The Adjacency Graph of Some LFSRs

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

September 2, 2014

Abstract

In this paper, we discuss the adjacency graph of feedback shift registers (FSRs) whose characteristic polynomial can be written as $g = (x_0 + x_1) * f$ for some linear function f. For f contains an odd number of terms, we present a method to calculate the adjacency graph of $\mathrm{FSR}_{(x_0+x_1)*f}$ from the adjacency graph of FSR_f. The parity of the weight of cycles in $\mathrm{FSR}_{(x_0+x_1)*f}$ can also be determined easily. For f contains an even number of terms, the theory is not so much complete. We need more information than the adjacency graph of FSR_f to determine the adjacency graph of $\mathrm{FSR}_{(x_0+x_1)*f}$. Besides, some properties about the cycle structure of linear feedback shift registers (LFSR) are presented.

1 Introduction

Feedback shift registers (FSRs) have been used and studied for many years [5]. Especially in cryptography, FSRs are the basic component in stream cipher [7]. 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 with large period output sequences. 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 [5]. 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].

In this paper, the 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. Since $(x_0+x_1)*f = f*(x_0+x_1)$ for linear function f, $\mathrm{FSR}_{(x_0+x_1)*f}$ is not only self-dual but also dividable according to [1] and [4]. Furthermore, $\mathrm{FSR}_{(x_0+x_1)*f}$ can be constructed from FSR_f by two different ways. So there is a relation between the adjacency graphs of $\mathrm{FSR}_{(x_0+x_1)*f}$ and FSR_f. For f contains an odd number of terms, the adjacency graph of $\mathrm{FSR}_{(x_0+x_1)*f}$ can be determined easily from the adjacency graph of FSR_f. For f contains an even number of terms, the theory is not so much complete. We need more information than the adjacency graph of FSR_f to determine the adjacency graph of $\mathrm{FSR}_{(x_0+x_1)*f}$.

This paper is organized as follows. In section 2, we present the basic knowledge about feedback shift registers, self-dual FSRs and dividable FSRs, and explain some notation that we will use in this paper. In section 3, the relation between the adjacency graph of $\mathrm{FSR}_{(x_0+x_1)*f}$ and FSR_f are discussed. Our discussion is divided into two cases according to the parity of the number of terms in f. At the end, we conclude this paper.

2 Preliminaries

The purpose of this section is to briefly review feedback shift registers, self-dual FSRs and dividable FSRs, and explain some notations that we will use in this paper.

2.1 Feedback shift registers

Let $\mathbb{F}_2$ be the finite field of two-element, and $\mathbb{F}_2^n$ be the vector space of dimension n over $\mathbb{F}_2$. A boolean function (or boolean polynomial) $f(x_0, x_1, \ldots, x_{n-1})$ in n variables is a map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.

An n-stage feedback shift register (FSR) consists of n binary storage cells and a characteristic polynomial f regulated by a single clock. We denote the FSR with characteristic polynomial f by FSR_f. Given a initial state $\mathbf{X}_0 = (x_0, x_1, \ldots, x_{n-1})$, FSR_f will output a sequence $\underline{x} = x_0x_1\cdots$. It is well known that, FSR_f always output the periodic sequences no matter what the initial state is, if and only if 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 is nonsingular.

For n-stage FSR_f, when start from a initial state $\mathbf{X}_0$, FSR_f will generate a cycle $C = (\mathbf{X}_0, \mathbf{X}_1, \ldots, \mathbf{X}_l)$, where $\mathbf{X}_{i+1}$ is the next state of $\mathbf{X}_i$ for $i = 1, 2, \ldots, l-1$ and $\mathbf{X}_0$ is the next state of $\mathbf{X}_l$, l is the length of the cycle. Define **the weight of cycle** C as $W(C) = \sum_{i=1}^{l} x_i$, where x_i is the first component of $\mathbf{X}_i$. Cycle C can be seen as an ordered set with element in $\mathbb{F}_2^n$. Sometimes, we do not discriminate between cycle $C = (\mathbf{X}_0, \mathbf{X}_1, \ldots, \mathbf{X}_l)$ and the set $\{\mathbf{X}_0, \mathbf{X}_1, \ldots, \mathbf{X}_l\}$.

From the above discussion, the set $\mathbb{F}_2^n$ is divided into cycles $C_1, C_2, \ldots, C_k$ by FSR_f. Reversely, it is easy to see, a division of $\mathbb{F}_2^n$ into cycles determines a n-stage FSR. So we can treat FSR_f as a set of cycles, and use the notation $\text{FSR}_f = \{C_1, C_2, \ldots, C_k\}$. An FSR is called a linear feedback shift register (LFSR) if its feedback function f is linear and nonlinear feedback shift register (NFSR) otherwise.

