The Adjacency Graphs of Linear Feedback Shift Registers with Primitive-like Characteristic Polynomials

Ming Li and Dongdai Lin

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

March 10, 2016

Abstract

We consider the adjacency graphs of the linear feedback shift registers (LFSRs) with characteristic polynomials of the form $l(x)p(x)$, where $l(x)$ is a polynomial of small degree and $p(x)$ is a primitive polynomial. It is shown that, their adjacency graphs are closely related to the association graph of $l(x)$ and the cyclotomic numbers over finite fields. By using this connection, we give a unified method to determine their adjacency graphs. As an application of this method, we explicitly calculate the adjacency graphs of LFSRs with characteristic polynomials of the form $(1+x+x^3+x^4)p(x)$, 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. In cryptograph, they are the elementary component for designing stream ciphers [3, 12]. The periods of the output sequences of an n-stage FSR are no more than 2^n. If this value is attained, we call the output sequences De Bruijn sequences and the FSR maximum length FSR [2]. The state cycle in a maximum length FSR is called a full cycle, fot it contains all the n-length binary tuples. De Bruijn sequences have many favorable properties, such as long period, large linear span and good randomness, and they have important applications in cryptography and modern communication systems [4, 7]. It is well known that there are $2^{2^{n-1}-n}$ De Bruijn sequences of order n [2, 7]. Even though their size is very large, we can construct only a very small fraction of them efficiently by now [1, 5–7, 14, 15, 21].

A classical method to construct De Bruijn sequences (or maximum length FSRs) is to consider an FSR producing several cycles which are then joined together to form a full cycle. Such a method is called the cycle joining method proposed by Golomb [8]. For the application of this method, we need to know the distribution of the conjugate pairs in the cycles of the FSR, which is generally difficult to analyze. The distribution of the conjugate pairs in the cycles of an FSR is defined to be the adjacency graph of this FSR [11]. Until now, only some special linear feedback shift registers (LFSRs) have been totally analyzed about their adjacency graphs. At the earliest, the maximum length LFSRs (generating m-sequences) were analysed and used to construct De Bruijn sequences. Then the pure circulating registers and pure summing registers were also used [5]. Recently, some attentions have been paid to the LFSRs with characteristic polynomials $(1+x)^m p(x)$, $(1+x^m)p(x)$ and $p_1(x)p_2(x)\cdots p_k(x)$, where $p(x)$ and $p_i(x)$, $i=1,2,\ldots,k$, are primitive polynomial and m is a small positive integer [13, 16–18, 20]. Their adjacency graphs were determined and a large class of De Bruijn sequences were constructed from them.

It can be seen that, the characteristic polynomials of these FSRs whose adjacency graphs are known by now, take the form of $l(x)p(x)$, where $l(x)$ is polynomial of small degree and $p(x)$ is a primitive polynomial (of large degree). We may call these characteristic polynomials primitive-like polynomials, because they are obtained by multiplying a polynomial $l(x)$ of small degree to a primitive polynomial $p(x)$. Then it is well-reasoned to ask that: does there exist a unified method to deal with the adjacency graphs of the LFSRs with primitive-like characteristic polynomials, and not just to analyse them one by one? We will give a affirmative answer to this question, and present such a method in this paper. The solution to this question lies in the observation that their adjacency graphs have a intrinsic connection with the association graph of the LFSR with characteristic polynomial $l(x)$ (see the definition in Section 3). Our result is that, in the case of $\gcd(\mathrm{per}(l(x)), \mathrm{per}(p(x))) = 1$, the adjacency graph of $\mathrm{FSR}(l(x)p(x))$ can be determined directly from the association graph of $\mathrm{FSR}(l(x))$; otherwise, some cyclotomic numbers are needed additionally. As an application of this method, we calculate the adjacency graphs of the LFSRs with characteristic polynomials of the form $(1+x+x^3+x^4)p(x)$ and construct a large class of De Bruijn sequences from them. The properties of association graphs are also considered in this paper, and a sufficient condition for their uniqueness is given. By this condition, we show that some adjacency graphs are isomorphic.

The remainder of this paper is organized as follows. In Section 2, we introduce some necessary preliminaries. In Section 3, the definition of association graphs of LFSRs is given. Section 4 considers the cycle structure of LFSRs with primitive-like characteristic polynomials. Section 5 gives a unified method to determine their adjacency graphs. Section 6 provides applications of the unified method to the LFSRs with characteristic polynomials of the form $(1+x+x^3+x^4)p(x)$, and determines their adjacency graphs. In Section 7, a large number of De Bruijn sequences are constructed from these LFSRs, and we make a conclusion on this paper in Section 8.

2 Preliminaries

2.1 Feedback Shift Registers

Let $\mathbb{F}_2 = \{0, 1\}$ be the binary finite field, and $\mathbb{F}_2^n$ be the nth-dimensional vector space over $\mathbb{F}_2$. An n-variable Boolean function $f(x_0, x_1, \ldots, x_{n-1})$ is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.

An n-stage feedback shift register (FSR) consists of n binary storage cells and a feedback function F regulated by a single clock. The characteristic function of this FSR is defined to be $f = F + x_n$. The FSR with characteristic function f is denoted by FSR(f). At every clock pulse, the current state $(s_0, s_1, \ldots, s_{n-1})$ is updated by $(s_1, s_2, \ldots, s_{n-1}, F(s_0, s_1, \ldots, s_{n-1}))$ and the bit s_0 is outputted. The output sequences of FSR(f), denoted by $G(f)$, are the 2^n sequences $\mathbf{s} = s_0 s_1 \ldots$, satisfying $s_{t+n} = F(s_t, s_{t+1}, \ldots, s_{t+n-1})$, or equivalently $f(s_t, s_{t+1}, \ldots, s_{t+n}) = 0$, for any $t \geq 0$. It is shown by Golomb [8] that all sequences in $G(f)$ are periodic if and only if the characteristic function f is nonsingular, i.e., of the form $f = x_0 + f_0(x_1, \ldots, x_{n-1}) + x_n$. In the following discussion, all characteristic functions are assumed to be nonsingular.

We use $(s_0 s_1 \ldots s_{p-1})$ to denote the periodic sequence $\mathbf{s} = s_0 s_1 \ldots s_{p-1} \ldots$ with period p. The period of $\mathbf{s}$ is denoted by per($\mathbf{s}$). We define the left shift operator L on periodic sequences by $L^i(\mathbf{s}) = (s_i s_{i+1} \ldots s_{i-1})$, where the subscripts are taken modulo p. Two periodic sequences $\mathbf{s}_1$ and $\mathbf{s}_2$ are called shift-equivalent if there exists an integer r such that $\mathbf{s}_1 = L^r \mathbf{s}_2$. The set $G(f)$ are partitioned into equivalent classes $G(f) = [\mathbf{s}_1] \cup [\mathbf{s}_2] \cup \cdots \cup [\mathbf{s}_k]$ such that two sequences are in the same equivalent class if and only if they are shift equivalent. Each equivalent class is called a cycle of FSR(f), and the partition is called the cycle structure of FSR(f). A cycle $[(s_0, s_1, \ldots, s_{p-1})]$ can also be represented using the state cycle form $[\mathbf{S}_0, \mathbf{S}_1, \ldots, \mathbf{S}_{p-1}]$, where $\mathbf{S}_i = (s_i, s_{i+1}, \ldots, s_{i+n-1})$ for $0 \leq i \leq p-1$, and the subscribes are taken modulo p. The state $\mathbf{S}_i$ is just the state of the FSR at the moment that the bit s_i is ready to be outputted.

An FSR is called a linear feedback shift register (LFSR) if its characteristic function f is linear [22]. For a linear Boolean function $f(x_0, x_1, \ldots, x_n) = a_0 x_0 + a_1 x_1 + \cdots + a_n x_n$, we can associate it with an univariate polynomial $l(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}_2[x]$. Most of the time, we do not discriminate between linear Boolean functions and univariate polynomials. And for convenience, we sometimes use FSR($l(x)$) to denote the LFSR with characteristic function $f(x)$. For an n-stage FSR, the periods of its output sequences are no more than 2^n. If this value is attained, we call the sequences De Bruijn sequences, and call the FSR maximum length FSR. The unique cycle in a maximum-length FSR is called full cycle. For an n-stage LFSR, the periods of its output sequences are no more than $2^n - 1$. If this value is attained, we call the sequences m-sequences, and call the FSR maximum length LFSR. It is known that, FSR($l(x)$) is a maximum length LFSR if and only if $l(x)$ is primitive, that is, the period of $l(x)$, denoted by per($l(x)$), is $2^n - 1$.

2.2 Adjacency Graphs

For a state $\mathbf{S} = (s_0, s_1, \ldots, s_{n-1})$, its conjugate is defined to be the state $\widehat{\mathbf{S}} = (\overline{s}_0, s_1, \ldots, s_{n-1})$, where $\overline{s}_0$ is the binary complement of s_0. Two cycles C_1 and C_2 are said to be adjacent if there exists a conjugate pair $(\mathbf{S}, \widehat{\mathbf{S}})$ such that the state $\mathbf{S}$ is on C_1 while its conjugate $\widehat{\mathbf{S}}$ is on C_2. Conjugate pairs can be used to join cycles. For two cycles C_1 and C_2 that share a conjugate pair $(\mathbf{S}, \widehat{\mathbf{S}})$, we can join the two cycles into one cycle by interchanging the successors of $\mathbf{S}$ and $\widehat{\mathbf{S}}$. This is the basic idea of the cycle joining method that proposed by Golomb. For the application of the cycle joining method, we need to find out the location of conjugate pairs shared by cycles. This leads us to the definition of adjacency graph.

Definition 1. *[11, 19] 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 $m > 0$ between two vertexes if and only if the two vertexes share m conjugate pairs.*

For any FSR, its adjacency graph is a connected graph, that is, we can always join the cycles in this FSR into a full cycle. This fact follows from the statement in [7]: C is a full 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 (see Figure 6) 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., a full cycle. Therefore, for a given FSR, the number of full cycles that we can get from it by using the cycle joining method, is equal to the number of maximum spanning trees of its adjacency graph.

Let C_1 and C_2 be two cycles in FSR(f), and $(\mathbf{S}, \widehat{\mathbf{S}})$ be a conjugate pair shared by the two cycles. By interchanging the predecessors of the two states $\mathbf{S}$ and $\widehat{\mathbf{S}}$ the two cycles C_1 and C_2 are joined together. Since the cycle structure of FSR(f) is changed, we get a new FSR. The characteristic function of the new FSR can be expressed in terms of the function f and the state $\mathbf{S}$. For convenience, we introduce a notation firstly. Let A be a set of states, in which there are no conjugate pairs. We use $I(A)$ to denote the Boolean function in variables $x_0, x_1, \ldots, x_{n-1}$, 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. Using this notation, the characteristic function of the new FSR is given by $f' = f + I(\mathbf{S})$.

2.3 Cyclotomic Numbers

Let $\mathbb{F}_{2^n}$ be the finite field of 2^n elements, and α be a primitive element in $\mathbb{F}_{2^n}$. The field $\mathbb{F}_{2^n}$ can be expressed as $\mathbb{F}_{2^n} = \{0, \alpha^0, \alpha^1, \ldots, \alpha^{2^n-2}\}$. Let $d \geq 1$ be a divisor of $2^n - 1$. The cyclotomic classes $C_0, C_1, \ldots, C_{d-1}$ of $\mathbb{F}_{2^n}$ are defined by $C_i = \{\alpha^{i+jd} \mid 0 \leq j \leq \frac{2^n-1}{d} - 1\}$ for $0 \leq i \leq d-1$. For two integers l and m with $0 \leq l, m \leq d-1$, the cyclotomic number $(l, m)_d$ over $\mathbb{F}_{2^n}$ is defined as the number of elements $x \in C_l$ such that $1 + x \in C_m$. It should be noted that, the cyclotomic number $(l, m)_d$ is not a fixed number for given l, m, d and n, but affected by the primitive element

α, that is, different primitive elements may give different cyclotomic numbers. We refer the reader to [9, 17] for more details.

Define $J = \{0, 1, \ldots, 2^n - 2\}$ and $J^* = J \setminus \{0\}$. Let Z be a mapping from J^* to itself such that $1 + \alpha^j = \alpha^{Z(j)}$. Then Z is a permutation of J^*. Similar to the cyclotomic numbers, the mapping Z is also affected by the primitive element α. A connection between the cyclotomic number $(l, m)_d$ and the mapping Z is that: $(l, m)_d = |\{(j, Z(j)) \mid j \equiv l(\mathrm{mod} d), Z(j) \equiv m(\mathrm{mod} d), j \in J^*\}|$.

