A Recursive Relation Between The Adjacency Graph of Some LFSRs and Its Applications

Ming Li Dongdai Lin

State Key Laboratory of Information Security,
Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093, China
E-mail: liming@iie.ac.cn, ddlin@iie.ac.cn

November 18, 2014

Abstract

In this paper, a general way to determine the adjacency graph of linear feedback shift registers (LFSRs) with characteristic polynomial $(1+x)c(x)$ from the adjacency graph of LFSR with characteristic polynomial $c(x)$ is discussed, where $c(x)$ can be any polynomial. As an application, the adjacency graph of LFSRs with characteristic polynomial $(1+x)^4p(x)$ are determined, where $p(x)$ is a primitive polynomial. Besides, some properties about the cycles in LFSRs are presented. The adjacency graph of LFSRs with characteristic polynomial $(1+x)^mp(x)$ are also discussed.

1 Introduction

Feedback shift registers (FSRs) have been used and studied for many years [6]. Especially in cryptography, FSRs are the basic component in stream cipher [8]. But some basic theories of FSRs have not been solved. The most important one may be construct FSRs that output sequences with large period. The adjacency graph of FSRs can be used to construct FSRs that output sequences with large period. When we change the successor of two states that in different cycles and are conjugate with each other, we get a big cycle from two small cycles [6]. Do it repeatedly, we can get FSRs that output sequences with efficient large period. So determine the adjacency graph of FSRs is important both from theory and practice [2].

The adjacency graph of LFSR with characteristic polynomial $1+x^n$ were determined by [13] and [14]. The adjacency graph of LFSR with characteristic polynomial $(1+x)^n$ were determined by [15]. The adjacency graph of complementary circulating register were determined by [16]. The adjacency graph of LFSR with characteristic polynomial $(1+x)^mp(x)$ for $m=1,2,3$ were determined by [4], [11] and [2]. But there are no results for $m \geq 4$. The adjacency graph of LFSR with characteristic polynomial $(1+x^3)p(x)$ were determined by [3].

In this paper, a recursive relation between the adjacency graph of FSR_f and $\mathrm{FSR}_{(x_0+x_1)*f}$ is discussed, where f is a linear boolean function. In [1], the FSRs whose characteristic polynomial g can be written as $g=f*(x_0+x_1)$ for some f were studied. In [5], the FSRs whose characteristic polynomial g can be written as $g=(x_0+x_1)*f$ for some f were studied. Since the operation $*$ is not commutative, $f*(x_0+x_1) \neq (x_0+x_1)*f$ generally. But when f is a linear boolean function, we have $f*(x_0+x_1)=(x_0+x_1)*f$. So in the linear case, we can combine the conclusion in [1] and [5], and get more results. First, we show some properties about the cycles in LFSR. Then we pay attention to the relation between the adjacency graph of FSR_f and $\mathrm{FSR}_{(x_0+x_1)*f}$, where f is a linear

boolean function. As an application, the adjacency graph of $\mathrm{FSR}_{(1+x)^4p(x)}$ is determined, where $p(x)$ is a primitive polynomial. Some result about $\mathrm{FSR}_{(1+x)^mp(x)}$ for $m > 4$ is also discussed.

This paper is organized as follows. In section 2, we present some basic knowledge about FSRs, and explain some notation that we will use. Some properties about the cycles in LFSRs are presented In section 3. In section 4, a recursive relation between the adjacency graph of FSR_f and $\mathrm{FSR}_{(x_0+x_1)*f}$ is presented. As an application, in section 5 the adjacency graph of $\mathrm{FSR}_{(1+x)^4p(x)}$ is determined. In section 6, we discuss the general case $\mathrm{FSR}_{(1+x)^mp(x)}$ for $m > 4$. At the end, we conclude this paper.

2 Preliminaries

The purpose of this section is to briefly review the basic knowledge about feedback shift registers, and explain some notations that will be used in this paper.

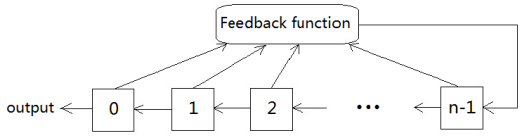
2.1 Feedback shift registers

Let $\mathbb{F}_2$ be the finite field of two-element. Let $\mathbb{F}_2^n$ be the vector space of dimension n over $\mathbb{F}_2$. A boolean function $f(x_0, x_1, \ldots, x_{n-1})$ in n variables is a map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. It is well known that an Boolean function can be uniquely represented by its algebraic normal form (ANF), which is a multivariate polynomial. For two boolean functions $f(x_0, x_1, \ldots, x_n)$ and $g(x_0, x_1, \ldots, x_m)$, we denote

$$f * g = f(g(x_0, x_1, \ldots, x_m), g(x_1, x_2 \ldots, x_{m+1}), \ldots, g(x_n, x_{n+1}, \ldots, x_{n+m})),$$

which is an $(n + m - 1)$-variable Boolean function. Note that the operation $*$ is not commutative, that is, $f * g$ and $g * f$ are not the same in general.

An n-stage feedback shift register (FSR) consists of n binary storage cells and a characteristic polynomial f regulated by a single clock. A sketch diagram is shown below. The feedback function, denoted by f_0, correspond to the characteristic polynomial $f = f_0 + x_n$. We denote the FSR with characteristic polynomial f by FSR_f.



A state of an FSR is a vector $(x_0, x_1, \ldots, x_{n-1})$, where x_i indicates the content of stage i. At every clock pulse, the state $(x_0, x_1, \ldots, x_{n-1})$ is updated by $(x_1, x_2, \ldots, f_0(x_0, \ldots, x_{n-1}))$. Therefore, f induces a next-state operation from $\mathbb{F}_2^n$ to itself

$$\theta_f : (x_0, x_1, \ldots, x_{n-1}) \mapsto (x_1, x_2, \ldots, f_0(x_0, \ldots, x_{n-1})).$$

It is well known that, θ_f is a bijection if and only f can be written as $f = x_0 + F(x_1, \ldots, x_{n-1}) + x_n$ for some F. In this case, we say FSR_f is nonsingular. Without specification, all the FSRs in this paper are nonsingular.

From an initial state $\mathbf{X}_0 = (x_0, x_1, \ldots, x_{n-1})$, after consecutive clock pulses, FSR_f generate a cycle $C = (\mathbf{X}_0, \mathbf{X}_1, \ldots, \mathbf{X}_{l-1})$, where $\mathbf{X}_{i+1}$ is the next state of $\mathbf{X}_i$ for $i = 1, 2, \ldots, l-2$, $\mathbf{X}_0$ is the next state of $\mathbf{X}_{l-1}$, and l is the length of the cycle. Cycle C can be seen as an ordered set with element in $\mathbb{F}_2^n$. So we can say a state is or not belong to a cycle. For simplicity, cycle C can be written as $C = (x_0, x_1, \ldots, x_{l-1})$, where x_i is the first component of $\mathbf{X}_i$. We call this notation sequence-notation. Define the weight of cycle C as $W(C) = \sum_{i=1}^{l} x_i$. It is obvious that, the set $\mathbb{F}_2^n$ is divided into cycles $C_1, C_2, \ldots, C_k$ by FSR_f. Reversely, a division of $\mathbb{F}_2^n$ into cycles determines an n-stage FSR. So we can treat FSR_f as a set of cycles, and use the notation $\mathrm{FSR}_f = \{C_1, C_2, \ldots, C_k\}$.

