The Adjacency Graphs of Some Feedback Shift Registers

Ming Li Yupeng Jiang and Dongdai Lin

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

November 5, 2015

Abstract

The adjacency graphs of feedback shift registers (FSRs) with characteristic function of the form $g = (x_0 + x_1) * f$ are considered in this paper. Some properties about these FSRs are given. It is proved that these FSRs contains only prime cycles and these cycles can be divided into two sets such that each set contains no adjacent cycles. When f is a linear function, more properties about these FSRs are derived. It is shown that, when f is a linear function and contains an odd number of terms, the adjacency graph of $\mathrm{FSR}((x_0 + x_1) * f)$ can be determined directly from the adjacency graph of $\mathrm{FSR}(f)$. As an application of these results, we determine the adjacency graphs of $\mathrm{FSR}((1 + x)^4 p(x))$ and $\mathrm{FSR}((1 + x)^5 p(x))$, where $p(x)$ is a primitive polynomial, and construct a large class of de Bruijn sequences from them.

Keywords: MSC(94A55), feedback shift register, adjacency graph, de Bruijn sequence.

1 Introduction

Feedback shift registers (FSRs) can be used to generate pseudo random sequences. The period of the output sequences of an n-stage FSRs is no more than 2^n. If this value is attained, we call the FSR maximum length FSR, and the sequence de Bruijn sequence. Maximum length FSRs (or de Bruijn sequences) are usually constructed by the cycle joining method introduced in [5]. For the application of this method, we need to know the distribution of the conjugate pairs in the cycles of the based FSR, which is usually difficult to analyze. Therefore, FSRs with simple cycle structures are good candidates for the based FSRs. Some linear feedback shift registers (LFSRs), such as the maximum length LFSRs, pure circulating registers and pure summing registers, have been used to construct maximum length FSRs [2–4]. Recently, the LFSRs with characteristic polynomials $(1 + x)^m p(x)$ and $(1 + x^m)p(x)$ were also used, where $p(x)$ is a primitive polynomial and m is a positive integer less than 4 [8, 11, 12, 14].

The adjacency graph of an FSR provides information on the distribution of conjugate pairs, and it is useful for constructing maximum length FSRs by the cycle joining method. In this paper, we consider the adjacency graphs of a class of FSRs, namely, the FSRs with characteristic function of the form $g = (x_0 + x_1) * f$. Some properties about these FSRs are given. It is proved that these FSRs are dividable (see Definition 2). When f is a linear function, some more properties about these FSRs are derived. For example, it is shown that in some cases the adjacency graph of FSR($(x_0 + x_1) * f$) can be determined directly from the adjacency graph of FSR(f) (see Section 4). As an application of these properties, we continue the work of Li et al. [11] to determine the adjacency graphs of FSR($(1+x)^4p(x)$) and FSR($(1+x)^5p(x)$), where $p(x)$ is a primitive polynomial. Two families of maximum length FSRs are constructed from them. We show that the sizes of the two families are $O(2^{5n})$ and $O(2^{7n})$, where n is the degree of $p(x)$. We also present an algorithm to generate such a maximum length FSR with both time complexity and memory complexity $O(n)$.

The paper is organized as follows. In Section 2, we introduce some necessary preliminaries. In Section 3, some properties of the FSRs with characteristic function of the form $g = (x_0+x_1)*f$ are given. In Section 4, we consider the case that f is a linear function. In Section 5, we determine the the adjacency graphs of FSR($(1 + x)^4p(x)$) and FSR($(1 + x)^5p(x)$). In Section 6, a large number of maximum length FSRs are constructed from FSR($(1 + x)^4p(x)$) and FSR($(1 + x)^5p(x)$). In Section 7, we make a conclusion about our work.

2 Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ be the finite field of two elements, and $\mathbb{F}_2^n$ 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 mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. It is well known that it can be uniquely represented by its algebraic normal form (ANF), which is a multivariate polynomial. The order of f, denoted by $\mathrm{ord}(f)$, is the highest subscript i for which x_i occurs in the ANF of f. Note that the order of f is not equal to the number of variables in f. 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 a Boolean function of order $n + m$ [6]. The operation $*$ is not commutative, that is, $f * g$ is not equal to $g * f$ generally. However, if f and g are linear Boolean functions, we have $f * g = g * f$. We say $(x_0 + x_1)$ is a left $*$-factor of g, denote by $(x_0 + x_1)\|_L g$, if $g = (x_0 + x_1) * h$ for some Boolean function h. For a given g, it is easy to verify whether we have $(x_0 + x_1)\|_L g$ or not.

An n-stage feedback shift register (FSR) consists of n binary storage cells and a characteristic function f regulated by a single clock. In what follows, the characteristic function f is supposed to be nonsingular, i.e., of the form $f = x_0+f_0(x_1, \ldots, x_{n-1})+x_n$. The FSR with characteristic function f is usually denoted by FSR(f). At every clock pulse, the current state $(s_0, s_1, \ldots, s_{n-1})$ is updated by $(s_1, s_2, \ldots, s_{n-1}, s_n)$ such that $f(s_0, s_1, \ldots, s_n) = 0$. From an initial state $\mathbf{S}_0 = (s_0, s_1, \ldots, s_{n-1})$, after consecutive clock pulses, FSR(f) will generate a cycle $C = [\mathbf{S}_0, \mathbf{S}_1, \ldots, \mathbf{S}_{l-1}]$ (can also be denoted by $C = [s_1, s_2, \ldots, s_{l-1}]_n$ or simply $C = [s_1, s_2, \ldots, s_{l-1}]$), where $\mathbf{S}_{i+1}$ is the next state of $\mathbf{S}_i$ for $i = 0, 1, \ldots, l - 2$ and $\mathbf{S}_0$ is the next state of $\mathbf{S}_{l-1}$. In this way, the set $\mathbb{F}_2^n$ is divided into cycles $C_1, C_2, \ldots, C_k$ by FSR(f), and reversely, a partition 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 $\text{FSR}(f) = \{C_1, C_2, \ldots, C_k\}$. We call FSR($f$) maximum length FSR if there is only one cycle in FSR(f), and the unique cycle in FSR(f) is usually called de Bruijn cycle or full cycle. The output sequences of FSR(f), denoted by $G(f)$, are the 2^n sequences $\mathbf{s} = s_0 s_1 \cdots$, such that $f(s_t, s_{t+1}, \ldots, s_{t+n}) = 0$ for $t \geq 0$. It was proved in [14] that

Lemma 1. *[14] $G((x_0 + x_1) * f) = G(f) \cup G(f + 1)$.*

For a state $\mathbf{S} = (s_0, s_1, \ldots, s_{n-1})$, its conjugate $\widehat{\mathbf{S}}$ is defined as $\widehat{\mathbf{S}} = (\overline{s}_0, s_1, \ldots, s_{n-1})$ where $\overline{s}_0$ is the binary complement of s_0. Two cycles C_1 and C_2 are adjacent if they are state disjoint and there exists a state $\mathbf{S}$ on C_1 whose conjugate $\widehat{\mathbf{S}}$ is on C_2. By interchanging the successors of $\mathbf{S}$ and $\widehat{\mathbf{S}}$, the two cycles C_1 and C_2 are joined together. This is the basic idea of the cycle joining method introduced in [5].

Definition 1. *[7, 13] 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.*

For any FSR, its adjacency graph is a connected graph. This fact follows from the statement in [4]: C is a de Bruijn cycle if and only if the existence of state $\mathbf{S}$ on C also implies the existence of its conjugate $\widehat{\mathbf{S}}$ on C. Every maximal spanning tree of an adjacency graph corresponds to a maximum length FSR, since this represents a choice of adjacencies that repeatedly join two cycles into one ending with exactly one cycle, i.e. de Bruijn cycle.

3 Some Properties of $\text{FSR}((x_0 + x_1) * f)$

Let f and g be the characteristic functions of two FSRs. It was proved in [14] that, $G(f) \subset G(g)$ and $\text{ord}(f) = \text{ord}(g) - 1$ implies $g = (x_0 + x_1) * f$.

Theorem 1. *The output sequences of* FSR(g) *are the disjoint union of the output sequences of two or more FSRs if and only if $(x_0 + x_1) \|_L g$.*

Proof. Suppose $g = (x_0 + x_1) * f$, then we have $G(g) = G(f) \cup G(f + 1)$. It can be verified that $G(f) \cap G(f + 1) = \emptyset$.

Suppose $G(g) = G(f_1) \cup G(f_2) \cup \cdots \cup G(f_k)$, such that $k \geq 2$ and $G(f_i) \cap G(f_j) = \emptyset$ for any $i \neq j$. Assume the sequence $\mathbf{s}$ generated by FSR(g) with initial state $(0, \ldots, 0, 1)$ belongs to $G(f_i)$. Let n be the number of stages in FSR(g). It can be verified that, $\mathbf{s}$ can not be generated by any FSR with stages less than $n - 1$. Therefore, we have $\text{ord}(f_i) = \text{ord}(g) - 1$. Since $G(f_i) \subset G(g)$ and $\text{ord}(f_i) = \text{ord}(g) - 1$, we get $g = (x_0 + x_1) * f_i$. □

For a given g, searching for the f such that $G(f) \subset G(g)$ is a hard work [15]. However, according to Theorem 1, decompose $G(g)$ into the disjoint union of the output sequences of FSRs, i.e., $G(g) = G(f_1) \cup G(f_2) \cup \cdots \cup G(f_k)$, is easy.