In the case that n is an even number, we have $3|2^n - 1$. The cyclotomic numbers of order 3 over $\mathbb{F}_{2^n}$ are fixed numbers (means that they are not affected by the primitive element α), and they are given in the following lemma.

Lemma 1. *[9, 10, 17] The cyclotomic numbers of order* 3 *over finite field* $\mathbb{F}_{2^n}$ *are given by* $(0, 0)_3 = A, (0, 1)_3 = (1, 0)_3 = (2, 2)_3 = B, (0, 2)_3 = (2, 0)_3 = (1, 1)_3 = C$ *and* $(1, 2)_3 = (2, 1)_3 = D$, *where* $A = \frac{2^n + (-2)^{\frac{n}{2}+1} - 8}{9}$, $B = C = \frac{2^n + (-2)^{\frac{n}{2}} - 2}{9}$, *and* $D = \frac{2^n + (-2)^{\frac{n}{2}+1} + 1}{9}$.

Let $p(x)$ be a primitive polynomial of degree n, and $M_{n \times n}$ be the companion matrix of $p(x)$. By the linear algebra theory, we have $p(M) = \mathbb{O}$, where $\mathbb{O}$ is the 0×0 zero matrix. Since $p(x)$ is a primitive polynomial of degree n over $\mathbb{F}_2$, the ring $\mathbb{F}_2[M]$ is isomorphic to the field $\mathbb{F}_{2^n}$. This isomorphism gives $I_n + M^j = M^{Z(j)}$. Let $\mathbf{s} = (s_0, s_1, \ldots, s_{2^n-2})$ be an m-sequence in $G(p(x))$. Write $\mathbf{s}$ in the state form: $\mathbf{s} = (\mathbf{S}_0, \mathbf{S}_1, \ldots, \mathbf{S}_{2^n-2})$, where $\mathbf{S}_i = (s_i, s_{i+1}, \ldots, s_{i+n-1})$ for $0 \leq i \leq 2^n - 2$, and the subscribes are taken modulo $2^n - 1$. Then we have $\mathbf{S}_i = \mathbf{S}_0 M^i$ for $0 \leq i \leq 2^n - 2$, Remember that $I_n + M^j = M^{Z(j)}$, we get that $\mathbf{S}_0(I_n + M^j) = \mathbf{S}_0 M^{Z(j)}$, which implies $\mathbf{S}_0 + \mathbf{S}_j = \mathbf{S}_{Z(j)}$. Therefore, we get the equation $\mathbf{s} + L^j \mathbf{s} = L^{Z(j)} \mathbf{s}$.

3 The Association Graphs of LFSRs

In this section, we give the definition of association graphs of LFSRs. Some examples are presented to illustrate the meaning of this definition. Let $\mathbf{a} = a_0, a_1, \ldots, a_i, \ldots$ and $\mathbf{b} = b_0, b_1, \ldots, b_i, \ldots$ be two sequences, and c be an element in $\mathbb{F}_2$. The sum of the two sequences $\mathbf{a} + \mathbf{b}$ and the scalar product $c \cdot \mathbf{a}$ are defined to be $\mathbf{a} + \mathbf{b} = a_0 + b_0, a_1 + b_1, \ldots, a_i + b_i, \ldots$, and $c \cdot \mathbf{a} = ca_0, ca_1, \ldots, ca_i, \ldots$. Let $l(x) \in \mathbb{F}_2[x]$ be a polynomial of degree m. Then there are 2^m sequences in the set $G(l(x))$. It is well known that, the set $G(l(x))$ is a vector space of dimension m over $\mathbb{F}_2$ when endowed with the two operations $+$ and $\cdot$ defined above.

Let $\mathbf{u}$ be a sequence in $G(l(x))$. Because $< G(l(x)), + >$ is a group, the mapping from $G(l(x))$ to itself:

$$\gamma_{\mathbf{u}} : \mathbf{a} \mapsto \mathbf{u} + \mathbf{a}$$

is a bijection. We note that, the bijection $\gamma_{\mathbf{u}}$ is not necessarily preserve the shift equivalent property, that is, for two shit equivalent sequences $\mathbf{a}$ and $\mathbf{b}$, their images $\gamma_{\mathbf{u}}(\mathbf{a})$ and $\gamma_{\mathbf{u}}(\mathbf{b})$ may not be shift equivalent. Therefore, two sequences in a same cycle of $G(l(x))$ may be mapped into different cycles. This lead us to the following definition.

Definition 2. *Let* $\mathbf{u}$ *be a sequence in* $G(l(x))$*,* $[\mathbf{v}]$ *and* $[\mathbf{w}]$ *be two cycles (may be the same) in* $G(l(x))$*. The association number of* $[\mathbf{v}]$ *and* $[\mathbf{w}]$ *with respect to* $\mathbf{u}$ *is defined by*

$$R_{\mathbf{u}}([\mathbf{v}],[\mathbf{w}]) = \left|\left\{(i,j) \mid L^i\mathbf{v} + L^j\mathbf{w} = \mathbf{u}, {}^{0\leq i\leq \mathrm{per}(\mathbf{v})-1}_{0\leq j\leq \mathrm{per}(\mathbf{w})-1}\right\}\right|.$$

It is easy to see that, the association number of $[\mathbf{v}]$ and $[\mathbf{w}]$ is exactly the number of sequences in $[\mathbf{v}]$ whose image under $\gamma_{\mathbf{u}}$ is located in the cycle $[\mathbf{w}]$. In another word, $R_{\mathbf{u}}([\mathbf{v}],[\mathbf{w}]) = |\{(\mathbf{a},\mathbf{b}) \mid \mathbf{a}+\mathbf{b} = \mathbf{u}, \mathbf{a} \in [\mathbf{v}], \mathbf{b} \in [\mathbf{w}]\}|$. An example of $\gamma_{\mathbf{u}}$, when $l(x) = 1 + x + x^3 + x^4$ and $\mathbf{u} = (000111)$, is given, see Figure 1. The cycle structure of this LFSR is $G(l(x)) = [(0)] \cup [(000111)] \cup [(001)] \cup [(01)] \cup [(011) \cup [(1)]]$.

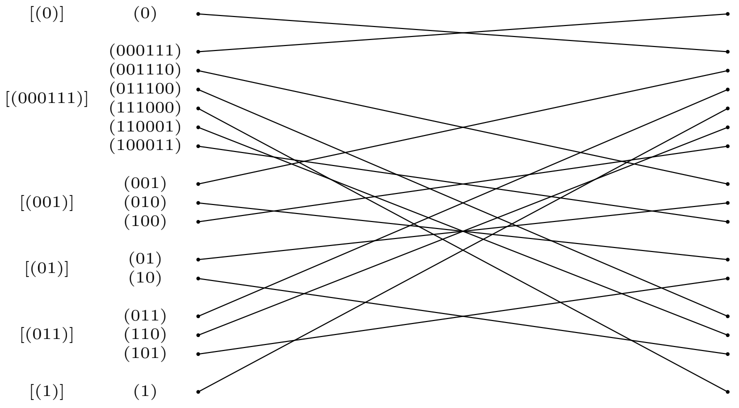

Figure 1: The mapping $\gamma_{\mathbf{u}}$ on $G(1 + x + x^3 + x^4)$, where $\mathbf{u} = (000111)$

According to Figure 1, the unique sequence in the cycle $[(0)]$ is mapped into the cycle $[(000111)]$, therefore, $R_{\mathbf{u}}([(0)],[(000111)]) = 1$. Two sequences in the cycle $[(001)]$ are mapped into the cycle $[(000111)]$, and one sequence is mapped into the cycle $[(01)]$, therefore, $R_{\mathbf{u}}([(001)],[(000111)]) = 2$ and $R_{\mathbf{u}}([(001)],[(01)]) = 1$. The other association numbers can be calculated similarly. We present their values as follows: $R_{\mathbf{u}}([(1)],[(000111)]) = R_{\mathbf{u}}([(01)],[(011)]) = 1$ and $R_{\mathbf{u}}([(011)],[(000111)]) = 2$. We can use a graph to characterise these relations of the cycles in $G(l)$. It is obvious that, these relations are influenced by the sequence $\mathbf{u}$.

Definition 3. *Let* $\mathbf{u}$ *be a sequence in* $G(l(x))$*. The association graph of* $\mathrm{FSR}(l(x))$ *with respect to* $\mathbf{u}$ *is an undirected graph, where the vertexes correspond to the cycles in* $G(l(x))$*, and there is an edge labeled with* $R_{\mathbf{u}}([\mathbf{v}],[\mathbf{w}])$ *between two vertices* $[\mathbf{v}]$ *and* $[\mathbf{w}]$*.*

Example 1. *Let* $l(x) = 1 + x + x^3 + x^4$*. The cycle structure of* $\mathrm{FSR}(l(x))$ *is* $G(l(x)) = [(0)] \cup [(000111)] \cup [(001)] \cup [(01)] \cup [(011) \cup [(1)]]$*. The association graph of* $\mathrm{FSR}(l(x))$ *with respect to* $\mathbf{u} = (000111)$ *is shown in Figure 2.*

The property of association graphs will be discussed further in Section 6. It appears to us that, there are no efficient methods to get the association graph for a given $l(x)$. In this paper, we assume that the association graph is calculated using the exhaustive search method, that is, $O(2^m)$ time is needed to obtain the association graph, where m is the degree of $l(x)$.

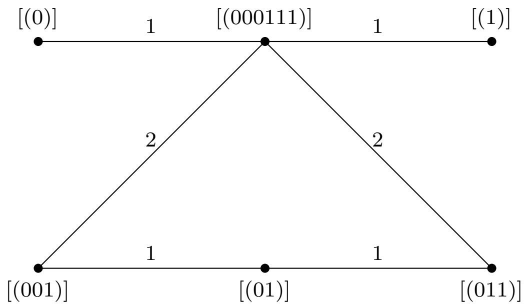

Figure 2: The association graph of $\text{FSR}(1 + x + x^3 + x^4)$ with respect to (000111)

4 The Cycle Structure of $\text{FSR}(l(x)p(x))$

In this section we determine the cycle structure of $\text{FSR}(l(x)p(x))$, where $l(x)$ is a polynomial and $p(x)$ is a primitive polynomial. For a periodic sequence $\mathbf{a}$, we use $[\mathbf{a}]$ to denote the cycle $[\mathbf{a}] = \{\mathbf{a}, L\mathbf{a}, \ldots, L^{\text{per}(\mathbf{a})-1}\mathbf{a}\}$. The sum of two cycles $[\mathbf{a}]$ and $[\mathbf{b}]$ is defined to be $[\mathbf{a}] + [\mathbf{b}] = \{\mathbf{s} + \mathbf{t} \mid \mathbf{s} \in [\mathbf{a}], \mathbf{t} \in [\mathbf{b}]\}$.

Lemma 2. *Let $\mathbf{u}$ and $\mathbf{s}$ be two periodic sequences such that their minimal polynomials are co-prime. Let $d = \gcd(\text{per}(\mathbf{u}), \text{per}(\mathbf{s}))$. Then $[\mathbf{u}] + [\mathbf{s}] = [\mathbf{u} + \mathbf{s}] \cup [L\mathbf{u} + \mathbf{s}] \cup \cdots \cup [L^{d-1}\mathbf{u} + \mathbf{s}]$. In particular, when $\gcd(\text{per}(\mathbf{u}), \text{per}(\mathbf{s})) = 1$, we have $[\mathbf{u}] + [\mathbf{s}] = [\mathbf{u} + \mathbf{s}]$.*

Proof. We first show that, $[L^i\mathbf{u} + \mathbf{s}] \subset [\mathbf{u}] + [\mathbf{s}]$ for any $0 \leq i \leq d - 1$. Let $\mathbf{a}$ be a sequence in $[L^i\mathbf{u} + \mathbf{s}]$. We can assume $\mathbf{a} = L^j(L^i\mathbf{u} + \mathbf{s})$ for some integer j. Then $\mathbf{a} = L^{i+j}\mathbf{u} + L^j\mathbf{s}$. Since $L^{i+j}\mathbf{u} \in [\mathbf{u}]$ and $L^j\mathbf{s} \in [\mathbf{s}]$, the sequence $\mathbf{a}$ belongs to $[\mathbf{u}] + [\mathbf{s}]$.