Next, we consider the output sequences of FSR_f. From an initial state $\mathbf{X}_0 = (x_0, x_1, \ldots, x_{n-1})$, after consecutive clock pulses, FSR_f output a sequence $\mathbf{x} = x_0 x_1 \cdots$ satisfying $f(x_t, x_{t+1}, \ldots, x_{t+n}) = 0$ for any $t \geq 0$. Let $G(f)$ be the set of sequences that FSR_f can output. Then $|G(f)| = 2^n$. Since FSR_f is nonsingular, $G(f)$ contains only periodic sequences. We use $(a_0 a_1 \cdots a_{p-1})$ to denote the periodic sequence $a_0 a_1 \cdots a_{p-1} \cdots$ with period p. For a periodic sequence $\mathbf{a}$, we use $p(\mathbf{a})$ to denote the period of $\mathbf{a}$. Let L be a map on periodic sequences: $L((a_0 a_1 \cdots a_{p-1})) = (a_1 a_2 \cdots a_{p-1} a_0)$. Two periodic sequences $\mathbf{a}$ and $\mathbf{b}$ are called shift equivalent, denoted by $\mathbf{a} \simeq \mathbf{b}$, if there exists an integer r such that $\mathbf{a} = L^r(\mathbf{b})$. It can be verified, $\simeq$ is an equivalence relation on $G(f)$. So $G(f)$ is divided into equivalent classes. We use the notation $[\mathbf{a}]$ to denote the equivalent class that contains $\mathbf{a}$. Then we have: $G(f) = \cup_{i=1}^{k} [\mathbf{x}_i]$, where k is the number of equivalent classes in $G(f)$ and $\mathbf{x}_i, \mathbf{x}_j \in G(f)$ belongs to different equivalent classes provided $i \neq j$.

Define a map from the equivalent classes in $G(f)$ to the cycles in FSR_f

$$\Theta : [(x_0 x_1 \cdots x_{l-1})] \mapsto (x_0, x_1, \ldots, x_{l-1}).$$

It can be verified, Θ is a bijection. For this reason, sometimes we use an equivalent class to denote a cycle. For example, if $(x_0, x_1, \ldots, x_{l-1}) \in G(f)$, then we can treat $[(x_0 x_1 \cdots x_{l-1})]$ as a cycle in FSR_f, and use the notation $[(x_0 x_1 \cdots x_{l-1})] \in FSR_f$. In section 5, we always use this notation.

For a state $\mathbf{X} = (x_0, x_1, \ldots, x_{n-1})$, its conjugate $\widehat{\mathbf{X}}$, companion $\widetilde{\mathbf{X}}$ and dual $\overline{\mathbf{X}}$ are defined as $\widehat{\mathbf{X}} = (\overline{x}_0, x_1, \ldots, x_{n-1})$, $\widetilde{\mathbf{X}} = (x_0, x_1, \ldots, \overline{x}_{n-1})$ and $\overline{\mathbf{X}} = (\overline{x}_0, \overline{x}_1, \ldots, \overline{x}_{n-1})$, where $\overline{x}$ denotes the binary complement of x. We call $(\mathbf{X}, \widehat{\mathbf{X}})$ a conjugate pair, $(\mathbf{X}, \widetilde{\mathbf{X}})$ a companion pair, and $(\mathbf{X}, \overline{\mathbf{X}})$ a dual pair. For a cycle $C = (\mathbf{X}_0, \mathbf{X}_1, \ldots, \mathbf{X}_{l-1})$, its dual cycle $\overline{C}$ is defined as $\overline{C} = (\overline{\mathbf{X}}_0, \overline{\mathbf{X}}_1, \ldots, \overline{\mathbf{X}}_{l-1})$. Two cycles C_1 and C_2 are adjacent if they are disjoint and there exists a state $\mathbf{X}$ in C_1 whose conjugate $\widehat{\mathbf{X}}$ (or companion $\widetilde{\mathbf{X}}$) is in C_2. It is well-known that two adjacent cycles C_1 and C_2 are joined into a single cycle when the successors of $\mathbf{X}$ and $\widehat{\mathbf{X}}$ are interchanged. This is the basic idea of the cycle joining method introduced in [6]. The problem of determining the number of conjugate pairs between cycles leads to the definition of adjacency graph.

Definition 1. *[10][9] For an FSR, its adjacency graph is an undirected graph where the vertexes correspond to the cycles in it, and there exists an edge labeled with an integer m between two vertexes if and only if the two vertexes share m conjugate pairs.*

2.2 LFSRs and m-sequences

An FSR is called a linear feedback shift register (LFSR) if its characteristic polynomial f is linear and nonlinear feedback shift register (NFSR) otherwise. For a linear boolean function $f(x_0, x_1, \ldots, x_n) = a_0 x_0 + a_1 x_1 + \cdots + a_n x_n$, we can associate it with a univariate polynomial $c(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}_2[x]$, and denote $c(x) = \phi(f)$, $f = \phi^{-1}(c(x))$. The function ϕ maps a linear Boolean function to a univariate polynomial over $\mathbb{F}_2[x]$, which is a one-to-one correspondence. It can be verified, $\phi(f * g) = \phi(f)\phi(g)$. So the operation $*$ is commutative in the linear case. Sometimes, it is convenient to use the univariate polynomial $\phi(f)$ instead of the linear function f in the linear case.

Let $\mathbf{a} = a_0 a_1 \cdots$ and $\mathbf{b} = b_0 b_1 \cdots$ be two sequences. Let $c \in \mathbb{F}_2$. Then the sum $\mathbf{a} + \mathbf{b}$ is defined to be $\mathbf{a} + \mathbf{b} = c_0 c_1 \cdots$ with $c_i = a_i + b_i$ for $i \geq 0$. The scalar multipication $c\mathbf{a}$ is defined to be $c\mathbf{a} = d_0 d_1 \cdots$ with $d_i = c \cdot a_i$ for $i \geq 0$. Then $G(c(x))$ is a vector space over $\mathbb{F}_2$ endowed with the two operations defined above for any $c(x) \in \mathbb{F}_2[x]$.

Lemma 1. *[17] Let $c_1(x), c_2(x) \in \mathbf{F}_2[x]$. Let $\mathbf{a} \in G(c_1(x))$ and $\mathbf{b} \in G(c_2(x))$. Then $\mathbf{a} + \mathbf{b} \in lcm(c_1(x), c_2(x))$. In particular, if $gcd(c_1(x), c_2(x)) = 1$, then $p(\mathbf{a} + \mathbf{b}) = lcm(p(\mathbf{a}), p(\mathbf{b}))$.*

For an n-stage LFSR, the period of its output sequence is no more than $2^n - 1$. If this value is attained, we call the sequence m-sequence, and the LFSR maximum LFSR. It is well known that, an LFSR generates m-sequences if and only if its characteristic polynomial is primitive [17]. For m-sequences, we have the famous shift-and-add property [17].

Lemma 2. *[17][3] Let* $\mathbf{s}$ *be a m-sequence with period* 2^n-1*. Then for any* $1 \le j \le 2^n-2$*, there exist an integer* $1 \le k \le 2^n-2$ *such that* $\mathbf{s}+L^j(\mathbf{s}) = L^k(\mathbf{s})$*. Further more, define a map from* $\{1,2,\ldots,2^n-2\}$ *to itself,* $Z: j \mapsto k$*. Then* Z *is a bijection.*

Proof. We only prove the second assertion. It suffices to prove Z is an injection. Suppose $Z(j_1) = Z(j_2)$. Then $\mathbf{s}+L^{j_1}(\mathbf{s}) = \mathbf{s}+L^{j_2}(\mathbf{s})$. So $L^{j_1}(\mathbf{s}) = L^{j_2}(\mathbf{s})$. This implies $j_1 = j_2$. □

We note that: for different choice of $\mathbf{s}$, the bijection Z is different generally. Some properties about the bijection Z can be found in [3].