Example 1. *Let* $g = x_0 + x_2 + x_3 + x_1x_2 + x_3x_4 + x_5$. *Since* $g = (x_0 + x_1) * (x_0 + x_1 + x_3 + x_1x_2 + x_2x_3 + x_4)$, *we have* $G(g) = G(f) \cup G(f+1)$ *where* $f = x_0 + x_1 + x_3 + x_1x_2 + x_2x_3 + x_4$. *For* f, *since* $f = (x_0 + x_1) * (x_0 + x_1x_2 + x_3)$, *we have* $G(f) = G(h) \cup G(h+1)$ *where* $h = x_0 + x_1x_2 + x_3$. *It can be verified that* $(x_0 + x_1) \nparallel_L h$. *Therefore,* $G(g) = G(f) \cup G(f+1) = G(h) \cup G(h+1) \cup G(f+1)$ *is the complete decomposition of* $G(g)$.

For a cycle $C = [s_1, s_2, \ldots, s_{l-1}]_n$, define the extended cycle of C as $C^+ = [s_1, s_2, \ldots, s_{l-1}]_{n+1}$, then Lemma 1 can be restated as

Lemma 2. *[14] Let* $\mathrm{FSR}(f) = \{C_1, C_2, \ldots, C_k\}$ *and* $\mathrm{FSR}(f+1) = \{D_1, D_2, \ldots, D_t\}$ *be two FSRs, then*

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

is an FSR with characteristic function $g = (x_0 + x_1) * f$.

We call a cycle $C = [s_0, s_1, \ldots, s_{l-1}]_n$ prime cycle if there are no conjugate pairs $(\mathbf{S}, \widehat{\mathbf{S}})$ in C. In the case C is a prime cycle, the reduced cycle of C is defined as $C^- = [s_0, s_1, \ldots, s_{l-1}]_{n-1}$.

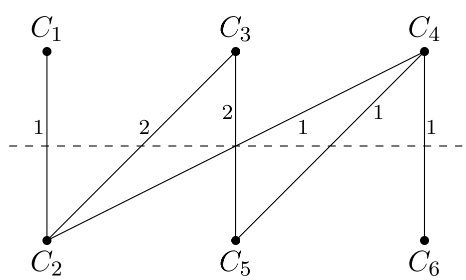
Definition 2. *An FSR is called dividable if it contains only prime cycles and these cycles can be divided into two sets such that each set contains no adjacent cycles.*

Example 2. *Let* $g = x_0 + x_1x_2 + x_2x_3 + x_4$ *be a Boolean function. There are* 6 *cycles in* $\mathrm{FSR}(g)$, *i.e.,*

$$C_1 = [0000], C_2 = [0001, 0010, 0100, 1000], C_3 = [0011, 0111, 1110, 1100, 1001],$$

$$C_4 = [0101, 1010], C_5 = [0110, 1101, 1011], C_6 = [1111].$$

These cycles are prime cycles and they can be divided into two sets $\{C_1, C_3, C_4\} \cup \{C_2, C_5, C_6\}$, *such that each set contains no adjacent cycles, therefore,* $\mathrm{FSR}(g)$ *is dividable. The adjacency graph of* $\mathrm{FSR}(g)$ *is shown below.*



Theorem 2. $\mathrm{FSR}(g)$ *is dividable if and only if* $(x_0 + x_1) \|_L g$.

Proof. Suppose $g = (x_0 + x_1) * f$ for some f. Let $\mathrm{FSR}(f) = \{C_1, C_2, \cdots, C_k\}$ and $\mathrm{FSR}(f+1) = \{D_1, D_2, \cdots, D_t\}$. By Lemma 2, $\mathrm{FSR}(g) = \{C_1^+, C_2^+, \cdots, C_k^+, D_1^+, D_2^+, \cdots, D_t^+\}$. It is easy to see, the cycles in $\mathrm{FSR}(g)$ are prime cycles. We divide these cycles into two sets: $\{C_1^+, C_2^+, \cdots, C_k^+\} \cup \{D_1^+, D_2^+, \cdots, D_t^+\}$. Then for the necessity part of the theorem it is enough to show that none of the two sets contains adjacent cycles. Suppose C_i^+ and C_j^+ are adjacent. Let $(\mathbf{S}, \widehat{\mathbf{S}})$ be a conjugate pair with $\mathbf{S} \in C_i^+$ and $\widehat{\mathbf{S}} \in C_j^+$. Denote $\mathbf{S}$ by $\mathbf{S} = (s_0, s_1, \ldots, s_{n-1})$, where n is the order of g. Then the state $(s_1, s_2, \ldots, s_{n-1})$ would be on both C_i and C_j, which is impossible. Therefore, there are no adjacent cycles in $\{C_1^+, C_2^+, \cdots, C_k^+\}$. Similarly, there are no adjacent cycles in $\{D_1^+, D_2^+, \cdots, D_t^+\}$.

Suppose $\mathrm{FSR}(g)$ is dividable. Then the cycles in $\mathrm{FSR}(g)$ are prime cycles and they can be divided into two sets, say $\{C_1, C_2, \cdots, C_k\} \cup \{D_1, D_2, \cdots, D_t\}$, such that none of the two sets contains adjacent cycles. We assert that: $\{C_1^-, C_2^-, \cdots, C_k^-\}$ and $\{D_1^-, D_2^-, \cdots, D_t^-\}$ are two partitions of $\mathbb{F}_2^{n-1}$, i.e., they are two $(n-1)$-stage FSRs, where n is the order of g. To prove the assertion, we need to show that, for any state $\mathbf{S} \in \mathbb{F}_2^{n-1}$ there exist some i and j such that $\mathbf{S}$ is on both C_i^- and D_j^-. Denote $\mathbf{S}$ by $\mathbf{S} = (s_0, s_1, \ldots, s_{n-2})$ and let $\mathbf{U} = (0, s_0, s_1, \ldots, s_{n-2})$ and $\mathbf{V} = (1, s_0, s_1, \ldots, s_{n-2})$. Since $(\mathbf{U}, \mathbf{V})$ is a conjugate pair, there exist some i and j such that $\mathbf{U}$ is on C_i and $\mathbf{V}$ is on D_j. Then it can be verified that $\mathbf{S}$ is on both C_i^- and D_j^-. Therefore, $\{C_1^-, C_2^-, \cdots, C_k^-\}$ and $\{D_1^-, D_2^-, \cdots, D_t^-\}$ are two $(n-1)$-stage FSRs. Let f and f' be the characteristic functions of the two FSR. The sufficiency part of the theorem is proved if f and f' have the relation $f = f' + 1$. Let $\mathbf{W} = (w_0, w_1, \ldots, w_{n-2})$ be a state of length $n-1$. Assume $\mathbf{W}$ is on C_i^- and D_j^-. Let $\mathbf{X} = (w_1, w_2, \ldots, w_{n-2}, x)$ and $\mathbf{Y} = (w_1, w_2, \ldots, w_{n-2}, y)$ be the two next states of $\mathbf{W}$ in C_i^- and D_j^- respectively. Since $(w_0, w_1, w_2, \ldots, w_{n-2}, x)$ is on C_i and $(w_0, w_1, w_2, \ldots, w_{n-2}, y)$ is on D_j, we have $(w_0, w_1, w_2, \ldots, w_{n-2}, x) \neq (w_0, w_1, w_2, \ldots, w_{n-2}, y)$, therefore, $x = \overline{y}$. This implies $f = f' + 1$. □

Theorem 3. *The number of n-stage dividable FSRs is $2^{2^{n-2}-1}$.*

Proof. Let $\mathrm{FSR}(f_1)$ and $\mathrm{FSR}(f_2)$ be two $(n-1)$-stage FSRs, then we have $(x_0+x_1)*f_1 = (x_0+x_1)*f_2 \Leftrightarrow f_1 - f_2 = x_1 * (f_1 - f_2) \Leftrightarrow f_1 = f_2$ *or* $f_1 = f_2 + 1$. Define a mapping ψ from the $(n-1)$-stage FSRs to the n-stage dividable FSRs: $\psi(\mathrm{FSR}(f)) = \mathrm{FSR}((x_0 + x_1) * f)$. Then ψ is a 2-to-1 mapping, and its image set is the n-stage dividable FSRs. □

By the definition, a dividable FSR contains only prime cycles, however, an FSR that contains only prime cycles may not be dividable.

Example 3. *Let $g = x_0 + x_1x_2x_4 + x_1x_3x_4 + x_5$ be a Boolean function.* $\mathrm{FSR}(g)$ *contains* 8 *cycles, i.e.,*

$$C_1 = [00000], C_2 = [00001, 00010, 00100, 01000, 10000],$$

$$C_3 = [00011, 00110, 01100, 11000, 10001],$$

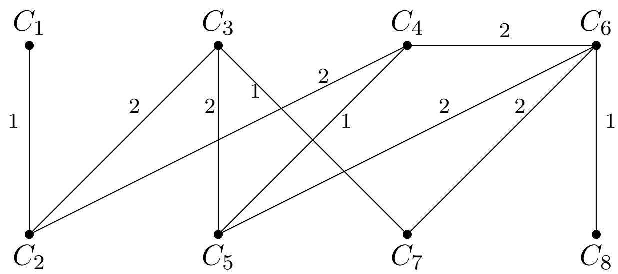
$$C_4 = [00101, 01010, 10100, 01001, 10010],$$

$$C_5 = [00111, 01110, 11100, 11001, 10011],$$

$$C_6 = [01011, 10111, 01111, 11110, 11101, 11010, 10101],$$

$$C_7 = [01101, 11011, 10110], C_8 = [11111].$$

It can be verified that, these cycles are prime cycles. However, $\mathrm{FSR}(g)$ *is not dividable, because* $(x_0 + x_1) \nmid_L g$. *The adjacency graph of* $\mathrm{FSR}(g)$ *is shown below.*



We call FSR(g) a linear feedback shift register (LFSR) if g is a linear Boolean function, i.e., g is of the form $g = c_0x_0 + c_1x_1 + \ldots + c_nx_n$. For a linear Boolean function g, it can be verified that, $(x_0 + x_1)\|_L g$ if and only if g contains an even number of terms.