For an n-stage 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 $C = (\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_l)$, $\overline{C}$ is defined as $\overline{C} = (\overline{\mathbf{X}}_1, \overline{\mathbf{X}}_2, \ldots, \overline{\mathbf{X}}_l)$. C is called a **primitive cycle** if $\overline{C} = C$ or $\overline{C} \cap C = \emptyset$. Two cycles C_1 and C_2 are **adjacent** if they are disjoint and there exists a state $\mathbf{X}$ on C_1 whose conjugate $\widehat{\mathbf{X}}$ (or companion $\widetilde{\mathbf{X}}$) is on 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 [5].

The problem of determining the number of conjugate pairs between cycles leads to the definition of adjacency graph.

Definition 1. *[9][8] 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 Self-dual FSRs and dividable FSRs

In [1], $\mathcal{D}$-morphism was proposed to construct FSRs. The constructed FSRs are just the self-dual FSRs (defined below).

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

$\mathcal{D}$-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 a n-stage cycle. Let $S = \{\mathbf{X} | \mathcal{D}(\mathbf{X}) \in C\}$. It can be verified, for any state $\mathbf{X} \in S$ there is one and only one state $\mathbf{Y}$ in S can be the successor of $\mathbf{X}$. Define $\mathbf{X} \to \mathbf{Y}$, the states in S form cycles. Denote the set of these cycles by $\mathcal{D}^{-1}(C)$. If $W(C)$ is odd, then there is only one cycle in $\mathcal{D}^{-1}(C)$. Write $\mathcal{D}^{-1}(C) = \{E\}$, we have $\overline{E} = E$. If $W(C)$ is even, then there are two cycles in $\mathcal{D}^{-1}(C)$. Write $\mathcal{D}^{-1}(C) = \{E, E'\}$, we have $\overline{E} = E'$.

Lemma 1. *[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, whose characteristic polynomial is $f * (x_0 + x_1)$.

Definition 2. *[1] FSR_g is called self-dual if FSR_g contains only primitive cycles.*

Lemma 2. *[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.

Lemma 3. *[4] Let $FSR_f = \{C_1, C_2, \ldots, C_k\}$ and $FSR_{f+1} = \{D_1, D_2, \ldots, D_t\}$ be two FSRs, then*

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

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

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. *[4] An FSR is called dividable if we can divide the vertexes in the adjacency graph of the FSR into two sets, such that the edges are all between the two sets.*

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

Since the operation $*$ is not commutative, $(x_0 + x_1) * f \neq f * (x_0 + x_1)$ generally. But when f is a linear boolean function, we have $(x_0 + x_1) * f = f * (x_0 + x_1)$. So in the linear case, combine the conclusions in [1] and [4], we get

Lemma 5. *[4] Let f be a linear boolean function. Then $FSR(x_0 + x_1) * f$ is not only self-dual but also dividable. Write $FSR_f = \{C_1, C_2, \ldots, C_k\}$ and $FSR_{f+1} = \{D_1, D_2, \ldots, D_t\}$. We have*

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

3 The adjacency graph of $\mathbf{FSR}_{(x_0+x_1)*f}$

In this section, we consider the adjacency graph of $\mathrm{FSR}_{(x_0+x_1)*f}$, where f is a linear boolean function. Our discussion can be divided into two cases.

3.1 The case that f contains an odd number of terms

First, we present a proposition about the weight of cycles in FSR_f, where f contains an odd number of terms.

Theorem 1. *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. □

Let C be a cycle in FSR_f. From the theorem above, we know C is a cycle of even weight. So there are two cycles in $\mathcal{D}^{-1}(C)$, write as $\mathcal{D}^{-1}(C) = \{E, \overline{E}\}$. It is obvious that, 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 $f(\mathbf{X}) \neq f(\overline{\mathbf{X}})$. This means when E is the extension of some cycle in FSR_f (FSR_{f+1}), $\overline{E}$ is the extension of some cycle in FSR_{f+1} (FSR_f).

Theorem 2. *Let f be a linear boolean function that contains an odd number of terms.*

1. *Let $C \in \mathrm{FSR}_f$. Write $\mathcal{D}^{-1}(C) = \{E, \overline{E}\}$. Suppose C contains r conjugate pairs. Then E and $\overline{E}$ share $2r$ conjugate pairs.*
2. *Let $C_1, C_2 \in \mathrm{FSR}_f$. Write $\mathcal{D}^{-1}(C_1) = \{E_1, \overline{E_1}\}$ and $\mathcal{D}^{-1}(C_2) = \{E_2, \overline{E}_2\}$, where E_1, E_2 are the extension of some two cycles in FSR_f, and $\overline{E}_1, \overline{E}_2$ are the extension of some two cycles 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 all share r conjugate pairs. And there are no conjugate pairs shared by E_1 and E_2, $\overline{E}_1$ and $\overline{E}_2$.*

Proof. **For 1**. Let $(\mathbf{X}, \widehat{\mathbf{X}})$ be a conjugate pair shared by E and $\overline{E}$. Without lose of generality, suppose $\mathbf{X} \in E$ and $\widehat{\mathbf{X}} \in \overline{E}$. Then $\mathcal{D}(\mathbf{X})$ and $\mathcal{D}(\widehat{\mathbf{X}})$ are both in C, and $(\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$ is a conjugate pair in C. Define a map φ from the conjugate pairs shared by E and $\overline{E}$ to the conjugate pairs in C as: $\varphi((\mathbf{X}, \widehat{\mathbf{X}})) = (\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$. We show that ψ is a two-to-one map.