2.3 Self-dual FSRs and dividable FSRs

In [1], $\mathcal{D}$-morphism was proposed.

$$\begin{aligned} \mathcal{D}: \quad & \mathbb{F}_2^{n+1} \to \mathbb{F}_2^n \\ & (x_0, x_1, \ldots, x_n) \mapsto (x_0+x_1, x_1+x_2, \ldots, x_{n-1}+x_n). \end{aligned}$$

$\mathcal{D}$-morphism is a two-to-one map. For any n-stage state $\mathbf{X} = (x_0, x_1, \ldots, x_{n-1})$, the two preimages of $\mathbf{X}$ are $\mathcal{D}_0^{-1}(\mathbf{X}) = (0, x_0, x_0+x_1, \ldots, x_0+x_1+\cdots+x_{n-1})$ and $\mathcal{D}_1^{-1}(\mathbf{X}) = (1, 1+x_0, 1+x_0+x_1, \ldots, 1+x_0+x_1+\cdots+x_{n-1})$. Let C be an n-stage cycle. Let $S = \{\mathbf{X} | \mathcal{D}(\mathbf{X}) \in C\}$. For any state $\mathbf{X} \in S$ we can find a state $\mathbf{Y} \in S$ such that: $\mathcal{D}(\mathbf{X}) \to \mathcal{D}(\mathbf{Y})$ in C and $\mathbf{Y}$ can be a successor of $\mathbf{X}$. Define $\mathbf{X} \to \mathbf{Y}$ in S. Then the states in S form cycles. Denote the set of these cycles by $\mathcal{D}^{-1}(C)$. Then we have the following fact [1]. In the case $W(C)$ is odd, $\mathcal{D}^{-1}(C)$ contains only one cycle. Let $\mathcal{D}^{-1}(C) = \{E\}$. Then we have $\overline{E} = E$. In the case $W(C)$ is even, $\mathcal{D}^{-1}(C)$ contains two cycles. Let $\mathcal{D}^{-1}(C) = \{E, E'\}$. Then we have $\overline{E} = E'$.

Lemma 3. *[1] Let* $FSR_f = \{C_1, C_2, \ldots, C_k\}$ *be an n-stage FSR. Then*

$$\mathcal{D}^{-1}(C_1) \cup \mathcal{D}^{-1}(C_2) \cup \cdots \cup \mathcal{D}^{-1}(C_k)$$

is an $(n+1)$*-stage FSR with characteristic polynomial* $f*(x_0+x_1)$*.*

Definition 2. *[1]* FSR_g *is called self-dual if* $C \in FSR_g$ *implies* $\overline{C} \in FSR_g$*.*

Lemma 4. *[1]* FSR_g *is self-dual if and only if* $g = f*(x_0+x_1)$ *for some* f*.*

Next, we consider another class of FSRs. Let $C = (\mathbf{X}_0, \mathbf{X}_1, \ldots, \mathbf{X}_{l-1})$ be an n-stage cycle, where l is the length of the cycle and $\mathbf{X}_i = (x_i, x_{i+1}, \ldots, x_{i+n-1})$ is an n-stage state in the cycle for $i = 0, \ldots, l-1$. The subscribes are taken modulo l (similarly hereinafter). Now we can construct another cycle $C^+ = (\mathbf{X}_0^+, \mathbf{X}_1^+, \ldots, \mathbf{X}_{l-1}^+)$, where $\mathbf{X}_i^+ = (x_i, x_{i+1}, \ldots, x_{i+n-1}, x_{i+n})$, $i = 0, 1, \ldots, l-1$. It is easy to verify that this definition makes sense. C^+ is an $(n+1)$-stage cycle of length l. We call C^+ the extended cycle of C. We call a cycle C prime cycle, if there is no conjugate pair (companion pair) in C. For a prime cycle $C = (\mathbf{X}_0, \mathbf{X}_1, \ldots, \mathbf{X}_{l-1})$, we can construct an $(n-1)$-stage cycle: $C^- = (\mathbf{X}_0^-, \mathbf{X}_1^-, \ldots, \mathbf{X}_{l-1}^-)$, where $\mathbf{X}_i^- = (x_i, x_{i+1}, \ldots, x_{i+n-2})$, $i = 0, 1, \ldots, l-1$. The definition makes sense, because the states in C^- are all different from each other, and $\mathbf{X} \to \mathbf{Y}$ implies $\mathbf{X}^- \to \mathbf{Y}^-$. We warn that, C^- is meaningful if and only if C is a prime cycle. We call C^- the reduced cycle of C.

Lemma 5. *[5] Let* $FSR_f = \{C_1, C_2, \ldots, C_k\}$ *and* $FSR_{f+1} = \{D_1, D_2, \ldots, D_t\}$ *be two n-stage FSRs, then*

$$\{C_1^+, C_2^+, \ldots, C_k^+, D_1^+, D_2^+, \ldots, D_t^+\}$$

is an $(n+1)$*-stage FSR with characteristic polynomial* $(x_0+x_1)*f$*.*

Note: *Define* $\mathcal{A} = \{C_1^+, C_2^+, \ldots, C_k^+\}$ *and* $\mathcal{B} = \{D_1^+, D_2^+, \ldots, D_t^+\}$*. Let* C *be a cycle in* $FSR_{(x_0+x_1)*f}$*. Let* $\mathbf{X}$ *be a state in* C*. Then we have:* $C \in \mathcal{A}$ *if and only if* $f(\mathbf{X}) = 0$*;* $C \in \mathcal{B}$ *if and only if* $f(\mathbf{X}) = 1$*.*

Definition 3. *[5]* FSR_g *is called dividable if we can divide the vertexes in the adjacency graph of* FSR_g *into two sets, such that the edges are all between the two sets.*

Lemma 6. *[5]* FSR_g *is dividable if and only if* $g = (x_0+x_1)*f$ *for some* f*.*

3 Some Properties About The Cycles in LFSRs

When f is a linear boolean function, we have $(x_0 + x_1) * f = f * (x_0 + x_1)$. The following conclusion is direct from lemma 3-6.

Theorem 1. *Let f be a linear boolean function. Then $FSR_{(x_0+x_1)*f}$ is self-dual and dividable. Write $FSR_f = \{C_1, C_2, \ldots, C_k\}$ and $FSR_{f+1} = \{D_1, D_2, \ldots, D_t\}$. We have*

$$\mathcal{D}^{-1}(C_1) \cup \mathcal{D}^{-1}(C_2) \cup \cdots \cup \mathcal{D}^{-1}(C_k) = \{C_1^+, C_2^+, \ldots, C_k^+, D_1^+, D_2^+, \ldots, D_t^+\}. \quad (1)$$

For a linear boolean function g, it is easy to see, FSR_g is dividable (or self-dual) if and only if g contains an even number of terms. Considering $\phi(g)$, $\mathrm{FSR}_{\phi(g)}$ is dividable (or self-dual) if and only if $\phi(g)(1) = 0$.

Theorem 2. *Let f be a linear boolean function. Suppose there are t cycles of even weight in FSR_f. Then there are t cycles in FSR_{f+1}.*

Proof. Suppose there are s cycles of odd weight in FSR_f, and there are u cycles in FSR_{f+1}. Consider the equation in theorem 1. On the left side of the equation (1), there are $s + 2t$ cycles. On the right side of the equation (1), there are $s+t+u$ cycles. So we get $s+2t = s+t+u$. This implies $u = t$. □

Theorem 3. *Let f be a linear boolean function that contains an odd number of terms. Then the cycles in FSR_f are all of even weight.*

Proof. Suppose C is a cycle in FSR_f of odd weight. Then there is only one cycle in $\mathcal{D}^{-1}(C)$. Let $\mathcal{D}^{-1}(C) = \{E\}$. We have $E = \overline{E}$. Write $\mathrm{FSR}_f = \{C_1, C_2, \ldots, C_k\}$ and $\mathrm{FSR}_{f+1} = \{D_1, D_2, \ldots, D_t\}$. Then, $E = C_i^+$ for some i or $E = D_j^+$ for some j. Suppose $E = C_i^+$ for some i (the case that $E = D_j^+$ for some j is similar). Then $f(\mathbf{X}) = 0$ for any $\mathbf{X} \in E$. Let $\mathbf{X}_1$ be a state in E. Since $E = \overline{E}$, its dual $\overline{\mathbf{X}}_1$ is also in E. Because there are an odd number of terms in f, we have $f(\mathbf{X}_1) \neq f(\overline{\mathbf{X}}_1)$. So we get a contradiction. □

Theorem 4. *Let f be a linear boolean function. FSR_f and FSR_{f+1} contain the same number of cycles if and only if f contains an odd number of terms.*

Proof. Suppose f contains an odd number of terms. Then the cycles in FSR_f are all of even weight. According to theorem 2, the number of cycles in FSR_{f+1} is the same as the number of even weight cycles in FSR_f. So FSR_f and FSR_{f+1} contain the same number of cycles. Suppose f contains an even number of terms. Then $f(1, 1, \ldots, 1) = 0$. This means the 1-cycle $((1, 1, \ldots, 1))$ which contains only the 1-state $(1, 1, \ldots, 1)$, is a cycle in FSR_f. Since the 1-cycle $((1, \ldots, 1))$ is a cycle of odd weight, there are at least one cycle of odd weight in FSR_f. So FSR_f contains more cycles than FSR_{f+1}. □

4 Determine the Adjacency Graph of $\mathrm{LFSR}_{(x_0+x_1)*f}$ From The Adjacency Graph of LFSR_f

In this section, we try to determine the adjacency graph of LFSR with characteristic polynomial $(x_0 + x_1) * f$ from the adjacency graph of LFSR with characteristic polynomial f, where f is a linear boolean function. Our discussion can be divided into two cases.