Theorem 4. *Let* FSR(g) *be a linear feedback shift register, then* FSR(g) *contains only prime cycles if and only if* $(x_0 + x_1)\|_L g$.

Proof. Suppose $(x_0+x_1)\|_L g$, then FSR(g) is dividable according to Theorem 2. So FSR(g) contains only prime cycles. Suppose $(x_0+x_1) \nparallel_L g$, then g contains an odd number of terms. It can be verified that, the next state of $(0, 1, \ldots, 1)$ in FSR(g) is $(1, 1, \ldots, 1)$. Since $(0, 1, \ldots, 1)$ and $(1, 1, \ldots, 1)$ are conjugate with each other, the cycle that contains these two states is not a prime cycle. $\square$

4 The Adjacency Graphs of Some LFSRs

D-morphism was proposed by Lempel [10]. It is a 2-to-1 mapping from $\mathbb{F}_2^{n+1}$ to $\mathbb{F}_2^n$: $D(s_0, s_1, \ldots, s_n) = (s_0 + s_1, s_1 + s_2, \ldots, s_{n-1} + s_n)$. The two preimages of a state $\mathbf{S} = (s_0, s_1, \ldots, s_{n-1})$ is $D_0^{-1}(\mathbf{S}) = (0, s_0, s_0+s_1, \ldots, s_0+s_1+\cdots+s_{n-1})$ and $D_1^{-1}(\mathbf{S}) = (1, 1+s_0, 1+s_0+s_1, \ldots, 1+s_0+s_1+\cdots+s_{n-1})$. Let $(\mathbf{S}, \widehat{\mathbf{S}})$ be a conjugate pair, then $(D_0^{-1}(\mathbf{S}), D_1^{-1}(\widehat{\mathbf{S}}))$ and $(D_1^{-1}(\mathbf{S}), D_0^{-1}(\widehat{\mathbf{S}}))$ are two conjugate pairs. For a cycle $C = [s_0, s_1, \ldots, s_{l-1}]$, its complement is defined as $\overline{C} = [\overline{s}_0, \overline{s}_1, \ldots, \overline{s}_{l-1}]$. Its weight is defined as the number of 1's among the s_i's, i.e., $W(C) = \sum_{i=0}^{l-1} s_i$. In the case $W(C)$ is even, define $D^{-1}(C) = \{[0, s_0, s_0+s_1, \cdots, s_0+s_1+\cdots+s_{l-2}]_{n+1}, [1, 1+s_0, 1+s_0+s_1, \cdots, 1+s_0+s_1+\cdots+s_{l-2}]_{n+1}\}$ which contains two complement cycles of order $n+1$. In the case $W(C)$ is odd, define $D^{-1}(C) = \{[0, s_0, \cdots, s_0 + s_1 + \cdots + s_{l-2}, 1, 1 + s_0, \cdots, 1 + s_0 + s_1 + \cdots + s_{l-2}]_{n+1}\}$ which contains one self-complement cycle of order $n+1$.

Lemma 3. *[10] Let* $\mathrm{FSR}(f) = \{C_1, C_2, \ldots, C_k\}$ *be an n-stage FSR, then*

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

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

Since the operation $*$ is not commutative, generally $(x_0 + x_1) * f \neq f * (x_0 + x_1)$. But when f is a linear Boolean function, we have $(x_0 + x_1) * f = f * (x_0 + x_1)$.

Theorem 5. *Let f be a linear Boolean function. Let* $\mathrm{FSR}(f) = \{C_1, C_2, \ldots, C_k\}$ *and* $\mathrm{FSR}(f+1) = \{D_1, D_2, \ldots, D_t\}$*, then we have*

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

Proof. It follows from Lemma 2 and Lemma 3. □

Theorem 6. *Let f be a linear Boolean function, then we have*

1. *The number of cycles in* $\mathrm{FSR}(f+1)$ *is equal to the number of even weight cycles in* $\mathrm{FSR}(f)$.
2. $\mathrm{FSR}(f)$ *contains only even weight cycles if and only if f contains an odd number of terms.*
3. $\mathrm{FSR}(f)$ *and* $\mathrm{FSR}(f+1)$ *contain the same number of cycles if and only if f contains an odd number of terms.*

Proof. 1. Let s and t be the number of odd weight cycles and even weight cycles in $\mathrm{FSR}(f)$ respectively, and u be the number of cycles in $\mathrm{FSR}(f+1)$. By the equation in Theorem 5, we have $s+2t = s+t+u$, which implies $t = u$.

2. Let f be a linear Boolean function that contains an odd number of terms. Suppose C is an odd weight cycle in $\mathrm{FSR}(f)$. Since $W(C)$ is odd, there is only one cycle in $D^{-1}(C)$. Denote the cycle in $D^{-1}(C)$ by E, then it can be verified that for any state $(s_0, s_1, \ldots, s_n)$ on E the state $(\overline{s}_0, \overline{s}_1, \ldots, \overline{s}_n)$ is also on E. According to Theorem 5, we have $E^- \in \mathrm{FSR}(f)$ or $E^- \in \mathrm{FSR}(f+1)$. Without lose of generality, assume $E^- \in \mathrm{FSR}(f)$. Then for any state $(s_0, s_1, \ldots, s_n)$ on E, we have $f(s_0, s_1, \ldots, s_n) = 0$. This is contradiction, because f contains an odd number of terms and $f(s_0, s_1, \ldots, s_n) = 0$ implies $f(\overline{s}_0, \overline{s}_1, \ldots, \overline{s}_n) = 1$. Let f be a linear Boolean function that contains an even number of terms, then the cycle that contains only the state $(1, 1, \ldots, 1)$ is an odd weight cycle in $\mathrm{FSR}(f)$. Therefore, $\mathrm{FSR}(f)$ contains at least one cycle of odd weight.

3. It follows from the two items above.

□

In the following, we investigate the relationship between the adjacency graphs of $\mathrm{FSR}((x_0 + x_1) * f)$ and $\mathrm{FSR}(f)$, where f is a linear Boolean function. This problem was first studied in [11], where some conclusions are obtained when f is a linear Boolean function that corresponding to a primitive polynomial. An open problem was also proposed there: for any two adjacent even weight cycles C_1 and C_2 in $\mathrm{FSR}((1+x)^m p(x))$, determine the number of conjugate pairs shared by their preimages $D^{-1}(C_1)$ and $D^{-1}(C_2)$, where $p(x)$ is a primitive polynomial. We pay attention to a generalized situation and continue this research. Our discussion is divided into two cases.

Let f be a linear Boolean function that contains an odd number of terms ($\mathrm{FSR}(f)$ is not dividable). According to Theorem 6, $\mathrm{FSR}(f)$ contains only even weight cycles. Let C be a cycle in $\mathrm{FSR}(f)$, then there are two cycles in $D^{-1}(C)$. Denote the two cycles by E and $\overline{E}$. It can be verified that, we always have (1) $E^- \in \mathrm{FSR}(f)$, $\overline{E}^- \in \mathrm{FSR}(f+1)$ or (2) $E^- \in \mathrm{FSR}(f+1)$, $\overline{E}^- \in \mathrm{FSR}(f)$.

Theorem 7. *Let f be a linear Boolean function that contains an odd number of terms.*

1. *Let C be a cycle in* $\mathrm{FSR}(f)$, *and $D^{-1}(C) = \{E, \overline{E}\}$. Suppose C contains r conjugate pairs, then E and $\overline{E}$ share $2r$ conjugate pairs.*