In the following we show that, for any sequence $\mathbf{a} \in [\mathbf{u}] + [\mathbf{s}]$, it always belongs to some cycle $[L^i\mathbf{u} + \mathbf{s}]$ for $0 \leq i \leq d - 1$. Since $\mathbf{a}$ is a sequence in $[\mathbf{u}] + [\mathbf{s}]$, we can assume $\mathbf{a} = L^j\mathbf{u} + L^k\mathbf{s}$. Write $j - k = qd + r$ where $0 \leq r \leq d - 1$. Because $d = \gcd(\text{per}(\mathbf{u}), \text{per}(\mathbf{s}))$, there exists two integers x and y such that $x\text{per}(\mathbf{u}) + y\text{per}(\mathbf{s}) = d$. Then $qy\text{per}(\mathbf{s}) \equiv qd(\text{modper}(\mathbf{u}))$, and $\mathbf{a} = L^j\mathbf{u} + L^k\mathbf{s} = L^k(L^{j-k}\mathbf{u} + \mathbf{s}) = L^{k+qy\text{per}(\mathbf{s})}(L^{j-k-qy\text{per}(\mathbf{s})}\mathbf{u} + L^{-qy\text{per}(\mathbf{s})}\mathbf{s}) = L^{k+qy\text{per}(\mathbf{s})}(L^{j-k-qy\text{per}(\mathbf{s})(\bmod \text{per}(\mathbf{u}))}\mathbf{u} + L^{-qy\text{per}(\mathbf{s})(\bmod \text{per}(\mathbf{s}))}\mathbf{s}) = L^{k+qy\text{per}(\mathbf{s})}(L^{j-k-qd}\mathbf{u} + \mathbf{s}) = L^{k+qy\text{per}(\mathbf{s})}(L^r\mathbf{u} + \mathbf{s}) \in [L^r\mathbf{u} + \mathbf{s}]$. □

By using Lemma 2, the cycle structure of $\text{FSR}(l(x)p(x))$ can be characterised by the cycle structure of $\text{FSR}(l(x))$ and $\text{FSR}(p(x))$. Our discussions are divided into two cases depending on whether $\gcd(\text{per}(l(x)), \text{per}(p(x))) = 1$ or not.

Theorem 1. *Let $l(x)$ be a polynomial, and $p(x)$ be a primitive polynomial such that $p(x) \nmid l(x)$. Let $G(l(x)) = [\mathbf{u}] \cup [\mathbf{v}] \cup \cdots \cup [\mathbf{w}]$ be the cycle structure of $\text{FSR}(l(x))$, and $G(p(x)) = [\mathbf{0}] \cup [\mathbf{s}]$ be the cycle structure of $\text{FSR}(p(x))$, where $\mathbf{s}$ is a m-sequence in $G(p(x))$. Then we have,*

1. *In the case of $\gcd(\text{per}(l(x)), \text{per}(p(x))) = 1$, the cycle structure of $\text{FSR}(l(x)p(x))$ is given by*

$$G(l(x)p(x)) = [\mathbf{u}] \cup [\mathbf{v}] \cup \cdots \cup [\mathbf{w}] \cup [\mathbf{u} + \mathbf{s}] \cup [\mathbf{v} + \mathbf{s}] \cup \cdots [\mathbf{w} + \mathbf{s}].$$

2. In the case of $\gcd(\mathrm{per}(l(x)),\mathrm{per}(p(x)))\neq 1$*, the cycle structure of* $\mathrm{FSR}(l(x)p(x))$ *is given by*

$$G(l(x)p(x))=[\mathbf{u}]\cup[\mathbf{v}]\cup\cdots\cup[\mathbf{w}]\cup\left(\bigcup_{i=0}^{d_{\mathbf{u}}-1}[L^i\mathbf{u}+\mathbf{s}]\right)\cup\left(\bigcup_{i=0}^{d_{\mathbf{v}}-1}[L^i\mathbf{v}+\mathbf{s}]\right)\cup\cdots\cup\left(\bigcup_{i=0}^{d_{\mathbf{w}}-1}[L^i\mathbf{w}+\mathbf{s}]\right),$$

where $d_{\mathbf{u}}=\gcd(\mathrm{per}(\mathbf{u}),\mathrm{per}(\mathbf{s})), d_{\mathbf{v}}=\gcd(\mathrm{per}(\mathbf{v}),\mathrm{per}(\mathbf{s}))$*, …, and* $d_{\mathbf{w}}=\gcd(\mathrm{per}(\mathbf{w}),\mathrm{per}(\mathbf{s}))$.

Proof. Since $p(x)$ is irreducible and $p(x)\nmid l(x)$, the two polynomials $l(x)$ and $p(x)$ are co-prime. By the theory of LFSRs, we have $G(l(x)p(x))=G(l(x))+G(p(x))$. Using the fact $G(l(x))=[\mathbf{u}]\cup[\mathbf{v}]\cup\cdots[\mathbf{w}]$ and $G(p(x))=[\mathbf{0}]\cup[\mathbf{s}]$, we get that $G(l(x)p(x))=([\mathbf{u}]\cup[\mathbf{v}]\cup\cdots\cup[\mathbf{w}])+([\mathbf{0}]\cup[\mathbf{s}])=(([\mathbf{u}]\cup[\mathbf{v}]\cup\cdots\cup[\mathbf{w}])+[\mathbf{0}])\cup(([\mathbf{u}]\cup[\mathbf{v}]\cup\cdots\cup[\mathbf{w}])+[\mathbf{s}])=([\mathbf{u}]\cup[\mathbf{v}]\cup\cdots\cup[\mathbf{w}])\cup(([\mathbf{u}]\cup[\mathbf{v}]\cup\cdots\cup[\mathbf{w}])+[\mathbf{s}])=[\mathbf{u}]\cup[\mathbf{v}]\cup\cdots\cup[\mathbf{w}]\cup([\mathbf{u}]+[\mathbf{s}])\cup([\mathbf{v}]+[\mathbf{s}])\cup\cdots\cup([\mathbf{w}]+[\mathbf{s}])$.

If $\gcd(\mathrm{per}(l(x)),\mathrm{per}(p(x)))=1$, then for any two sequences $\mathbf{a}\in G(l(x))$ and $\mathbf{b}\in G(p(x))$ we have $\gcd(\mathrm{per}(\mathbf{a}),\mathrm{per}(\mathbf{b}))=1$, and by Lemma 2, $[\mathbf{a}]+[\mathbf{b}]=[\mathbf{a}+\mathbf{b}]$. Therefore, $G(l(x)p(x))=[\mathbf{u}]\cup[\mathbf{v}]\cup\cdots\cup[\mathbf{w}]\cup([\mathbf{u}]+[\mathbf{s}])\cup([\mathbf{v}]+[\mathbf{s}])\cup\cdots\cup([\mathbf{w}]+[\mathbf{s}])=[\mathbf{u}]\cup[\mathbf{v}]\cup\cdots\cup[\mathbf{w}]\cup[\mathbf{u}+\mathbf{s}]\cup[\mathbf{v}+\mathbf{s}]\cup\cdots\cup[\mathbf{w}+\mathbf{s}]$.

If $\gcd(\mathrm{per}(l(x)),\mathrm{per}(p(x)))\neq 1$, then it is not necessarily that $\gcd(\mathrm{per}(\mathbf{a}),\mathrm{per}(\mathbf{b}))=1$ for any two sequences $\mathbf{a}\in G(l(x))$ and $\mathbf{b}\in G(p(x))$. Assume $\gcd(\mathrm{per}(\mathbf{a}),\mathrm{per}(\mathbf{b}))=d$, then by Lemma 2, $[\mathbf{a}]+[\mathbf{b}]=\bigcup_{i=0}^{d-1}[L^i\mathbf{a}+\mathbf{b}]$. Using this fact, we get that $G(l(x)p(x))=[\mathbf{u}]\cup[\mathbf{v}]\cup\cdots\cup[\mathbf{w}]\cup\left(\bigcup_{i=0}^{d_{\mathbf{u}}-1}[L^i\mathbf{u}+\mathbf{s}]\right)\cup\left(\bigcup_{i=0}^{d_{\mathbf{v}}-1}[L^i\mathbf{v}+\mathbf{s}]\right)\cup\cdots\cup\left(\bigcup_{i=0}^{d_{\mathbf{w}}-1}[L^i\mathbf{w}+\mathbf{s}]\right)$. □

5 The Adjacency Graph of $\mathrm{FSR}(l(x)p(x))$

In this section, we consider the adjacency graph of $\mathrm{FSR}(l(x)p(x))$, where $l(x)$ is a polynomial and $p(x)$ is a primitive polynomial. We always assume $p(x)\nmid l(x)$. Let $\mathbf{a}$ be the sequence generated by $\mathrm{FSR}(l(x)p(x))$ with initial state $(1,0,\dots,0)$. Since the two polynomials $l(x)$ and $p(x)$ are co-prime, by the theory of LFSR, there is a unique pair $(\mathbf{u}\in G(l(x)),\mathbf{s}\in G(p(x)))$ such that $\mathbf{u}+\mathbf{s}=\mathbf{a}$. The sequence $\mathbf{u}$ is called the representative of $G(l(x))$ determined by $p(x)$. We should note that, the representative of $G(l(x))$ relies on the choice of $p(x)$. Different $p(x)$ may result in different representatives.

Suppose $\deg l(x)=m$ and $\deg p(x)=n$. We can obtain the representative of $G(l(x))$ in time $O(2^m+n)$, see Algorithm 1. In this algorithm, we use $\mathrm{FSR}(l(x),\mathbf{S})$ to denote the sequence generated by $\mathrm{FSR}(l(x))$ with initial state $\mathbf{S}$, and $\mathbf{U}|_k$ to denote the first k bits of the bit string $\mathbf{U}$.

Once the representative of $G(l(x))$ is obtained, we can calculate the association graph of $G(l(x))$ with respect to its representative. By the discussion at the end of Section 3, this work can be done in time $O(2^m)$. We assume that m is a small positive integer, for example, $m<30$. Then an ordinary computer can do the work. With the message of the association graph of $G(l(x))$, the adjacency graph of $G(l(x)p(x))$ can be determined. Our discussions are divided into two cases, the case of $\gcd(\mathrm{per}(l(x)),\mathrm{per}(p(x)))=1$ and the case of $\gcd(\mathrm{per}(l(x)),\mathrm{per}(p(x)))\neq 1$. The former case is relatively easy to tackle. For the latter case, some cycolotomic numbers are needed to fully determine the adjacency graph.

Algorithm 1 Generation of the representative of $G(l(x))$ determined by $p(x)$

```
Input: The two polynomials $l(x)$ and $p(x)$.
Output: The representative of $G(l(x))$ determined by $p(x)$.
for $\mathbf{S} \in \mathbb{F}_2^m$ do
    $\mathbf{T} \leftarrow \mathrm{FSR}(l(x), \mathbf{S})|_{m+n}$
    $\mathbf{U} \leftarrow \mathbf{T} + (1, 0, \ldots, 0)$
    $\mathbf{U_0} \leftarrow \mathbf{U}|_n$
    if $\mathbf{U} = \mathrm{FSR}(p(x), \mathbf{U_0})|_{m+n}$ then
        $\mathbf{u} \leftarrow \mathrm{FSR}(l(x), \mathbf{S})$
    end if
end for
return $\mathbf{u}$
```

5.1 In the case of $\gcd(\mathrm{per}(l(x)), \mathrm{per}(p(x))) = 1$

In this subsection, we consider the adjacency graph of $\mathrm{FSR}(l(x)p(x))$ in the case that $\mathrm{per}(l(x))$ and $\mathrm{per}(p(x))$ are co-prime. The cycle structure of $\mathrm{FSR}(l(x)p(x))$ has been discussed in Section 4. By the result there, when $\mathrm{per}(l(x))$ and $\mathrm{per}(p(x))$ are co-prime, the cycles in $G(l(x)p(x))$ are of the form $[\mathbf{v}]$ or $[\mathbf{v} + \mathbf{s}]$, where $\mathbf{v}$ is a sequence in $G(l(x))$ and $\mathbf{s}$ is a m-sequence in $G(p(x))$.

Theorem 2. *Let $\mathbf{v}$ and $\mathbf{w}$ be two sequences in $G(l(x))$, and $p(x)$ be a primitive polynomial such that $\gcd(\mathrm{per}(l(x)), \mathrm{per}(p(x))) = 1$. Let $\mathbf{u} \in G(l(x))$ be representative of $G(l(x))$ determined by $p(x)$. Then we can get the adjacency graph of $\mathrm{FSR}(l(x)p(x))$ by using the following formula:*

1. *There are no conjugate pairs shared by $[\mathbf{v}]$ and $[\mathbf{w}]$;*
2. *The two cycles $[\mathbf{v}]$ and $[\mathbf{w} + \mathbf{s}]$ share $R_{\mathbf{u}}(\mathbf{v}, \mathbf{w})$ conjugate pairs;*
3. *The two cycles $[\mathbf{v} + \mathbf{s}]$ and $[\mathbf{w} + \mathbf{s}]$ share $(2^n - 2)R_{\mathbf{u}}(\mathbf{v}, \mathbf{w})$ conjugate pairs,*

where n is the degree of $p(x)$.