Since $\mathbf{X} \in E$ and $\widehat{\mathbf{X}} \in \overline{E}$, we have $\overline{\mathbf{X}} \in \overline{E}$ and $\overline{\widehat{\mathbf{X}}} \in E$. So $(\overline{\mathbf{X}}, \overline{\widehat{\mathbf{X}}})$ is a conjugate pair shared by E and $\overline{E}$. It is obvious that $\varphi((\mathbf{X}, \widehat{\mathbf{X}})) = \varphi((\overline{\mathbf{X}}, \overline{\widehat{\mathbf{X}}}))$. Furthermore, suppose $(\mathbf{X}_1, \widehat{\mathbf{X}}_1)$ is a conjugate pair shared by E and $\overline{E}$ such that $\varphi((\mathbf{X}_1, \widehat{\mathbf{X}}_1)) = \varphi((\mathbf{X}, \widehat{\mathbf{X}}))$. Without lose of generality, suppose $\mathbf{X}_1 \in E$ and $\widehat{\mathbf{X}}_1 \in \overline{E}$. Then $(\mathcal{D}(\mathbf{X}_1), \mathcal{D}(\widehat{\mathbf{X}}_1)) = (\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$ (**this equation means they are the same conjugate pair**) implies $\mathbf{X}_1 = \mathbf{X}$ or $\mathbf{X}_1 = \overline{\widehat{\mathbf{X}}}$. So we get $(\mathbf{X}_1, \widehat{\mathbf{X}}_1) = (\mathbf{X}, \widehat{\mathbf{X}})$ or $(\mathbf{X}_1, \widehat{\mathbf{X}}_1) = (\overline{\mathbf{X}}, \overline{\widehat{\mathbf{X}}})$.

Let $(\mathbf{Y}, \widehat{\mathbf{Y}})$ be a conjugate pair in C. Consider the four states: $\mathcal{D}_0^{-1}(\mathbf{Y})$, $\mathcal{D}_1^{-1}(\mathbf{Y})$, $\mathcal{D}_0^{-1}(\widehat{\mathbf{Y}})$ and $\mathcal{D}_1^{-1}(\widehat{\mathbf{Y}})$. Without lose of generality, suppose $\mathcal{D}_0^{-1}(\mathbf{Y}) \in E$. Then $\mathcal{D}_1^{-1}(\mathbf{Y}) \in \overline{E}$. Since $(\mathcal{D}_0^{-1}(\mathbf{Y}), \mathcal{D}_1^{-1}(\widehat{\mathbf{Y}}))$ is a conjugate pair, and E is a prime cycle. We get $\mathcal{D}_1^{-1}(\widehat{\mathbf{Y}}) \in \overline{E}$. As the dual of $\mathcal{D}_1^{-1}(\widehat{\mathbf{Y}})$, $\mathcal{D}_0^{-1}(\widehat{\mathbf{Y}})$ belong to E. So $(\mathcal{D}_0^{-1}(\mathbf{Y}), \mathcal{D}_1^{-1}(\widehat{\mathbf{Y}}))$ and $(\mathcal{D}_0^{-1}(\widehat{\mathbf{Y}}), \mathcal{D}_1^{-1}(\mathbf{Y}))$ are two conjugate pairs shared by E and $\overline{E}$. Furthermore, we have $\varphi((\mathcal{D}_0^{-1}(\mathbf{Y}), \mathcal{D}_1^{-1}(\widehat{\mathbf{Y}}))) = \varphi((\mathcal{D}_0^{-1}(\widehat{\mathbf{Y}}), \mathcal{D}_1^{-1}(\mathbf{Y}))) = (\mathbf{Y}, \widehat{\mathbf{Y}})$. So ψ is a two-to-one map.

For 2. It is easy to see, there are no conjugate pairs shared by E_1 and E_2, $\overline{E}_1$ and $\overline{E}_2$.

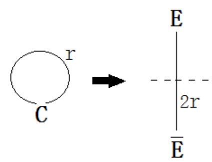
Next, we consider the conjugate pairs shared by E_1 and $\overline{E}_2$ (for conjugate pairs shard by $\overline{E}_1$ and E_2, the discussion is similar).

Let $(\mathbf{X}, \widehat{\mathbf{X}})$ be a conjugate pair shared by E_1 and $\overline{E}_2$. Without lose of generality, suppose $\mathbf{X} \in E_1$ and $\widehat{\mathbf{X}} \in \overline{E}_2$. Then $\mathcal{D}(\mathbf{X}) \in C_1$, $\mathcal{D}(\widehat{\mathbf{X}}) \in C_2$ and $(\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$ is a conjugate pair shared by C_1 and C_2. Define a map φ from the conjugate pairs shared by E_1 and $\overline{E}_2$ to the conjugate pairs shared by C_1 and C_2 as: $\varphi((\mathbf{X}, \widehat{\mathbf{X}})) = (\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$. We show that φ is a bijection.