4.1 The case that f contains an odd number of terms

Let f be a linear boolean function that contains an odd number of terms. According to theorem 3, the cycles in FSR_f are all of even weight. Let C be a cycle in FSR_f. Then there are two cycles in $\mathcal{D}^{-1}(C)$, denoted as $\mathcal{D}^{-1}(C) = \{E, \overline{E}\}$. According to theorem 1, E and $\overline{E}$ are the extension of some two cycles in FSR_f or FSR_{f+1}. Let $\mathbf{X}$ be a state in E. Then $\overline{\mathbf{X}}$ is a state in $\overline{E}$. Since f contains

an odd number of terms, we have $f(\mathbf{X}) \neq f(\overline{\mathbf{X}})$. According to Note 1, this implies when E is the extension of some cycle in FSR_f (FSR_{f+1}), then $\overline{E}$ is the extension of some cycle in FSR_{f+1} (FSR_f).

Theorem 5. *Let f be a linear boolean function that contains an odd number of terms.*

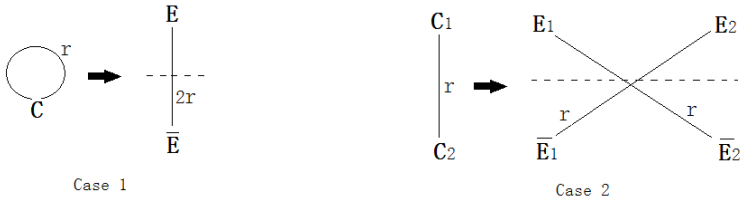
1. *Let $C \in \mathrm{FSR}_f$. Let $\mathcal{D}^{-1}(C) = \{E, \overline{E}\}$. Suppose C contains r conjugate pairs. Then E and $\overline{E}$ share $2r$ conjugate pairs.*
2. *Let $C_1, C_2 \in \mathrm{FSR}_f$. Let $\mathcal{D}^{-1}(C_1) = \{E_1, \overline{E}_1\}$ and $\mathcal{D}^{-1}(C_2) = \{E_2, \overline{E}_2\}$, where $E_1^-, E_2^- \in FSR_f$, and $\overline{E}_1^-, \overline{E}_2^- \in FSR_{f+1}$. Suppose C_1 and C_2 share r conjugate pairs. Then E_1 and $\overline{E}_2$, $\overline{E}_1$ and E_2 both share r conjugate pairs.*

Proof. 1. Let $(\mathbf{X}_i, \widehat{\mathbf{X}}_i), i = 1, 2, \ldots, r$ be the r conjugate pairs in C. Then $(\mathcal{D}_0^{-1}(\mathbf{X}_i), \mathcal{D}_1^{-1}(\widehat{\mathbf{X}}_i))$, $(\mathcal{D}_1^{-1}(\mathbf{X}_i), \mathcal{D}_0^{-1}(\widehat{\mathbf{X}}_i))$, $i = 1, 2, \ldots, r$, are the $2r$ conjugate pairs shared by E and $\overline{E}$.

2. It is obvious that, there are no conjugate pairs shared by E_1 and E_2, $\overline{E}_1$ and $\overline{E}_2$. Let $(\mathbf{X}_i, \widehat{\mathbf{X}}_i), i = 1, 2, \ldots, r$ be the r conjugate pairs shared by C_1 and C_2 with $\mathbf{X}_i \in C_1$ and $\widehat{\mathbf{X}}_i \in C_2$. Let $\mathcal{D}_{b_i}^{-1}(\mathbf{X}_i) \in E_1$, where $b_i \in \mathbb{F}_2$ for $i = 1, 2, \ldots, r$. Then $\mathcal{D}_{1-b_i}^{-1}(\mathbf{X}_i) \in \overline{E}_1$ for $i = 1, 2, \ldots, r$. Since there are no conjugate pairs shard by E_1 and E_2, we know $\mathcal{D}_{1-b_i}^{-1}(\widehat{\mathbf{X}}_i) \in \overline{E}_2$, for $i = 1, 2, \ldots, r$. Consequently, $\mathcal{D}_{b_i}^{-1}(\widehat{\mathbf{X}}_i) \in E_2$, for $i = 1, 2, \ldots, r$. So $(\mathcal{D}_{b_i}^{-1}(\mathbf{X}_i), \mathcal{D}_{1-b_i}^{-1}(\widehat{\mathbf{X}}_i))$, $i = 1, 2, \ldots, r$ are the r conjugate pairs shared by E_1 and $\overline{E}_2$. $(\mathcal{D}_{1-b_i}^{-1}(\mathbf{X}_i), \mathcal{D}_{b_i}^{-1}(\widehat{\mathbf{X}}_i))$, $i = 1, 2, \ldots, r$ are the r conjugate pairs shared by $\overline{E}_1$ and E_2.

□

The conclusion in theorem 2 can be shown by the graph below.



4.2 The case that f contains an even number of terms

For a linear boolean function f, FSR_f is dividable if and only if f contains an even number of terms. So, FSR_f contains only prime cycles providing that f contains an even number of terms.

Let C be a cycle in FSR_f of even weight. Then there are two cycles in $\mathcal{D}^{-1}(C)$, denoted as $\mathcal{D}^{-1}(C) = \{E, \overline{E}\}$. Let $\mathbf{X}$ be a state in E. Then $\overline{\mathbf{X}}$ is a state in $\overline{E}$. Since f contains an even number of terms, we have $f(\mathbf{X}) = f(\overline{\mathbf{X}})$. It means that, when E is the extension of some cycle in FSR_f (or FSR_{f+1}), then $\overline{E}$ is the extension of some cycle in FSR_f (or FSR_{f+1}) too. So there are no conjugate pairs shared by E and $\overline{E}$.

Theorem 6. *Let f be a linear boolean function that contains an even number of terms.*

1. *Let $C_1, C_2 \in \mathrm{FSR}_f$ be two cycles of odd weight. Let $D^{-1}(C_1) = \{E_1\}$ and $D^{-1}(C_2) = \{E_2\}$. Suppose C_1 and C_2 share r conjugate pairs, then E_1 and E_2 share $2r$ conjugate pairs.*
2. *Let $C_1 \in \mathrm{FSR}_f$ be a cycle of odd weight and $C_2 \in \mathrm{FSR}_f$ be a cycle of even weight. Let $D^{-1}(C_1) = \{E_1\}$ and $D^{-1}(C_2) = \{E_2, \overline{E}_2\}$. Suppose C_1 and C_2 share r conjugate pairs. Then E_1 and E_2, E_1 and $\overline{E}_2$ both share r conjugate pairs.*

3. *Let $C_1, C_2 \in \mathrm{FSR}_f$ be two cycles of even weight. Let $D^{-1}(C_1) = \{E_1, \overline{E}_1\}$ and $D^{-1}(C_2) = \{E_2, \overline{E}_2\}$. Suppose C_1 and C_2 share r conjugate pairs. Then there exist an integer u with $0 \le u \le r$ such that: E_1 and E_2, $\overline{E}_1$ and $\overline{E}_2$ both share u conjugate pairs; E_1 and $\overline{E}_2$, $\overline{E}_1$ and E_2 both share $r-u$ conjugate pairs.*

Proof. 1. Let $(\mathbf{X}_i, \widehat{\mathbf{X}}_i), i = 1, 2, \ldots, r$ be the r conjugate pairs shared by C_1 and C_2 with $\mathbf{X}_i \in C_1$ and $\widehat{\mathbf{X}}_i \in C_2$. Then $(\mathcal{D}_0^{-1}(\mathbf{X}_i),\ \mathcal{D}_1^{-1}(\widehat{\mathbf{X}}_i))$, $(\mathcal{D}_1^{-1}(\mathbf{X}_i), \mathcal{D}_0^{-1}(\widehat{\mathbf{X}}_i))$, $i = 1, 2, \ldots, r$, are the $2r$ conjugate pairs shared by C_1 and C_2.