Proof. Suppose that the two cycles $[\mathbf{v}]$ and $[\mathbf{w}]$ share a conjugate pair. Then there exists an $(m+n)$-length bit string $(v_0, v_1, \ldots, v_{m+n-1})$ such that, $(v_0, v_1, \ldots, v_{m+n-1})$ is a state on $[\mathbf{v}]$ and $(\overline{v}_0, v_1, \ldots, v_{m+n-1})$ is a state on $[\mathbf{w}]$, which implies that, the m-length bit string $(v_1, v_2, \ldots, v_m)$ is contained in both $[\mathbf{v}]$ and $[\mathbf{w}]$. This is impossible, because the two cycles $[\mathbf{v}]$ and $[\mathbf{w}]$ are generated by the m-stage LFSR, $\mathrm{FSR}(l(x))$, and every m-length state can appear only once.

By the definition of cycle representative, there exist an sequence $\mathbf{s}' \in G(p(x))$ such that $\mathbf{u} + \mathbf{s}' = \mathbf{a}$, where $\mathbf{a}$ is the sequence generated by $\mathrm{FSR}(l(x)p(x))$ with initial state $\mathbf{E} = (1, 0, \ldots, 0)$. Without lose of generality, we can suppose $\mathbf{s}' = \mathbf{s}$. Then the equation $\mathbf{u} + \mathbf{s} = \mathbf{a}$ holds. Write the two sequences $\mathbf{u}$ and $\mathbf{s}$ in the state form: $\mathbf{u} = (\mathbf{U}_0, \mathbf{U}_1, \ldots, \mathbf{U}_{\mathrm{per}(\mathbf{u})-1})$ and $\mathbf{s} = (\mathbf{S}_0, \mathbf{S}_1, \ldots, \mathbf{S}_{2^n-2})$, where each state is of length $\deg l(x)p(x)$. Then $\mathbf{u} + \mathbf{s} = \mathbf{a}$ implies $\mathbf{U}_0 + \mathbf{S}_0 = \mathbf{E}$.

For the proof of Item 2 of this theorem, we need to show that, there is an 1-to-1 correspondence between the set $\{(i, j) \mid L^i\mathbf{v} + L^j\mathbf{w} = \mathbf{u}, 0 \le i \le \mathrm{per}(\mathbf{v}) - 1, 0 \le j \le \mathrm{per}(\mathbf{w}) - 1\}$ and the set of conjugate pairs shared by the two cycles $[\mathbf{v}]$ and $[\mathbf{w}]$. Write the two cycles $[\mathbf{v}]$ and $[\mathbf{w}]$ in the state cycle form: $[\mathbf{v}] = [\mathbf{V}_0, \mathbf{V}_1, \ldots, \mathbf{V}_{\mathrm{per}(\mathbf{v})-1}]$ and $[\mathbf{w}] = [\mathbf{W}_0, \mathbf{W}_1, \ldots, \mathbf{W}_{\mathrm{per}(\mathbf{v})-1}]$, where each state is of length $\deg(l(x)p(x))$.

Suppose there is a pair of integers (i,j) with $0 \le i \le \mathrm{per}(\mathbf{v})-1, 0 \le j \le \mathrm{per}(\mathbf{w})-1$ such that $L^i\mathbf{v} + L^j\mathbf{w} = \mathbf{u}$. Then we have $\mathbf{V}_i + \mathbf{W}_j = \mathbf{U}_0$. Substitute the state $\mathbf{U}_0$ by $\mathbf{S}_0 + \mathbf{E}$, we get that $\mathbf{V}_i + \mathbf{W}_j = \mathbf{S}_0 + \mathbf{E}$, which implies that $\mathbf{V}_i = \mathbf{W}_j + \mathbf{S}_0 + \mathbf{E}$. Therefore, $(\mathbf{V}_i, \mathbf{W}_j + \mathbf{S}_0)$ is a conjugate pair shared by the two cycles $[\mathbf{v}]$ and $[\mathbf{w}+\mathbf{s}]$. It is easy to see that, different pair (i,j) gives different conjugata pair $(\mathbf{V}_i, \mathbf{W}_j + \mathbf{S}_0)$ shared by the two cycles $[\mathbf{v}]$ and $[\mathbf{w}+\mathbf{s}]$.

On the other hand, suppose there is a conjugate pair $(\mathbf{X}, \mathbf{Y})$ shared by the two cycles $[\mathbf{v}]$ and $[\mathbf{w}+\mathbf{s}]$. We can assume $\mathbf{X} = \mathbf{V}_i$ and $\mathbf{Y} = \mathbf{W}_j + \mathbf{S}_k$ for some integers $0 \le i \le \mathrm{per}(\mathbf{v}) - 1, \le j \le \mathrm{per}(\mathbf{w}) - 1$ and $0 \le k \le \mathrm{per}(\mathbf{s}) - 1$. First, we show that $k = 0$. If $k \ne 0$, since $(\mathbf{V}_i, \mathbf{W}_j + \mathbf{S}_k)$ is a conjugate pair, we have that $\mathbf{V}_i + \mathbf{W}_j + \mathbf{S}_k = \mathbf{E}$. Substitute the state $\mathbf{E}$ by $\mathbf{U}_0 + \mathbf{S}_0$, we get that $\mathbf{V}_i + \mathbf{W}_j + \mathbf{S}_k = \mathbf{U}_0 + \mathbf{S}_0$. By simple deformation and using the equation $\mathbf{S}_0 + \mathbf{S}_k = \mathbf{S}_{Z(k)}$ (this equation is valid because $k \ne 0$), we get $\mathbf{V}_i + \mathbf{W}_j + \mathbf{U}_0 = \mathbf{S}_{Z(k)}$. Let $\mathcal{T}$ be the next state operation corresponding to $\mathrm{FSR}(l(x)p(x))$, that is, $\mathcal{T} : (x_0, x_1, \ldots, x_{\deg l(x)p(x)-1}) \mapsto (x_1, \ldots, x_{\deg l(x)p(x)-1}, F(x_0, x_1, \ldots, x_{\deg l(x)p(x)-1}))$, where F is the feedback function of $\mathrm{FSR}(l(x)p(x))$. Then we have $\mathcal{T}^t(\mathbf{V}_i + \mathbf{W}_j + \mathbf{U}_0) = \mathcal{T}^t(\mathbf{S}_{Z(k)})$, that is, $\mathcal{T}^t\mathbf{V}_i + \mathcal{T}^t\mathbf{W}_j + \mathcal{T}^t\mathbf{U}_0 = \mathcal{T}^t\mathbf{S}_{Z(k)}$, which implies $\mathbf{V}_{i+t} + \mathbf{W}_{j+t} + \mathbf{U}_t = \mathbf{S}_{Z(k)+t}$ for any integer t. Therefore, we have $L^i\mathbf{v} + L^j\mathbf{w} + \mathbf{u} = L^{Z(k)}\mathbf{s}$. However, this is impossible, because the sequence $L^i\mathbf{v} + L^j\mathbf{w} + \mathbf{u}$ belongs to $G(l(x))$ and the sequence $L^{Z(k)}\mathbf{s}$ belongs to $G(p(x))$, and since the two polynomial $l(x)$ and $p(x)$ are co-prime, the intersection of $G(l(x))$ and $G(p(x))$ is $\{\mathbf{0}\}$. So we finished the proof of $k = 0$. We can assume $\mathbf{X} = \mathbf{V}_i$ and $\mathbf{Y} = \mathbf{W}_j + \mathbf{S}_0$. Since $(\mathbf{X}, \mathbf{Y})$ is a conjugate pair, we have $\mathbf{V}_i = \mathbf{W}_j + \mathbf{S}_0 + \mathbf{E}$, which implies $\mathbf{V}_i + \mathbf{W}_j = \mathbf{U}_0$. Then $\mathcal{T}^t\mathbf{V}_i + \mathcal{T}^t\mathbf{W}_j = \mathcal{T}^t\mathbf{U}_0$ for any integer t, and $L^i\mathbf{v} + L^j\mathbf{w} = \mathbf{u}$. So we have proved Item 2.

The proof of Item 3 is similar to that of Item 2. We need to show that, there is an (2^n-2)-to-1 surjection from the set of conjugate pairs shared by the two cycles $[\mathbf{v}+\mathbf{s}]$ and $[\mathbf{w}+\mathbf{s}]$ to the set $\{(i,j) \mid L^i\mathbf{v} + L^j\mathbf{w} = \mathbf{u}, {}^{0 \le i \le \mathrm{per}(\mathbf{v})-1}_{0 \le j \le \mathrm{per}(\mathbf{w})-1}\}$.

Suppose there is a pair of integers (i,j) with $0 \le i \le \mathrm{per}(\mathbf{v})-1, 0 \le j \le \mathrm{per}(\mathbf{w})-1$ such that $L^i\mathbf{v} + L^j\mathbf{w} = \mathbf{u}$. Then we have $\mathbf{V}_i + \mathbf{W}_j = \mathbf{U}_0$. Substitute the state $\mathbf{U}_0$ by $\mathbf{S}_0 + \mathbf{E}$, we get that $\mathbf{V}_i + \mathbf{W}_j = \mathbf{S}_0 + \mathbf{E}$, which implies that $\mathbf{V}_i = \mathbf{W}_j + \mathbf{S}_0 + \mathbf{E}$. Add to each side of the equation the state $\mathbf{S}_k$, where $1 \le k \le 2^n - 2$. We get $\mathbf{V}_i + \mathbf{S}_k = \mathbf{W}_j + \mathbf{S}_0 + \mathbf{S}_k + \mathbf{E} = \mathbf{W}_j + \mathbf{S}_{Z(k)} + \mathbf{E}$, which implies that $(\mathbf{V}_i + \mathbf{S}_k, \mathbf{W}_j + \mathbf{S}_{Z(k)})$ is a conjugate pair shared by the two cycles $[\mathbf{v}+\mathbf{s}]$ and $[\mathbf{w}+\mathbf{s}]$ for any $1 \le k \le 2^n - 2$. Since for each such pair (i,j), there are at least $2^n - 2$ pair of conjugates shared by the two cycles $[\mathbf{v}+\mathbf{s}]$ and $[\mathbf{w}+\mathbf{s}]$. Totally, the two cycles share at least $(2^n-2)R_{\mathbf{u}}(\mathbf{v},\mathbf{w})$ conjugate pairs.

