De Bruijn Sequences, Adjacency Graphs and Cyclotomy

Ming Li[1] and Dongdai Lin[2]

Abstract

We study the problem of constructing De Bruijn sequences by joining cycles of linear feedback shift registers (LFSRs) with reducible characteristic polynomials. The main difficulty for joining cycles is to find the location of conjugate pairs between cycles, and the distribution of conjugate pairs in cycles is defined to be adjacency graphs. Let $l(x)$ be a characteristic polynomial, and $l(x) = l_1(x)l_2(x)\cdots l_r(x)$ be a decomposition of $l(x)$ into pairwise co-prime factors. Firstly, we show a connection between the adjacency graph of FSR($l(x)$) and the association graphs of FSR($l_i(x)$), $1 \leq i \leq r$. By this connection, the problem of determining the adjacency graph of FSR($l(x)$) is decomposed to the problem of determining the association graphs of FSR($l_i(x)$), $1 \leq i \leq r$, which is much easier to handle. Then, we study the association graphs of LFSRs with irreducible characteristic polynomials and give a relationship between these association graphs and the cyclotomic numbers over finite fields. At last, as an application of these results, we explicitly determine the adjacency graphs of some LFSRs, and show that our results cover the previous ones.

Keywords: MSC(94A55), De Bruijn sequence, feedback shift register, adjacency graph, irreducible polynomial, cyclotomy.

1 Introduction

Binary De Bruijn sequences of order n are sequences of period 2^n such that each n-tuple appears exactly once in one period. These sequences have many favorable properties, such as long period, large linear span and good randomness, and they are widely used in cryptography and modern communication systems [6]. It is well known [3] that the number of n-th order De Bruijn sequences is $2^{2^{n-1}-n}$. Even though the number of sequences of given order is very large, today it is only known how to efficiently construct small fractions of this large number [1, 4, 5, 12, 13, 22]. An excellent survey of algorithms for generating De Bruijn sequences is given in [6].

A classical method for constructing De Bruijn sequences is to consider a feedback shift register (FSR) producing several cycles which are joined together to form a full cycle. This method is known as the cycle joining method, proposed by Golomb [7]. For the application of this method, we need to know the location of conjugate pairs between cycles. The distribution of conjugate

[1]M. Li is with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China, and the University of Chinese Academy of Sciences, Beijing, China. E-mail: liming@iie.ac.cn.

[2]D.D. Lin is with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China. E-mail: ddlin@iie.ac.cn.

pairs in the cycles of an FSR is defined to be the adjacency graph of this FSR [10]. In recent years, constructing De Bruijn by using the adjacency graphs of FSRs has raised extensive attentions. Because the cycle structure of nonlinear feedback shift registers (NFSRs) are hard to study, there are few results on their adjacency graphs, and most of the known results are about linear feedback shift registers (LFSRs). By now, many linear feedback shift registers (LFSRs) have been analyzed about their adjacency graphs, for example, the LFSRs with characteristic polynomials of the form $p(x)$, $(1+x)^m p(x)$, $(1+x^m)p(x)$ 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 positive integer ≤ 5 [11, 14–17, 21]. Their adjacency graphs were determined and a large number of De Bruijn sequences were constructed from them.

Recently, a general method to determine the adjacency graphs of a class of LFSRs was given in [18]. There the authors considered the LFSRs with primitive-like characteristic polynomials (i.e., having the form $l(x)p(x)$, where $l(x)$ is a polynomial of small degree and $p(x)$ is a primitive polynomial) and gives a unified way to determine their adjacency graphs. Specifically, the authors proposed the concept of association graphs of LFSRs, and they showed how to convert the problem of determining the adjacency graph of $\mathrm{FSR}(l(x)p(x))$ to the problem of determining the association graph of $\mathrm{FSR}(l(x))$. Since $l(x)$ is a polynomial of small degree, the association graph of $\mathrm{FSR}(l(x))$ can be determined efficiently. Consequently, the adjacency graph of $\mathrm{FSR}(l(x)p(x))$ is easily obtained. As an application of their method, the authors explicitly determined the adjacency graph of $\mathrm{FSR}((1+x+x^3+x^4)p(x))$.

In this paper, we pay attention to the LFSRs with reducible characteristic polynomials, and study the problem of constructing De Bruijn sequences from them. We will present a way to determine their adjacency graphs, and give some properties about them. Let $l(x)$ be a characteristic polynomial and $l(x) = l_1(x)l_2(x)\cdots l_r(x)$ be a decomposition of $l(x)$ into pairwise co-prime factors. Firstly, by using the theory of LFSRs we express the cycles of $\mathrm{FSR}(l(x))$ in terms of the cycles of $\mathrm{FSR}(l_i(x))$, $1 \leq i \leq r$. Then we decompose the problem of determining the adjacency graph of $\mathrm{FSR}(l(x))$ to the problem of determining the association graphs of $\mathrm{FSR}(l_i(x))$, $1 \leq i \leq r$. We show that, if the periods of $l_1(x), l_2(x), \ldots, l_r(x)$ are pairwise co-prime then the adjacency graph of $\mathrm{FSR}(l(x))$ is totally determined by the association graphs of $\mathrm{FSR}(l_i(x))$, $1 \leq i \leq r$; otherwise the adjacency graph of $\mathrm{FSR}(l(x))$ is related to the solutions of a set of equations. Since the concept of association graph is of importance, we study especially the association graphs of LFSRs with irreducible characteristic polynomials, and give a connection between the association graphs and the cyclotomic numbers over finite fields. Finally, as an application of our results, we explicitly determine the adjacency graphs of some LFSRs, and show that our results cover the previous ones.

The paper is organized as follows. In Section 2, we introduce some preliminaries. In Section 3, we present an efficient method to decompose a sequence in $G(l(x))$. Section 4 analyzes the cycle structure of $\mathrm{FSR}(l(x))$. Section 5 gives the connection between the adjacency graph of $\mathrm{FSR}(l(x))$ and the association graphs of $\mathrm{FSR}(l_i(x))$, $1 \leq i \leq r$. Section 6 considers the association graphs of LFSRs with irreducible characteristic polynomials. We suggest some applications of our results in Section 7, and 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, see Figure 1.

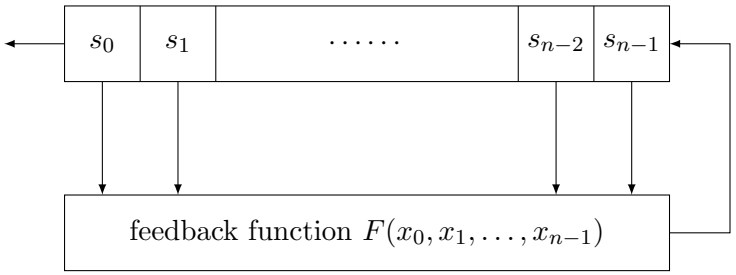

Figure 1: feedback shift register

The characteristic function of this FSR is defined to be $f = F + x_n$, and we use FSR(f) to denote the FSR with characteristic function 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 2^n output sequences of FSR(f) is denoted by $G(f)$. It is shown by Golomb [7] 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. The next state operation $\mathcal{T}$ of FSR(f) is a bijection on $\mathbb{F}_2^n$, $\mathcal{T} : (x_0, x_1, \ldots, x_{n-1}) \mapsto (x_1, \ldots, x_{n-1}, F(x_0, x_1, \ldots, x_{n-1}))$.

Let $\mathbf{s} = s_0 s_1 \ldots s_{p-1} \ldots$ be a periodic sequence with period $\mathrm{per}(\mathbf{s}) = p$. For convenience we denote $\mathbf{s}$ by $\mathbf{s} = (s_0 s_1 \ldots s_{p-1})$. 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 $0 \le i \le p-1$, 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 output.

An FSR is called a linear feedback shift register (LFSR) if its characteristic function f is linear; otherwise, it is called a nonlinear feedback shift register (NFSR). With a linear characteristic function $f(x_0, x_1, \ldots, x_n) = a_0x_0 + a_1x_1 + \cdots + a_nx_n$, a univariate polynomial

$c(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}_2[x]$ can be associated, that is usually called the characteristic polynomial of the LFSR. In the case of LFSRs it is more convenient to use the term characteristic polynomial rather than characteristic function.

For an n-stage FSR, the periods of its output sequences are limited by 2^n. If this value is attained, we call the sequences De Bruijn sequences, and the FSR a maximum length FSR. The unique cycle in a maximum length FSR is called a De Bruijn cycle or a full cycle. For an n-stage LFSR, the periods of its output sequences are limited by $2^n - 1$. If this value is attained, we call the sequences m-sequences, and the FSR a maximum length LFSR. It is well known that, FSR($l(x)$) is a maximum length LFSR if and only if $l(x)$ is primitive, that is, the period of $l(x)$ is $\mathrm{per}(l(x)) = 2^n - 1$.

2.2 Association Graphs

The concept of association graphs of LFSRs was proposed in [18] to deal with the adjacency graphs of LFSRs with primitive-like characteristic polynomials.