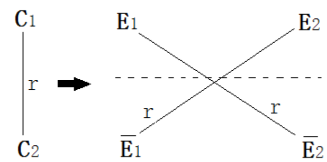
Suppose $(\mathbf{X}_1, \widehat{\mathbf{X}}_1)$ is a conjugate pair shared by E_1 and $\overline{E}_2$ such that $\varphi((\mathbf{X}_1, \widehat{\mathbf{X}}_1)) = (\mathbf{X}, \widehat{\mathbf{X}})$. Without lose of generality, suppose $\mathbf{X}_1 \in E_1$ and $\widehat{\mathbf{X}}_1 \in \overline{E}_2$. Then $(\mathcal{D}(\mathbf{X}_1), \mathcal{D}(\widehat{\mathbf{X}}_1)) = (\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$ implies $\mathbf{X}_1 = \mathbf{X}$. So we get $(\mathbf{X}_1, \widehat{\mathbf{X}}_1) = (\mathbf{X}, \widehat{\mathbf{X}})$.

Let $(\mathbf{Y}, \widehat{\mathbf{Y}})$ be a conjugate pair shared by C_1 and C_2. Consider the four states: $\mathcal{D}_0^{-1}(\mathbf{Y})$, $\mathcal{D}_1^{-1}(\mathbf{Y})$, $\mathcal{D}_0^{-1}(\widehat{\mathbf{Y}})$ and $\mathcal{D}_1^{-1}(\widehat{\mathbf{Y}})$. It is easy to see, one of $\mathcal{D}_0^{-1}(\mathbf{Y})$ and $\mathcal{D}_1^{-1}(\mathbf{Y})$ belongs to E_1, and one of $\mathcal{D}_0^{-1}(\widehat{\mathbf{Y}})$ and $\mathcal{D}_1^{-1}(\widehat{\mathbf{Y}})$ belongs to $\overline{E}_2$. Without lose of generality, suppose $\mathcal{D}_0^{-1}(\mathbf{Y}) \in E_1$. Since $(\mathcal{D}_0^{-1}(\mathbf{Y}), \mathcal{D}_1^{-1}(\widehat{\mathbf{Y}}))$ is a conjugate pair and there are no conjugate pairs shard by E_1 and E_2, we get $\mathcal{D}_1^{-1}(\widehat{\mathbf{Y}})$ belongs to $\overline{E}_2$. So $(\mathcal{D}_0^{-1}(\mathbf{Y}), \mathcal{D}_1^{-1}(\widehat{\mathbf{Y}}))$ is a conjugate pair shared by E_1 and $\overline{E}_2$. It is obvious that $\varphi((\mathcal{D}_0^{-1}(\mathbf{Y}), \mathcal{D}_1^{-1}(\widehat{\mathbf{Y}}))) = (\mathbf{Y}, \widehat{\mathbf{Y}})$. So φ is a bijection. $\square$

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

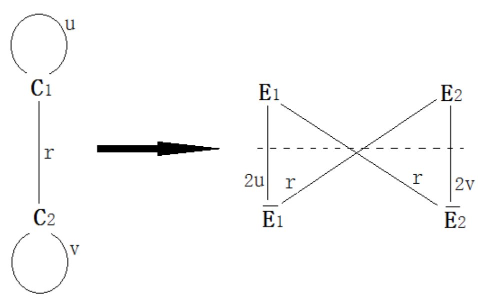


Case 1



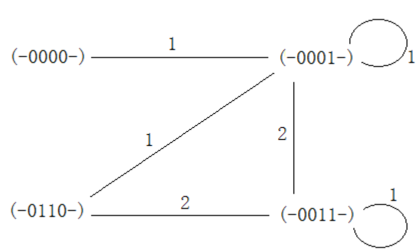
Case 2

Combine the two cases, we get



With this tool, the adjacency graph of $\mathrm{FSR}_{(x_0+x_1)*f}$ can be determined from the adjacency graph of FSR_f, providing that f contains an odd number of terms. In order to express cycles briefly, we introduce a notation for cycles. Let f be a boolean function. We denote a cycle $C \in \mathrm{FSR}_f$ as $C = (-\mathbf{X}-)_f$, where $\mathbf{X}$ is a state in C. Since there is only one cycle in FSR_f that contains $\mathbf{X}$, there is no ambiguity for this notation. The function f in this notation can be omitted, providing there is no confusion.

