. ☐

Lemma 3.3.4. *a is a m-sequence in $\mathbb{F}_q, p(a) = q^n - 1$.Any a successive n states*

$$S_m, S_{m+1}, S_{m+2}, \cdots, S_{m+n-1}, m \geq 0$$

are linearly independent in $\mathbb{F}_q$

Chapter 4

The pseudo-randomness of m-sequence

4.1 The pseudo-randomness of m-sequence

In $\mathbb{F}_2$

Theorem 4.1.1. *a is a m-sequence in* $\mathbb{F}_2, p(a) = 2^n - 1,$

Arrange a period of a in a circle successively.$0 < k \leq n, \forall k$*-tuple*$(b_1 \O L_2, \cdots, b_k)$ *in* $\mathbb{F}_2$ *appear*

$$\begin{cases} 2^n - k & (b_1, b_2, \cdots, b_k) \neq (0, 0, \cdots, 0) \\ 2^{n-k} - 1 & (b_1, b_2, \cdots, b_k) = (0, 0, \cdots, 0) \end{cases}$$

time in the circle.

Corollary 4.1.2. *a is a m-sequence in* $\mathbb{F}_2$*.* $p(a) = 2^n - 1$*, 1 appear* 2^{n-1} *times, 0 appear* $2^{n-1} - 1$

Definition 4.1.3. η *is a group isomorphism from additive group of* $\mathbb{F}_2$ *to* $\{+1, -1\}$ *which is a multiplicative group.*

$$\eta : \quad \mathbb{F}_2 \longrightarrow \{+1, -1\}$$
$$0 \longmapsto +1$$
$$1 \longmapsto -1$$

a is a periodic sequence in$\mathbb{F}_2$*,the autocorrelation function of a:*

$$C_a(t) \triangleq \sum_{i=0}^{p(a)-1} \eta(a_i)\eta(a_{i+t})$$

Note:

(1)$C_a(t) = p(a), t|p(a).$

(2)$C_a(p(a) + k) = C_a(k), \forall k \geq 0$

(3)$C_a(t) = \sum_{i=0}^{p(a)+1} \eta(a_i + a_{i+t})$

Theorem 4.1.4. *a is a m-sequence in* $\mathbb{F}$*.* $p(a) = 2^n - 1, C_a(t) = -1$ *if* $t \nmid 2^n - 1$

Proof. $a = (a_0, a_1, a_2, \cdots)$,assume the min.poly. of a is f(x).

$$f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n, \quad c_0, c_n \neq 0$$

a satisfies with:

$$c_0 a_k + c_1 a_{k-1} + c_2 a_{k-2} + \cdots + c_n a_{k-n}, k \geq 0(*)$$

$L^t(a) = (a_t, a_{t+1}, a_{t+2}, \cdots)$, $a + L^t(a)$ also satisfies with (*)

$$t \nmid 2^n - 1, a + L^t(a) \neq 0$$

according to Thm4.2 $a + L^t(a)$ is m-sequence.

$$C_a(t) = \sum_{i=0}^{p(a)-1} \eta(a_i)\eta(a_{i+t}) = \sum_{i=0}^{p(a)-1} \eta(a_i + a_{i+t}) = 2^{n-1} \cdots (-1) + (2^{n-1} - 1) = -1$$

$\square$

Definition 4.1.5. *a is a periodical sequence.If* $C_a(t) = -1, t \nmid p(a)$*,a is a pseudo-random-sequence.*

Theorem 4.1.6. *m-sequence is a pseudo-random-sequence.*

Chapter 5

NLFSR

5.1 Basic Concepts

In the section, we are going to study a bit of NLFSR(Nonlinear feedback shift register).

Definition 5.1.1. *The Initital state of FSR(Feedback shift register) is* $(a_0, a_1, \cdots, a_{n-1})$*.Its Feedback function is* $f(x_1, x_2, \cdots, x_n)$*.*

If $f(0, x_2, \cdots, x_n) = f(1, x_2, \cdots, x_n)$*, then we say* f *is* ***degenerated****, otherwise it is* ***non-degenerated****. If* f *is degenerated, let* $g(x_1, x_2, \cdots, x_n) = f(0, x_1, x_2, \cdots, x_{n-1})$*.*

When it comes to FSR, we always assume it is non-degenerated.

$V(\mathbb{F}_n)$ *is a set that contains all states generated by* $f(x)$*.* $|V(\mathbb{F}_n)| = 2^n$*.*

We often use ***state diagram*** G_f *to study FSR sequence.* G_f *is a directed graph with* 2^n *vertices and* 2^n *arcs. It determines* ***state-transition transition*** T_f *from* $V(\mathbb{F}_n)$ *to* $V(\mathbb{F}_n)$*.* T_f *is defined as follows.*

$$T_f : V(\mathbb{F}_n) \to V(\mathbb{F}_n)$$
$$(a_1, a_2, \cdots, a_n) \mapsto (a_2, a_3, \cdots, a_n, f(a_1, a_2, \cdots, a_n))$$

Theorem 5.1.2. *The state diagrams of n-level FSR must have cycles.*

Proof. Initial state $S_0 = (a_0, a_1, \cdots, a_{n-1})$. Let $S_k = T_f S_{k-1} = (a_k, a_{k+1}, a_{k+n-1}).k = 1, 2, \cdots$. Notice that $|V(\mathbb{F}_n)| = 2^n$. Thus in $S_0, S_1, \cdots, S_{2^n}$, there must be at least two identical states.