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

$$\mathbf{a} + \mathbf{b} = a_0 + b_0, a_1 + b_1, \ldots, a_i + b_i, \ldots,$$
$$c \cdot \mathbf{a} = ca_0, ca_1, \ldots, ca_i, \ldots.$$

Let $l(x) \in \mathbb{F}_2[x]$ be a polynomial of degree n. Then $G(l(x))$ contains 2^n periodic sequences, and it is a vector space of dimension n over $\mathbb{F}_2$ when endowed with the two operations $+$ and $\cdot$ defined above (see Chapter 8 of [19]). 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. It should be noted that, the bijection $\gamma_{\mathbf{u}}$ is not necessarily preserve the shift equivalent property, that is, for two shift 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 1. *[18] Let* $\mathbf{u}$ *be a sequence in* $G(l(x))$, $[\mathbf{s}_1]$ *and* $[\mathbf{s}_2]$ *be two cycles in* $G(l)$. *The association number of* $[\mathbf{s}_1]$ *and* $[\mathbf{s}_2]$ *with respect to* $\mathbf{u}$ *is defined by*

$$R_{\mathbf{u}}([\mathbf{s}_1], [\mathbf{s}_2]) = |\{(i, j) \mid L^i \mathbf{s_1} + L^j \mathbf{s_2} = \mathbf{u}, \\ 0 \le i \le \mathrm{per}(\mathbf{s}_1) - 1, 0 \le j \le \mathrm{per}(\mathbf{s}_2) - 1\}|.$$

It is easy to see that, the association number $R_{\mathbf{u}}([\mathbf{s}_1], [\mathbf{s}_2])$ is exactly the number of sequences in $[\mathbf{s}_1]$ whose image under $\gamma_{\mathbf{u}}$ is located in the cycle $[\mathbf{s}_2]$. In another word, $R_{\mathbf{u}}([\mathbf{s}_1], [\mathbf{s}_2]) = |\{(\mathbf{a}, \mathbf{b}) \mid \mathbf{a} + \mathbf{b} = \mathbf{u}, \mathbf{a} \in [\mathbf{s}_1], \mathbf{b} \in [\mathbf{s}_2]\}|$. We can use a graph to characterise these relations of the cycles in $G(l(x))$. Note that, these relations are influenced by the sequence $\mathbf{u}$.

Definition 2. *[18] 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 if* $R_{\mathbf{u}}([\mathbf{s}_1],[\mathbf{s}_2]) > 0$ *then there is an edge labeled with* $R_{\mathbf{u}}([\mathbf{s}_1],[\mathbf{s}_2])$ *between the two vertices* $[\mathbf{s}_1]$ *and* $[\mathbf{s}_2]$*.*

We refer the reader to Section VI of [18] for the basic properties of association graphs. In Section 6 of this paper, we will give the connection between the association graphs and cyclotomic numbers over finite fields.

2.3 Adjacency Graphs and Cyclotomy

For a state $\mathbf{S} = (s_0, s_1, \ldots, s_{n-1})$, its conjugate is defined to be $\widehat{\mathbf{S}} = (\overline{s}_0, s_1, \ldots, s_{n-1})$, 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 [7]. 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 3. *[10,20] 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.*

We should note that, adjacency graphs are special association graphs (see Theorem 5 of [18]). Specifically, the adjacency graph of $\mathrm{FSR}(f)$ is just the association graph of $\mathrm{FSR}(f)$ with respect to the sequence $\mathbf{e}$, where $\mathbf{e}$ is generated by $\mathrm{FSR}(f)$ with initial state $(1, 0, \ldots, 0)$.

It was shown by Fredricksen that, C is a full cycle if and only if the existence of a state $\mathbf{S}$ on C also implies the existence of its conjugate $\widehat{\mathbf{S}}$ on C (see Page 211 of [6]). This result implies that the adjacency graph of any FSR is a connected graph. Moreover, 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 a full cycle [2]. Therefore, for a given FSR, the number of full cycles that can be constructed from it by using the cycle joining method, is equal to the number of maximum spanning trees of its adjacency graph.

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 [8, 15] for more details.

In [9], some relationships between the adjacency graphs of LFSRs with irreducible characteristic polynomials and the cyclotomic numbers over finite fields was given. Let $g(x)$ be an irreducible polynomial of degree n. The authors there defined an 1-to-1 mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$. Under this mapping, the (state) cycles generated by FSR($g(x)$) correspond to the cyclotomic classes of $\mathbb{F}_{2^n}$ and a conjugate pair $(\mathbf{X}, \widehat{\mathbf{X}})$ corresponds to a pair of elements $(\gamma, 1+\gamma)$ in $\mathbb{F}_{2^n}$. By using this correspondence the authors showed that, the number of conjugate pairs shared by any two cycles of FSR($g(x)$) is equal to some cyclotomic number over $\mathbb{F}_{2^n}$. In Section 6 of this paper, we will also define a mapping to deal with the association graph of FSR($g(x)$). The mapping we will define is a little different from that in [9], but has the similar properties. We will show that the association number of any two cycles of FSR($g(x)$) is equal to some cyclotomic number over $\mathbb{F}_{2^n}$.

3 The Direct Sum Decomposition of $G(l(x))$

Let $l(x)$ be a characteristic polynomial of degree m, and $l(x) = l_1(x)l_2(x)\cdots l_r(x)$ be a decomposition of $l(x)$ into pairwise co-prime factors. We note that, it is not necessarily that $l_i(x)$ is an irreducible polynomial or a power of an irreducible polynomial. We only require that these factors are co-prime with each other. Let m_i be the degree of $l_i(x)$ for $1 \le i \le r$. Without lose of generality, we can assume $m_1 \le m_2 \le \cdots \le m_r$. Since $l_i(x), i = 1, 2, \ldots, r$ are pairwise co-prime, the vector space $G(l(x))$ has the direct sum decomposition (see Chapter 8 of [19]):

$$G(l(x)) = G(l_1(x)) + G(l_2(x)) + \cdots + G(l_r(x)),$$

which implies that, every sequence in $G(l(x))$ can be uniquely written as a sum of r sequences in $G(l_1(x))$, $G(l_2(x))$, $\cdots$, $G(l_r(x))$ respectively. Let $\mathbf{e}$ be the sequence generated by FSR($l(x)$) with the initial state $\mathbf{E} = (1, 0, \ldots, 0)$. By the above discussion, $\mathbf{e}$ can be uniquely written as

$$\mathbf{e} = \mathbf{e}_1 + \mathbf{e}_2 + \cdots + \mathbf{e}_r,$$

where $\mathbf{e}_i \in G(l_i(x))$ for $i = 1, 2, \ldots, r$. We call the sequence $\mathbf{e}_i$ the representative of $G(l_i(x))$ for $i = 1, 2, \ldots, r$. The concept of representatives will be used later in this paper. Firstly, we present an efficient method to determine these representatives.

For a bit string $\mathbf{a} = a_0, a_1, \ldots$, we use $\mathbf{a}|_m$ to denote its first m bits, that is, $\mathbf{a}|_m = a_0, a_1, \ldots, a_m$. Consider the first m bits of $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_r$. Let them be,

$$\begin{aligned}
\mathbf{e}_1|_m &= e_{1,0}, \ldots, e_{1,m_1-1}, e_{1,m_1}, \ldots, e_{1,m-1},\\
\mathbf{e}_2|_m &= e_{2,0}, \ldots, e_{2,m_2-1}, e_{2,m_2}, \ldots, e_{2,m-1},\\
&\cdots\cdots\cdots\\
\mathbf{e}_r|_m &= e_{r,0}, \ldots, e_{r,m_r-1}, e_{r,m_r}, \ldots, e_{r,m-1}.
\end{aligned}$$

Because $\mathbf{e}_1 + \mathbf{e}_2 + \cdots + \mathbf{e}_r = \mathbf{e}$, we know that,

$$\mathbf{e}_1|_m + \mathbf{e}_2|_m + \cdots + \mathbf{e}_r|_m = \mathbf{e}|_m = \mathbf{E}.$$

This equation is a vector equation, and it contains actually m equations. Recall that, $\mathbf{e}_i$ is a sequence in $G(l_i(x))$, hence the bit string $\mathbf{e}_i|_m$ satisfies the linear equation corresponding to $l_i(x)$. Consequently, these bits $e_{i,m_i}, \ldots, e_{i,m-1}$ can be written as linear combinations of $e_{i,0}, \ldots, e_{i,m_i-1}$. Therefore, the equation $\mathbf{e}_1|_m + \mathbf{e}_2|_m + \cdots + \mathbf{e}_r|_m = \mathbf{E}$ has only m unknowns,

$$e_{1,0}, \ldots, e_{1,m_1-1}, e_{2,0}, \ldots, e_{2,m_2-1}, \cdots, e_{r,0}, \ldots, e_{r,m_r-1}.$$

This implies that, the equation is a system of m linear equations with m unknowns, and it can be solved in time $O(m^2) \sim O(m^3)$. Once the first m_i bits of $\mathbf{e}_i$ is obtained, then the sequence $\mathbf{e}_i$ is totally determined.