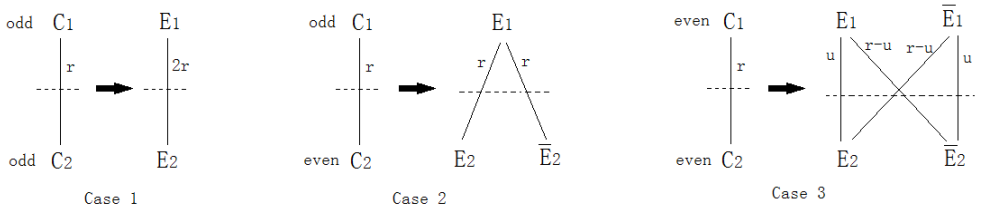
2. Let $(\mathbf{X}_i, \widehat{\mathbf{X}}_i), i = 1, 2, \ldots, r$ be the r conjugate pairs shared by C_1 and C_2 with $\mathbf{X}_i \in C_1$ and $\widehat{\mathbf{X}}_i \in C_2$. Let $\mathcal{D}_{b_i}^{-1}(\widehat{\mathbf{X}}_i) \in E_2$, where $b_i \in \mathbb{F}_2$ for $i = 1, 2, \ldots, r$. Then $\mathcal{D}_{1-b_i}^{-1}(\widehat{\mathbf{X}}_i) \in \overline{E}_2$ for $i = 1, 2, \ldots, r$. So $(\mathcal{D}_{1-b_i}^{-1}(\mathbf{X}_i), \mathcal{D}_{b_i}^{-1}(\widehat{\mathbf{X}}_i))$, $i = 1, 2, \ldots, r$ are the r conjugate pairs shared by E_1 and E_2. $(\mathcal{D}_{b_i}^{-1}(\mathbf{X}_i), \mathcal{D}_{1-b_i}^{-1}(\widehat{\mathbf{X}}_i))$, $i = 1, 2, \ldots, r$ are the r conjugate pairs shared by E_1 and $\overline{E}_2$.

3. Let $(\mathbf{X}_i, \widehat{\mathbf{X}}_i), i = 1, 2, \ldots, r$ be the r conjugate pairs shared by C_1 and C_2 with $\mathbf{X}_i \in C_1$ and $\widehat{\mathbf{X}}_i \in C_2$. Let $\mathcal{D}_{b_i}^{-1}(\mathbf{X}_i) \in E_1$, where $b_i \in \mathbb{F}_2$ for $i = 1, 2, \ldots, r$. Then $\mathcal{D}_{1-b_i}^{-1}(\mathbf{X}_i) \in \overline{E}_1$ for $i = 1, 2, \ldots, r$. Let $\mathcal{D}_{c_i}^{-1}(\widehat{\mathbf{X}}_i) \in E_2$, where $c_i \in \mathbb{F}_2$ for $i = 1, 2, \ldots, r$. Then $\mathcal{D}_{1-c_i}^{-1}(\widehat{\mathbf{X}}_i) \in \overline{E}_2$ for $i = 1, 2, \ldots, r$. Define u be the number of elements in set $\{i | b_i + c_i = 1\}$. Then $\{\mathcal{D}_{b_i}^{-1}(\mathbf{X}_i), \mathcal{D}_{c_i}^{-1}(\widehat{\mathbf{X}}_i) | b_i + c_i = 1, i = 1, 2, \ldots, r\}$ are the u conjugate pairs shared by E_1 and E_2. $\{\mathcal{D}_{1-b_i}^{-1}(\mathbf{X}_i), \mathcal{D}_{1-c_i}^{-1}(\widehat{\mathbf{X}}_i) | b_i + c_i = 1, i = 1, 2, \ldots, r\}$ are the u conjugate pairs shared by $\overline{E}_1$ and $\overline{E}_2$. $\{\mathcal{D}_{b_i}^{-1}(\mathbf{X}_i), \mathcal{D}_{1-c_i}^{-1}(\widehat{\mathbf{X}}_i) | b_i + c_i = 0, i = 1, 2, \ldots, r\}$ are the $r-u$ conjugate pairs shared by E_1 and $\overline{E}_2$. $\{\mathcal{D}_{1-b_i}^{-1}(\mathbf{X}_i), \mathcal{D}_{c_i}^{-1}(\widehat{\mathbf{X}}_i) | b_i + c_i = 0, i = 1, 2, \ldots, r\}$ are the $r-u$ conjugate pairs shared by $\overline{E}_1$ and E_2.

□

Note 1. *In case 3 of theorem 4, the integer u can not be determined by r generally (see section 5). We need some other information to determine u. So when f is a linear function that contains an even number of terms, the adjacency graph of $FSR_{(x_0+x_1)*f}$ can not be determined just from the adjacency graph of FSR_f using the method above.*

The conclusion in theorem 4 can be shown by the graph below.



5 The Adjacency Graph of LFSRs with Characteristic Polynomial $(1+x)^4 p(x)$

Since $\phi(x_0 + x_1) = 1 + x$ and $\phi(f * g) = \phi(f)\phi(g)$, the conclusion in section 4 is meant to determine the adjacency graph of $\mathrm{FSR}_{(1+x)c(x)}$ from the adjacency graph of $\mathrm{FSR}_{c(x)}$, where $c(x) \in \mathbb{F}_2[x]$. As an application, we use the result in section 4 to determine the adjacency graph of LFSRs with characteristic polynomial $(1+x)^4 p(x)$, where $p(x)$ is a primitive polynomial over $\mathbb{F}_2(x)$.

As discussed in section 2.1, we can use an equivalent class in $G(f)$ to denote a cycle in FSR_f. Let $\mathbf{x} = (x_0 x_1 \ldots x_{l-1}) \in G(f)$ be a sequence with period l. Then $[\mathbf{x}]$ can be used to denote the cycle $C = (\mathbf{X}_0, \mathbf{X}_1, \ldots, \mathbf{X}_{l-1}) \in FSR_f$, where $\mathbf{X}_i = (x_i, x_{i+1}, \ldots, x_{i+n-1})$, for $i = 0, 1, \ldots, l-1$. The subscribes are taken modulo l. In this section, we always use an equivalent class to denote a cycle.

Lemma 7. *Let* $[\mathbf{a}]$ *and* $[\mathbf{b}]$ *be two cycles in* $FSR_{c_1(x)}$ *and* $FSR_{c_2(x)}$ *respectively. If* $gcd(c_1(x), c_2(x)) = 1$ *and* $gcd(p(\mathbf{a}), p(\mathbf{b})) = 1$, *then* $[\mathbf{a}+\mathbf{b}]$ *is a cycle in* $FSR_{c_1(x)c_2(x)}$ *and* $W([\mathbf{a}+\mathbf{b}]) \equiv p(\mathbf{a})W([\mathbf{b}]) + p(\mathbf{b})W([\mathbf{a}])\text{mod}2$.

Proof. According to lemma 1, $\mathbf{a}+\mathbf{b} \in G(c_1(x)c_2(x))$. So $[\mathbf{a}+\mathbf{b}] \in FSR_{c_1(x)c_2(x)}$.