Example 1. *Let $f = x_0 + x_2 + x_4$. The four cycles in FSR_f can be written as $C_1 = (-0000-)_f$, $C_2 = (-0001-)_f$, $C_3 = (-0011-)_f$ and $C_4 = (-0110-)_f$. The adjacency graph of FSR_f is shown below.*

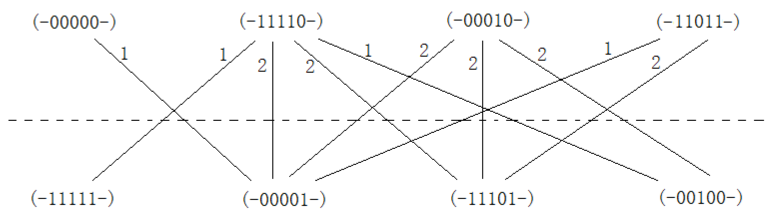


Define g as $g = (x_0 + x_1) * f = x_0 + x_1 + x_2 + x_3 + x_4 + x_5$. Since $\mathcal{D}_0^{-1}((0000)) = (00000)$ and $\mathcal{D}_1^{-1}((0000)) = (11111)$, we get $D^{-1}((-0000-)_f) = \{(-00000-)_g, (-11111-)_g\}$. By $f(00000) = 0$, we *know $(-00000-)_g$ is the extension of some cycle in FSR_f (see the note for lemma 3). By $f(11111) = 1$, we know $(-11111-)_g$ is the extension of some cycle in FSR_{f+1}. In this way, we get all the cycles in FSR_g, and divide them into two set:*

$$\mathcal{A} = \{E_1 = (-00000-)_g, E_2 = (-11110-)_g, E_3 = (-00010-)_g, E_4 = (-11011-)_g\}$$

$$\mathcal{B} = \{\overline{E}_1 = (-11111-)_g, \overline{E}_2 = (-00001-)_g, \overline{E}_3 = (-11101-)_g, \overline{E}_4 = (-00100-)_g\}.$$

where $\mathcal{A}$ contains the cycles that are of extension of some cycles in FSR_f, and $\mathcal{B}$ contains the cycles that are of extension of some cycles in FSR_{f+1}. Then, the adjacency of FSR_g can be determined according to theorem 2:



Next, we consider the weight of cycles in $\mathrm{FSR}_{(x_0+x_1)*f}$, where f is a linear boolean function that contains an odd number of terms. Let C be a cycle in $\mathrm{FSR}_{(x_0+x_1)*f}$ of length l. Write $C = (-\mathbf{X}-)_f$. If $f(\mathbf{X}) = 0$, then C is the extension of some cycle in FSR_f. Because the cycles in FSR_f are all of even weight and $W(D) = W(D^+)$ for any cycle D, we get that C is a cycle of even weight. If $f(\mathbf{X}) = 1$, then $f(\overline{\mathbf{X}}) = 0$. So $\overline{C} = (-\overline{\mathbf{X}}-)_f$ is a cycle of even weight. Since $W(C) \equiv W(\overline{C}) + l \bmod 2$, C is a cycle of even (odd) weight if and only if l is even (odd). In this way, the parity of the weight of cycles in $\mathrm{FSR}_{(x_0+x_1)*f}$ can be determined easily.

Example 2. *Continue the discussion in example 1. Since $(-00000-)_g, (-11110-)_g, (-00010-)_g$ and $(-11011-)_g$ are the extension of some cycles in FSR_f, they are all of even weight. Because $(-00001-)_g$ is a cycle of length 6 and $\overline{(-00001-)_g} = (-11110-)_g$ is a cycle of even weight, $(-00001-)_g$ is a cycle of even weight. Similarly, $(-11101-)_g$ is a cycle of even weight. $(-11111-)_g$ and $(-00100-)_g$ are cycles of odd weight.*

3.2 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.

Theorem 3. *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. It can be seen from lemma 5, the number of cycles in FSR_{f+1} is the same as the number of even weight cycles in FSR_f [4]. 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}. □

Let C be a cycle in FSR_f of even weight. Then there are two cycles in $\mathcal{D}^{-1}(C)$, denote 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, $f(\mathbf{X}) = f(\mathbf{X})$. 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 4. *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. Write $D^{-1}(C_1) = \{E_1\}$ 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. Write $D^{-1}(C_1) = \{E_1\}$ 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 $\overline{E}_2$ all share r conjugate pairs. And there are no conjugate pairs shared by E_2 and $\overline{E}_2$.*

3. *Let $C_1, C_2 \in \mathrm{FSR}_f$ be two cycles of even weight. Write $D^{-1}(C_1) = \{E_1, \overline{E}_1\}$ and $D^{-1}(C_2) = \{E_2, \overline{E}_2\}$. Suppose C_1 and C_2 share r conjugate pairs. Then we can find an integer u with $0 \le u \le r$ such that: E_1 and E_2, $\overline{E}_1$ and $\overline{E}_2$ all share u conjugate pairs; E_1 and $\overline{E}_2$, $\overline{E}_1$ and E_2 all share $r-u$ conjugate pairs. And there are no conjugate pairs shared by E_1 and $\overline{E}_1$, E_2 and $\overline{E}_2$.*

Proof. **For 1**. Let $(\mathbf{X}, \widehat{\mathbf{X}})$ be a conjugate pair shared by E_1 and E_2, it is easy to see $(\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$ is a conjugate pair shared by C_1 and C_2. Define a map φ from the conjugate pairs shared by E_1 and E_2 to the conjugate pairs shared by C_1 and C_2 as: $\varphi((\mathbf{X}, \widehat{\mathbf{X}})) = (\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$. We show that ψ is a two-to-one map.