For the representatives, we have the following property.

Theorem 1. *The minimal polynomial of* $\mathbf{e}_i$ *is* $l_i(x)$ *for* $1 \leq i \leq r$.

Proof. Since the sequence $\mathbf{e}$ is nonzero and it contains $m-1$ successive 0s, it can not be generated by any LFSR whose stages $\leq m-1$. So the minimal polynomial of $\mathbf{e}$ is $l(x)$. Suppose the minimal polynomial of $\mathbf{e}_i$ is not $l_i(x)$, but a proper divisor of $l_i(x)$. Then the minimal polynomial of the sum $\mathbf{e}_1 + \mathbf{e}_2 + \cdots + \mathbf{e}_r = \mathbf{e}$ would be a proper divisor of $l(x)$, which is a contradiction. □

4 The Cycle Structure of $G(l(x))$

In this section, we consider the cycle structure of $\mathrm{FSR}(l(x))$. We will express the cycles in $\mathrm{FSR}(l(x))$ in terms of the cycles in $\mathrm{FSR}(l_i(x)), i = 1, 2, \ldots, r$. For a periodic sequence $\mathbf{a}$, we use $[\mathbf{a}]$ to denote the cycle $[\mathbf{a}] = \{\mathbf{a}, L\mathbf{a}, \ldots, L^{\mathrm{per}(\mathbf{a})-1}\mathbf{a}\}$. The sum of two cycles $[\mathbf{a}]$ and $[\mathbf{b}]$ is defined to be $[\mathbf{a}] + [\mathbf{b}] = \{\mathbf{s} + \mathbf{t} \mid \mathbf{s} \in [\mathbf{a}], \mathbf{t} \in [\mathbf{b}]\}$. The following lemma deals with the sum of two cycles.

Lemma 1. *[18] Let* $\mathbf{s}_1$ *and* $\mathbf{s}_2$ *be two periodic sequences such that their minimal polynomials are co-prime. Let* $d = \gcd(\mathrm{per}(\mathbf{s}_1), \mathrm{per}(\mathbf{s}_2))$. *Then* $[\mathbf{s}_1]+[\mathbf{s}_2] = [\mathbf{s}_1+\mathbf{s}_2] \cup [L\mathbf{s}_1+\mathbf{s}_2] \cup \cdots \cup [L^{d-1}\mathbf{s}_1+\mathbf{s}_2]$. *In particular, if* $\gcd(\mathrm{per}(\mathbf{s}_1), \mathrm{per}(\mathbf{s}_2)) = 1$, *then* $[\mathbf{s}_1] + [\mathbf{s}_2] = [\mathbf{s}_1 + \mathbf{s}_2]$.

This lemma can be generalised to deal with the sum of more than two cycles.

Lemma 2. *Let* $\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_r$ *be periodic sequences such that their minimal polynomials are pairwise co-prime. Let* $d_i = \gcd(\mathrm{per}(\mathbf{s}_1 + \cdots + \mathbf{s}_i), \mathrm{per}(\mathbf{s}_{i+1}))$ *for* $i = 1, 2, \ldots, r-1$. *Then,*

$$\begin{aligned}&[\mathbf{s}_1] + [\mathbf{s}_2] + \cdots + [\mathbf{s}_r] \\ &= \cup_{I_1=0}^{d_1-1} \cup_{I_2=0}^{d_2-1} \cdots \cup_{I_{r-1}=0}^{d_{r-1}-1} [L^{I_1+I_2+\cdots+I_{r-1}}\mathbf{s}_1 + L^{I_2+\cdots+I_{r-1}}\mathbf{s}_2 + \cdots + L^{I_{r-1}}\mathbf{s}_{r-1} + \mathbf{s}_r].\end{aligned}$$

In particular, if $\mathrm{per}(\mathbf{s}_1), \mathrm{per}(\mathbf{s}_2), \ldots, \mathrm{per}(\mathbf{s}_r)$ *are pairwise co-prime, then*

$$[\mathbf{s}_1] + [\mathbf{s}_2] + \cdots + [\mathbf{s}_r] = [\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r].$$

Proof.

$$
\begin{aligned}
&[\mathbf{s}_1] + [\mathbf{s}_2] + \cdots + [\mathbf{s}_r] \\
&= \left(\cup_{I_1=0}^{d_1-1} [L^{I_1}\mathbf{s}_1 + \mathbf{s}_2]\right) + [\mathbf{s}_3] + \cdots + [\mathbf{s}_r] \\
&= \left(\cup_{I_1=0}^{d_1-1} \cup_{I_2=0}^{d_2-1} [L^{I_1+I_2}\mathbf{s}_1 + L^{I_2}\mathbf{s}_2 + \mathbf{s}_3]\right) + [\mathbf{s}_4] + \cdots + [\mathbf{s}_r] \\
&\quad \cdots \\
&= \cup_{I_1=0}^{d_1-1} \cup_{I_2=0}^{d_2-1} \cdots \cup_{I_{r-1}=0}^{d_{r-1}-1} [L^{I_1+I_2+\cdots+I_{r-1}}\mathbf{s}_1 + L^{I_2+\cdots+I_{r-1}}\mathbf{s}_2 + \cdots + L^{I_{r-1}}\mathbf{s}_{r-1} + \mathbf{s}_r]
\end{aligned}
$$

□

By using this lemma, we can express the cycles in $G(l(x))$ in terms of the cycles in $G(l_i(x))$, $1 \leq i \leq r$. We first recall some properties about the periods of polynomials. Let $c(x)$ be a polynomial satisfying $c(x) \neq 0$. The period of $c(x)$ is defined to be the least positive integer k such that $c(x) \mid x^k + 1$. Some basic properties about the periods of polynomials are given in [19]. It is not hard to show that, if the periods of $l_1(x), l_2(x), \ldots, l_r(x)$ are pairwise co-prime then $l_1(x), l_2(x), \ldots, l_r(x)$ must be pairwise co-prime. However, these polynomials being pairwise co-prime does not guarantee that their periods are pairwise co-prime.

Theorem 2. *Let $l(x)$ be a characteristic polynomial and $l(x) = l_1(x)l_2(x)\cdots l_r(x)$ be a decomposition of $l(x)$ into pairwise co-prime factors. Let the cycle structure of $G(l_1(x))$,$G(l_2(x))$,..., $G(l_r(x))$ be,*

$$
\begin{aligned}
G(l_1(x)) =& [\mathbf{s}_{1,1}] \cup [\mathbf{s}_{1,2}] \cup \cdots \cup [\mathbf{s}_{1,k_1}] \\
G(l_2(x)) =& [\mathbf{s}_{2,1}] \cup [\mathbf{s}_{2,2}] \cup \cdots \cup [\mathbf{s}_{2,k_2}] \\
&\vdots \\
G(l_r(x)) =& [\mathbf{s}_{r,1}] \cup [\mathbf{s}_{r,2}] \cup \cdots \cup [\mathbf{s}_{r,k_r}],
\end{aligned}
$$

where k_i is the number of cycles in $G(l_i(x))$ for $1 \leq i \leq r$. Then the cycle structure of $G(l(x))$ is given by,

$$
\begin{aligned}
G(l(x)) = &\left(\cup_{i_1=1}^{k_1} \cup_{i_2=1}^{k_2} \cdots \cup_{i_r=1}^{k_r}\right) \left(\cup_{I_1=0}^{d_1-1} \cup_{I_2=0}^{d_2-1} \cdots \cup_{I_{r-1}=0}^{d_{r-1}-1}\right) \\
&[L^{I_1+I_2\cdots+I_{r-1}}\mathbf{s}_{1,i_1} + L^{I_2\cdots+I_{r-1}}\mathbf{s}_{2,i_2} + \cdots + L^{I_{r-1}}\mathbf{s}_{r-1,i_{r-1}} + \mathbf{s}_{r,i_r}],
\end{aligned}
$$

where $d_j = \gcd(\mathrm{per}(\mathbf{s}_{1,i_1} + \cdots + \mathbf{s}_{j,i_j}), \mathrm{per}(\mathbf{s}_{j+1,i_{j+1}}))$ for $j = 1, 2, \ldots, r-1$.

