A Group-theory Method to The Cycle Structures of Feedback Shift Registers

Ming Li Yupeng Jiang and Dongdai Lin

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

April 21, 2015

Abstract

In this paper, we consider the cycle structures of feedback shift registers (FSRs). At the beginning, the cycle structures of two special classes of FSRs, pure circulating registers (PCRs) and pure summing registers (PSRs), are studied and it is proved that there are no other FSRs have the same cycle structure of an PCR (or PSR). Then, we regard n-stage FSRs as permutations over 2^n elements. According to the group theory, two permutations have the same cycle structure if and only if they are conjugate with each other. Since a conjugate of an FSR may no longer an FSR, it is interesting to consider the permutations that always transfer an FSR to an FSR. It is proved that there are exactly two such permutations, the identity mapping and the mapping that map every state to its dual. Furthermore, we prove that they are just the two permutations that transfer any maximum length FSR to an maximum length FSR.

Keywords: feedback shift register, cycle structure, symmetric group, pure circulating register, pure summing register.

1 Introduction

Feedback shift registers (FSRs) are useful in generating periodic sequences, and they are mostly used in communication and cryptographic systems [5]. Non-linear feedback shift

registers (NFSRs) are a generalization of linear feedback shift registers (LFSRs) in which the feedback function is non-linear. LFSRs were widely used in stream cipher designs due to their simplicity and fast implementation. However, stream ciphers based on LFSRs have been found to be susceptible to algebraic attacks and correlation attacks [2, 3, 13]. As an alternative, NFSRs become popular building blocks for stream ciphers recently. For example, the eSTREAM Stream Cipher project hardware finalists, Grain, Mickey and Trivium.

The investigation of NFSRs started in the pioneering book of Golomb [5] and has continued for decades. However, while the theory behind LFSRs is well understood, many fundamental problems related to NFSRs remain open. For example, it is not known how to determine the cycle structure of a general NFSR, though the cycle structures of few special types of NFSRs were adequately investigated, say symmetric NFSRs [7,11,12], and it is also not known how to efficiently construct NFSRs that output sequences with large periods. Sequences generated by maximum length NFSRs are known as de Bruijn sequences [9]. In a de Bruijn sequences of order n all 2^n different binary n-tuples appear exactly once. An n-stage LFSR has the maximum period of $2^n - 1$ if and only if its characteristic polynomial is primitive, however, for NFSRs no similar property has been found so far. An excellent survey of algorithms for generating de Bruijn sequences is given in [4].

Our work aims to get insight into the cycle structures of FSRs. At the beginning, we consider the cycle structures of pure circulating registers (PCRs) and pure summing registers (PSRs). A PCR is an FSR with feedback from the first stage to the last stage. Many properties about PCRs, such as the cycle structures and adjacency graphs, are clear [8, 10]. In this paper we show the uniqueness of the cycle structures of PCRs, that is, there are no other FSRs with the same cycle structure of an PCR. An PSR is an FSR that feed back the sum of all stages to the last stage. Similar to PCRs, we calculate the cycle structures of PSRs and show their uniqueness.

Determining the cycle structure of a general FSR is known to be notoriously hard. Usually the characteristic function is analysed, and the operation of joining and disjoining cycles was discussed in Golomb's book [5]. But this method doesn't work when the number of minterms which need to be analysed is big. So we take a different approach in this paper. We consider the symmetric group of $\mathbb{F}_2^n$ which contains all the permutation of $\mathbb{F}_2^n$. It is well known that, an n-stage FSR can be treated as a permutation of $\mathbb{F}_2^n$, but a permutation of $\mathbb{F}_2^n$ may not correspond to an n-stage FSR. Denote the FSR with characteristic function f by FSR_f and the corresponding permutation by θ_f, then according to the group theory the cycle structure of FSR_f is the same as that of FSR_g if and only if θ_f is conjugate with θ_g, i.e., there exists a permutation σ such that $\sigma^{-1}\theta_f\sigma = \theta_g$. Since a permutation of $\mathbb{F}_2^n$ may not an n-stage FSR, we consider the permutation σ such that $\sigma^{-1}\theta_f\sigma$ is an n-stage FSR for any θ_f, and show that, there are only two such bijections, the identity mapping and the mapping maps every

state to its dual. Furthermore we show that, they are just the two bijections that transfer any maximum length FSR to an maximum length FSR.