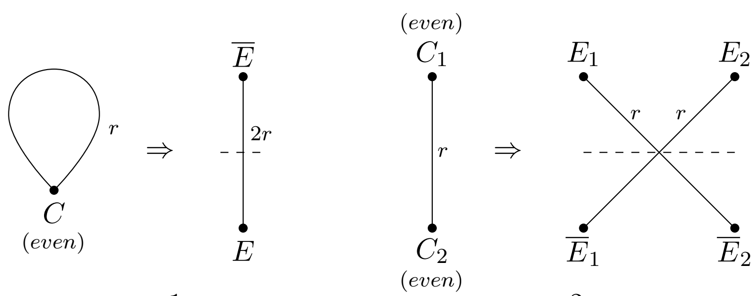
2. *Let C_1, C_2 be two cycles in* FSR(f), *and* $D^{-1}(C_1) = \{E_1, \overline{E}_1\}$, $D^{-1}(C_2) = \{E_2, \overline{E}_2\}$, *then we can assume* $E_1^-, E_2^- \in$ FSR(f) *and* $\overline{E}_1^-, \overline{E}_2^- \in$ FSR$(f+1)$. *Suppose C_1 and C_2 share r conjugate pairs, then both E_1 and $\overline{E}_2$, $\overline{E}_1$ and E_2 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. For $i \in \{1, 2, \ldots, r\}$, let $b_i \in \{0, 1\}$ such that $D_{b_i}^{-1}(\mathbf{X}_i) \in E$ and $D_{1-b_i}^{-1}(\mathbf{X}_i) \in \overline{E}$. Since E and $\overline{E}$ belong to FSR$((x_0 + x_1) * f)$ which is dividable, there are no conjugate pairs in E or $\overline{E}$. Remember that $(D_{b_i}^{-1}(\mathbf{X}_i), D_{1-b_i}^{-1}(\widehat{\mathbf{X}}_i))$ is a conjugate pair, we have $D_{1-b_i}^{-1}(\widehat{\mathbf{X}}_i)$ is on the cycle $\overline{E}$. Similarly, $D_{b_i}^{-1}(\widehat{\mathbf{X}}_i)$ is on the cycle E. Therefore, $(D_{b_i}^{-1}(\mathbf{X}_i),\ D_{1-b_i}^{-1}(\widehat{\mathbf{X}}_i))$, $(D_{b_i}^{-1}(\widehat{\mathbf{X}}_i),\ D_{1-b_i}^{-1}(\mathbf{X}_i))$, for $i = 1, 2, \ldots, r$, are $2r$ conjugate pairs shared by E and $\overline{E}$. It remains to show that there are no other conjugate pairs. Let $(\mathbf{Y}, \widehat{\mathbf{Y}})$ be a conjugate pair shared by E and $\overline{E}$ with $\mathbf{Y} \in E$ and $\widehat{\mathbf{Y}} \in \overline{E}$, then $(D(\mathbf{Y}), D(\widehat{\mathbf{Y}}))$ is a conjugate pair in C. Assume $(D(\mathbf{Y}), D(\widehat{\mathbf{Y}})) = (\mathbf{X}_i, \widehat{\mathbf{X}}_i)$ for some $i \in \{1, 2, \ldots, r\}$, then the conjugate pair $(\mathbf{Y}, \widehat{\mathbf{Y}})$ is $(D_{b_i}^{-1}(\mathbf{X}_i),\ D_{1-b_i}^{-1}(\widehat{\mathbf{X}}_i))$ or $(D_{b_i}^{-1}(\widehat{\mathbf{X}}_i),\ D_{1-b_i}^{-1}(\mathbf{X}_i))$.

2. Since $E_1^-, E_2^- \in$ FSR(f), there are no conjugate pairs shared by E_1 and E_2. Similarly, there are no conjugate pairs shared by $\overline{E}_1$ 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 $\widehat{\mathbf{X}}_i \in C_2$. For $i \in \{1, 2, \ldots, r\}$, let $b_i \in \{0, 1\}$ such that $D_{b_i}^{-1}(\mathbf{X}_i) \in E_1$ and $D_{1-b_i}^{-1}(\mathbf{X}_i) \in \overline{E}_1$. Since there are no conjugate pairs shared by E_1 and E_2, $D_{1-b_i}^{-1}(\widehat{\mathbf{X}}_i)$ is on $\overline{E}_2$ and $D_{b_i}^{-1}(\widehat{\mathbf{X}}_i)$ is on E_2. Therefore, $(D_{b_i}^{-1}(\mathbf{X}_i),\ D_{1-b_i}^{-1}(\widehat{\mathbf{X}}_i))$, for $i = 1, 2, \ldots, r$, are r conjugate pairs shared by E_1 and $\overline{E}_2$. Next we show that there are no other conjugate pairs shared by E_1 and $\overline{E}_2$. Let $(\mathbf{Y}, \widehat{\mathbf{Y}})$ be a conjugate pair shared by E_1 and $\overline{E}_2$ with $\mathbf{Y} \in E_1$ and $\widehat{\mathbf{Y}} \in \overline{E}_2$, then $(D(\mathbf{Y}), D(\widehat{\mathbf{Y}}))$ is a conjugate pair shared by C_1 and C_2 with $D(\mathbf{Y}) \in C_1$ and $D(\widehat{\mathbf{Y}}) \in C_2$. Assume $(D(\mathbf{Y}), D(\widehat{\mathbf{Y}})) = (\mathbf{X}_i, \widehat{\mathbf{X}}_i)$ for some $i \in \{1, 2, \ldots, r\}$, then we have $(\mathbf{Y}, \widehat{\mathbf{Y}}) = (D_{b_i}^{-1}(\mathbf{X}_i), D_{1-b_i}^{-1}(\widehat{\mathbf{X}}_i))$. So there are exactly r conjugate pairs shared by E_1 and $\overline{E}_2$. Similarly, $(D_{1-b_i}^{-1}(\mathbf{X}_i),\ D_{b_i}^{-1}(\widehat{\mathbf{X}}_i))$, $i = 1, 2, \ldots, r$, are the r conjugate pairs shared by $\overline{E}_1$ and E_2.

□

The conclusion in Theorem 7 is illustrated by the following graph.



case 1 case 2

Let f be a linear Boolean function that contains an even number of terms (FSR(f) is dividable), then FSR(f) contains only prime cycles. Let C be a even weight cycle in FSR(f), then there are two cycles in $D^{-1}(C)$. Denote the two cycles by E and $\overline{E}$. It can be verified that, we always have (1) $E^-, \overline{E}^- \in$ FSR(f) or (2) $E^-, \overline{E}^- \in$ FSR$(f+1)$. Since E^- and $\overline{E}^-$ belong to the same FSR, there are no conjugate pairs shared by E and $\overline{E}$.

Theorem 8. *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 odd weight cycles. 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 an odd weight cycle and $C_2 \in \mathrm{FSR}(f)$ be an even weight cycle. 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 both E_1 and E_2, E_1 and $\overline{E}_2$ share r conjugate pairs.*

3. *Let $C_1, C_2 \in \mathrm{FSR}(f)$ be two even weight cycles. 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 some integer u with $0 \le u \le r$ such that: both E_1 and E_2, $\overline{E}_1$ and $\overline{E}_2$ share u conjugate pairs; both E_1 and $\overline{E}_2$, $\overline{E}_1$ and E_2 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 $(D_0^{-1}(\mathbf{X}_i),\ D_1^{-1}(\widehat{\mathbf{X}}_i))$, $(D_1^{-1}(\mathbf{X}_i),\ D_0^{-1}(\widehat{\mathbf{X}}_i))$, for $i = 1, 2, \ldots, r$, are $2r$ conjugate pairs shared by C_1 and C_2. Let $(\mathbf{Y}, \widehat{\mathbf{Y}})$ be a conjugate pair shared by E_1 and E_2 with $\mathbf{Y} \in E_1$ and $\widehat{\mathbf{Y}} \in E_2$, then $(D(\mathbf{Y}), D(\widehat{\mathbf{Y}}))$ is a conjugate pair shared by C_1 and C_2 with $D(\mathbf{Y}) \in C_1$ and $D(\widehat{\mathbf{Y}}) \in C_2$. Assume $(D(\mathbf{Y}), D(\widehat{\mathbf{Y}}))= (\mathbf{X}_i, \widehat{\mathbf{X}}_i)$ for some $i \in \{1, 2, \ldots, r\}$, then the conjugate pair $(\mathbf{Y}, \widehat{\mathbf{Y}})$ is $(D_0^{-1}(\mathbf{X}_i), D_1^{-1}(\widehat{\mathbf{X}}_i))$ or $(D_1^{-1}(\mathbf{X}_i), D_0^{-1}(\widehat{\mathbf{X}}_i))$.