Suppose there is a conjugate pair $(\mathbf{X}, \mathbf{Y})$ shared by the two cycles $[\mathbf{v}+\mathbf{s}]$ and $[\mathbf{w}+\mathbf{s}]$. We can assume $\mathbf{X} = \mathbf{V}_i + \mathbf{S}_{k_1}$ and $\mathbf{Y} = \mathbf{W}_j + \mathbf{S}_{k_2}$ for some integers $0 \le i \le \mathrm{per}(\mathbf{v})-1, 0 \le j \le \mathrm{per}(\mathbf{w})-1$ and $0 \le k_1, k_2 \le \mathrm{per}(\mathbf{s}) - 1$. First, we show that $k_2 = Z(k_1)$. Since $(\mathbf{V}_i + \mathbf{S}_{k_1}, \mathbf{W}_j + \mathbf{S}_{k_2})$ is a conjugate pair, we get that $\mathbf{V}_i + \mathbf{S}_{k_1} = \mathbf{W}_j + \mathbf{S}_{k_2} + \mathbf{E}$, which implies that $\mathbf{V}_i + \mathbf{W}_j + \mathbf{E} = \mathbf{S}_{k_1} + \mathbf{S}_{k_2}$. If $\mathbf{S}_{k_1} + \mathbf{S}_{k_2} = 0$, then $\mathbf{V}_i = \mathbf{W}_j + \mathbf{E}$, which is impossible (by Item 1). If $\mathbf{S}_{k_1} + \mathbf{S}_{k_2} = \mathbf{S}_k$ and $k \ne 0$, then $\mathbf{V}_i+\mathbf{W}_j+\mathbf{E}=\mathbf{S}_k$. Since $\mathbf{E}=\mathbf{S}_0+\mathbf{U}_0$, we get that $\mathbf{V}_i+\mathbf{W}_j+\mathbf{U}_0=\mathbf{S}_k+\mathbf{S}_0=\mathbf{S}_{Z(k)}$, which implies that $L^i\mathbf{v}+L^j\mathbf{w}+\mathbf{u}=L^{Z(k)}\mathbf{s}$. But this is impossible, because the sequence $L^i\mathbf{v}+L^j\mathbf{w}+\mathbf{u}$ belongs to $G(l(x))$ and the sequence $L^{Z(k)}\mathbf{s}$ belongs to $G(p(x))$, and the intersection of $G(l(x))$ and $G(p(x))$ is $\{\mathbf{0}\}$. Therefore, $\mathbf{S}_{k_1}+\mathbf{S}_{k_2}=\mathbf{S}_0$, that is, $k_2=Z(k_1)$. So we can assume $\mathbf{X}=\mathbf{V}_i+\mathbf{S}_k$ and $\mathbf{Y}=\mathbf{W}_j+\mathbf{S}_{Z(k)}$ for some integers $0\le i\le \mathrm{per}(\mathbf{v})-1, 0\le j\le \mathrm{per}(\mathbf{w})-1$ and $0\le k\le \mathrm{per}(\mathbf{s})-1$. Then we have the equation $\mathbf{V}_i+\mathbf{S}_k=\mathbf{W}_j+\mathbf{S}_{Z(k)}+\mathbf{E}$. Since $\mathbf{S}_{Z(k)}=\mathbf{S}_0+\mathbf{S}_k$, this implies that $\mathbf{V}_i=\mathbf{W}_j+\mathbf{S}_0+\mathbf{E}=\mathbf{W}_j+\mathbf{U}_0$. Therefore, $L^i\mathbf{v}+L^j\mathbf{w}=\mathbf{u}$. This completes the proof. □

Remark 1. *In Theorem 2, we did't require that* $\mathbf{v}$ *and* $\mathbf{w}$ *are different sequences. When* $\mathbf{v}=\mathbf{w}$*, by this theorem, there are no conjugate pairs in the cycle* $[\mathbf{v}]$*, and there are* $\frac{1}{2}(2^n-2)R_{\mathbf{u}}(\mathbf{v},\mathbf{v})$ *conjugate pairs in the cycle* $[\mathbf{v}+\mathbf{s}]$*. So this theorem considers all the adjacency relations of the cycles in* $G(l(x)p(x))$*.*

5.2 In the case of $\gcd(\mathrm{per}(l(x)),\mathrm{per}(p(x)))\neq 1$

For the case that $\mathrm{per}(l(x))$ and $\mathrm{per}(p(x))$ are not co-prime, the cycles in $G(l(x)p(x))$ are of the form $[\mathbf{v}]$ or $[L^i\mathbf{v}+\mathbf{s}]$, where $\mathbf{v}$ is a sequence in $G(l(x))$ and $\mathbf{s}$ is a m-sequence in $G(p(x))$.

Theorem 3. *Let* $\mathbf{v}$ *and* $\mathbf{w}$ *be two sequences in* $G(l(x))$*, and* $p(x)$ *be a primitive polynomial such that* $\gcd(\mathrm{per}(l(x)),\mathrm{per}(p(x)))=1$*. Let* $\mathbf{u}\in G(l(x))$ *and* $\mathbf{s}\in G(p(x))$ *be two sequences such that* $\mathbf{u}+\mathbf{s}$ *is the sequence generated by* $G(l(x)p(x))$ *with initial state* $(1,0,\dots,0)$*. Then we can get the adjacency graph of* $\mathrm{FSR}(l(x)p(x))$ *by using the following formula:*

1. *There are no conjugate pairs shared by* $[\mathbf{v}]$ *and* $[\mathbf{w}]$*;*
2. *The two cycles* $[\mathbf{v}]$ *and* $[L^b\mathbf{w}+\mathbf{s}]$ *share*
$$\left|\left\{(i,j)\mid L^i\mathbf{v}+L^j\mathbf{w}=\mathbf{u}, j\equiv b(\mathrm{mod}\, d_{\mathbf{w}}), {}^{0\le i\le \mathrm{per}(\mathbf{v})-1}_{0\le j\le \mathrm{per}(\mathbf{w})-1}\right\}\right|$$
conjugate pairs;
3. *The two cycles* $[L^a\mathbf{v}+\mathbf{s}]$ *and* $[L^b\mathbf{w}+\mathbf{s}]$ *share*
$$\left|\left\{(i,j,k)\mid L^i\mathbf{v}+L^j\mathbf{w}=\mathbf{u}, \substack{k\equiv i-a(\bmod d_{\mathbf{v}})\\ Z(k)\equiv j-b(\bmod d_{\mathbf{w}})}, \substack{0\le i\le \mathrm{per}(\mathbf{v})-1\\ 0\le j\le \mathrm{per}(\mathbf{w})-1\\ 1\le k\le 2^n-2}\right\}\right|$$
conjugate pairs,

where $n=\deg p(x)$*,* $d_{\mathbf{v}}=\gcd(\mathrm{per}(\mathbf{v}),2^n-1)$ *and* $d_{\mathbf{w}}=\gcd(\mathrm{per}(\mathbf{w}),2^n-1)$*.*

Proof. It can be shown as in the proof of Theorem 2 that, there are no conjugate pairs shared by the two cycles $[\mathbf{v}]$ and $[\mathbf{w}]$.

Now we consider the conjugate pairs shared by the two cycles $[\mathbf{v}]$ and $[L^b\mathbf{w}+\mathbf{s}]$. We have to show that, there is an 1-to-1 correspondence between the set $\{(i,j)\mid L^i\mathbf{v}+L^j\mathbf{w}=\mathbf{u}, j\equiv b(\mathrm{mod}\, d_{\mathbf{w}}), {}^{0\le i\le \mathrm{per}(\mathbf{v})-1}_{0\le j\le \mathrm{per}(\mathbf{w})-1}\}$ and the set of conjugate pairs shared by the two cycles $[\mathbf{v}]$ and $[L^b\mathbf{w}+\mathbf{s}]$. Write the four sequences $\mathbf{u},\mathbf{v},\mathbf{w}$ and $\mathbf{s}$ in the state form (each state is of length $\deg l(x)p(x)$):

$$\mathbf{u}=(\mathbf{U}_0,\mathbf{U}_1,\dots,\mathbf{U}_{\mathrm{per}(\mathbf{u})-1}),\mathbf{v}=(\mathbf{V}_0,\mathbf{V}_1,\dots,\mathbf{V}_{\mathrm{per}(\mathbf{v})-1}),$$

$$\mathbf{w} = (\mathbf{W}_0, \mathbf{W}_1, \ldots, \mathbf{W}_{\text{per}(\mathbf{w})-1}), \mathbf{s} = (\mathbf{S}_0, \mathbf{S}_1, \ldots, \mathbf{S}_{2^n-2}).$$

Then we have $\mathbf{U}_0 + \mathbf{S}_0 = \mathbf{E}$, where $\mathbf{E} = (1, 0, \ldots, 0)$. It is easy to see that, the states in the cycle $[L^b\mathbf{w} + \mathbf{s}]$ are exactly those $\mathbf{W}_{k_1} + \mathbf{S}_{k_2}$ satisfying $0 \le k_1 \le \text{per}(\mathbf{w}), 0 \le k_2 \le \text{per}(\mathbf{s})$ and $k_1 - k_2 \equiv b(\text{mod} d_{\mathbf{w}})$.

Suppose there exist a pair of integers (i, j) with $0 \le i \le \text{per}(\mathbf{v}) - 1, 0 \le j \le \text{per}(\mathbf{w}) - 1$ such that $L^i\mathbf{v} + L^j\mathbf{w} = \mathbf{u}$ and $j \equiv b(\text{mod} d_{\mathbf{w}})$. Then we have $\mathbf{V}_i + \mathbf{W}_j = \mathbf{U}_0$. Substitute $\mathbf{U}_0$ by $\mathbf{S}_0 + \mathbf{E}$, we get that $\mathbf{V}_i = \mathbf{W}_j + \mathbf{S}_0 + \mathbf{E}$. Since $j \equiv b(\text{mod} d_{\mathbf{w}})$, it can be verified that the state $\mathbf{W}_j + \mathbf{S}_0$ is on the cycle $[L^b\mathbf{w} + \mathbf{s}]$. Therefore, $(\mathbf{V}_i, \mathbf{W}_j + \mathbf{S}_0)$ is a conjugate pair shared by the two cycles $[\mathbf{v}]$ and $[L^b\mathbf{w} + \mathbf{s}]$.

Suppose there is a conjugate pair $(\mathbf{X}, \mathbf{Y})$ shared by the two cycles $[\mathbf{v}]$ and $[L^b\mathbf{w} + \mathbf{s}]$. We can assume that $\mathbf{X} = \mathbf{V}_i$ and $\mathbf{Y} = \mathbf{W}_j + \mathbf{S}_k$ for some integers $0 \le i \le \text{per}(\mathbf{v}) - 1, 0 \le j \le \text{per}(\mathbf{w}) - 1$ and $0 \le k \le 2^n - 2$, and the two integers j and k satisfy $j - k \equiv b(\text{mod} d_{\mathbf{w}})$. As in the proof of Item 2 of Theorem 2, we can show that $k = 0$. Then since $(\mathbf{X}, \mathbf{Y})$ is a conjugate pair, we get the equation $\mathbf{V}_i = \mathbf{W}_j + \mathbf{S}_0 + \mathbf{E}$. Substitute $\mathbf{S}_0 + \mathbf{E}$ by $\mathbf{U}_0$, we get that $\mathbf{V}_i = \mathbf{W}_j + \mathbf{U}_0$, which implies $L^i\mathbf{v} + L^j\mathbf{w} = \mathbf{u}$. In this way, we get a pair of integers (i, j) satisfying: $L^i\mathbf{v} + L^j\mathbf{w} = \mathbf{u}, j \equiv b(\text{mod} d_{\mathbf{w}}), 0 \le i \le \text{per}(\mathbf{v}) - 1, 0 \le j \le \text{per}(\mathbf{w}) - 1$.

In the following, we prove Item 3 of this theorem. We show that, there is a 1-to-1 correspondence between the set $|\{(i,j,k) \mid L^i\mathbf{v} + L^j\mathbf{w} = \mathbf{u}, {}_{\substack{k\equiv i-a(\bmod d_{\mathbf{v}}) \\ Z(k)\equiv j-b(\bmod d_{\mathbf{w}})}}, {}_{\substack{0\le i\le \text{per}(\mathbf{v})-1 \\ 0\le j\le \text{per}(\mathbf{w})-1 \\ 1\le k\le 2^n-2}}\}|$ and the set of conjugate pairs shared by the two cycles $[L^a\mathbf{v} + \mathbf{s}]$ and $[L^b\mathbf{w} + \mathbf{s}]$.

Suppose there is a triple of integers (i, j, k) with $0 \le i \le \text{per}(\mathbf{v}) - 1$, $0 \le j \le \text{per}(\mathbf{w}) - 1$ and $1 \le k \le 2^n - 2$ such that $L^i\mathbf{v} + L^j\mathbf{w} = \mathbf{u}$, $k \equiv i - a(\text{mod} d_{\mathbf{v}})$ and $Z(k) \equiv j - b(\text{mod} d_{\mathbf{w}})$. Then we have $\mathbf{V}_i + \mathbf{W}_j = \mathbf{U}_0$. Substitute $\mathbf{U}_0$ by $\mathbf{S}_0 + \mathbf{E}$, we get that $\mathbf{V}_i = \mathbf{W}_j + \mathbf{S}_0 + \mathbf{E}$. Add the state $\mathbf{S}_k$ to this equation, we get $\mathbf{V}_i + \mathbf{S}_k = \mathbf{W}_j + \mathbf{S}_{Z(k)} + \mathbf{E}$. Since $k \equiv i - a(\text{mod} d_{\mathbf{v}})$ and $Z(k) \equiv j - b(\text{mod} d_{\mathbf{w}})$, it can be verified that the state $\mathbf{V}_i + \mathbf{S}_k$ is on the cycle $[L^a\mathbf{v} + \mathbf{s}]$ and the state $\mathbf{W}_j + \mathbf{S}_{Z(k)}$ is on the cycle $[L^b\mathbf{w} + \mathbf{s}]$. Therefore, $(\mathbf{V}_i + \mathbf{S}_k, \mathbf{W}_j + \mathbf{S}_{Z(k)})$ is a conjugate pair shared by the two cycles $[L^a\mathbf{v} + \mathbf{s}]$ and $[L^b\mathbf{w} + \mathbf{s}]$.