The rest of this paper is organized as follows. In section 2, we present some basic knowledge of FSRs. In section 3, we consider the cycle structures of PCRs and PSRs. In section 4, we pay attention to the transition mappings between FSRs, and at the end, we conclude this paper.

2 Preliminaries

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

2.1 Feedback shift registers

Let $\mathbb{F}_2$ be the finite field of two elements, and $\mathbb{F}_2^n$ be the vector space of dimension n over $\mathbb{F}_2$. A Boolean function $f(x_0, x_1, \ldots, x_{n-1})$ in n variables is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, and it can be uniquely represented by its algebraic normal form (ANF), which is a multivariate polynomial.

An n-stage feedback shift register (FSR) consists of n binary storage cells and a characteristic function f regulated by a single clock, where f is a Boolean function in $(n+1)$ variables. The FSR with characteristic function f is usually denoted by FSR_f. A state of an FSR is a vector $(x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^n$, where x_i indicates the content of stage i for $i \in \{0, 1, \cdots, n-1\}$. At every clock pulse, the state $(x_0, x_1, \ldots, x_{n-1})$ is updated by $(x_1, x_2, \ldots, x_{n-1}, x_n)$ satisfying $f(x_0, x_1, \ldots, x_n) = 0$, therefore, f induces a next-state operation from $\mathbb{F}_2^n$ to itself

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

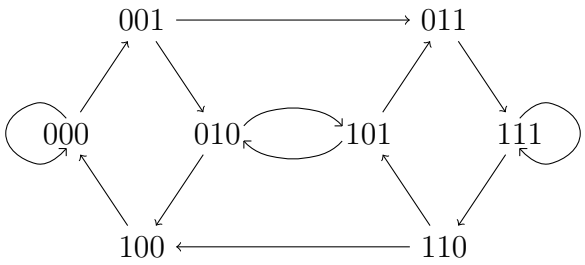
It is well known that, θ_f is a bijection if and only f is nonsingular, i.e., of the form $f = x_0 + F(x_1, \ldots, x_{n-1}) + x_n$, where F is a Boolean function in $n-1$ variables, and in this case, we say FSR_f is nonsingular. Without specification, all the FSRs and characteristic functions in this paper are nonsingular. From an initial state $\mathbf{X}_0 = (x_0, x_1, \ldots, x_{n-1})$, after consecutive clock pulses, FSR_f will generate a cycle $C = (\mathbf{X}_0, \mathbf{X}_1, \ldots, \mathbf{X}_{l-1})$, where $\mathbf{X}_{i+1}$ is the next state of $\mathbf{X}_i$ for $i = 0, 2, \ldots, l-1$ and $\mathbf{X}_0$ is the next state of $\mathbf{X}_{l-1}$. In this way, the set $\mathbb{F}_2^n$ is divided into cycles $C_1, C_2, \ldots, C_k$ by FSR_f, and reversely, it is easy to see, a partition of $\mathbb{F}_2^n$ into cycles determines an n-stage FSR. So we can treat FSR_f as a set of cycles, and use the notation

$$\mathrm{FSR}_f = \{C_1, C_2, \ldots, C_k\}.$$

The set of 2^n sequences $\mathbf{x} = x_0x_1\cdots$ satisfying $f(x_t, x_{t+1}, \ldots, x_{t+n}) = 0$ for any $t \geq 0$ is denoted by $G(f)$. For a state $\mathbf{X} = (x_0, x_1, \ldots, x_{n-1})$, its conjugate $\widehat{\mathbf{X}}$, companion $\widetilde{\mathbf{X}}$ and dual $\overline{\mathbf{X}}$ are defined as $\widehat{\mathbf{X}} = (\overline{x}_0, x_1, \ldots, x_{n-1})$, $\widetilde{\mathbf{X}} = (x_0, x_1, \ldots, \overline{x}_{n-1})$ and $\overline{\mathbf{X}} = (\overline{x}_0, \overline{x}_1, \ldots, \overline{x}_{n-1})$, where $\overline{x}$ denotes the binary complement of x. We call $(\mathbf{X}, \widehat{\mathbf{X}})$ a conjugate pair, $(\mathbf{X}, \widetilde{\mathbf{X}})$ a companion pair, and $(\mathbf{X}, \overline{\mathbf{X}})$ a dual pair.