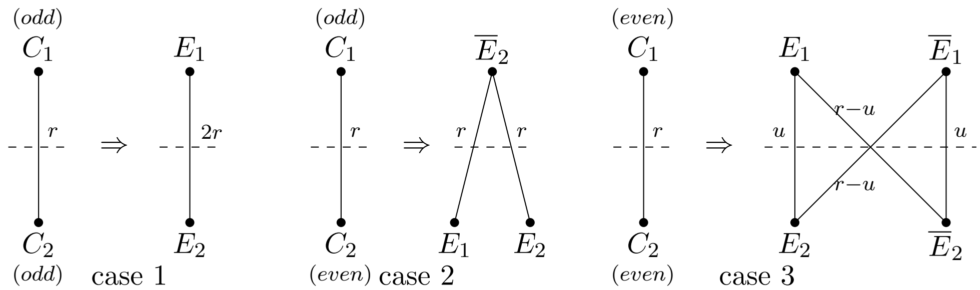
2. Let $(\mathbf{X}_i, \widehat{\mathbf{X}}_i), i = 1, 2, \ldots, r$ be the r conjugate pairs shared by C_1 and C_2 with $\mathbf{X}_i \in C_1$ and $\widehat{\mathbf{X}}_i \in C_2$. For $i \in \{1, 2, \ldots, r\}$, let $b_i \in \{0, 1\}$ such that $D_{b_i}^{-1}(\widehat{\mathbf{X}}_i) \in E_2$ and $D_{1-b_i}^{-1}(\widehat{\mathbf{X}}_i) \in \overline{E}_2$, then $(D_{1-b_i}^{-1}(\mathbf{X}_i),\ D_{b_i}^{-1}(\widehat{\mathbf{X}}_i))$, for $i = 1, 2, \ldots, r$, are r conjugate pairs shared by E_1 and E_2, and $(D_{b_i}^{-1}(\mathbf{X}_i),\ D_{1-b_i}^{-1}(\widehat{\mathbf{X}}_i))$, for $i = 1, 2, \ldots, r$, are r conjugate pairs shared by E_1 and $\overline{E}_2$. Next we show that there are no other conjugate pairs shared by E_1 and E_2. Let $(\mathbf{Y}, \widehat{\mathbf{Y}})$ be a conjugate pair shared by E_1 and E_2 with $\mathbf{Y} \in E_1$ and $\widehat{\mathbf{Y}} \in E_2$, then $(D(\mathbf{Y}), D(\widehat{\mathbf{Y}}))$ is a conjugate pair shared by C_1 and C_2 with $D(\mathbf{Y}) \in C_1$ and $D(\widehat{\mathbf{Y}}) \in C_2$. Assume $(D(\mathbf{Y}), D(\widehat{\mathbf{Y}})) = (\mathbf{X}_i, \widehat{\mathbf{X}}_i)$ for some $i \in \{1, 2, \ldots, r\}$, then we have $(\mathbf{Y}, \widehat{\mathbf{Y}}) = (D_{1-b_i}^{-1}(\mathbf{X}_i), D_{b_i}^{-1}(\widehat{\mathbf{X}}_i))$. So there are exactly r conjugate pairs shared by E_1 and E_2. Similarly, there are exactly 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 $\widehat{\mathbf{X}}_i \in C_2$. For $i \in \{1, 2, \ldots, r\}$, let $b_i \in \{0, 1\}$ such that $D_{b_i}^{-1}(\mathbf{X}_i) \in E_1$ and $D_{1-b_i}^{-1}(\mathbf{X}_i) \in \overline{E}_1$, and $c_i \in \{0, 1\}$ such that $D_{c_i}^{-1}(\widehat{\mathbf{X}}_i) \in E_2$ and $D_{1-c_i}^{-1}(\widehat{\mathbf{X}}_i) \in \overline{E}_2$. Let u be the number of elements in the set $\{i : b_i + c_i = 1\}$, then $(D_{b_i}^{-1}(\mathbf{X}_i),\ D_{c_i}^{-1}(\widehat{\mathbf{X}}_i))$ such that $b_i + c_i = 1$ for $i = 1, 2, \ldots, r$, are u conjugate pairs shared by E_1 and E_2. Next we show there are no other conjugate pairs shared by E_1 and E_2. Let $(\mathbf{Y}, \widehat{\mathbf{Y}})$ be a conjugate pair shared by E_1 and E_2 with $\mathbf{Y} \in E_1$ and $\widehat{\mathbf{Y}} \in \overline{E}_2$, then $(D(\mathbf{Y}), D(\widehat{\mathbf{Y}}))$ is a conjugate pair shared by C_1 and C_2 with $D(\mathbf{Y}) \in C_1$ and $D(\widehat{\mathbf{Y}}) \in C_2$. Assume $(D(\mathbf{Y}), D(\widehat{\mathbf{Y}})) = (\mathbf{X}_i, \widehat{\mathbf{X}}_i)$ for some $i \in \{1, 2, \ldots, r\}$, then we have $(\mathbf{Y}, \widehat{\mathbf{Y}}) = (D_{b_i}^{-1}(\mathbf{X}_i), D_{c_i}^{-1}(\widehat{\mathbf{X}}_i))$ with $b_i + c_i = 1$. Therefore, E_1 and E_2 share exactly u conjugate pairs. Similarly, $(D_{1-b_i}^{-1}(\mathbf{X}_i),$ $D_{1-c_i}^{-1}(\widehat{\mathbf{X}}_i))$ such that $b_i + c_i = 1$ for $i = 1, 2, \ldots, r$, are the u conjugate pairs shared by $\overline{E}_1$ and $\overline{E}_2$, $(D_{b_i}^{-1}(\mathbf{X}_i), D_{1-c_i}^{-1}(\widehat{\mathbf{X}}_i))$ such that $b_i + c_i = 0$ for $i = 1, 2, \ldots, r$, are the $r-u$ conjugate pairs shared by E_1 and $\overline{E}_2$, and $(D_{1-b_i}^{-1}(\mathbf{X}_i), D_{c_i}^{-1}(\widehat{\mathbf{X}}_i))$ such that $b_i + c_i = 0$ for $i = 1, 2, \ldots, r$, are the $r-u$ conjugate pairs shared by $\overline{E}_1$ and E_2.

□

Note 1. *In the case 3 of Theorem 8, we just provide a general range $0 \le u \le r$, and it seems hard to investigate the relationship between the two parameters u and r. An example that explains this phenomenon can be found in [11].*

The conclusion in Theorem 8 is illustrated by the following graph.



5 The Adjacency Graphs of $\mathrm{FSR}((1+x)^4p(x))$ and $\mathrm{FSR}((1+x)^5p(x))$

For a linear Boolean function $f(x_0, x_1, \ldots, x_n) = a_0x_0 + a_1x_1 + \cdots + a_nx_n$, we associate it with a univariate polynomial $c(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}_2[x]$. Sometimes, it is convenient to use univariate polynomials instead of linear Boolean functions. Some results about LFSRs can be found in [5]. It is well known that, an LFSR generates m-sequences if and only if its characteristic polynomial is primitive [16]. For m-sequences, we have the famous shift-and-add property [16].

Lemma 4. *[12, 16] Let $\mathbf{s}$ be an 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 $\mathbf{s} + L^j(\mathbf{s}) = L^k(\mathbf{s})$. Furthermore, the mapping from $\{1, 2, \ldots, 2^n - 2\}$ to itself, $Z : j \mapsto k$, is a bijection.*

Let $p(x)$ be a primitive polynomial. The adjacency graphs of LFSRs with characteristic polynomial $(1 + x)^m p(x)$ for $m = 1, 2, 3$ were studied in [14], [8] and [11]. But there are no results for $m \ge 4$. In what follows, we deal with this problem for $m = 1, 2, 3, 4, 5$ step by step. We use $\mathbf{a} = (a_0, a_1, \ldots, a_{l-1})$ to denote the periodic sequence $\mathbf{a} = a_0a_1 \cdots , a_{l-1} \cdots$ with period l, and use $[\mathbf{a}]$ to denote the cycle $[a_0, a_1, \ldots, a_{l-1}]$. The period of $\mathbf{a}$ is denoted by $\mathrm{per}(\mathbf{a})$.

Lemma 5. *Let $p(x)$ be a primitive polynomial. Let $\mathbf{a} + \mathbf{s}$ be a sequence in $\mathrm{FSR}((1 + x)^m p(x))$, where $\mathbf{a} \in \mathrm{FSR}((1 + x)^m)$ and $\mathbf{s} \in \mathrm{FSR}(p(x))$ is an m-sequence. Then we have*

1. $\mathrm{per}(\mathbf{a} + \mathbf{s}) = \mathrm{per}(\mathbf{a})\mathrm{per}(\mathbf{s})$.
2. $\mathrm{W}([\mathbf{a} + \mathbf{s}]) \equiv \mathrm{W}([\mathbf{a}]) \bmod 2$.
3. $D^{-1}([\mathbf{a} + \mathbf{s}]) = \{[\mathbf{b} + \mathbf{s}] : \mathbf{b} \in D^{-1}([\mathbf{a}])\}$.

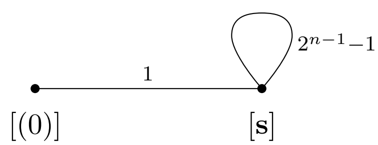
Proof. 1. Let $(1+x)^c$ be the minimal polynomial of $\mathbf{a}$, where $c \le m$. Then the period of $\mathbf{a}$ is 2^t, where t is the integer such that $2^{t-1} < c \le 2^t$. Since $\gcd((1+x)^c, p(x)) = 1$ and $\gcd(\mathrm{per}(\mathbf{a}), \mathrm{per}(\mathbf{s})) = 1$, we get $\mathrm{per}(\mathbf{a} + \mathbf{s}) = \mathrm{lcm}(\mathrm{per}(\mathbf{a}), \mathrm{per}(\mathbf{s})) = \mathrm{per}(\mathbf{a})\mathrm{per}(\mathbf{s})$.

2. Denote $\mathbf{a}$ and $\mathbf{s}$ by $\mathbf{a} = (a_0, a_1, \cdots, a_{2^t-1})$ and $\mathbf{s} = (s_0, s_1, \cdots, s_{2^n-2})$, where n is the degree of $p(x)$. Then we have, $W([\mathbf{a}+\mathbf{s}]) \equiv \left(\sum_{i=0}^{2^t-1} a_i + 2^t \cdot s_0\right) + \cdots + \left(\sum_{i=0}^{2^t-1} a_i + 2^t \cdot s_{2^n-2}\right) \equiv (2^n - 1) \cdot \sum_{i=0}^{2^t-1} a_i + 2^t \cdot \sum_{j=0}^{2^n-2} s_j \equiv \sum_{i=0}^{2^t-1} a_i \equiv \mathrm{W}([\mathbf{a}]) \bmod 2$.