Without lose of generality, suppose $\mathbf{X} \in E_1$ and $\widehat{\mathbf{X}} \in E_2$. Then $\overline{\mathbf{X}} \in E_1$ and $\widehat{\overline{\mathbf{X}}} \in E_2$. So $(\overline{\mathbf{X}}, \widehat{\overline{\mathbf{X}}})$ is a conjugate pair shared by E_1 and E_2. It is obvious that $\varphi((\mathbf{X}, \widehat{\mathbf{X}})) = \varphi((\overline{\mathbf{X}}, \widehat{\overline{\mathbf{X}}}))$. Furthermore, suppose $(\mathbf{X}_1, \widehat{\mathbf{X}}_1)$ is a conjugate pair shard by E_1 and E_2 such that $\varphi((\mathbf{X}_1, \widehat{\mathbf{X}}_1)) = \varphi((\mathbf{X}, \widehat{\mathbf{X}}))$. Without lose of generality, suppose $\mathbf{X}_1 \in E_1$ and $\widehat{\mathbf{X}}_1 \in E_2$. Then $(\mathcal{D}(\mathbf{X}_1), \mathcal{D}(\widehat{\mathbf{X}}_1)) = (\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$ implies $\mathbf{X}_1 = \mathbf{X}$ or $\mathbf{X}_1 = \overline{\mathbf{X}}$. So we get $(\mathbf{X}_1, \widehat{\mathbf{X}}_1) = (\mathbf{X}, \widehat{\mathbf{X}})$ or $(\mathbf{X}_1, \widehat{\mathbf{X}}_1) = (\overline{\mathbf{X}}, \widehat{\overline{\mathbf{X}}})$.

Let $(\mathbf{Y}, \widehat{\mathbf{Y}})$ be a conjugate pair shared by C_1 and C_2. Consider the four states: $\mathcal{D}_0^{-1}(\mathbf{Y})$, $\mathcal{D}_1^{-1}(\mathbf{Y})$, $\mathcal{D}_0^{-1}(\widehat{\mathbf{Y}})$ and $\mathcal{D}_1^{-1}(\widehat{\mathbf{Y}})$. Without lose of generality, suppose $\mathbf{Y} \in C_1$ and $\widehat{\mathbf{Y}} \in C_2$. Then $\mathcal{D}_0^{-1}(\mathbf{Y})$ and $\mathcal{D}_1^{-1}(\mathbf{Y})$ all belong to E_1, $\mathcal{D}_0^{-1}(\widehat{\mathbf{Y}})$ and $\mathcal{D}_1^{-1}(\widehat{\mathbf{Y}})$ all belong to E_1. So $(\mathcal{D}_0^{-1}(\mathbf{Y}), \mathcal{D}_1^{-1}(\widehat{\mathbf{Y}}))$ and $(\mathcal{D}_1^{-1}(\mathbf{Y}), \mathcal{D}_0^{-1}(\widehat{\mathbf{Y}}))$ are two conjugate pairs shared by E_1 and E_2. Furthermore, $\varphi((\mathcal{D}_0^{-1}(\mathbf{Y}), \mathcal{D}_1^{-1}(\widehat{\mathbf{Y}}))) = \varphi((\mathcal{D}_1^{-1}(\mathbf{Y}), \mathcal{D}_0^{-1}(\widehat{\mathbf{Y}}))) = (\mathbf{Y}, \widehat{\mathbf{Y}})$. So ψ is a two-to-one map.

For 2. It is easy to see, there are no conjugate pairs shared by E_2 and $\overline{E}_2$.

Next, we consider the conjugate pairs shared by E_1 and E_2 (for conjugate pairs shard by E_1 and $\overline{E}_2$, the discussion is similar).

Let $(\mathbf{X}, \widehat{\mathbf{X}})$ be a conjugate pair shared by E_1 and $\overline{E}_2$. Without lose of generality, suppose $\mathbf{X} \in E_1$ and $\widehat{\mathbf{X}} \in \overline{E}_2$. Then $\mathcal{D}(\mathbf{X}) \in C_1$, $\mathcal{D}(\widehat{\mathbf{X}}) \in C_2$ and $(\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$ is a conjugate pair shared by C_1 and C_2. Define a map φ from the conjugate pairs shared by E_1 and $\overline{E}_2$ to the conjugate pairs shared by C_1 and C_2 as: $\varphi((\mathbf{X}, \widehat{\mathbf{X}})) = (\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$. We show that φ is a bijection.