Let $n_1 \leq 2^n$ be the minimal number satisfying that $\exists n_0 < n_1$, s.t. $S_{n_1} = S_{n_0}$. Thus S_{n_0} is unique. Then $S_0, S_1, \cdots, S_{n_0}, S_{n_0+1}, \cdots, S_{n_1-1}$ are distinct. Hence, $S_{n_0}, S_{n_0+1}, \cdots, S_{n_1-1}$ form a cycle. □

Note: The length of the cycle is ofen called the period of the cycle. $S_0, S_1, \cdots, S_{n_0-1}$ are in a branch of the cycle.

Corollary 5.1.3. $\forall$ *n-level FSR sequence,* $\exists$ *a non-negative integer* n_0*, s.t.*$a_{n_0}, a_{n_0+1}, \cdots$ *is a periodic sequence. Its period* $\leq 2^n$*, which is independent of* n_0*.*

5.2 State Diagrams of FSRs

Now lets study the state diagram of FSR. A diagram without branches has more elegant and simple structure that composes of only several cycles. As you probably have find out, a probem arises. In what circumstances it has no branches? The following are some sufficient and necessary conditions that ensure no branches in the diagram.

Theorem 5.2.1. *The state-diagram of n-level FSR has no branches if and only if the diagram is composed of cycles which has no commmon vertices.*

Theorem 5.2.2. *The state-diagram of n-level FSR whose feedback function is $f(x_1, x_2, \cdots, x_n)$ has no branches if and only if T_f is bijective.*

Proof. If G_f has no branches, then it is composed of cycles which have no common vertices. Thus T_f is bijective.

Suppose T_f is bijective. Initial state $S_0, S_k = T_f S_{k-1}, k = 1, 2, \cdots$.

Let n_0, n_1 satisfying the conditions in **Theorem 5.1.2**. Then $S_0, S_1, S_2, \cdots, S_{n_0}, \cdots, S_{n_1-1}$ are distinct.

If $n_0 \neq 0$, then $T_f(S_{n_0-1} = S_0, T_f(S_{n_1-1} = S_{n_1} = S_0$. Notice that $S_{n_0-1} \neq S_{n_1-1}$, which contradicts the fact that T_f is bijective.

Thus $n_0 = 0$, which means that G_f has no branches. □

5.3 Main theorems

Theorem 5.3.1. *The state-diagram of n-level FSR whose feedback function is $f(x_1, x_2, \cdots, x_n)$ has no branches if and only f can be expressed as $f(x_1, x_2, ..., x_n) = x_1 + f_0(x_2, x_3, \cdots, x_n)$.*

Proof. $\forall$ State $(a_1, a_2, \cdots, a_n) \neq (b_1, b_2, \cdots, b_n)$,

$$T_f(a_1, a_2, \cdots, a_n) = (a_2, \cdots, a_n, f(a_1, \cdots, a_n))$$

$$T_f(b_1, b_2, \cdots, b_n) = (b_2, \cdots, b_n, f(b_1, \cdots, b_n))$$

If $a_1 = b_1, (a_2, \cdots, a_n) \neq (b_2, \cdots, b_n)$,then

$$T_f(a_1, \cdots, a_n) \neq T_f(b_1, \cdots, b_n)$$

If $a_1 \neq b_1, i.e. b_1 = \overline{a}_1, (a_2, \cdots, a_n) = (b_2, \cdots, b_n)$,then

$$f(\overline{a}_1, a_2, \cdots, a_n) = a_1 + 1 + f_0(a_2, \cdots, a_n) = 1 + f(a_1, a_2, \cdots, a_n)$$

Then

$$\begin{aligned} T_f(a_1, a_2, \cdots, a_n) &= (a_2, \cdots, a_n, f(a_1, a_2, \cdots, a_n)) \\ &\neq (a_2, \cdots, a_n, f(\overline{a}_1, a_2, \cdots, a_n)) \\ &= T_f(\overline{a}_1, a_2, \cdots, a_n) \end{aligned}$$

In conclusion, T_f is bijective $\rightarrow G_f$ has no branches.

On the other hand, suppose

$$f(x_1, x_2, \cdots, x_n) = x_1 f_1(x_2, \cdots, x_n) + f_0(x_2, \cdots, x_n)$$

If $f_1(x_2, \cdots, x_n) \neq 0$, then $\exists (a_2, \cdots, a_n) \in \mathbb{F}_{2^n-1}$, s.t. $f(a_2, \cdots, a_n) = 0$.
$\forall a_1 \in \mathbb{F}_2$,

$$f(a_1, a_2, \cdots, a_n) = f_0(a_2, \cdots, a_n) = f(\overline{a}_1, a_2, \cdots, a_n)$$

$$T_f(a_1, a_2, \cdots, a_n) = T_f(\overline{a}_1, a_2, \cdots, a_n)$$

Then T_f is not bijective. G_f has no branches. □

Note: we call feedback function $f(x_1, x_2, \cdots, x_n)$ non-singular. If $f(x_1, x_2, \cdots, x_n)$ can be expressed as $f(x_1, x_2, \cdots, x_n) = x_1 + f_0(x_2, \cdots, x_n)$

Index

REFERENCES

[1] Zhexian Wan. *Algebra and Coding*[M]. Third Edition. Beijing: China Higher Education Press, 2007.187