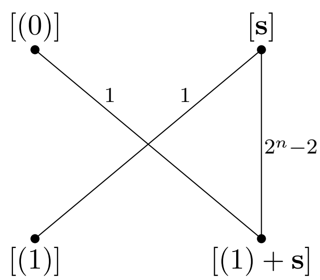
3. Let $[\mathbf{b}]$ be a cycle in $D^{-1}([\mathbf{a}])$. We need to show $D([\mathbf{b}+\mathbf{s}]) = [\mathbf{a}+\mathbf{s}]$. From $D([\mathbf{b}]) = [\mathbf{b}+L(\mathbf{b})] = [\mathbf{a}]$ we know, there exists some integer u such that $\mathbf{b}+L(\mathbf{b}) = L^u(\mathbf{a})$. According to Lemma 4, there exists some integer v such that $\mathbf{s}+L(\mathbf{s}) = L^v(\mathbf{s})$. From $\mathrm{per}(\mathbf{a}+\mathbf{s}) = \mathrm{per}(\mathbf{a})\mathrm{per}(\mathbf{s})$ we know, $[L^u(\mathbf{a})+L^v(\mathbf{s})] = [\mathbf{a}+\mathbf{s}]$. Then the proof can be done as follows: $D([\mathbf{b}+\mathbf{s}]) = [\mathbf{b}+\mathbf{s}+L(\mathbf{b}+\mathbf{s})) = [\mathbf{b}+L(\mathbf{b})+\mathbf{s}+L(\mathbf{s})] = [L^u(\mathbf{a})+L^v(\mathbf{s})] = [\mathbf{a}+\mathbf{s}]$.

□

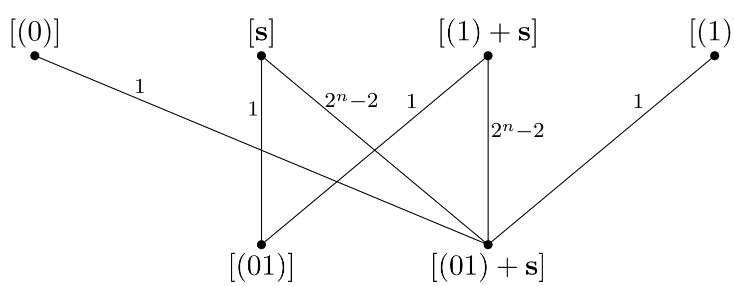
There are two cycles in FSR$(p(x))$, i.e., $[(0)]$ and $[\mathbf{s}]$, and they are even weight cycles. The adjacency graph of FSR$(p(x))$ is shown below.



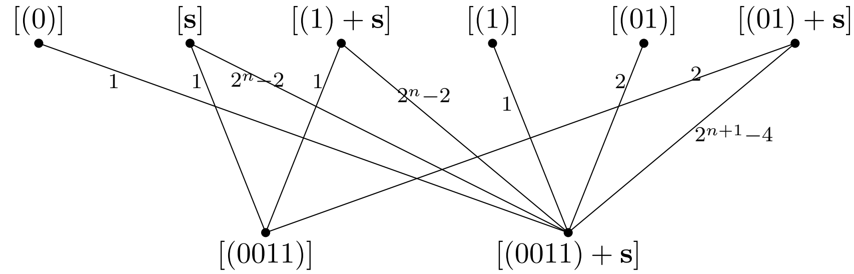
According to Lemma 5, $D^{-1}([(0)]) = \{[(0)], [(1)]\}$ and $D^{-1}([\mathbf{s}]) = D^{-1}([(0)+\mathbf{s}]) = \{[\mathbf{s}], [(1)+\mathbf{s}]\}$, therefore, there are four cycles in FSR$((1+x)p(x))$: $[(0)], [(1)], [\mathbf{s}], [(1)+\mathbf{s}]$. Since $W([(1)+\mathbf{s}]) \equiv W([(1)]) \equiv 1 \bmod 2$, the two cycles $[(0)]$ and $[\mathbf{s}]$ are of even weight, and the other two cycles are of odd weight. By Theorem 7, the adjacency graph of FSR$((1+x)p(x))$ is determined.



Similarly, we can calculate the cycles in FSR$((1+x)^2p(x))$: $[(0)], [(1)], [\mathbf{s}], [(1)+\mathbf{s}], [(01)], [(01)+\mathbf{s}]$. Since $W([(1)+\mathbf{s}]) \equiv W([(1)]) \equiv 1 \bmod 2$ and $W([(01)+\mathbf{s}]) \equiv W([(01)]) \equiv 1 \bmod 2$, the two cycles $[(0)]$ and $[\mathbf{s}]$ are of even weight, and the other four cycles are of odd weight. By Theorem 8, the adjacency graph of FSR$((1+x)^2p(x))$ is obtained.



In the same way, we get the adjacency graph of FSR($(1+x)^3p(x)$).



For the adjacency graph of FSR($(1+x)^4p(x)$), we have to deal with the parameter u in the case 3 of Theorem 8. In the following theorem we will solve this problem. The method we will use is suggested by Li et al. [12].

Theorem 9. *There are* 12 *cycles in* FSR($(1+x)^4p(x)$)*:* $[(0)]$, $[(1)]$, $[\mathbf{s}]$, $[(1)+\mathbf{s}]$, $[(01)+\mathbf{s}]$, $[(01)]$, $[(0011)+\mathbf{s}]$, $[(0011)]$, $[(0001)]$, $[(0111)]$, $[(0001)+\mathbf{s}]$, $[(0111)+\mathbf{s}]$. *Denote them by* $C_1, C_2, \cdots, C_{12}$ *respectively, then the number of conjugate pairs shared by these cycles is shown by the following two tables, where* $a = 2^n - 2$.

Table 1: In the case $[(0)]$ is adjacent with $[(0001)+\mathbf{s}]$

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
C_9	0	0	1	0	1	0	2	0
C_{10}	0	0	0	1	1	0	2	0
C_{11}	1	0	a	0	a	1	$2a$	2
C_{12}	0	1	0	a	a	1	$2a$	2

Table 2: In the case $[(0)]$ is adjacent with $[(0111)+\mathbf{s}]$

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
C_9	0	0	0	1	1	0	2	0
C_{10}	0	0	1	0	1	0	2	0
C_{11}	0	1	0	a	a	1	$2a$	2
C_{12}	1	0	a	0	a	1	$2a$	2

Proof. In order to deal with the parameter u in the case 3 of Theorem 8, we need to determine the numbers of conjugate pairs shared by

$$[(0)] \text{ and } [(0001)+\mathbf{s}],\ [\mathbf{s}] \text{ and } [(0001)],\ [\mathbf{s}] \text{ and } [(0001)+\mathbf{s}].$$

In the case $[(0)]$ is adjacent with $[(0001)+\mathbf{s}]$, since there is only one state in $[(0)]$, $[(0)]$ share 1 conjugate pair with $[(0001)+\mathbf{s}]$. In the following, we consider the number of conjugate pairs shared by $[\mathbf{s}]$ and $[(0001)]$, $[\mathbf{s}]$ 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 $[\mathbf{s}]$ as cycles of order $n+4$. There are two states $\mathbf{U}_0$ and $\mathbf{S}_0$ in $[(0001)]$ and $[\mathbf{s}]$ respectively such that:

$$\mathbf{U}_0 + \mathbf{S}_0 = \mathbf{E}, \tag{1}$$

which 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, we can assume $\mathbf{s} = (s_0 s_1 \cdots s_{2^n-2})$, where s_i is the first component of $\mathbf{S}_i$ for $i = 0, 1, \cdots, 2^n - 2$. According to Lemma 4, $\mathbf{s} + L^j(\mathbf{s}) = L^{Z(j)}(\mathbf{s})$, therefore, we have

$$\mathbf{S}_0 + \mathbf{S}_j = \mathbf{S}_{Z(j)}. \tag{2}$$

By combining the two state equations (1) and (2), we get

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

Since Z is a bijection on $\{1, 2, \ldots, 2^n - 2\}$, equation (3) means that the conjugate of $\mathbf{S}_j$ with $j \neq 0$ belongs to $[(0001) + \mathbf{s}]$. Therefore $[\mathbf{s}]$ shares 1 conjugate pair with $[(0001)]$ and shares $2^n - 2$ conjugate pairs with $[(0001) + \mathbf{s}]$.

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

The following example shows that, both of the two cases in Theorem 9 can happen.

Example 4. *Let* $p_1(x) = x^5 + x^4 + x^2 + x + 1$ *be a primitive polynomial and* $\mathbf{s}_1 = (0000111001101111101000100101011) \in G(p_1(x))$ *be an m-sequence, then* $[(0001) + \mathbf{s}_1] = [(\underline{100000000}11101000011111011111101011001101000111000011011100111001010101101111010010100010101111100110000100100101100010011 01)]$. *Therefore,* $[(0)]$ *is adjacent with* $[(0001) + \mathbf{s}_1]$ *in* $\mathrm{FSR}((1+x)^4 p_1(x))$.

Let $p_2(x) = x^5 + x^3 + x^2 + x + 1$ *be a primitive polynomial and* $\mathbf{s}_2 = (0000101101010001110111110010011) \in G(p_2(x))$ *be an m-sequence, then* $[(0111) + \mathbf{s}_2] = [(\underline{100000000}1011111011110010110111111001100011100100011111000010011010101000010100010110000111010100110010010011101101011010001)]$. *Therefore,* $[(0)]$ *is adjacent with* $[(0111) + \mathbf{s}_2]$ *in* $\mathrm{FSR}((1+x)^4 p_2(x))$.