Since $gcd(c_1(x), c_2(x)) = 1$, we have $p(\mathbf{a}+\mathbf{b}) = lcm(p(\mathbf{a}), p(\mathbf{b}))$. Considering that $gcd(p(\mathbf{a}), p(\mathbf{b})) = 1$, we get $p(\mathbf{a}+\mathbf{b}) = p(\mathbf{a})p(\mathbf{b})$. Let $\mathbf{a} = (a_0 a_1 \cdots a_{p-1})$ and $\mathbf{b} = (b_0 b_1 \cdots b_{q-1})$. Then $W([\mathbf{a}+\mathbf{b}]) \equiv \left(\sum_{i=0}^{p-1} a_i + p \cdot b_0\right) + \cdots + \left(\sum_{i=0}^{p-1} a_i + p \cdot b_{q-1}\right) \equiv q \cdot \sum_{i=0}^{p-1} a_i + p \cdot \sum_{j=0}^{q-1} b_j \equiv p(\mathbf{a})W([\mathbf{b}]) + p(\mathbf{b})W([\mathbf{a}])\text{mod}2$. □

Lemma 8. *Let* $[\mathbf{a}]$ *be a cycle in* $FSR_{(1+x)^m}$, *where* m *is a positive integer. Let* $[\mathbf{s}]$ *be a cycle in* $FSR_{p(x)}$, *where* $p(x)$ *is a primitive polynomial and* s *is a* m*-sequence. Then* $\mathcal{D}^{-1}([\mathbf{a}+\mathbf{s}]) \subset FSR_{(1+x)^{m+1}p(x)}$ *and*

1. *If* $W([\mathbf{a}])$ *is odd,* $\mathcal{D}^{-1}([\mathbf{a}+\mathbf{s}]) = \{[\mathbf{b}+\mathbf{s}]\}$, *where* $[\mathbf{b}]$ *is the cycle in* $\mathcal{D}^{-1}([\mathbf{a}])$.
2. *If* $W([\mathbf{a}])$ *is even,* $\mathcal{D}^{-1}([\mathbf{a}+\mathbf{s}]) = \{[\mathbf{c}+\mathbf{s}], [\bar{\mathbf{c}}+\mathbf{s}]\}$, *where* $[\mathbf{c}]$ *and* $[\bar{\mathbf{c}}]$ *are the two cycles in* $\mathcal{D}^{-1}([\mathbf{a}])$.

Proof. Since $\mathbf{a} \in G((1+x)^m)$ and $\mathbf{s} \in G(p(x))$, we get $\mathbf{a}+\mathbf{s} \in G((1+x)^m p(x))$. So $[\mathbf{a}+\mathbf{s}] \in FSR_{(1+x)^m p(x)}$ and $\mathcal{D}^{-1}([\mathbf{a}+\mathbf{s}]) \subset FSR_{(1+x)^{m+1}p(x)}$.

Let t be the integer such that $2^{t-1} < m \leq 2^t$. Then the period of $(1+x)^m$ is 2^t. From the theory of LFSRs we know, $p(\mathbf{a})|2^t$. Let n be the degree of $p(x)$. Then $p(\mathbf{s}) = 2^n - 1$. By $gcd(2^t, 2^n - 1) = 1$ we know $gcd(p(\mathbf{a}), p(\mathbf{s})) = 1$. According to lemma 7, $W([\mathbf{a}+\mathbf{s}]) \equiv p(\mathbf{a})W([\mathbf{s}]) + p(\mathbf{s})W([\mathbf{a}])\text{mod}2$. It is easy to see, the parity of $W([\mathbf{a}+\mathbf{s}])$ is the same as that of $W([\mathbf{a}])$.

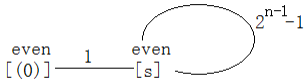
If $W([\mathbf{a}])$ is odd, then $W([\mathbf{a}+\mathbf{s}])$ is odd. There is only one cycle in $\mathcal{D}^{-1}([\mathbf{a}+\mathbf{s}])$. So we just need to check that $\mathcal{D}([\mathbf{b}+\mathbf{s}]) = [\mathbf{a}+\mathbf{s}]$. From $\mathcal{D}([\mathbf{b}]) = [\mathbf{b}+L(\mathbf{b})] = [\mathbf{a}]$ we know, $\mathbf{b}+L(\mathbf{b}) = L^u(\mathbf{a})$ for some integer u. According to lemma 2, $\mathbf{s}+L(\mathbf{s}) = L^v(\mathbf{s})$ for some integer v. From $p(\mathbf{a}+\mathbf{s}) = p(\mathbf{a})p(\mathbf{s})$ we know, $[L^u(\mathbf{a})+L^v(\mathbf{s})] = [\mathbf{a}+\mathbf{s}]$. Then the proof can be done as follows: $D([\mathbf{b}+\mathbf{s}]) = [\mathbf{b}+\mathbf{s}+L(\mathbf{b}+\mathbf{s})) = [\mathbf{b}+L(\mathbf{b})+\mathbf{s}+L(\mathbf{s})] = [L^u(\mathbf{a})+L^v(\mathbf{s})] = [\mathbf{a}+\mathbf{s}]$.

For the case $W([\mathbf{a}])$ is even, the proof is similar. □

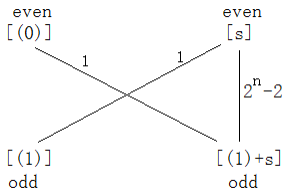
The adjacency graph of $\text{FSR}_{(1+x)^m p(x)}$, $m = 1, 2, 3$ were determined by [4], [11] and [2]. But there are no results for $m \geq 4$. Next, we use our method to determine the adjacency graph of $\text{FSR}_{(1+x)^m p(x)}$ for $m = 1, 2, 3, 4$ step by step. Some results for $m > 4$ are derived in section 6.

The cycles in $\text{FSR}_{(1+x)^m p(x)}$ can be determined from the cycles in $\text{FSR}_{(1+x)^{m-1} p(x)}$ according to lemma 8. The parity of the weight of cycles in $\text{FSR}_{(1+x)^m p(x)}$ can be determined from the parity of the weight of cycles in $\text{FSR}_{(1+x)^{m-1} p(x)}$ according to lemma 7. The adjacency graph of $\text{FSR}_{(1+x)^m p(x)}$ can be determined from the adjacency graph of $\text{FSR}_{(1+x)^{m-1} p(x)}$ according to theorem 5 and theorem 6. If the case 3 in theorem 6 is encountered, we need some other skills to determine the parameter u, otherwise, the adjacency graph can be determined directly.

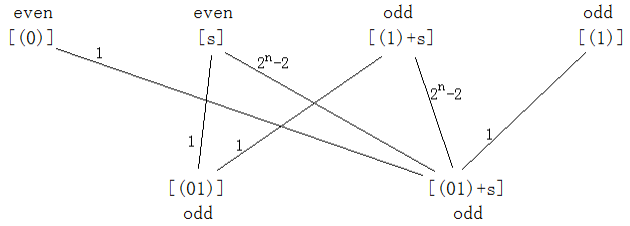
Let $p(x)$ be a primitive polynomial of degree n. Let $\mathbf{s} \in G(p(x))$ be a m-sequence. Then $\text{FSR}_{p(x)} = \{[(0)], [\mathbf{s}]\}$. The adjacency graph of $\text{FSR}_{p(x)}$ can be determined easily.



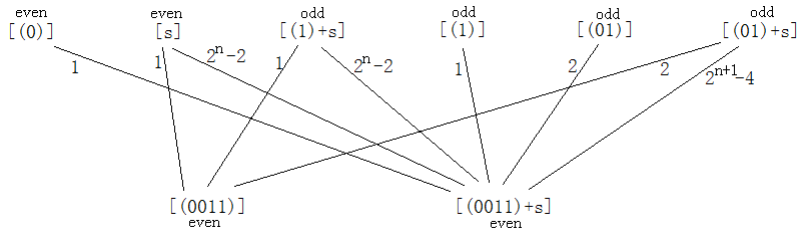
It is obvious that, $[(0)]$ and $[\mathbf{s}]$ are both cycles of even weight. By calculation, $\mathcal{D}^{-1}([(0)]) = \{[(0)], [(1)]\}$. According to lemma 8, $\mathcal{D}^{-1}([\mathbf{s}]) = \mathcal{D}^{-1}([(0)+\mathbf{s}]) = \{[\mathbf{s}], [(1)+\mathbf{s}]\}$. So $\text{FSR}_{(1+x)p(x)} = \mathcal{D}^{-1}([(0)]) \cup \mathcal{D}^{-1}([\mathbf{s}]) = \{[(0)], [(1)], [s], [(1)+s]\}$. According to theorem 5, the adjacency graph of $\text{FSR}_{(1+x)p(x)}$ can be determined.