Suppose there is a conjugate pair $(\mathbf{X}, \mathbf{Y})$ shared by the two cycles $[L^a\mathbf{v}+\mathbf{s}]$ and $[L^b\mathbf{w}+\mathbf{s}]$. We can assume that $\mathbf{X} = \mathbf{V}_i+\mathbf{S}_{k_1}$ and $\mathbf{Y} = \mathbf{W}_j+\mathbf{S}_{k_2}$ for some integers $0 \le i \le \text{per}(\mathbf{v})-1, 0 \le j \le \text{per}(\mathbf{w})-1$ and $0 \le k_1, k_2 \le 2^n-2$. Then as in the proof of Item 2 of Theorem 2, we can show that $k_2 = Z(k_1)$. Therefore, we can assume $\mathbf{X} = \mathbf{V}_i + \mathbf{S}_k$ and $\mathbf{Y} = \mathbf{W}_j + \mathbf{S}_{Z(k)}$. Since $(\mathbf{X}, \mathbf{Y})$ is a conjugate pair, we get the equation $\mathbf{V}_i + \mathbf{S}_k = \mathbf{W}_j + \mathbf{S}_{Z(k)} + \mathbf{E}$ which is equivalent to $\mathbf{V}_i = \mathbf{W}_j + \mathbf{S}_0 + \mathbf{E}$. Substitute $\mathbf{S}_0 + \mathbf{E}$ by $\mathbf{U}_0$, we get that $\mathbf{V}_i = \mathbf{W}_j + \mathbf{U}_0$, which implies $L^i\mathbf{v} + L^j\mathbf{w} = \mathbf{u}$. Because $\mathbf{V}_i + \mathbf{S}_k$ is a state on the cycle $[L^a\mathbf{v} + \mathbf{s}]$ and $\mathbf{W}_j + \mathbf{S}_{Z(k)}$ is a state on the cycle $[L^b\mathbf{w} + \mathbf{s}]$, the integer k satisfies $k \equiv i-a(\bmod d_{\mathbf{v}})$ and $Z(k) \equiv j-b(\bmod d_{\mathbf{w}})$. In this way, we get a triple (i, j, k) satisfying: $L^i\mathbf{v} + L^j\mathbf{w} = \mathbf{u}, k \equiv i - a(\text{mod} d_{\mathbf{v}}), Z(k) \equiv b - j(\text{mod} d_{\mathbf{w}})$. □

Remark 2. *In Theorem 3, we did't require that* $\mathbf{v}$ *and* $\mathbf{w}$ *are different sequences. When* $\mathbf{v} = \mathbf{w}$*, by this theorem, there are no conjugate pairs in the* $[\mathbf{v}]$*, and there are*

$$\frac{1}{2}\left|\left\{(i,j,k) \mid L^i\mathbf{v} + L^j\mathbf{v} = \mathbf{u}, {}_{\substack{k\equiv i-a(\bmod d_{\mathbf{v}}) \\ Z(k)\equiv j-a(\bmod d_{\mathbf{v}})}}, {}_{\substack{0\le i,j\le \text{per}(\mathbf{v})-1 \\ 1\le k\le 2^n-2}}\right\}\right|$$

conjugate pairs in the cycle $[L^a\mathbf{v}+\mathbf{s}]$. So this theorem considers all the adjacency relations of the cycles in $G(l(x)p(x))$.

To determine the adjacency graph of $\mathrm{FSR}(l(x)p(x))$ in the case of $\gcd(\mathrm{per}(l(x)),\mathrm{per}(p(x)))\neq 1$, we have to count the number of solutions of the congruence equations in Theorem 3. In fact, the number of solutions is equal to the sum of some cyclotomic numbers over finite field $\mathbb{F}_{2^n}$. To explain this, we need the following lemma.

Lemma 3. *Let $\mathbf{s}$ be an m-sequence of period 2^n-1, and $Z(\cdot)$ be the mapping with respect to $\mathbf{s}$ (see Section 2.3). Let d_1 and d_2 be two divisors of 2^n-1, a and b be two integers with $0\le a\le d_1-1$ and $0\le b\le d_2-1$. Denote $d=\mathrm{lcm}(d_1,d_2)$ and $d_1'=\frac{d}{d_1}, d_2'=\frac{d}{d_2}$. Then we have,*

$$\left|\left\{k \mid {}^{k\equiv a(\bmod d_1)}_{Z(k)\equiv b(\bmod d_2)}, 1\le k\le 2^n-2\right\}\right| = \sum_{x=0}^{d_1'-1}\sum_{y=0}^{d_2'-1}(a+xd_1,b+yd_2)_d\,,$$

where $(a+xd_1,b+yd_2)_d$ is the cyclotomic number over field $\mathbb{F}_{2^n}$ with respect to $\mathbf{s}$.

Proof.

$$\begin{aligned}
&\left|\left\{k \mid {}^{k\equiv a(\bmod d_1)}_{Z(k)\equiv b(\bmod d_2)}, 1\le k\le 2^n-2\right\}\right|\\
=&\sum_{x=0}^{d_1'-1}\left|\left\{k \mid {}^{k\equiv a+xd_1(\bmod d)}_{Z(k)\equiv b(\bmod d_2)}, 1\le k\le 2^n-2\right\}\right|\\
=&\sum_{x=0}^{d_1'-1}\sum_{y=0}^{d_2'-1}\left|\left\{k \mid {}^{k\equiv a+xd_1(\bmod d)}_{Z(k)\equiv b+yd_2(\bmod d)}, 1\le k\le 2^n-2\right\}\right|\\
=&\sum_{x=0}^{d_1'-1}\sum_{y=0}^{d_2'-1}(a+xd_1,b+yd_2)_d\,.
\end{aligned}$$

□

By Lemma 3, the number of solutions of the congruence equations in Theorem 3 can be expressed in terms of cyclotomic numbers over field $\mathbb{F}_{2^n}$. The reader can verify that, the number of solution of the congruence equations in Item 3 of Theorem 3 is,

$$\begin{aligned}
&\left|\left\{(i,j,k) \mid L^i\mathbf{v}+L^j\mathbf{w}=\mathbf{u}, {}^{k\equiv i-a(\bmod d_{\mathbf{v}})}_{Z(k)\equiv j-b(\bmod d_{\mathbf{w}})}, \begin{smallmatrix}0\le i\le \mathrm{per}(\mathbf{v})-1\\ 0\le j\le \mathrm{per}(\mathbf{w})-1\\ 1\le k\le 2^n-2\end{smallmatrix}\right\}\right|\\
=&\sum_{(i,j)}\left|\left\{k \mid {}^{k\equiv i-a(\bmod d_{\mathbf{v}})}_{Z(k)\equiv j-b(\bmod d_{\mathbf{w}})}, 1\le k\le 2^n-2\right\}\right| \qquad (1)\\
=&\sum_{(i,j)}\sum_{x=0}^{d_{\mathbf{v}}'-1}\sum_{y=0}^{d_{\mathbf{w}}'-1}(i-a+xd_{\mathbf{v}},j-b+yd_{\mathbf{w}})_d\,,
\end{aligned}$$

Where $d=lcm(d_{\mathbf{v}},d_{\mathbf{w}}), d_{\mathbf{v}}'=\frac{d}{d_{\mathbf{v}}}, d_{\mathbf{w}}'=\frac{d}{d_{\mathbf{w}}}$, and (i,j) runs over the set $\{(i,j)\mid L^i\mathbf{v}+L^j\mathbf{w}=\mathbf{u}, 0\le i\le \mathrm{per}(\mathbf{v})-1, 0\le j\le \mathrm{per}(\mathbf{w})-1\}$. We should note that, these cyclotomic numbers are with respect to the sequence $\mathbf{s}$.

6 Applications

The process of calculating the adjacency graph of $\mathrm{FSR}(l(x)p(x))$ can be summarized by the following three steps:

1. Find the representative of $G(l(x))$ determined by $p(x)$ using Algorithm 1.
2. Calculate the association graph of $\mathrm{FSR}(l(x))$ with respect to the representative of $G(l(x))$.
3. Determine the adjacency graph of $\mathrm{FSR}(l(x))$ by Theorems 2 and 3.
    (a) In the case of $\gcd(\mathrm{per}(l(x)), \mathrm{per}(p(x))) = 1$, it can be determined directly.
    (b) In the case of $\gcd(\mathrm{per}(l(x)), \mathrm{per}(p(x))) \neq 1$, some cyclotomic numbers are needed.

Suppose that $\deg l(x) = m$ and $\deg p(x) = n$. Then the total work can be done in time $O(2^m + n)$. It seems that, for this method to work, we need to know the two polynomials $l(x)$ and $p(x)$ beforehand, that is, the specific expressions of $l(x)$ and $p(x)$ are needed before the work be startted. Nevertheless, we will show that this method can be applied to the situation that, only the polynomials $l(x)$ is given, and we will pay our attention to this situation. Firstly, we derive some properties of the association graphs and the adjacency graphs.

6.1 Properties of the association graphs and the adjacency graphs

Usually, the representative of $G(l(x))$ relies on the choice of $p(x)$. But, there are some sequences in $G(l(x))$ which can never be the representative of $G(l(x))$, no matter which $p(x)$ is considered.

Theorem 4. *For any proper divisor $l_1(x)$ of $l(x)$, The representative of $G(l(x))$ are not lie in $G(l_1(x))$, no matter which primitive polynomial $p(x)$ is considered.*

Proof. We just need to show that, the minimal polynomial of the representative of $G(l(x))$ is $l(x)$. By the definition, the representative of $G(l(x))$ is the sequence $\mathbf{u} \in G(l(x))$ such that $\mathbf{u} + \mathbf{s} = \mathbf{a}$, where $\mathbf{a}$ is the sequence generated by $\mathrm{FSR}(l(x)p(x))$ with the initial state $(1, 0, \ldots, 0)$. It is obvious that, the minimal polynomial of $\mathbf{a}$ is $l(x)p(x)$. Suppose the minimal polynomial of $\mathbf{u}$ is not $l(x)$, but a proper divisor of $l(x)$. Since the minimal polynomial of $\mathbf{s}$ is $p(x)$, the minimal polynomial of the sum $\mathbf{u} + \mathbf{s}$ would be a proper divisor of $l(x)p(x)$, which is a contradiction. □

Different representatives of $G(l)$ often define different association graphs of $G(l)$. However, sometimes they define the same association graph.

Theorem 5. *The association graph of $\mathrm{FSR}(l(x))$ with respect to $\mathbf{u}$ is the same as that with respect to any sequence in the cycle $[\mathbf{u}]$.*

Proof. For the proof of this theorem, we need to show that, $R_{\mathbf{u}}([\mathbf{v}],[\mathbf{w}]) = R_{L^k\mathbf{u}}([\mathbf{v}],[\mathbf{w}])$ for any integer k and any two cycles $[\mathbf{v}]$ and $[\mathbf{w}]$ in $G(l(x))$. This is indeed the case because $R_{\mathbf{u}}([\mathbf{v}],[\mathbf{w}]) = |\{(\mathbf{a},\mathbf{b}) \mid \mathbf{a}+\mathbf{b} = \mathbf{u}, \mathbf{a} \in [\mathbf{v}], \mathbf{b} \in [\mathbf{w}]\}| = |\{(L^k\mathbf{a}, L^k\mathbf{b}) \mid L^k\mathbf{a} + L^k\mathbf{b} = L^k\mathbf{u}, L^k\mathbf{a} \in L^k[\mathbf{v}], L^k\mathbf{b} \in L^k[\mathbf{w}]\}| = |\{(L^k\mathbf{a}, L^k\mathbf{b}) \mid L^k\mathbf{a} + L^k\mathbf{b} = L^k\mathbf{u}, L^k\mathbf{a} \in [\mathbf{v}], L^k\mathbf{b} \in [\mathbf{w}]\}| = |\{(\mathbf{a}', \mathbf{b}') \mid \mathbf{a}' + \mathbf{b}' = L^k\mathbf{u}, \mathbf{a}' \in [\mathbf{v}], \mathbf{b}' \in [\mathbf{w}]\}| = R_{L^k\mathbf{u}}([\mathbf{v}],[\mathbf{w}])$. □

Theorem 6. *Let $l(x)$ be a polynomial such that, there is only one cycle in the set $G(l(x)) \setminus \cup_{l_1(x)|l(x), l_1(x)\neq l(x)} G(l_1(x))$. Let n be an integer satisfying $\gcd(\mathrm{per}(l(x), 2^n - 1)) = 1$. Then the adjacency graphs of* FSR$(l(x)p(x))$ *are isomorphic for all primitive polynomial $p(x)$ of degree n.*

Proof. The set $G(l(x)) \setminus \cup_{l_1(x)|l(x), l_1(x)\neq l(x)} G(l_1(x))$ equals to the set $\{\mathbf{a} \mid m(\mathbf{a}) \neq l(x), \mathbf{a} \in G(l(x))\}$, where $m(\mathbf{a})$ is the minimal polynomial of the sequence $\mathbf{a}$. Suppose there is only one cycle, denoted by $[\mathbf{u}]$, in this set. By Theorem 4, the representative of $G(l(x))$ lies in the cycle $[\mathbf{u}]$ when a primitive polynomial $p(x)$ is considered. Then by Theorem 5, the association graph of FSR$(l(x))$ determined by its representative is unique, that is, it does not affected by the choice of $p(x)$. At last, in the case of $\gcd(\mathrm{per}(l(x), 2^n - 1)) = 1$, the adjacency graphs of FSR$(l(x)p(x))$ are totally determined by the association graph of FSR$(l(x))$ by Theorem 2. Therefore, they are isomorphic for all primitive polynomial $p(x)$ of degree n. □

6.2 The adjacency graph of FSR$((1 + x + x^3 + x^4)p(x))$

In this subsection, we use the general method proposed in Section 5 to calculate the adjacency graphs of LFSRs with characteristic polynomials of the form $(1 + x + x^3 + x^4)p(x)$, where $p(x)$ is a primitive polynomial of degree n. The adjacency graphs of these LFSRs have not been considered before.