In particular, if the periods of $l_1(x), l_2(x), \ldots, l_r(x)$ are pairwise co-prime, then,

$$
G(l(x)) = \cup_{i_1=1}^{k_1} \cup_{i_2=1}^{k_2} \cdots \cup_{i_r=1}^{k_r} [\mathbf{s}_{1,i_1} + \mathbf{s}_{2,i_2} + \cdots + \mathbf{s}_{r,i_r}].
$$

Proof. Because $l_1(x), l_2(x), \ldots, l_r(x)$ are pairwise co-prime polynomials, we have the direct sum decomposition $G(l(x)) = G(l_1(x)) + G(l_2(x)) + \cdots + G(l_r(x))$. Then we get that,

$$\begin{aligned}
G(l(x)) =& G(l_1(x)) + G(l_2(x)) + \cdots + G(l_r(x)) \\
=& \left(\cup_{i_1=1}^{k_1}[\mathbf{s}_{1,i_1}]\right) + \left(\cup_{i_2=1}^{k_2}[\mathbf{s}_{1,i_2}]\right) + \cdots + \left(\cup_{i_r=1}^{k_r}[\mathbf{s}_{1,i_r}]\right) \\
=& \left(\cup_{i_1=1}^{k_1}\cup_{i_2=1}^{k_2}\cdots\cup_{i_r=1}^{k_r}\right)\left([\mathbf{s}_{1,i_1}] + [\mathbf{s}_{1,i_2}] + \cdots + [\mathbf{s}_{1,i_r}]\right) \\
=& \left(\cup_{i_1=1}^{k_1}\cup_{i_2=1}^{k_2}\cdots\cup_{i_r=1}^{k_r}\right)\left(\cup_{I_1=0}^{d_1-1}\cup_{I_2=0}^{d_2-1}\cdots\cup_{I_{r-1}=0}^{d_{r-1}-1}\right) \\
& [L^{I_1+I_2\cdots+I_{r-1}}\mathbf{s}_{1,i_1} + L^{I_2\cdots+I_{r-1}}\mathbf{s}_{2,i_2} + \cdots + L^{I_{r-1}}\mathbf{s}_{r-1,i_{r-1}} + \mathbf{s}_{r,i_r}],
\end{aligned}$$

where the last equation is valid because of Lemma 2.

If the periods of $l_1(x), l_2(x), \ldots, l_r(x)$ are pairwise co-prime, then for any r sequences $\mathbf{s}_1 \in G(l_1(x)), \mathbf{s}_2 \in G(l_2(x)), \ldots, \mathbf{s}_r \in G(l_r(x))$ their periods must be pairwise co-prime, which implies that these parameters $d_1, d_2, \ldots, d_{r-1}$ all equal to 1. Therefore, $G(l(x)) = \cup_{i_1=1}^{k_1}\cup_{i_2=1}^{k_2}\cdots\cup_{i_r=1}^{k_r}[\mathbf{s}_{1,i_1} + \mathbf{s}_{2,i_2} + \cdots + \mathbf{s}_{r,i_r}]$. □

By this theorem, the cycles in $G(l(x))$ has the form $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$, where $\mathbf{s}_i$ is a sequence in $G(l_i(x))$ and a_i is an integer satisfying $0 \le a_i \le \mathrm{per}(\mathbf{s}_i)$ for $1 \le i \le r$. In particular, if the periods of $l_1(x), l_2(x), \ldots, l_r(x)$ are pairwise co-prime, then the cycles in $G(l(x))$ has the form $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$, where $\mathbf{s}_i$ is a sequence in $G(l_i(x))$ for $i = 1, 2, \ldots, r$.

We should note that, different arrays $(a_1, a_2, \ldots, a_r) \neq (b_1, b_2, \ldots, b_r)$ may give the same cycle $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r] = [L^{b_1}\mathbf{s}_1 + L^{b_2}\mathbf{s}_2 + \cdots + L^{b_r}\mathbf{s}_r]$. Theorem 2 shows a full list of the cycles in $G(l(x))$ without repeating, but it does not mean that different arrays always result in different cycles. The following theorem gives the condition for two cycles be the same one.

Theorem 3. *Let* $C_1 = [L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$ *and* $C_2 = [L^{b_1}\mathbf{s}_1 + L^{b_2}\mathbf{s}_2 + \cdots + L^{b_r}\mathbf{s}_r]$ *be two cycles in* $G(l(x))$. *Then* $C_1 = C_2$ *if and only if* $\gcd(\mathrm{per}(\mathbf{s}_i), \mathrm{per}(\mathbf{s}_j)) \mid (a_i - a_j) - (b_i - b_j)$ *for any* $1 \le i \ne j \le r$.

Proof. Suppose $C_1 = C_2$, then there exists an integer k such that,

$$L^k\left(L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r\right) = L^{b_1}\mathbf{s}_1 + L^{b_2}\mathbf{s}_2 + \cdots + L^{b_r}\mathbf{s}_r,$$

which implies that,

$$L^{a_1+k}\mathbf{s}_1 + L^{a_2+k}\mathbf{s}_2 + \cdots + L^{a_r+k}\mathbf{s}_r = L^{b_1}\mathbf{s}_1 + L^{b_2}\mathbf{s}_2 + \cdots + L^{b_r}\mathbf{s}_r.$$

Then by a simple deformation we get that,

$$\left(L^{a_1+k}\mathbf{s}_1 + L^{b_1}\mathbf{s}_1\right) = \left(L^{a_2+k}\mathbf{s}_2 + L^{b_2}\mathbf{s}_2\right) + \cdots + \left(L^{a_r+k}\mathbf{s}_r + L^{b_r}\mathbf{s}_r\right).$$

Since

$$\left(L^{a_1+k}\mathbf{s}_1 + L^{b_1}\mathbf{s}_1\right) \in G(l_1(x))$$

and

$$\left(L^{a_2+k}\mathbf{s}_2 + L^{b_2}\mathbf{s}_2\right) + \cdots + \left(L^{a_r+k}\mathbf{s}_r + L^{b_r}\mathbf{s}_r\right) \in G(l_2(x)\cdots l_r(x)),$$

and the two polynomials $l_1(x)$ and $l_2(x)\cdots l_r(x)$ are co-prime, we know that $L^{a_1+k}\mathbf{s}_1 + L^{b_1}\mathbf{s}_1 = \mathbf{0}$, the zero sequence. Similarly, we can show that $L^{a_2+k}\mathbf{s}_2 + L^{b_2}\mathbf{s}_2 = \cdots = L^{a_r+k}\mathbf{s}_r + L^{b_r}\mathbf{s}_r = \mathbf{0}$. Therefore, k satisfies the following congruence equations.

$$\begin{cases} k \equiv a_1 - b_1 \bmod \mathrm{per}(\mathbf{s}_1) \\ k \equiv a_2 - b_2 \bmod \mathrm{per}(\mathbf{s}_2) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ k \equiv a_r - b_r \bmod \mathrm{per}(\mathbf{s}_r) \end{cases}$$

It is not hard to show that, these congruence equations have a solution if and only if $\gcd(\mathrm{per}(\mathbf{s}_i), \mathrm{per}(\mathbf{s}_j)) \mid (a_i - a_j) - (b_i - b_j)$ for any $1 \le i \ne j \le r$. □

5 The Adjacency Graph of FSR($l(x)$)

In this section, we consider the adjacency graph of FSR($l(x)$). We will give formulas for the number of conjugate pairs shared by any two cycles in $G(l(x))$. According to Theorem 2, the cycles in $G(l(x))$ has the form $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$, where $\mathbf{s}_i$ is a sequence in $G(l_i(x))$ and a_i is an integer satisfying $0 \le a_i \le \mathrm{per}(\mathbf{s}_i)$ for $1 \le i \le r$.

Theorem 4. *Let $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$ and $[L^{b_1}\mathbf{t}_1 + L^{b_2}\mathbf{t}_2 + \cdots + L^{b_r}\mathbf{t}_r]$ be two cycles in $G(l(x))$, where $\mathbf{s}_i$ and $\mathbf{t}_i$ are two sequences in $G(l_i(x))$, and a_i and b_i are two integers satisfying $0 \le a_i \le \mathrm{per}(\mathbf{s}_i), 0 \le b_i \le \mathrm{per}(\mathbf{t}_i)$ for any $1 \le i \le r$. Then the number of conjugate pairs shared by the two cycles is equal to the number of arrays $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ that satisfy the following four conditions:*

1. *$L^{u_i}\mathbf{s}_i + L^{v_i}\mathbf{t}_i = \mathbf{e}_i$ for any $1 \le i \le r$.*
2. *$\gcd(\mathrm{per}(\mathbf{s}_i), \mathrm{per}(\mathbf{s}_j)) \mid (u_i - u_j) - (a_i - a_j)$ for any $1 \le i \ne j \le r$.*
3. *$\gcd(\mathrm{per}(\mathbf{t}_i), \mathrm{per}(\mathbf{t}_j)) \mid (v_i - v_j) - (b_i - b_j)$ for any $1 \le i \ne j \le r$.*
4. *$0 \le u_i \le \mathrm{per}(\mathbf{s}_i), 0 \le v_i \le \mathrm{per}(\mathbf{t}_i)$ for any $1 \le i \le r$.*

where $\mathbf{e}_i$ is the representative of $G(l_i(x))$ for $1 \le i \le r$.