Suppose $(\mathbf{X}_1, \widehat{\mathbf{X}}_1)$ is a conjugate pair shard by E_1 and E_2 such that $\varphi((\mathbf{X}_1, \widehat{\mathbf{X}}_1)) = \varphi((\mathbf{X}, \widehat{\mathbf{X}}))$. Without lose of generality, suppose $\mathbf{X}_1 \in E_1$ and $\widehat{\mathbf{X}}_1 \in E_2$. Then $(\mathcal{D}(\mathbf{X}_1), \mathcal{D}(\widehat{\mathbf{X}}_1)) = (\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$ implies $\mathbf{X} = \mathbf{X}_1$. So we get $(\mathbf{X}_1, \widehat{\mathbf{X}}_1) = (\mathbf{X}, \widehat{\mathbf{X}})$.

Let $(\mathbf{Y}, \widehat{\mathbf{Y}})$ be a conjugate pair shared by C_1 and C_2. Consider the four states: $\mathcal{D}_0^{-1}(\mathbf{Y})$, $\mathcal{D}_1^{-1}(\mathbf{Y})$, $\mathcal{D}_0^{-1}(\widehat{\mathbf{Y}})$ and $\mathcal{D}_1^{-1}(\widehat{\mathbf{Y}})$. Without lose of generality, suppose $\mathbf{Y} \in C_1$ and $\widehat{\mathbf{Y}} \in C_2$. Then $\mathcal{D}_0^{-1}(\mathbf{Y})$ and $\mathcal{D}_1^{-1}(\mathbf{Y})$ all belong to E_1, one of $\mathcal{D}_0^{-1}(\widehat{\mathbf{Y}})$ and $\mathcal{D}_1^{-1}(\widehat{\mathbf{Y}})$ belong to E_1. So $(\mathcal{D}_0^{-1}(\mathbf{Y}), \mathcal{D}_1^{-1}(\widehat{\mathbf{Y}}))$ or $(\mathcal{D}_1^{-1}(\mathbf{Y}), \mathcal{D}_0^{-1}(\widehat{\mathbf{Y}}))$ is a conjugate pair shared by E_1 and E_2. Furthermore, $\varphi((\mathcal{D}_0^{-1}(\mathbf{Y}), \mathcal{D}_1^{-1}(\widehat{\mathbf{Y}}))) = \varphi((\mathcal{D}_1^{-1}(\mathbf{Y}), \mathcal{D}_0^{-1}(\widehat{\mathbf{Y}}))) = (\mathbf{Y}, \widehat{\mathbf{Y}})$. This implies ψ is a surjection. So ψ is a bijection.

For 3. It is easy to see, there are no conjugate pairs shared by E_1 and $\overline{E}_1$, E_2 and $\overline{E}_2$.

Suppose there are u conjugate pairs shared by E_1 and E_2. Then it is obvious that $\overline{E}_1$ and $\overline{E}_2$ share u conjugate pairs. Next, we consider the conjugate pairs shared by E_1 and $\overline{E}_2$. Let $(\mathbf{X}, \widehat{\mathbf{X}})$ be a conjugate pair shared by E_1 and E_2 or E_1 and $\overline{E}_2$. Without lose of generality, suppose $\mathbf{X} \in E_1$ and $\widehat{\mathbf{X}} \in E_2$ or $\overline{E}_2$. Then $\mathcal{D}(\mathbf{X}) \in C_1$, $\mathcal{D}(\widehat{\mathbf{X}}) \in C_2$ and $(\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$ is a conjugate pair shared by C_1 and

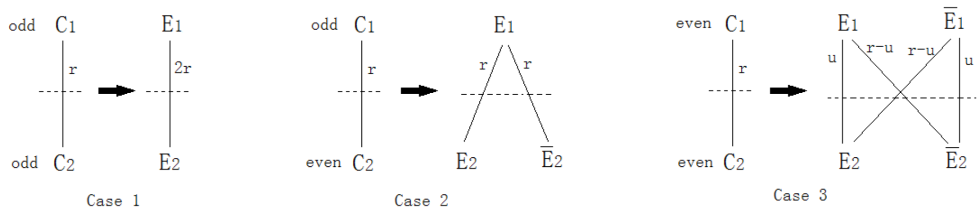
C_2. Define a map φ from the conjugate pairs shared by E_1 and E_2 or E_1 and $\overline{E}_2$ to the conjugate pairs shared by C_1 and C_2 as: $\varphi((\mathbf{X}, \widehat{\mathbf{X}})) = (\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$. We show that φ is a bijection.

Suppose $(\mathbf{X}_1, \widehat{\mathbf{X}}_1)$ is a conjugate pair shard by E_1 and E_2 or E_1 and $\overline{E}_2$ such that $\varphi((\mathbf{X}_1, \widehat{\mathbf{X}}_1)) = \varphi((\mathbf{X}, \widehat{\mathbf{X}}))$. Without lose of generality, suppose $\mathbf{X}_1 \in E_1$ and $\widehat{\mathbf{X}}_1 \in E_2$ or $\overline{E}_2$. Then $(\mathcal{D}(\mathbf{X}_1), \mathcal{D}(\widehat{\mathbf{X}}_1)) = (\mathcal{D}(\mathbf{X}), \mathcal{D}(\widehat{\mathbf{X}}))$ implies $\mathbf{X} = \mathbf{X}_1$. So we get $(\mathbf{X}_1, \widehat{\mathbf{X}}_1) = (\mathbf{X}, \widehat{\mathbf{X}})$.