There are six cycles in $G(1 + x + x^3 + x^4)$, and they are $[(0)], [(000111)], [(001)], [(01)], [(011)]$ and $[(1)]$. For convenience, we denote,

$$\mathbf{v}_1 = (0), \mathbf{v}_2 = (000111), \mathbf{v}_3 = (001), \mathbf{v}_4 = (01), \mathbf{v}_5 = (011), \mathbf{v}_6 = (1).$$

It can be verified that, the minimal polynomials of the sequences in $[(0)] \cup [(001)] \cup [(01)] \cup [(011)] \cup [(1)]$ are all proper divisors of $1 + x + x^3 + x^4$. Therefore, by Theorem 4, the representative of $G(1 + x + x^3 + x^4)$ lies in the cycle $[(000111)]$ (no matter which $p(x)$ is considered). Then according to Theorem 5, the association graph of FSR$(1 + x + x^3 + x^4)$ with respect to its representative is unique. The association graph has been given in Example 1 (see Figure 2).

Since the period of $1 + x + x^3 + x^4$ is 6 and the period of $p(x)$ is $2^n - 1$ which is an odd number, there are only two possible values for $\gcd(\mathrm{per}(1 + x + x^3 + x^4), \mathrm{per}(p(x)))$, that is, 1 and 3. In the case that n is odd, $\gcd(\mathrm{per}(1 + x + x^3 + x^4), \mathrm{per}(p(x))) = 1$, and in the case that n is even, $\gcd(\mathrm{per}(1 + x + x^3 + x^4), \mathrm{per}(p(x))) = 3$. We let $\mathbf{u}$ be the representative of $G(1 + x + x^3 + x^4)$ determined by $p(x)$ (by the above discussion, $\mathbf{u}$ belongs to the cycle $[(000111)]$), and $\mathbf{s}$ be the sequence in $G(p(x))$ such that $\mathbf{u} + \mathbf{s} = \mathbf{a}$, where $\mathbf{a}$ is the sequence generated by FSR$(l(x)p(x))$ with initial state $(1, 0, \ldots, 0)$.

In the case that n is odd, the cycle structure of $\mathrm{FSR}((1+x+x^3+x^4)p(x))$ is given by $G((1+x+x^3+x^4)p(x)) = \left(\cup_{i=1}^{6}[\mathbf{v}_i]\right) \bigcup \left(\cup_{i=1}^{6}[\mathbf{v}_i+\mathbf{s}]\right)$. Its adjacency graph can be determined directly according to Theorem 2, and we show it in Figure 3. We use a to denote the number 2^n-2. In order to be more clearly, a dashed line is used when one of the two cycles is also a cycle in $G(l(x))$.

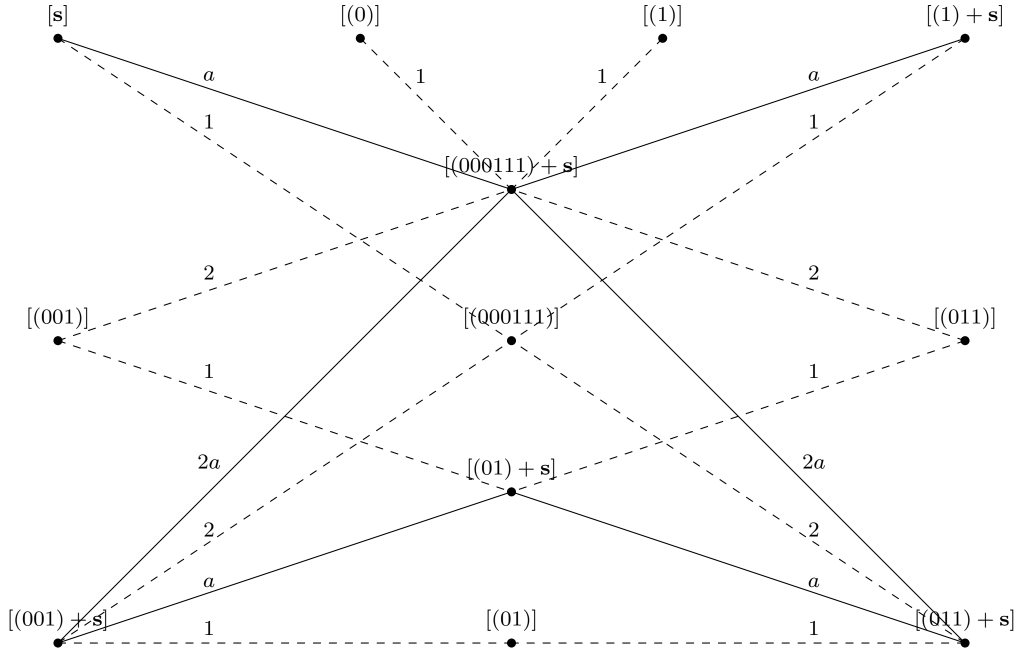

Figure 3: The adjacency graph of $\mathrm{FSR}((1+x+x^3+x^4)p(x))$ when $\deg(p(x))$ is odd

In the case that n is even, we have to know firstly which sequence in the cycle $[(000111)]$ is the representative of $G(1+x+x^3+x^4)$ determined by $p(x)$ (remember that when n is odd, we don't have to do that, because the adjacency graphs of $\mathrm{FSR}(l(x)p(x))$ are isomorphic for all $p(x)$ of degree n by Theorem 6). Since there are six sequences in the cycle $[(000111)]$, there are six cases need to be considered. In the following, we assume that $\mathbf{u} = (000111)$ is the representative of $G(1+x+x^3+x^4)$ determined by $p(x)$. The other cases can be handled similarly. The cycle structure of $\mathrm{FSR}((1+x+x^3+x^4)p(x))$ is given by $G((1+x+x^3+x^4)p(x)) = \left(\cup_{i=1}^{6}[\mathbf{v}_i]\right) \bigcup \left(\cup_{i=1,4,6}[\mathbf{v}_i+\mathbf{s}]\right) \bigcup \left(\cup_{i=2,3,5} \cup_{j=0}^{2} [L^j\mathbf{v}_i+\mathbf{s}]\right)$.

The adjacency relations of the cycles in $G((1+x+x^3+x^4)p(x))$ can be determined by using Theorem 3. We take the two cycles $[L^1\mathbf{v}_2+\mathbf{s}] = [(001110)+\mathbf{s}]$ and $[L^2\mathbf{v}_3+\mathbf{s}] = [(100)+\mathbf{s}]$ for example to show how to calculate the number of conjugate pairs shared by them. The reader can verify that, there are two pairs (i,j) with $0 \le i \le \mathrm{per}(\mathbf{v}_2)-1$ and $0 \le j \le \mathrm{per}(\mathbf{v}_3)-1$ such that $L^i\mathbf{v}_2 + L^j\mathbf{v}_3 = \mathbf{u}$. The two pairs are $(1,0)$ and $(5,2)$, that is, we have $L^1\mathbf{v}_2 + L^0\mathbf{v}_3 = \mathbf{u}$ and $L^5\mathbf{v}_2 + L^2\mathbf{v}_3 = \mathbf{u}$. Then the number of conjugate pairs shared by the two cycles is given by $N([L^1\mathbf{v}_2+\mathbf{s}],[L^2\mathbf{v}_3+\mathbf{s}]) = \sum_{(i,j)} \left|\left\{k \mid \substack{k\equiv i-1(\bmod 3)\\ Z(k)\equiv j-2(\bmod 3)}, 1 \le k \le 2^n-2\right\}\right| = (0,1)_3 + (1,0)_3 = 2B = \frac{2}{9}\left(2^n+(-2)^{\frac{n}{2}}-2\right)$, (see Lemma 1). Similarly, we can calculate the conjugate pairs shared by other cycles. The adjacency graph is shown in Figure 4. For simplicity, we print only the lines between the cycles in $G((1+x+x^3+x^4)p(x)) \setminus G(1+x+x^3+x^4)$, and the numbers shared by cycles are listed in Graph 1. The numbers A, B, C and D are from Lemma 1.

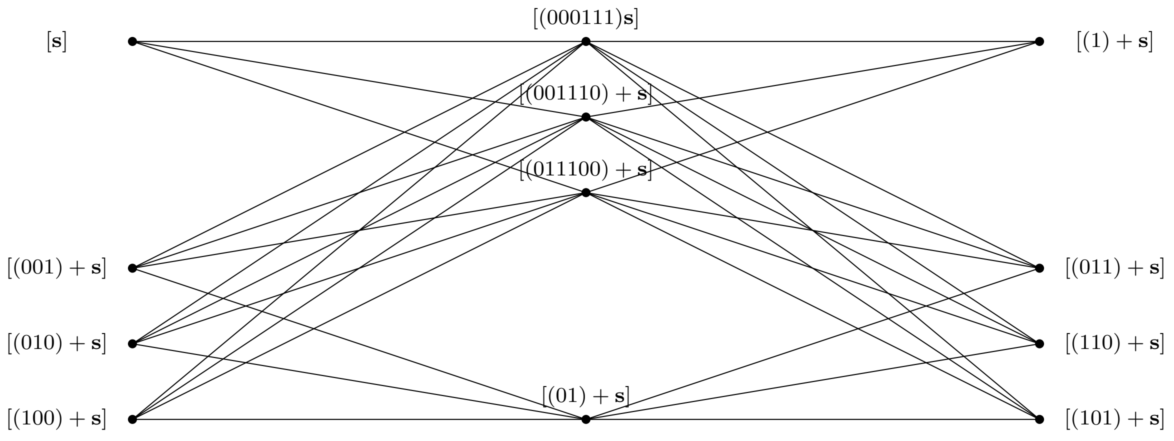

Figure 4: The adjacency graph of FSR$((1+x+x^3+x^4)p(x))$ when $\deg(p(x))$ is even

Table 1: The number of conjugate pairs shared by cycles in $G((1+x+x^3+x^4)p(x))$ when $\deg(p(x))$ is even

	[s]	[(001) + s]	[(010) + s]	[(100) + s]	[(1) + s]	[(011) + s]	[(110) + s]	[(101) + s]
[(000111) + s]	A+2C	B+D	2D	2C	A+2C	2C	2B	2D
[(001110) + s]	B+C+D	A+D	2C	2B	B+C+D	2B	A+D	2C
[(011100) + s]	B+C+D	2C	2B	A+D	B+C+D	A+D	2C	2B
[(01) + s]	0	B+C+D	A+B+C	B+C+D	0	B+C+D	B+C+D	A+B+C

7 Construction of De Bruijn sequences

It is straightforward to join the cycles in FSR$((1+x+x^3+x^4)p(x))$ to form a full cycle by using its adjacency graph given in Section 6. For simplicity, we only consider the case that n is odd, where $n = \deg p(x)$. In this case, we have $\gcd(\mathrm{per}(1+x+x^3+x^4), \mathrm{per}(p(x))) = 1$. The adjacency graph of this LFSR is given in Figure 3. Since we are interested in De Bruijn sequences of large period, we assume n is a large integer.