Similarly, we get $\mathrm{FSR}_{(1+x)^2p(x)} = \{[(0)], [(01)], [(1)], [\mathbf{s}], [(01)+\mathbf{s}], [(1)+\mathbf{s}]\}$. According to theorem 6, the adjacency graph of $\mathrm{FSR}_{(1+x)^2p(x)}$ can be determined.

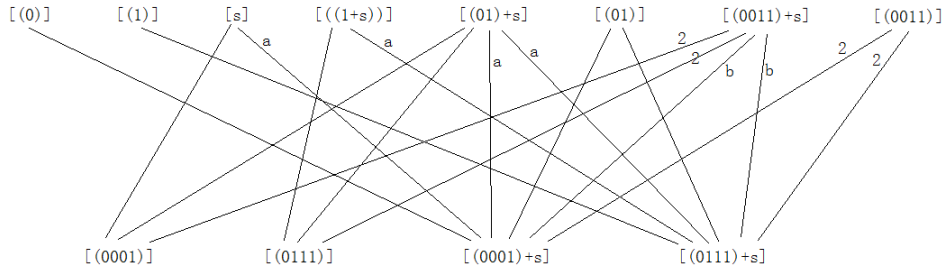


$\mathrm{FSR}_{(1+x)^3p(x)} = \{[(0)], [(0011)], [(01)], [(1)], [\mathbf{s}], [(0011)+\mathbf{s}], [(01)+\mathbf{s}], [(1)+\mathbf{s}]\}$. According to theorem 6, the adjacency graph of $\mathrm{FSR}_{(1+x)^3p(x)}$ can be determined.

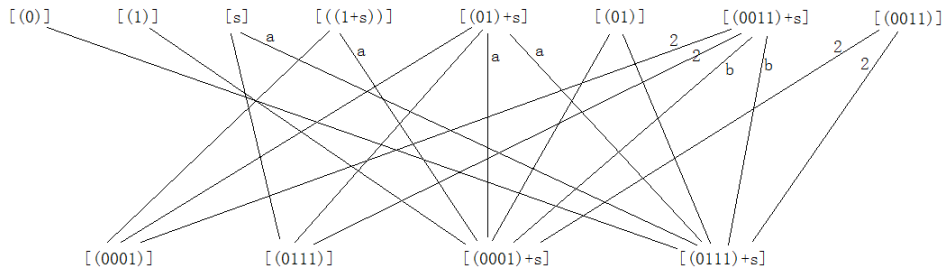


For $\mathrm{FSR}_{(1+x)^4p(x)}$, the cycles and the parity of the weight of cycles in $\mathrm{FSR}_{(1+x)^4p(x)}$ can be determined similarly. $\mathrm{FSR}_{(1+x)^4p(x)} = \{[(0)], [(0001)], [(0011)], [(01)], [(0111)], [(1)], [\mathbf{s}], [(0001)+\mathbf{s}], [(0011)+\mathbf{s}], [(01)+\mathbf{s}], [(0111)+\mathbf{s}], [(1)+\mathbf{s}]\}$. There are four cycles $[(0)]$, $[\mathbf{s}]$, $[(0011)]$ and $[(0011)+\mathbf{s}]$ in $\mathrm{FSR}_{(1+x)^3p(x)}$ that are of weight. We have to deal with the parameter u in the case 3 of theorem 6. Since $\mathcal{D}^{-1}([(0)]) = \{[(0)], [(1)]\}$, $\mathcal{D}^{-1}([\mathbf{s}]) = \{[\mathbf{s}], [(1)+\mathbf{s}]\}$, $\mathcal{D}^{-1}([(0011)]) = \{[(0001)], [(0111)]\}$, and $\mathcal{D}^{-1}([(0011)+\mathbf{s}]) = \{[(0001)+\mathbf{s}], [(0111)+\mathbf{s}]\}$, to determine the adjacency graph of $\mathrm{FSR}_{(1+x)^4p(x)}$, it suffices to determine the number of conjugate pairs shared by $[(0)]$ and $[(0001)+\mathbf{s}]$, $[\mathbf{s}]$ and $[(0001)]$, $[\mathbf{s}]$ and $[(0001)+\mathbf{s}]$. The method we use can be found in [3].

Theorem 7. *In the case* $[(0)]$ *is adjacent with* $[(0001)+\mathbf{s}]$*, the adjacency graph of* $FSR_{(1+x)^4p(x)}$ *is shown below*



In the case $[(0)]$ *is adjacent with* $[(0111)+\mathbf{s}]$*, the adjacency graph of* $FSR_{(1+x)^4p(x)}$ *is shown below*



where a and b denote the number 2^n-2 and $2^{n+1}-4$ respectively, and the number 1 is omitted.

Proof. In the case [(0)] is adjacent with $[(0001)+\mathbf{s}]$, since there is only one state in [(0)], [(0)] share 1 conjugate pair with $[(0001)+\mathbf{s}]$. Next, we consider the number of conjugate pairs shared by [**s**] and [(0001)], [**s**] and $[(0001)+\mathbf{s}]$. Since [(0)] is adjacent with $[(0001)+\mathbf{s}]$, the $(n+4)$-stage state $\mathbf{E}=(1,0,\cdots,0)$ belongs to $[(0001)+\mathbf{s}]$. Treat [(0001)] and [**s**] as $(n+4)$-stage cycles. There are two states $\mathbf{U}_0$ and $\mathbf{S}_0$ in [(0001)] and [**s**] respectively such that:

$$\mathbf{U}_0+\mathbf{S}_0=\mathbf{E}. \tag{2}$$

This implies $\mathbf{S}_0=\widehat{\mathbf{U}}_0$. So the conjugate of $\mathbf{S}_0$ belongs to [(0001)]. Denote $[(0001)]=(\mathbf{U}_0,\mathbf{U}_1,\mathbf{U}_2,\mathbf{U}_3)$ and $[\mathbf{s}]=(\mathbf{S}_0,\mathbf{S}_1,\ldots,\mathbf{S}_{2^n-2})$. Without lose of generality, let $\mathbf{s}=(s_0s_1\cdots s_{2^n-2})$, where s_i is the first component of $\mathbf{S}_i$ for $i=0,1,\cdots,2^n-2$. According to lemma 2, $\mathbf{s}+L^j(\mathbf{s})=L^{Z(j)}(\mathbf{s})$. So

$$\mathbf{S}_0+\mathbf{S}_j=\mathbf{S}_{Z(j)}. \tag{3}$$

Combine (2) and (3), we get

$$\mathbf{U}_0+\mathbf{S}_j=\widehat{\mathbf{S}}_{Z(j)}. \tag{4}$$

Considering that Z is a bijection on $\{1,2,\ldots,2^n-2\}$, equation 4 means the conjugate of $\mathbf{S}_j$ with $j\neq 0$ belongs to $[(0001)+\mathbf{s}]$. So [**s**] share 1 conjugate pair with [(0001)] and share 2^n-2 conjugate pairs with $[(0001)+\mathbf{s}]$.

For the case [(0)] is adjacent with $[(0111)+\mathbf{s}]$, the proof is similar. □

The following example shows the two cases in theorem 7 is both possible.