Proof. Write the cycles $[\mathbf{s}_1], [\mathbf{s}_2], \ldots, [\mathbf{s}_r]$ and $[\mathbf{t}_1], [\mathbf{t}_2], \ldots, [\mathbf{t}_r]$ in the state cycle form, where each

state is of length m.

$$\begin{aligned}
[\mathbf{s}_1] =&[\mathbf{S}_{1,0}, \mathbf{S}_{1,1}, \ldots, \mathbf{S}_{1,\mathrm{per}(\cdot)-1}] & [\mathbf{t}_1] =&[\mathbf{T}_{1,0}, \mathbf{T}_{1,1}, \ldots, \mathbf{T}_{1,\mathrm{per}(\cdot)-1}] \\
[\mathbf{s}_2] =&[\mathbf{S}_{2,0}, \mathbf{S}_{2,1}, \ldots, \mathbf{S}_{2,\mathrm{per}(\cdot)-1}] & [\mathbf{t}_2] =&[\mathbf{T}_{2,0}, \mathbf{T}_{2,1}, \ldots, \mathbf{T}_{2,\mathrm{per}(\cdot)-1}] \\
\vdots & & \vdots & \\
[\mathbf{s}_r] =&[\mathbf{S}_{r,0}, \mathbf{S}_{r,1}, \ldots, \mathbf{S}_{r,\mathrm{per}(\cdot)-1}] & [\mathbf{t}_r] =&[\mathbf{T}_{r,0}, \mathbf{T}_{r,1}, \ldots, \mathbf{T}_{r,\mathrm{per}(\cdot)-1}]
\end{aligned}$$

For simplicity, we use the notation $\mathrm{per}(\cdot)$ to denote the period of the corresponding sequence. We need to show that there is an 1-to-1 correspondence between the conjugate pairs shared by the two cycles $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$ and $[L^{b_1}\mathbf{t}_1 + L^{b_2}\mathbf{t}_2 + \cdots + L^{b_r}\mathbf{t}_r]$ and the arrays $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ that satisfy the four conditions.

Suppose there exists an array $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ that satisfy the four conditions. Since this array satisfies Condition 1 we have,

$$L^{u_1}\mathbf{s}_1 + L^{v_1}\mathbf{t}_1 + L^{u_2}\mathbf{s}_2 + L^{v_2}\mathbf{t}_2 + \cdots + L^{u_r}\mathbf{s}_r + L^{v_r}\mathbf{t}_r = \mathbf{e},$$

which implies

$$\mathbf{S}_{1,u_1} + \mathbf{T}_{1,v_1} + \mathbf{S}_{2,u_2} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{S}_{r,u_r} + \mathbf{T}_{r,v_r} = \mathbf{E}, \tag{1}$$

where $\mathbf{E} = (1, 0, \ldots, 0)$. Define,

$$\mathbf{X} = \mathbf{S}_{1,u_1} + \mathbf{S}_{2,u_2} + \cdots + \mathbf{S}_{r,u_r}, \quad \mathbf{Y} = \mathbf{T}_{1,v_1} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{T}_{r,v_r}.$$

Then the above equation shows that, $(\mathbf{X}, \mathbf{Y})$ is a conjugate pair.

Since the array $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ satisfies Condition 2, that is, $\gcd(\mathrm{per}(\mathbf{s}_i), \mathrm{per}(\mathbf{s}_j)) \mid (u_i - u_j) - (a_i - a_j)$ for any $1 \le i \ne j \le r$, by Theorem 3 we know that $\mathbf{X}$ is a state on the cycle $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$. Similarly, Condition 3 ensures that $\mathbf{Y}$ is a state on the cycle $[L^{b_1}\mathbf{t}_1 + L^{b_2}\mathbf{t}_2 + \cdots + L^{b_r}\mathbf{t}_r]$. Therefore, $(\mathbf{X}, \mathbf{Y})$ is a conjugate pair shared by the two cycles $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$ and $[L^{b_1}\mathbf{t}_1 + L^{b_2}\mathbf{t}_2 + \cdots + L^{b_r}\mathbf{t}_r]$.

On the other hand, suppose $(\mathbf{X}, \mathbf{Y})$ is a conjugate pair shared by the two cycles $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$ and $[L^{b_1}\mathbf{t}_1 + L^{b_2}\mathbf{t}_2 + \cdots + L^{b_r}\mathbf{t}_r]$. We can assume,

$$\mathbf{X} = \mathbf{S}_{1,u_1} + \mathbf{S}_{2,u_2} + \cdots + \mathbf{S}_{r,u_r}, \quad \mathbf{Y} = \mathbf{T}_{1,v_1} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{T}_{r,v_r}.$$

Since $\mathbf{X}$ is state on the cycle $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$ and $\mathbf{Y}$ is state on the cycle $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$, by Theorem 3 we know that the array $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ satisfies Condition 2 and Condition 3.

Because $(\mathbf{X}, \mathbf{Y})$ is a conjugate pair, the equation $\mathbf{X} + \mathbf{Y} = \mathbf{E}$ holds. This implies that,

$$\mathbf{S}_{1,u_1} + \mathbf{T}_{1,v_1} + \mathbf{S}_{2,u_2} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{S}_{r,u_r} + \mathbf{T}_{r,v_r} = \mathbf{E}.$$

Let $\mathcal{T}$ be the next state operation corresponding to $\mathrm{FSR}(l(x))$. For any integer $t \ge 0$, we have

$$\mathcal{T}^t\left(\mathbf{S}_{1,u_1} + \mathbf{T}_{1,v_1} + \mathbf{S}_{2,u_2} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{S}_{r,u_r} + \mathbf{T}_{r,v_r}\right) = \mathcal{T}^t\mathbf{E},$$

which implies

$$\mathcal{T}^t\mathbf{S}_{1,u_1} + \mathcal{T}^t\mathbf{T}_{1,v_1} + \mathcal{T}^t\mathbf{S}_{2,u_2} + \mathcal{T}^t\mathbf{T}_{2,v_2} + \cdots + \mathcal{T}^t\mathbf{S}_{r,u_r} + \mathcal{T}^t\mathbf{T}_{r,v_r} = \mathcal{T}^t\mathbf{E}.$$

Therefore, the following equation holds,

$$L^{u_1}\mathbf{s}_1 + L^{v_1}\mathbf{t}_1 + L^{u_2}\mathbf{s}_2 + L^{v_2}\mathbf{t}_2 + \cdots + L^{u_r}\mathbf{s}_r + L^{v_r}\mathbf{t}_r = \mathbf{e}.$$

Then by the uniqueness of the decomposition of $\mathbf{e}$, we get that

$$L^{u_1}\mathbf{s}_1 + L^{v_1}\mathbf{t}_1 = \mathbf{e}_1, L^{u_2}\mathbf{s}_2 + L^{v_2}\mathbf{t}_2 = \mathbf{e}_2, \cdots, L^{u_r}\mathbf{s}_r + L^{v_r}\mathbf{t}_r = \mathbf{e}_r.$$

This shows that the array $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ satisfies Condition 1. □

According to the proof of Theorem 4, the conjugate pairs shared by the two cycles $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$ and $[L^{b_1}\mathbf{t}_1 + L^{b_2}\mathbf{t}_2 + \cdots + L^{b_r}\mathbf{t}_r]$ are exactly those $(\mathbf{S}_{1,u_1} + \mathbf{S}_{2,u_2} + \cdots + \mathbf{S}_{r,u_r}, \mathbf{T}_{1,v_1} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{T}_{r,v_r})$, where the array $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ satisfies the four conditions.

We note that, in Theorem 4 we didn't require that the two cycles $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$ and $[L^{b_1}\mathbf{t}_1 + L^{b_2}\mathbf{t}_2 + \cdots + L^{b_r}\mathbf{t}_r]$ are different. When the two cycles are the same one, we can obtain the number of conjugate pairs that located in the cycle $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$. Therefore, Theorem 4 considers all the adjacency relations of the cycles in $\mathrm{FSR}(l(x))$.

In Theorem 4, Conditions 2 and 3 are used to ensure that the two states $\mathbf{X}$ and $\mathbf{Y}$ are located on the two cycles respectively. If the periods of $l_1(x), l_2(x), \ldots, l_r(x)$ are pairwise co-prime, then the two conditions are no longer needed, and in this case we get a more concise formula.

Corollary 1. *In the case that the periods of $l_1(x), l_2(x), \ldots, l_r(x)$ are pairwise co-prime, let $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$ and $[\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]$ be two cycles in $G(l(x))$, where $\mathbf{s}_i$ and $\mathbf{t}_i$ are two sequences in $G(l_i(x))$ for any $1 \le i \le r$. Then the two cycles share*

$$R_{\mathbf{e}_1}([\mathbf{s}_1], [\mathbf{t}_1])R_{\mathbf{e}_2}([\mathbf{s}_2], [\mathbf{t}_2]) \cdots R_{\mathbf{e}_r}([\mathbf{s}_r], [\mathbf{t}_r])$$

conjugate pairs, where $\mathbf{e}_i$ is the representative of $G(l_i(x))$ for $1 \le i \le r$.