Let $(\mathbf{Y}, \widehat{\mathbf{Y}})$ be a conjugate pair shared by C_1 and C_2. Consider the four states: $\mathcal{D}_0^{-1}(\mathbf{Y})$, $\mathcal{D}_1^{-1}(\mathbf{Y})$, $\mathcal{D}_0^{-1}(\widehat{\mathbf{Y}})$ and $\mathcal{D}_1^{-1}(\widehat{\mathbf{Y}})$. Without lose of generality, suppose $\mathbf{Y} \in C_1$ and $\widehat{\mathbf{Y}} \in C_2$. Then one of $\mathcal{D}_0^{-1}(\mathbf{Y})$ and $\mathcal{D}_1^{-1}(\mathbf{Y})$ belongs to E_1, both $\mathcal{D}_0^{-1}(\widehat{\mathbf{Y}})$ and $\mathcal{D}_1^{-1}(\widehat{\mathbf{Y}})$ belong to $E_2 \cup \overline{E}_2$. So $(\mathcal{D}_0^{-1}(\mathbf{Y}), \mathcal{D}_1^{-1}(\widehat{\mathbf{Y}}))$ or $(\mathcal{D}_1^{-1}(\mathbf{Y}), \mathcal{D}_0^{-1}(\widehat{\mathbf{Y}}))$ is a conjugate pair shared by E_1 and E_2 or E_1 and $\overline{E}_2$. This implies ψ is a surjection. So ψ is a bijection. Since there are u conjugate pairs shared by E_1 and E_2, we get that there are $r-u$ conjugate pairs shared by E_1 and $\overline{E}_2$. At last, it obvious that, $\overline{E}_1$ and E_2 share $r-u$ conjugate pairs. $\square$

Note: *In case 3 of theorem 4, the integer u can not be determined by r (see example 3). 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 use the method above.*

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



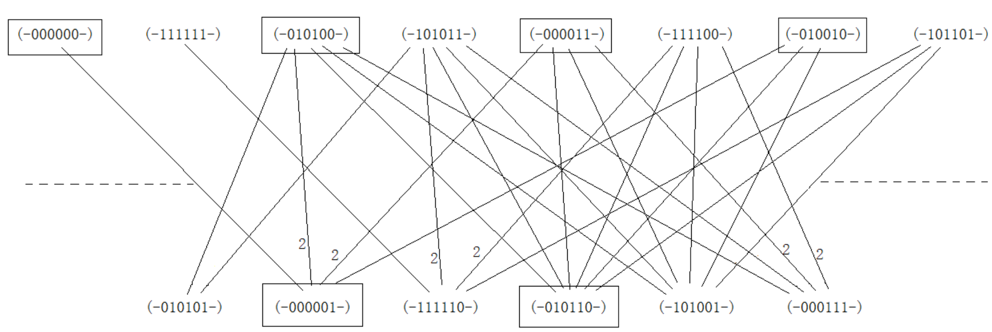
Example 3. *Continue with example 1 and example 2. Define $h = (x_0 + x_1) * g = x_0 + x_6$. Consider the adjacency graph of FSR_h. Since the parity of weight of cycles in FSR_g are known, we can get all the cycles in FSR_h easily. Divide them into two sets (see the note for lemma 3)*

$$\mathcal{A} = \{(-000000-)_h, (-111111-)_h, (-010100-)_h, (-101011-)_h, (-000011-)_h,$$

$$(-111100-)_h, (-010010-)_h, (-101101-)_h\}$$

$$\mathcal{B} = \{(-010101-)_h, (-000001-)_h, (-111110-)_h, (-010110-)_h, (-101001-)_h, (-000111-)_h\}$$

where $\mathcal{A}$ contains the cycles that are of extension of some cycles in FSR_f, and $\mathcal{B}$ contains the cycles that are of extension of some cycles in FSR_{f+1}. Since the u in theorem 4 in unknown, we have to find the number of conjugate pairs shared by some cycles first (the cycles that surrounded by a rectangle). Then the adjacency of FSR_h can be determined according to theorem 4:



4 Conclusion

The relation between the adjacency graph of FSRf and FSR$_{(x_0+x_1)*f}$ is discussed, where f is a linear boolean function. For f contains a odd number of terms, we can get the adjacency graph of FSR$_{(x_0+x_1)*f}$ easily from the adjacency graph of FSR$_f$ using our method. But for f contains an even number of terms, the theory is not so much complete. That may be the next work we need to do. Besides, some properties about LFSRs are proposed.

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

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

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

[6] 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.

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

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

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