Example 1. *Let $p_1(x)=x^5+x^4+x^2+x+1$ be a primitive polynomial and $s_1=(0000111001101111101$ $000100101011)\in G(p_2(x))$ be a m-sequence. Then, $[(0001)+s_1]=[(\underline{1000000001}1110100001111101111$ $1101011001101000111000011011100111001010101101111010010100010101111100110000100100101100$ $01001101)]$. Let $p_2(x)=x^5+x^3+x^2+x+1$ be a primitive polynomial and $s_2=(0000101101010001110111$ $11110010011)\in G(p_1(x))$ be a m-sequence. Then, $[(0111)+s_2]=[(\underline{1000000001}0111110111100101101111$ $1110011000111001000111110000100110101010000101000101100001110101001100100100111011010110$ $10001)]$.*

6 Some Properties About LFSRs with Characteristic Polynomial $(1+x)^m p(x)$

Theorem 8. *Let k_m be the number of cycles in $FSR_{(1+x)^m p(x)}$, where $p(x)$ is a primitive polynomial. Let t be the integer such that $2^{t-1}<m\leq 2^t$. Then for $m\geq 2$ we have*

$$k_m=4+\sum_{i=1}^{t-1}\left(2^{2^i-i+1}-2^{2^{i-1}-i+1}\right)+2^{m-t+1}-2^{2^{t-1}-t+1}$$

Proof. The period of $(1+x)^m$ is 2^t. Let C_1 be a cycles in $FSR_{(1+x)^m}$, and C_2 be a cycles in $FSR_{p(x)}$. Denote the length of cycle C by $len(C)$. Then $len(C_1)|2^t$ and $len(C_2)|2^n-1$, where n is the degree of $p(x)$. By $gcd(2^t, 2^n-1)=1$, we know $gcd(len(C_1), len(C_2))=1$. Since $p(x)$ is a primitive polynomial, $gcd((1+x)^m, p(x))=1$ for any m. Let l_m be the number of cycles in $FSR_{(1+x)^m}$. Since there are two cycles in $FSR_{p(x)}$, we have $k_m = 2l_m$.

Consider the cycles in $FSR_{(1+x)^m} \backslash FSR_{(1+x)^{m-1}}$. They are all of length 2^t. So we get $l_m - l_{m-1} = \frac{2^m - 2^{m-1}}{2^t} = 2^{m-t-1}$. This implies $k_m - k_{m-1} = 2^{m-t}$. Use this equation and the fact $k_1 = 4$, we get

$$\begin{aligned}
k_n &= k_1 + (k_2 - k_1) + (k_3 - k_2) + \cdots + (k_m - k_{m-1}) \\
&= 4 + \frac{2^2}{2} + \frac{2^3 + 2^4}{2^2} + \cdots + \frac{2^{2^{t-2}+1} + \cdots + 2^{2^{t-1}}}{2^{t-1}} + \frac{2^{2^{t-1}+1} + \cdots + 2^m}{2^t} \\
&= 4 + \sum_{i=1}^{t-1} \left(\frac{2^{2^{i-1}+1} + \cdots + 2^{2^i}}{2^i} \right) + \frac{2^{2^{t-1}+1} + \cdots + 2^m}{2^t} \\
&= 4 + \sum_{i=1}^{t-1} \left(2^{2^i - i + 1} - 2^{2^{i-1} - i + 1} \right) + 2^{m-t+1} - 2^{2^{t-1} - t + 1}
\end{aligned}$$

□

It can be seen, the cycles in $FSR_{\phi^{-1}(p(x))+1}$, $FSR_{\phi^{-1}((1+x)p(x))+1}$ and $FSR_{\phi^{-1}((1+x^3)p(x))+1}$ are all of odd weight. Generally, we have the following theorem.

Theorem 9. *The cycles in $FSR_{\phi^{-1}((1+x)^{m-1}p(x))+1}$ are all of odd weight if and only if $m = 2^t$ for some integer t.*

Proof. Let k_m be the number of cycles in $FSR_{(1+x)^m p(x)}$. Let t and t' be integers such that $2^{t-1} < m \leq 2^t$ and $2^{t'-1} < m+1 \leq 2^{t'}$. From the proof of theorem 8 we know, $k_m - k_{m-1} = 2^{m-t}$ and $k_{m+1} - k_m = 2^{m+1-t'}$. This implies there are 2^{m-t} and $2^{m+1-t'}$ cycles of even weight in $FSR_{(1+x)^{m-1}p(x)}$ and $FSR_{(1+x)^m p(x)}$ respectively. Since $FSR_{(1+x)^m p(x)}$ consists of cycles in $FSR_{(1+x)^{m-1}p(x)}$ and $FSR_{\phi^{-1}((1+x)^{m-1}p(x))+1}$, the cycles in $FSR_{\phi^{-1}((1+x)^{m-1}p(x))+1}$ are all of odd weight if and only if $FSR_{(1+x)^m p(x)}$ and $FSR_{(1+x)^{m-1}p(x)}$ have the same number of even weight cycles. That is $t' = t+1$. It is easy to see, $t = t'$ if and only if $m = 2^t$. □

By this theorem, the adjacency graph of $FSR_{(1+x)^{2^t+1}p(x)}$ can be determined directly from the adjacency graph of $FSR_{(1+x)^{2^t}p(x)}$ without bothered by the parameter u in theorem 6. Especially, the adjacency graph of $FSR_{(1+x)^5 p(x)}$ can be determined directly from the adjacency graph of $FSR_{(1+x)^4 p(x)}$. Due to the complexity, we do not present it here.

7 Conclusion

A recursive relation between the adjacency graph of FSRf and FSR$_{(x_0+x_1)*f}$ is discussed, where f is a linear boolean function. As an application, the adjacency graph of LFSRs with characteristic polynomial $(1+x)^4 p(x)$ are determined, where $p(x)$ is a primitive polynomial.

References

[1] Abraham Lempel, On a Homomorphism of the de Bruijn Graph and Its Applications to the Design of Feedback Shift Registers. IEEE Transactions on computer. December 1970.

[2] Chaoyun Li, Xiangyong Zeng, Tor Helleseth, Chunlei Li, Lei Hu, The Properties of a Class of Linear FSRs and Their Applications to the Construction of Nonlinear FSRs. IEEE Transactions on Information Theory. May 2014.

[3] Chaoyun Li, Xiangyong Zeng, Chunlei Li, Tor Helleseth, A Class of De Bruijn Sequences. IEEE Transactions on Information Theory. 2014.

[4] Johannes Mykkeltveit, On the Cycle Structure of Some Nonlinear Shift Register Sequences. Information and Control. 1979.

[5] Ming Li and Dongdai Lin, A Class of FSRs and Their Adjacency Graphs. IACR Cryptology ePrint Archive 2014.

[6] Solomon W. Golomb, Shift Register Sequences. San Francisco, Calif. Holden-Day, 1967.

[7] Tian Tian and Wenfeng Qi, On decomposition of an NFSR into a cascade connection of two smaller NFSRs. Submitted to Applicable Algebra in Engineering, Communication and Computing. 2014.

[8] Martin Hell, Thomas Johansson, Alexander Maximov and Willi Meier, The Grain Family of Stream Ciphers. New Stream Cipher Designs. 2008

[9] K. B. Magleby, The synthesis of nonlinear feedback shift registers. Stanford Electron. 1963.

[10] E. R. Hauge and J. Mykkeltveit, On the classification of deBruijn sequences. Discrete Math. Jan. 1996.

[11] F.Hemmati, A large class of nonlinear shift register sequences. IEEE Transactions on Information Theory. Mar 1982.

[12] Rudolf Lidl, Finite fields. Cambridge university press. 1997.

[13] Eric J, Van Lantschoot, Double adjacencies between cycles of a circulating shift register. IEEE transactions on computers. Oct 1973.

[14] Johannes Mykkeltveit, Generating and counting the double adjacencies in a pure circulating shift register. IEEE transactions on computers. Mar 1975.

[15] Farhad Hemmati, Donald L. Schilling, George Eichmann. Adjacencies between the cycles of a shift register with characteristic polynomial $(1 + x)^n$. IEEE transactions on computers. July 1984.

[16] Erik R. Hauge, On the cycles and adjacencies in the complementary circulating register. Discrete Mathematics. 145 1995.

[17] N. Zierler, Linear recurring sequences. J. Soc. Indust. Appl. Math, Mar. 1959.