Proof. In this special case, we know that the periods of $\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_r$ are pairwise co-prime, that is, $\gcd(\mathrm{per}(\mathbf{s}_i), \mathrm{per}(\mathbf{s}_j)) = 1$ for any $1 \le i \ne j \le r$. Consequently, Condition 2 of Theorem 4 is always valid. Similarly, Condition 3 is also always valid. Then by Theorem 4, the number of conjugate pairs shared by the two cycles is equal to the number of arrays $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ that satisfy the following two conditions:

1. $L^{u_i}\mathbf{s}_i + L^{v_i}\mathbf{t}_i = \mathbf{e}_i$ for any $1 \le i \le r$.
2. $0 \le u_i \le \mathrm{per}(\mathbf{s}_i), 0 \le v_i \le \mathrm{per}(\mathbf{t}_i)$ for any $1 \le i \le r$.

By the definition of association numbers, the number of pairs (u_i, v_i) that satisfy the two conditions is $R_{\mathbf{e}_i}([\mathbf{s}_i], [\mathbf{t}_i])$. Because these pairs $(u_1, v_1), (u_2, v_2), \ldots, (u_r, v_r)$ are independent with each other, the number of arrays $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ that satisfy the two conditions is $R_{\mathbf{e}_1}([\mathbf{s}_1], [\mathbf{t}_1]) R_{\mathbf{e}_2}([\mathbf{s}_2], [\mathbf{t}_2]) \cdots R_{\mathbf{e}_r}([\mathbf{s}_r], [\mathbf{t}_r])$. □

It is easy to verify that, the conjugate pairs shared by the two cycles $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$ and $[\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]$ are exactly those $(\mathbf{S}_{1,u_1} + \mathbf{S}_{2,u_2} + \cdots + \mathbf{S}_{r,u_r}, \mathbf{T}_{1,v_1} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{T}_{r,v_r})$, where the array $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ satisfies $L^{u_1}\mathbf{s}_1 + L^{v_1}\mathbf{t}_1 = \mathbf{e}_1, L^{u_2}\mathbf{s}_2 + L^{v_2}\mathbf{t}_2 = \mathbf{e}_2, \cdots, L^{u_r}\mathbf{s}_r + L^{v_r}\mathbf{t}_r = \mathbf{e}_r$. Hence, the problem of finding conjugate pairs shared by any two cycles in $G(l(x))$ is decomposed into the problems of finding the association relations between the cycles in $G(l_i(x))$ for $i = 1, 2, \ldots, r$, which are obviously easier to handle.

We note that, in Corollary 1, we didn't require the two cycles $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$ and $[\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]$ are different. When the two cycles are the same one, we get that, there are $\frac{1}{2} R_{\mathbf{e}_1}([\mathbf{s}_1], [\mathbf{s}_1]) R_{\mathbf{e}_2}([\mathbf{s}_2], [\mathbf{s}_2]) \cdots R_{\mathbf{e}_r}([\mathbf{s}_r], [\mathbf{s}_r])$ conjugate pairs in the cycle $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$. Therefore, Corollary 1 considers all the adjacency relations of the cycles in $\mathrm{FSR}(l(x))$.

6 Irreducible Polynomials and Cyclotomy

By the results in Section 5, the adjacency graph of $\mathrm{FSR}(l(x))$ relies on the association graphs of $\mathrm{FSR}(l_1(x)), \mathrm{FSR}(l_2(x)), \ldots, \mathrm{FSR}(l_r(x))$. So it is helpful to study the association graphs of LFSRs. In [18], the authors presents some basic properties about association graphs. In this section, we pay attention to the LFSRs with irreducible characteristic polynomials, and give a connection between their association graphs and the cyclotomic numbers over finite fields.

Let $g(x)$ be an irreducible polynomial of degree n and period p. Let $q = \frac{2^n - 1}{p}$. By the theory of LFSRs, $G(g(x))$ contains the zero cycle $[\mathbf{0}]$ and q cycles of length p. Denote the q non-zero cycles by $[\mathbf{s}_0], [\mathbf{s}_1], \ldots, [\mathbf{s}_{q-1}]$, where $\mathbf{s}_0, \mathbf{s}_2, \ldots, \mathbf{s}_{q-1}$ are non-zero sequences in $G(g(x))$ that in different cycles. Let β be a root of g in some extended field of $\mathbb{F}_2$. Then we can construct a finite field $\mathbb{F}_{2^n}$ with $g(x)$ as a defining polynomial. Let $\alpha \in \mathbb{F}_{2^n}$ be a primitive element satisfying $\alpha^q = \beta$, then $\mathbb{F}_{2^n} = \mathbb{F}_2(\alpha) = \{0, \alpha^0, \alpha^1, \ldots, \alpha^{2^n - 2}\}$. It is well known that, for any sequence $\mathbf{a} \in G(g)$, there exists a unique $\gamma \in \mathbb{F}_{2^n}$ such that $\mathbf{a} = (a_i)_{i=0}^{\infty} = (\mathrm{Tr}(\gamma\beta^i))_{i=0}^{\infty}$, where the trace function Tr is from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ and a_i is the i-th element of $\mathbf{a}$. This is usually called the trace representation of $\mathbf{a}$. Define a mapping from $G(g)$ to $\mathbb{F}_{2^n}$,

$$\Psi : G(g) \to \mathbb{F}_{2^n}, \quad \mathbf{a} \mapsto \gamma.$$

The mapping is defined in a different way from that in [9], but has the similar properties.

Theorem 5. *The mapping Ψ is an 1-to-1 mapping and has the properties that, for any sequences $\mathbf{a}$ and $\mathbf{b}$ in $G(g)$, we have $\Psi(L\mathbf{a}) = \Psi(\mathbf{a})\beta$ and $\Psi(\mathbf{a} + \mathbf{b}) = \Psi(\mathbf{a}) + \Psi(\mathbf{b})$.*

Proof. Let $\mathbf{a} = (a_i)_{i=0}^{\infty}$ and $\mathbf{b} = (b_i)_{i=0}^{\infty}$ be two sequences in $G(g(x))$. If $\Psi(\mathbf{a}) = \Psi(\mathbf{b})$, then

$a_i = \mathrm{Tr}(\Psi(\mathbf{a})\beta^i) = \mathrm{Tr}(\Psi(\mathbf{b})\beta^i) = b_i$ holds for any $i \geq 0$, which implies $\mathbf{a} = \mathbf{b}$. Therefore, Ψ is an injection. Since $G(g)$ and $\mathbb{F}_{2^n}$ have the same size, Ψ must be an 1-to-1 mapping.

Let $\Psi(\mathbf{a}) = \gamma$ and $\Psi(\mathbf{b}) = \delta$. By the definition of Ψ, we get that, $\Psi(L\mathbf{a}) = \Psi((a_{i+1})_{i=0}^{\infty}) = \Psi(\mathrm{Tr}(\gamma\beta^{i+1})_{i=0}^{\infty}) = \Psi(\mathrm{Tr}(\gamma\beta\beta^i)_{i=0}^{\infty}) = \gamma\beta = \Psi(\mathbf{a})\beta$, and $\Psi(\mathbf{a}+\mathbf{b}) = \Psi((a_i)_{i=0}^{\infty} + (b_i)_{i=0}^{\infty}) = \Psi(\mathrm{Tr}(\gamma\beta^i)_{i=0}^{\infty} + \mathrm{Tr}(\delta\beta^i)_{i=0}^{\infty}) = \Psi(\mathrm{Tr}((\gamma+\delta)\beta^i)_{i=0}^{\infty}) = \gamma + \delta = \Psi(\mathbf{a}) + \Psi(\mathbf{b})$. □

These properties of Ψ induce a correspondence between the cycles in $G(g)$ and the cyclotomic classes in $\mathbb{F}_{2^n}$. Consider the following cyclotomic classes,

$$\begin{aligned} C_0 &= \{\beta^0, \beta^1, \ldots, \beta^{p-1}\} \\ C_1 &= \{\alpha\beta^0, \alpha\beta^1, \ldots, \alpha\beta^{p-1}\} \\ &\cdots \\ C_{q-1} &= \{\alpha^{q-1}\beta^0, \alpha^{q-1}\beta^1, \ldots, \alpha^{q-1}\beta^{p-1}\} \end{aligned}$$

The class C_i is the i-th cyclotomic class of $\mathbb{F}_{2^n}$. The set $\mathbb{F}_{2^n} \setminus \{0\}$ is partitioned into disjoint classes, i.e., $\mathbb{F}_{2^n} \setminus \{0\} = C_0 \cup C_1 \cup \cdots \cup C_{q-1}$. Given a cycle $[\mathbf{s}_i]$ in $G(g)$, this cycle contains $\mathbf{s}_i$ and all its shift equivalent sequences,

$$[\mathbf{s}_i] = \{\mathbf{s}_i, L\mathbf{s}_i, \ldots, L^{p-1}\mathbf{s}_i\}.$$

Since $\Psi(L\mathbf{a}) = \Psi(\mathbf{a})\beta$ holds for any $\mathbf{a} \in G(g(x))$, the set

$$\{\Psi(\mathbf{s}_i), \Psi(L\mathbf{s}_i), \ldots, \Psi(L^{p-1}\mathbf{s}_i)\},$$

is a cyclotomic class of $\mathbb{F}_{2^n}$. For convenience, we use $\Psi([\mathbf{s}_i])$ to denote this set. Because Ψ is an 1-to-1 mapping, different cycles in $G(g)$ must give different cyclotomic classes, and there is an 1-to-1 correspondence between the cycles in $G(g)$ and the cyclotomic classes of $\mathbb{F}_{2^m}$. Without lose of generality, in the following discussion we assume $\Psi([\mathbf{s}_i]) = C_i$ for $0 \leq i \leq q-1$.