The adjacency graph of $\mathrm{FSR}((1+x)^5 p(x))$ can be determined directly without being bothered by the parameter u in Theorem 8. By Lemma 5, there are 16 cycles in $\mathrm{FSR}((1+x)^5 p(x))$: $[(0)]$, $[(1)]$, $[(01)]$, $[\mathbf{s}]$, $[(1) + \mathbf{s}]$, $[(01) + \mathbf{s}]$, $[(0011) + \mathbf{s}]$, $[(0011)]$, $[(0001) + \mathbf{s}]$, $[(0111) + \mathbf{s}]$, $[(0001)]$, $[(0111)]$, $[(00001111)]$, $[(00101101)]$, $[(00001111) + \mathbf{s}]$, $[(00101101) + \mathbf{s}]$. Denote them by $D_1, D_2, \cdots, D_{16}$ respectively, then the number of conjugate pairs shared by these cycles is shown by the following two tables, where $a = 2^n - 2$.

Theorem 10. *Let* f_m *be the linear Boolean function corresponding to the polynomial* $(1+x)^m p(x)$. *If* $m = 2^t - 1$ *for some integer* t, $\mathrm{FSR}(f_m + 1)$ *contains only odd weight cycles; otherwise,* $\mathrm{FSR}(f_m + 1)$ *contains only even weight cycles.*

Proof. According to the theory of LFSRs, the number of cycles in $\mathrm{FSR}(f_m + 1)$ is $2^{m+1-\lceil \log(m+1) \rceil}$. By Theorem 6, the number of even weight cycles in $\mathrm{FSR}(f_m)$ is the same as the number of cycles in

Table 3: In the case $[(0)]$ is adjacent with $[(00001111)+\mathbf{s}]$

	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8	D_9	D_{10}	D_{11}	D_{12}
D_{13}	0	0	0	1	1	0	2	0	2	2	0	0
D_{14}	0	0	0	0	0	2	2	0	2	2	0	0
D_{15}	1	1	0	a	a	0	$2a$	2	$2a$	$2a$	2	2
D_{16}	0	0	2	0	0	$2a$	$2a$	2	$2a$	$2a$	2	2

Table 4: In the case $[(0)]$ is adjacent with $[(00101101)+\mathbf{s}]$

	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8	D_9	D_{10}	D_{11}	D_{12}
D_{13}	0	0	0	0	0	2	2	0	2	2	0	0
D_{14}	0	0	0	1	1	0	2	0	2	2	0	0
D_{15}	0	0	2	0	0	$2a$	$2a$	2	$2a$	$2a$	2	2
D_{16}	1	1	0	a	a	0	$2a$	2	$2a$	$2a$	2	2

$\mathrm{FSR}(f_m+1)$, therefore, there are $2^{m+1-\lceil\log(m+1)\rceil}$ even weight cycles in $\mathrm{FSR}(f_m)$. By this formula, the number of even weight cycles in $\mathrm{FSR}(f_{m+1})$ is $2^{m+2-\lceil\log(m+2)\rceil}$. Since $G(f_{m+1})=G(f_m)\cup G(f_m+1)$, the number of even weight cycles in $\mathrm{FSR}(f_m+1)$ is $2^{m+2-\lceil\log(m+2)\rceil}-2^{m+1-\lceil\log(m+1)\rceil}$. It can be verified that

$$2^{m+2-\lceil\log(m+2)\rceil}-2^{m+1-\lceil\log(m+1)\rceil}=\begin{cases}0 & \text{if } m=2^t-1 \text{ for some integer } t,\\ 2^{m+1-\lceil\log(m+1)\rceil} & \text{otherwise.}\end{cases}$$

This completes the proof. □

6 De Bruijn Sequences from $\mathrm{FSR}((1+x)^4p(x))$ and $\mathrm{FSR}((1+x)^5p(x))$

In this Section, two families of de Bruijn sequences are constructed from the LFSRs with characteristic polynomials $(1+x)^4p(x)$ and $(1+x)^5p(x)$, where $p(x)$ is a primitive polynomial of degree n. Since we are interested in de Bruijn sequences of large period, we assume n is a large integer.

The first construction is based on Theorem 9 where the adjacency graph of $\mathrm{FSR}((1+x)^4p(x))$ is given. There are 12 cycles in such an LFSR. The 12 cycles are divided into two classes according to their length. The cycles in the first class are called short cycles since there are a small number of states in them:

$$[(0)],[(1)],[(01)],[(0011)],[(0001)],[(0111)],$$

and the cycles in the second class are called long cycles:

$$[\mathbf{s}],[(1)+\mathbf{s}],[(01)+\mathbf{s}],[(0011)+\mathbf{s}],[(0001)+\mathbf{s}],[(0111)+\mathbf{s}].$$

According to Theorem 9, there are two possibilities for the adjacency graph of these LFSRs, depending on the position of the state $\mathbf{E}=(1,0,\dots,0)$ which may on the cycle $[(0001)+\mathbf{s}]$ or the cycle $[(0111)+\mathbf{s}]$. At first, we need to determine the location of $\mathbf{E}$.

Denote the four states in the short cycle $[(0001)]$ by $\mathbf{U}_0, \mathbf{U}_1, \mathbf{U}_2$ and $\mathbf{U}_3$. For $i = 0, 1, 2, 3$, let $\mathbf{X}_i$ be the state of length n obtained from the first n bits of the state $\mathbf{U}_i + \mathbf{E}$, and let $\mathbf{Y}_i$ be the first $n+4$ bits generated by the LFSR with characteristic polynomial $p(x)$ on the initial state $\mathbf{X}_i$. If $\mathbf{Y}_i = \mathbf{U}_i + \mathbf{E}$ for some $i \in \{0, 1, 2, 3\}$, then $\mathbf{E}$ is in the cycle $[(0001) + \mathbf{s}]$, otherwise, $\mathbf{E}$ is in the cycle $[(0111) + \mathbf{s}]$. This method can be carried in time $O(n)$, therefore, the adjacency graph of $\mathrm{FSR}((1+x)^4 p(x))$ can be determined easily. Without lose of generality, we always assume that Case 1 of Theorem 9 is satisfied in what follows.

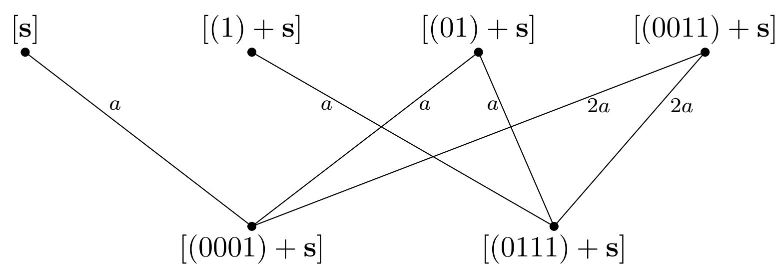
A class of maximum length FSRs can be constructed from these LFSRs using the cycle joining method. Let A be a set of states, in which there are no conjugate pairs. We use $I(A)$ to denote the Boolean function, which takes value 1 at the states in A and the states whose conjugate lies in A, and takes value 0 at the other points.

Theorem 11. *Let $f(x_0, x_1, \cdots, x_{n+4})$ be the Boolean function corresponding to $(1+x)^4 p(x)$. Choose a state from each short cycle randomly, and let A be the set of these states. Then the FSRs that take the following Boolean functions as their characteristic functions are maximum length FSRs.*

1. $g = f(x_0, x_1, \cdots, x_{n+4}) + I(\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \overline{\mathbf{X}}_3, \mathbf{X}_4) + I(A)$
2. $g = f(x_0, x_1, \cdots, x_{n+4}) + I(\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \mathbf{X}_4, \overline{\mathbf{X}}_4) + I(A)$

where $\mathbf{X}_1 \in [\mathbf{s}], \mathbf{X}_2 \in [(1) + \mathbf{s}], \mathbf{X}_3 \in [(01) + \mathbf{s}], \mathbf{X}_4 \in [(0011) + \mathbf{s}]$ are chosen randomly such that their conjugates are not in short cycles.

Proof. Regardless of the short cycles, the adjacency graph of $\mathrm{FSR}((1+x)^4 p(x))$ can be simplified as follows, where a denotes the number $2^n - 2$.