There are 12 cycles in $G((1+x+x^3+x^4)p(x))$. 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 on them:

$$[(0)], [(000111)], [(001)], [(001)], [(01)], [(011)],$$

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

$$[\mathbf{s}], [(000111)+\mathbf{s}], [(001)+\mathbf{s}], [(001)+\mathbf{s}], [(01)+\mathbf{s}], [(011)+\mathbf{s}].$$

Since for any state on the short cycles its conjugate is located on the long cycles, it is easy to join the short cycles into the long cycles, and in the following, we will pay our attention to the conjugate pairs shared by long cycles. Regardless of the short cycles, the adjacency graph of $\mathrm{FSR}((1+x+x^3+x^4)p(x))$ can be simplified as follows, where a denotes the number 2^n-2 (see Figure 5).

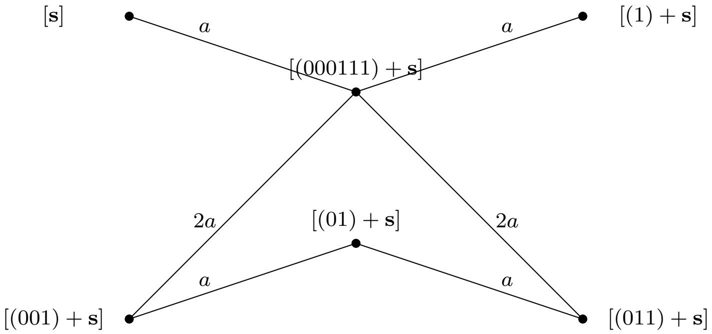

Figure 5: The simplified adjacency graph of $\mathrm{FSR}((1+x+x^3+x^4)p(x))$ when $\deg(p(x))$ is odd

To find out which conjugate pairs are shared by cycles (not just the number of conjugate pairs shared by cycles), we have to know the representative of $G(l(x))$ determined by $p(x)$. By using Algorithm 1, the representative can be found in time $O(2^m+n)$. Since we suppose m is a small positive integer, this can be done efficiently. By Theorem 4, the representative is located on the cycle $[(000111)]$. In the following we assume that the representative is the sequence $\mathbf{u}=(000111)$. We write the two sequences (000111) and $\mathbf{s}$ in the state form: $(000111)=(\mathbf{U}_0,\mathbf{U}_1,\ldots,\mathbf{U}_5)$ and $\mathbf{s}=(\mathbf{S}_0,\mathbf{S}_1,\ldots,\mathbf{S}_{2^n-2})$, each state is of length $n+4$. Then we have $\mathbf{U}_0+\mathbf{S}_0=(1,0,\ldots,0)$. The four sequences $(1),(001),(01)$ and (011), are also written in the state form: $(1)=(\mathbf{V}_0),(001)=(\mathbf{W}_0,\mathbf{W}_1,\mathbf{W}_2),(01)=(\mathbf{X}_0,\mathbf{X}_1)$ and $(011)=(\mathbf{Y}_0,\mathbf{Y}_1,\mathbf{Y}_2)$, each state is of length $n+4$. By the proof of Theorem 2, the conjugate pairs shared by these cycles can be explicitly given, see Table 2.

Table 2: The conjugate pairs shared by cycles in $G((1+x+x^3+x^4)p(x))$

cycle pairs	the set of conjugate pairs shared by cycles
$<[\mathbf{s}],[(000111)+\mathbf{s}]>$	$(\mathbf{S}_j,\mathbf{U}_0+\mathbf{S}_{Z(j)}),1\le j\le 2^n-2$
$<[(1)+\mathbf{s}],[(000111)+\mathbf{s}]>$	$(\mathbf{V}_0+\mathbf{S}_j,\mathbf{U}_3+\mathbf{S}_{Z(j)}),1\le j\le 2^n-2$
$<[(001)+\mathbf{s}],[(000111)+\mathbf{s}]>$	$(\mathbf{W}_0+\mathbf{S}_j,\mathbf{U}_1+\mathbf{S}_{Z(j)}),(\mathbf{W}_2+\mathbf{S}_j,\mathbf{U}_5+\mathbf{S}_{Z(j)}),1\le j\le 2^n-2$
$<[(011)+\mathbf{s}],[(000111)+\mathbf{s}]>$	$(\mathbf{Y}_0+\mathbf{S}_j,\mathbf{U}_2+\mathbf{S}_{Z(j)}),(\mathbf{Y}_1+\mathbf{S}_j,\mathbf{U}_4+\mathbf{S}_{Z(j)}),1\le j\le 2^n-2$
$<[(001)+\mathbf{s}],[(01)+\mathbf{s}]>$	$(\mathbf{W}_1+\mathbf{S}_j,\mathbf{X}_0+\mathbf{S}_{Z(j)}),1\le j\le 2^n-2$
$<[(011)+\mathbf{s}],[(01)+\mathbf{s}]>$	$(\mathbf{Y}_2+\mathbf{S}_j,\mathbf{X}_1+\mathbf{S}_{Z(j)}),1\le j\le 2^n-2$

Theorem 7. *Let $f(x_0,x_1,\ldots,x_{n+4})$ be the linear Boolean function corresponding to the polynomial $(1+x+x^3+x^4)p(x)$. Choose a state from each short cycle randomly, and let A be the set of these states. Define $\mathcal{S}=\{\mathbf{S}_j\mid 1\le j\le 2^n-2\}$, Then the FSRs that take the following Boolean functions as their characteristic functions are maximum length FSRs:*

1. $g = f(x_0, x_1, \dots, x_{n+4}) + I(\mathbf{Z}_1, \mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_5) + I(A)$,

2. $g = f(x_0, x_1, \dots, x_{n+4}) + I(\mathbf{Z}_1, \mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_6) + I(A)$,

3. $g = f(x_0, x_1, \dots, x_{n+4}) + I(\mathbf{Z}_1, \mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_5, \mathbf{Z}_6) + I(A)$,

4. $g = f(x_0, x_1, \dots, x_{n+4}) + I(\mathbf{Z}_1, \mathbf{Z}_2, \mathbf{Z}_4, \mathbf{Z}_5, \mathbf{Z}_6) + I(A)$,

where $\mathbf{Z}_1 \in \mathcal{S}$*,* $\mathbf{Z}_2 \in \mathbf{V}_0 + \mathcal{S}$*,* $\mathbf{Z}_3 \in (\mathbf{Y}_0 + \mathcal{S}) \cup (\mathbf{Y}_1 + \mathcal{S})$*,* $\mathbf{Z}_4 \in \mathbf{Y}_2 + \mathcal{S}$*,* $\mathbf{Z}_5 \in \mathbf{W}_1 + \mathcal{S}$ *and* $\mathbf{Z}_6 \in (\mathbf{W}_0 + \mathcal{S}) \cup (\mathbf{W}_2 + \mathcal{S})$ *are chosen randomly.*

Proof. Regardless of the short cycles, the adjacency graph of FSR$(1 + x + x^3 + x^4)p(x)$ is shown in Figure 5. The maximum spanning trees of this simplified graph are divided into four classes, and we show them in Figure 6. For the class (A), we can choose $\mathbf{Z}_1 \in \mathcal{S}$, $\mathbf{Z}_2 \in \mathbf{V}_0 + \mathcal{S}$, $\mathbf{Z}_3 \in (\mathbf{Y}_0 + \mathcal{S}) \cup (\mathbf{Y}_1 + \mathcal{S})$, $\mathbf{Z}_4 \in \mathbf{Y}_2 + \mathcal{S}$ and $\mathbf{Z}_5 \in \mathbf{W}_1 + \mathcal{S}$ randomly and use them to join the long cycles into one cycle. By Table 2, the reader can verify that, they indeed can be used to join the long cycles together. Then, we choose a state from each small cycles to form the set A, and by these states the small cycles are joined into long cycles. Therefore, the FSRs that take $g = f(x_0, x_1, \dots, x_{n+4}) + I(\mathbf{Z}_1, \mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_5) + I(A)$ as their characteristic functions are maximum length FSRs. For the other classes (B), (C) and (D), the proof is similar. □

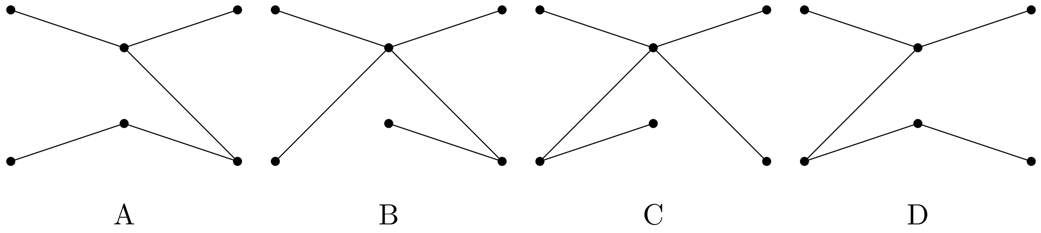

Figure 6: The maximum spanning trees in the simplified version of the adjacency graph of FSR$((1+x+x^3+x^4)p(x))$

It is shown by Jansen et al. [14]: for any $n \geq 4$, if we apply the cycle joining method to two different n-stage LFSRs, the resulting maximum length FSRs are different. Using this fact, we can count the number of De Bruijn sequences we have constructed in Theorem 7. The set A defined in Theorem 7 has $1 \cdot 6 \cdot 3 \cdot 3 \cdot 2 \cdot 3 = 324$ choices, the five states $\mathbf{Z}_i, 1 \leq i \leq 5$ have $a, a, 2a, a$ and a choices respectively, and the Boolean function f has $\frac{\phi(2^n-1)}{n}$ choices, where $a = 2^n - 2$ and $\phi(\cdot)$ is the Euler's totient function. Therefore, there are $324 \cdot a \cdot a \cdot 2a \cdot a \cdot a \cdot \frac{\phi(2^n-1)}{n} = \frac{648a^5\phi(2^n-1)}{n} = O(2^{6n})$ Boolean functions of type (1). Totally, there are $\frac{3888a^5\phi(2^n-1)}{n} = O(2^{6n})$ Boolean functions in Theorem 7. At last, we note that, the time we need to get a Boolean function in Theorem 7 is $O(2^m + n)$.

8 Conclusion

We presented a general method to calculate the adjacency graphs of LFSRs with primitive-like characteristic polynomials. As an application of this method, we explicitly determined the adjacency graphs of LFSRs with characteristic polynomials of the form $(1+x+x^3+x^4)p(x)$, where $p(x)$ is a primitive polynomial, and construct a large class of De Bruijn sequences from them.

References

[1] F. S. Annexstein, "Generating de Bruijn sequences: an efficient implementation," *IEEE Trans. Computers*, vol. 46, no. 2, pp. 198-200, Feb. 1997.

[2] N. G. de Bruijn, "A combinatorial problem," *Proc. Kon. Ned. Akad. Wetensch*, vol. 49, pp. 758-764, 1946.

[3] C. Cannière and B. Preneel, "Trivium," in New Stream Cipher Designs: The eSTREAM Finalists, ser. *Lecture Notes in Computer Science.* New York: Springer-Verlag, 2008, vol. 4986, pp. 244 – 266.

[4] A. H. Chan, R. A. Games and E. L. Key, "On the complexities of de Bruijn sequences," *J. Comb. Theory*, Ser. A, vol. 33, no. 3, pp. 233-246, Nov. 1982.

[5] 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.

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

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

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

[9] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*, Cambridge University Press, New York, NY, 2005.

[10] E. R. Hauge and T. Helleseth, "De Bruijn sequences, irreducible codes and cyclotomy," *Discrete Math.*, vol. 159, no. 1, pp. 143-154, Nov. 1996.

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

[12] M. Hell, T. Johansson, A. Maximov, and W. Meier, "The grain family of stream ciphers," in New Stream Cipher Designs: The eSTREAM Finalists, ser. *Lecture Notes in Computer Science.* New York: Springer-Verlag, 2008, vol. 4986, pp. 179 – 190.

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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] C.Y. Li, X.Y. Zeng, C.L. Li, T. Helleseth, and M. Li, "Construction of de Bruijn sequences from LFSRs with reducible characteristic polynomials," IEEE Trans. Inf. Theory, vol. 62, no. 1, pp. 610-624, Jan. 2016.

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

[20] 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.

[21] J. Mykkeltveit and J. Szmidt, "On cross joining de Bruijn sequences," Contemporary Mathematics, vol. 632, pp. 333-344, 2015.

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