Theorem 6. *Let* $\mathbf{s}$ *be a sequence in* $G(g)$*, and let* $\Psi(\mathbf{s}) = \alpha^a\beta^b$*, where* a *and* b *are two integers satisfying* $0 \leq a \leq q-1$ *and* $0 \leq b \leq p-1$*. Then the association number of* $[\mathbf{s}_i]$ *and* $[\mathbf{s}_j]$ *with respect to* $\mathbf{s}$ *is*

$$R_{\mathbf{s}}([\mathbf{s}_i], [\mathbf{s}_j]) = (i-a, j-a)_q,$$

where the two integers $i-a$ *and* $j-a$ *are reduced modulo* q*.*

Proof. Let γ be an element in $\mathbb{F}_{2^m}$. We use $\gamma + C_i$ to denote the set $\{\gamma + \delta \mid \delta \in C_i\}$, and γC_i to denote the set $\{\gamma\delta \mid \delta \in C_i\}$. We need to prove that $|(\alpha^a\beta^b + C_i) \cap C_j| = (i-a, j-a)_q$. This can be done as follows,

$$\begin{aligned} |(\alpha^a\beta^b + C_i) \cap C_j| &= |\alpha^{-a}\beta^{-b}((\alpha^a\beta^b + C_i) \cap C_j)| \\ &= |\alpha^{-a}((\alpha^a + C_i) \cap C_j)| \\ &= |(1 + C_{i-a}) \cap C_{j-a})| \\ &= (i-a, j-a)_q. \end{aligned}$$

□

It is shown in [9] (see Theorem 4 of [9]) that the conjugate pairs shared by any two cycles of FSR($g(x)$) is equal to some cyclotomic number over $\mathbb{F}_{2^n}$, while this theorem shows that the association number of any two cycles of FSR($g(x)$) is equal to some cyclotomic number. Because adjacency graphs are special association graphs (see Theorem 5 of [18]), this theorem partially generalized the result in [9].

7 Applications

7.1 Applications to the product of primitive polynomials

Let $p(x)$ be a primitive polynomial of degree n. Then $G(p(x))$ contains two cycles, $[\mathbf{0}]$ and $[\mathbf{s}]$, where $\mathbf{0}$ is the zero sequence and $\mathbf{s}$ is an m-sequence in $G(p(x))$. Since the cycle structure of FSR($p(x)$) is very simply, its association graph can be obtained directly.

Theorem 7. *Let $p(x)$ be a primitive polynomial of degree n, and $G(p(x)) = [\mathbf{0}] \cup [\mathbf{s}]$ where $\mathbf{s}$ is an m-sequence in $G(p(x))$. The association numbers of the cycles in $G(p(x))$ with respect to any nonzero sequence $\mathbf{u} \in G(p(x))$ is*

$$R_{\mathbf{u}}([\mathbf{0}], [\mathbf{0}]) = 0, R_{\mathbf{u}}([\mathbf{0}], [\mathbf{s}]) = 1, R_{\mathbf{u}}([\mathbf{s}], [\mathbf{s}]) = 2^n - 2.$$

Proof. It is easy to see that $R_{\mathbf{u}}([\mathbf{0}], [\mathbf{0}]) = 0$ and $R_{\mathbf{u}}([\mathbf{0}], [\mathbf{s}]) = 1$. In the following, we show that $R_{\mathbf{u}}([\mathbf{s}], [\mathbf{s}]) = 2^n - 2$. By the definition of association numbers, $R_{\mathbf{u}}([\mathbf{s}], [\mathbf{s}]) = |\{\mathbf{s}_1 \mid \mathbf{u} + \mathbf{s}_1 \in [\mathbf{s}], \mathbf{s}_1 \in [\mathbf{s}]\}| = |G(p(x)) \setminus \{\mathbf{0}, \mathbf{u}\}| = 2^n - 2$. This completes the proof. □

In [18], the association graphs of LFSRs is assumed to be obtained by using the exhaustive search method, that is, for a given polynomial $l(x)$ of degree m and a sequence $\mathbf{u} \in G(l(x))$, we need time $O(2^m)$ to calculate the association graph of FSR($l(x)$) with respect to $\mathbf{u}$. However, by Theorem 7 if $l(x)$ is a primitive polynomial then its association graph can be obtained directly. We should note that, Corollary 1 together with Theorem 7 give the adjacency graph of $G(p_1(x)p_2(x)\cdots p_r(x))$, where $p_1(x), p_2(x), \ldots, p_r(x)$ are primitive polynomials such that $\deg p_1(x), \deg p_1(x), \ldots, \deg p_1(x)$ are pairwise co-prime. These adjacency graphs have been studied in [16] using a different method.

It is easy to verify that, the degrees of $p_1(x), p_1(x), \ldots, p_1(x)$ are pairwise co-prime implies that the periods of $p_1(x), p_2(x), \ldots, p_r(x)$ are pairwise co-prime. By Theorem 2, if this is the case then the cycles in $G(p_1(x)p_2(x)\cdots p_r(x))$ have the form of $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$, where $\mathbf{s}_i$ is a sequence in $G(p_i(x))$.

Corollary 2. *[16] Let $p_1(x), p_2(x), \ldots, p_r(x)$ be primitive polynomials with their degrees pairwise co-prime. Let $[\mathbf{s}_1+\mathbf{s}_2+\cdots+\mathbf{s}_r]$ and $[\mathbf{t}_1+\mathbf{t}_2+\cdots+\mathbf{t}_r]$ be two cycles in $G(p_1(x)p_2(x)\cdots p_r(x))$, where $\mathbf{s}_i$ and $\mathbf{t}_i$ are two nonzero sequences in $G(p_i(x))$ for $1 \le i \le r$. Then the number of con-*

jugate pairs shared by the two cycles is

$$\left(\prod_{\{i|\mathbf{s}_i\neq\mathbf{0},\mathbf{t}_i\neq\mathbf{0}\}}(2^{n_i}-2)\right)\left(\prod_{\{i|\mathbf{s}_i=\mathbf{0},\mathbf{t}_i\neq\mathbf{0}\}}1\right)\left(\prod_{\{i|\mathbf{s}_i\neq\mathbf{0},\mathbf{t}_i=\mathbf{0}\}}1\right)\left(\prod_{\{i|\mathbf{s}_i=\mathbf{0},\mathbf{t}_i=\mathbf{0}\}}0\right).$$

Proof. Let $\mathbf{e}$ be the sequence generated by $\mathrm{FSR}(p_1(x)p_2(x)\cdots p_r(x))$ with the initial state (1, 0, ..., 0). The sequence $\mathbf{e}$ has the unique decomposition $\mathbf{e}=\mathbf{e}_1+\mathbf{e}_2+\cdots+\mathbf{e}_r$ such that $\mathbf{e}_r\in G(p_i(x))$ for $1\le i\le r$. By Theorem 1, the minimal polynomial of $\mathbf{e}_i$ is $p_i(x)$, that is, $\mathbf{e}_i\neq\mathbf{0}$ for $1\le i\le r$. By Corollary 1, the number of conjugate pairs shared by the two cycles is $R_{\mathbf{e}_1}([\mathbf{s}_1],[\mathbf{t}_1])R_{\mathbf{e}_2}([\mathbf{s}_2],[\mathbf{t}_2])\cdots R_{\mathbf{e}_r}([\mathbf{s}_r],[\mathbf{t}_r])$. Then we can finish the proof by applying Theorem 7 to this formula. □

In fact, Corollary 1 together with Theorem 6 also give some results on the adjacency graphs of LFSRs whose characteristic polynomials are a product of irreducible polynomials. Let $g_1(x),g_2(x),\ldots,g_r(x)$ be irreducible polynomials with their periods pairwise co-prime (which implies that $g_1(x),g_2(x),\ldots,g_r(x)$ are pairwise co-prime). Then the number of conjugate pairs shared by any two cycles in $G(g_1(x)g_2(x)\ldots g_r(x))$ is a product of some cyclotomic numbers.