If we choose a state $\mathbf{X}_1$ from $[\mathbf{s}]$ whose conjugate is not in short cycles and change its successor with its conjugate, the two cycles $[\mathbf{s}]$ and $[(0001) + \mathbf{s}]$ are joined into one cycle. Similarly, by changing the successor of $\mathbf{X}_2$ with its conjugate, the two cycles $[(1) + \mathbf{s}]$ and $[(0111) + \mathbf{s}]$ are joined together, and by changing the successor of $\mathbf{X}_4$ with its conjugate, the two cycles $[(0011) + \mathbf{s}]$ and $[(0001) + \mathbf{s}]$ (or $[(0011) + \mathbf{s}]$ and $[(0111) + \mathbf{s}]$) are joined together. Since the conjugates of $\mathbf{X}_3$ and $\overline{\mathbf{X}}_3$ lie in $[(0001) + \mathbf{s}]$ and $[(0111) + \mathbf{s}]$ (or $[(0111) + \mathbf{s}]$ and $[(0001) + \mathbf{s}]$) respectively, by changing the successors of $\mathbf{X}_3$ and $\overline{\mathbf{X}}_3$ with their conjugates simultaneously, the three cycles $[(01) + \mathbf{s}]$, $[(0001) + \mathbf{s}]$ and $[(0111) + \mathbf{s}]$ are joined into a single one. Finally, considering the short cycles, if we choose a state from each short cycles and change their successors with their conjugates, all the six short cycles are joined to the long cycles. Therefore, the FSRs with characteristic function $f(x_0, x_1, \cdots, x_{n+4}) + I(\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \overline{\mathbf{X}}_3, \mathbf{X}_4) + I(A)$ are maximum length FSRs. Similarly, the FSRs with characteristic function $f(x_0, x_1, \cdots, x_{n+4}) + I(\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \mathbf{X}_4, \overline{\mathbf{X}}_4) + I(A)$ are also maximum length FSRs. □

To count the number of maximum length FSRs we have constructed, we need the following lemma which was proved in [9]

Lemma 6. *[9] For $n \geq 4$, if we apply the cycle joining method to two different n-stage LFSRs, the resulting de Bruijn sequences are different.*

The set A defined in Theorem 11 has $1 \cdot 1 \cdot 2 \cdot 4 \cdot 4 \cdot 4 = 128$ choices, the four states $\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \mathbf{X}_4$ have $a, a, 2a$ and $4a$ choices respectively, and the Boolean function f has $\phi(2^n - 1)/n$ choices where $\phi(\cdot)$ is the Euler's totient function. For the Boolean functions in Theorem 11 of type (1), replacing the state $\mathbf{X}_3$ by $\overline{\mathbf{X}}_3$ result in a same g, therefore, there are totally

$$\frac{128 \cdot a \cdot a \cdot 2a \cdot 4a \cdot \phi(2^n - 1)}{2n} = 512a^4\phi(2^n - 1)/n$$

functions of type (1). Similarly, there are totally $512a^4\phi(2^n - 1)/n$ functions of type (2). So the number of maximum length FSRs we have constructed from FSR($(1 + x)^4 p(x)$) is

$$\frac{1024(2^n - 2)^4\phi(2^n - 1)}{n} = O(2^{5n}).$$

In the following, we present an algorithm to generate the four states $\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \mathbf{X}_4$ satisfying the condition of Theorem 11 (takes $\mathbf{X}_3$ for example). This algorithm may fail at a negligible probability (given below). If it fails, we just need to run it again.

Algorithm 1 Generation of $\mathbf{X}_3$

1. Choose an n-stage state $\mathbf{X}$ randomly. Let $\mathbf{Y}$ be the first $n + 4$ bits generated by the LFSR with characteristic polynomial $p(x)$ on the initial state $\mathbf{X}$ (treat $\mathbf{Y}$ as an $(n+4)$-stage state).
2. Choose a state $\mathbf{U}$ from the short cycle [(01)] randomly.
3. If the state $\widehat{\mathbf{U}} + \mathbf{Y}$ lies in the short cycles, output "fail"; otherwise, output $\mathbf{U} + \mathbf{Y}$.

There are $2(2^n - 1)$ states in the cycle $[(01) + \mathbf{s}]$, of which there are two states whose conjugates are in short cycles. So the fail probability of the algorithm is $\varepsilon = \frac{1}{2^n - 1}$, which is negligible when n is big. The time complexity of this algorithm is $O(n)$ which is also the time we need to get a Boolean function in Theorem 11.

Another family of maximum length FSRs can be constructed from FSR($(1 + x)^5 p(x)$) using the same method. Divide the cycles in FSR($(1 + x)^5 p(x)$) into two classes according to their length. The cycles in the first class are called short cycles:

$$[(0)], [(1)], [(01)], [(0011)], [(0001)], [(0111)], [(00001111)], [(00101101)],$$

and the cycles in the second class are called long cycles:

$$[\mathbf{s}], [(1)+\mathbf{s}], [(01)+\mathbf{s}], [(0011)+\mathbf{s}], [(0001)+\mathbf{s}], [(0111)+\mathbf{s}], [(00001111)+\mathbf{s}], [(00101101)+\mathbf{s}].$$

The adjacency graph of FSR($(1+x)^5 p(x)$) has two possibilities, depending on the position of the state $\mathbf{E} = (1, 0, \ldots, 0)$ which may lies in either the cycle $[(00001111)+\mathbf{s}]$ or the cycle $[(00101101)+\mathbf{s}]$. We always assume the former case in what follows. Similar to Theorem 11 we have,

Theorem 12. *Let $f(x_0, x_1, \cdots, x_{n+5})$ be the Boolean function corresponding to $(1+x)^5 p(x)$. Choose a state from each short cycle randomly, and let A be the set of these states. Then the FSRs that take the following Boolean function as their characteristic functions are maximum length FSRs.*

1. $g = f(x_0, x_1, \cdots, x_{n+5}) + I(\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \mathbf{X}_4, \overline{\mathbf{X}}_4, \mathbf{X}_5, \mathbf{X}_6) + I(A)$
2. $g = f(x_0, x_1, \cdots, x_{n+5}) + I(\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \mathbf{X}_4, \mathbf{X}_5, \overline{\mathbf{X}}_5, \mathbf{X}_6) + I(A)$
3. $g = f(x_0, x_1, \cdots, x_{n+5}) + I(\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \mathbf{X}_4, \mathbf{X}_5, \mathbf{X}_6, \overline{\mathbf{X}}_6) + I(A)$

where $\mathbf{X}_1 \in [\mathbf{s}], \mathbf{X}_2 \in [(1)+\mathbf{s}], \mathbf{X}_3 \in [(01)+\mathbf{s}], \mathbf{X}_4 \in [(0011)+\mathbf{s}], \mathbf{X}_5 \in [(0001)+\mathbf{s}], \mathbf{X}_6 \in [(0111)+\mathbf{s}]$ are chosen randomly such that their conjugates are not in short cycles.

The time we need to get a Boolean function in Theorem 12 is $O(n)$. The number of maximum length FSRs we have constructed from FSR($(1+x)^5 p(x)$) is

$$\frac{1572864(2^n-2)^6 \phi(2^n-1)}{n} = O(2^{7n}).$$

7 Conclusion

Some properties about the FSRs with characteristic function of the form $g = (x_0 + x_1) * f$ are given in this paper. As an application of these result, we determine the adjacency graphs of LFSRs with characteristic polynomials $(1+x)^4 p(x)$ and $(1+x)^5 p(x)$ where $p(x)$ is a primitive polynomial. A large class of maximum length FSR are constructed from these LFSRs. For further research, more relations between the two parameters u and r in Theorem 8 need to be found.

References

[1] N. G. de Bruijn, "A combinatorial problem," Proc. Kon. Ned. Akad. Wetensch, vol. 49, pp. 758-746, 1946.

[2] T. Etzion and A. Lempel, "Algorithms for the generation of full-length shift-register sequences," IEEE Trans. Inf. Theory, vol. 30, no. 3, pp. 480-484, May 1984.

[3] H. Fredricksen, "A class of nonlinear de Bruijn cycles," J. Comb. Theory, Ser. A, vol. 19, no. 2, pp. 192-199, Sep. 1975.

[4] H. Fredricksen, "A survey of full length nonlinear shift register cycle algorithms," SIAM Rev., vol.24, no. 2, pp. 195-221, Apr. 1982.

[5] S. W. Golomb, Shift Register Sequences, San Francisco, CA: Holden-Day, 1967.

[6] D. H. Green and K. R. Dimond, "Nonlinear product-feedback shift registers," Proc. IEE, vol. 117, no. 4, pp. 681-686, Apr. 1970.

[7] E. R. Hauge and J. Mykkeltveit, "On the classification of deBruijn sequences," Discrete Math., vol. 148, no. 1, pp. 65-83, Jan. 1996.

[8] F. Hemmati, "A large class of nonlinear shift register sequences," IEEE Trans. Inf. Theory, vol. 28, no. 2, pp. 355-359, Mar. 1982.

[9] C. J. A. Jansen, W. G. Franx and D. E. Boekee, "An efficient algorithm for the generation of deBruijn cycles," IEEE Trans. Inf. Theory, vol. 37, no. 5, pp. 1475-1478, Sep. 1991.

[10] A. Lempel, "On a homomorphism of the de Bruijn graph and its applications to the design of feedback shift registers," IEEE Trans. computers, vol. 19, no. 12, pp. 1204-1209, Dec. 1970.

[11] C.Y. Li, X.Y. Zeng, T. Helleseth, C.L. Li and L. Hu, "The properties of a class of linear FSRs and their applications to the construction of nonlinear FSRs," IEEE Trans. Inf. Theory, vol. 60, no. 5, pp. 3052-3061, May 2014.

[12] C.Y. Li, X.Y. Zeng, C.L. Li, and T. Helleseth, "A Class of De Bruijn Sequences," IEEE Trans. Inf. Theory, vol. 60, no. 12, pp. 7955-7969, Dec. 2014.

[13] K. B. Magleby, "The synthesis of nonlinear feedback shift registers," Tech. Rep. 6207-1, Stanford Electronic Labs, Stanford, CA, 1963.

[14] J. Mykkeltveit, M. K. Siu and P. Tong, "On the cycle structure of some nonlinear shift register sequences," Inf. Contr., vol. 43, no. 2, pp. 202-215, Nov. 1979.

[15] T. Tian and W. F. Qi, "On the largest affine sub-families of a family of NFSR sequences," Des. Code Cryptogr., vol. 71, no. 1, pp. 163-181, Apr. 2014.

[16] N. Zierler, "Linear recurring sequences," J. Soc. Indust. Appl. Math., vol. 7, no. 1, pp. 31-48, Mar. 1959.