7.2 Applications to primitive-like polynomials

Primitive-like polynomials are defined to be the polynomials of the form $l(x)p(x)$, where $l(x)$ is a polynomial of small degree and $p(x)$ is a primitive polynomial [18]. Let $\deg l(x)=m$ and $\deg p(x)=n$. For simplicity, we consider here only the case of $\gcd(\mathrm{per}(l(x)),\mathrm{per}(p(x)))=1$. Let $\mathbf{e}$ be the sequence generated by $\mathrm{FSR}(l(x)p(x))$ with the initial state $(1,0,\ldots,0)$, and $\mathbf{e}=\mathbf{u}+\mathbf{s}$ be the decomposition of $\mathbf{e}$ such that $\mathbf{u}\in G(l(x))$ and $\mathbf{s}\in G(p(x))$. It was shown in [18] that, the adjacency graph of $\mathrm{FSR}(l(x)p(x))$ is related to the association graph of $\mathrm{FSR}(l(x))$ with respect to $\mathbf{u}$. The decomposition $\mathbf{e}=\mathbf{u}+\mathbf{s}$ is assumed to be obtained in time $O(n2^m)$ and the association graph of $\mathrm{FSR}(l(x))$ is assumed to be obtained in time $O(2^m)$. Therefore, by the results there determining the adjacency graph of $\mathrm{FSR}(l(x)p(x))$ needs time $O(n2^m)$. In fact, the time complicity can be optimized by using the results in this paper.

Let $l(x)=l_1(x)l_2(x)\cdots l_r(x)$ be a decomposition of $l(x)$ into pairwise co-prime factors. Let the degree of $l_i(x)$ be m_i for $1\le i\le r$. Without lose of generality, we assume $m_1\le m_2\le\cdots\le m_r$. Let $\mathbf{e}=\mathbf{e}_1+\mathbf{e}_2+\cdots+\mathbf{e}_r+\mathbf{s}$ be the decomposition of $\mathbf{e}$ such that $\mathbf{e}_i\in G(l_i(x))$ for $1\le i\le r$ and $\mathbf{s}\in G(p(x))$. By the discussion in Section 3, the decomposition of $\mathbf{e}$ can be obtained in time $O((m+n)^3)$. Then, by Corollary 1 we can get the adjacency graph of $\mathrm{FSR}(l(x)p(x))$ by analyzing the association graphs of $\mathrm{FSR}(l_i(x))$ with respect to $\mathbf{e}_i$ for $1\le i\le r$, which needs time $O(2^{m_1}+2^{m_2}+\cdots+2^{m_r})$. Therefore, the total time to determine the adjacency graph of $\mathrm{FSR}(l(x)p(x))$ is $O((m+n)^3+2^{m_1}+2^{m_2}+\cdots+2^{m_r})$, which can be much smaller than $O(n2^m)$.

We use an example to explain the above discussion. The adjacency graph of $\mathrm{FSR}((1+x+x^3+x^4)p(x))$ has been analyzed in [18]. Since $1+x+x^3+x^4=(1+x^2)(1+x+x^2)$, instead of analyzing the association graph of $\mathrm{FSR}(1+x+x^3+x^4)$ with respect to $\mathbf{u}=(000111)$ (see Figures

1 and 2 in [18]), we can analyze the association graphs of FSR$(1+x^2)$ and FSR$(1+x+x^2)$ with respect to $\mathbf{e}_1 = (10)$ and $\mathbf{e}_2 = (101)$ respectively. The two mappings $\gamma_{\mathbf{e}_1}$ and $\gamma_{\mathbf{e}_2}$ are shown in Figures 2 and 3.

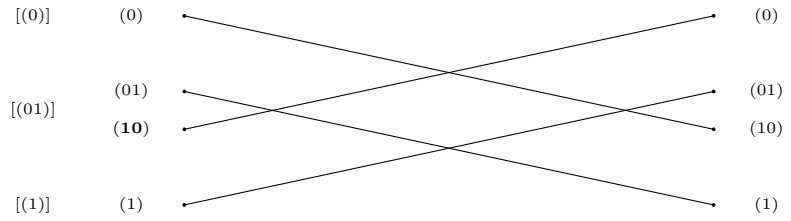

Figure 2: The mapping $\gamma_{\mathbf{e}_1}$ on $G(1+x^2)$, where $\mathbf{e}_1 = (10)$

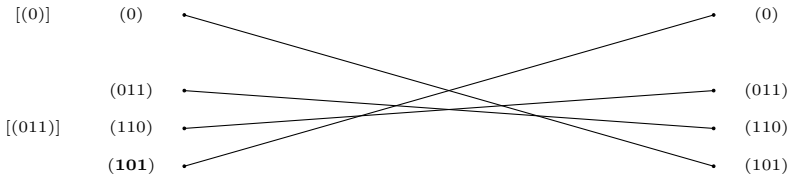

Figure 3: The mapping $\gamma_{\mathbf{e}_2}$ on $G(1+x+x^2)$, where $\mathbf{e}_2 = (101)$

The association graphs of FSR$(1+x^2)$ and FSR$(1+x+x^2)$ with respect to $\mathbf{e}_1 = (10)$ and $\mathbf{e}_2 = (101)$ respectively can be easily determined from two mappings $\gamma_{\mathbf{e}_1}$ and $\gamma_{\mathbf{e}_2}$, and they will not be given here. The cycle structure of $G(1+x^2)$, $G(1+x+x^2)$ and $G(p(x))$ are,

$$\begin{aligned} G(1+x^2) &= [(0)] \cup [(01)] \cup [(1)] \\ G(1+x+x^2) &= [(0)] \cup [(011)] \\ G(p(x)) &= [(0)] \cup [\mathbf{s}]. \end{aligned}$$

By Theorem 2, the cycle structure of FSR$((1+x^2)(1+x+x^2)p(x))$ is,

$$\begin{aligned} & G((1+x^2)(1+x+x^2)p(x)) \\ =& [(0)+(0)+(0)] \cup [(01)+(0)+(0)] \cup [(1)+(0)+(0)] + \\ & [(0)+(011)+(0)] \cup [(01)+(011)+(0)] \cup [(1)+(011)+(0)] + \\ & [(0)+(0)+\mathbf{s}] \cup [(01)+(0)+\mathbf{s}] \cup [(1)+(0)+\mathbf{s}] + \\ & [(0)+(011)+\mathbf{s}] \cup [(01)+(011)+\mathbf{s}] \cup [(1)+(011)+\mathbf{s}] \\ =& [(0)] \cup [(01)] \cup [(1)] + [(011)] \cup [(000111)] \cup [(001)] + \\ & [\mathbf{s}] \cup [(01)+\mathbf{s}] \cup [(1)+\mathbf{s}] + [(011)+\mathbf{s}] \cup [(000111)+\mathbf{s}] \cup [(001)+\mathbf{s}]. \end{aligned}$$

From the association graphs of FSR$(1+x^2)$, FSR$(1+x+x^2)$ and FSR$(p(x))$, the adjacency graph of FSR$((1+x+x^2)(1+x^2)p(x))$ can be determined. We take the two cycles $[(011)]$ and

$[(000111) + \mathbf{s}]$ for example to show how to calculate the number of conjugate pairs shared by them. Because $[(011)] = [(0) + (011) + (0)]$ and $[(000111) + \mathbf{s}] = [(01) + (011) + \mathbf{s}]$, by Corollary 1 the number of conjugate pairs shared by the two cycles is

$$R_{\mathbf{e}_1}([(0)], [(01)])R_{\mathbf{e}_2}([(011)], [(011)])R_{\mathbf{s}}([(0)], [\mathbf{s}]) = 2,$$

which coincides with the result in [18].

8 Conclusion

We studied the relationship between the adjacency graphs and the association graphs of LFSRs. By using this relationship, the problem of determining the adjacency graphs of LFSRs is decomposed to the problem of determining the association graphs of LFSRs with small orders, which is much easier to handle. We also studied the association graphs of LFSRs with irreducible characteristic polynomials, and showed that these association graphs are related to the cyclotomic numbers over finite fields. At the end, we suggested some applications of these results.

References

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

[2] S. Chaiken and D. J. Kleitman, "Matrix tree theorems," *J. Combinat. Theory A*, vol. 24, no. 3, pp. 377 – 381, May 1978.

[3] N. G. de Bruijn, "A combinatorial problem," *Koninklijke Nederlandse Akademie Wetenschappen*, vol. 49, pp. 758-764, Jun. 1946.

[4] 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.

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

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

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

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

[9] E. R. Hauge and T. Helleseth, "De Bruijn sequences, irreducible codes and cyclotomy," *Discrete Math.*, vol. 159, nos. 1-3, pp. 143-154, Nov. 1996.

[10] E. R. Hauge and J. Mykkeltveit, "On the classification of deBruijn sequences," *Discrete Math.*, vol. 148, nos. 1-2, pp. 65-83, Jan. 1996.

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

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] C. Y. Li, X. 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.

[17] M. Li, Y. Jiang, and D. Lin, "The adjacency graphs of some feedback shift registers," in *Proc. Designs, Codes, Cryptogr.*, pp. 1-19, doi: 10.1007/s10623-016-0187-6.

[18] M. Li, D. Lin, "The adjacency graphs of linear feedback shift registers with primitive-like characteristic polynomials," in *Proc. IEEE Trans. Inf. Theory*, doi: 10.1109/TIT.2016.2634420

[19] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 1997.

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

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

[22] J. Mykkeltveit and J. Szmidt, "On cross joining de Bruijn sequences," in *Proc. Topics Finite Field Contem. Math.*, vol. 632, Providence, RI, USA, 2015, pp. 335-346.