2.2 De Bruijn graphs

The n-th order de Bruijn graph G_n is a directed graph of 2^n vertices and 2^{n+1} directed edges. The vertices, also be called states, are labelled by the 2^n binary n-tuples $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$. The graph is regular of degree 2 with two edges into and out of each vertex. There is an directed edge from $(x_1, x_2, \cdots, x_n)$ to $(y_1, y_2, \cdots, y_n)$ if and only if $y_i = x_{i+1}$ for $i = 1, 2, \ldots, n-1$. We call $\mathbf{X}$ a predecessor of $\mathbf{Y}$ and $\mathbf{Y}$ a successor of $\mathbf{X}$ if there is an directed edge from $\mathbf{X}$ to $\mathbf{Y}$. $(\mathbf{X}_0, \mathbf{X}_1, \ldots, \mathbf{X}_{l-1})$ is called a cycle in G_n if $\mathbf{X}_{i+1}$ is a successor of $\mathbf{X}_i$ for $i = 0, 1, \ldots, l-2$, and $\mathbf{X}_0$ is a successor of $\mathbf{X}_{l-1}$ in G_n. The de Bruijn graph of order 3 is shown below.



We call σ an automorphism of G_n if σ is a bijection of the vertices in G_n and there is a an directed edge from $\mathbf{X}$ to $\mathbf{Y}$ implies there is a an directed edge from $\sigma(\mathbf{X})$ to $\sigma(\mathbf{Y})$. Let I and D be the identity mapping and the dual mapping of the vertices in G_n respectively, that is, $I(\mathbf{X}) = \mathbf{X}$ and $D(\mathbf{X}) = \overline{\mathbf{X}}$ for any vertex $\mathbf{X}$ in G_n. It can be verified, both I and D are automorphisms of G_n, and it was proved in [14] that, there are no other automorphisms.

Lemma 1. *[14] There are only two automorphisms of G_n, that is, I and D.*

3 The Cycle Structures of PCRs and PSRs

In this section, we consider the cycle structures of pure circulating registers (PCRs) and pure summing registers (PSRs) and show their uniqueness. To begin with, we present the definition of the cycle structures of FSRs.

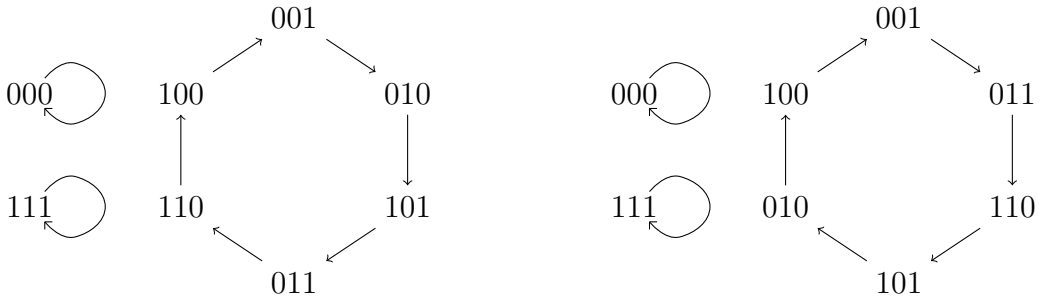
Definition 1. *Let FSR_f be a feedback shift register with characteristic function f. Suppose FSR_f contains n_1 cycles with length l_1, n_2 cycles with length l_2, $\cdots$, and n_k cycles with length l_k. Then the cycle structure of FSR_f is denoted by*

$$\Sigma_f = n_1[l_1] + n_2[l_2] + \cdots + n_k[l_k].$$

Two n-stage feedback shift registers FSR_f and FSR_g are said to be with the same cycle structure, denoted by $\Sigma_f = \Sigma_g$, if for any integer $1 \leq l \leq 2^n$, FSR_f and FSR_g contain the same number of cycles with length l.

Let $\Sigma_f = n_1[l_1] + n_2[l_2] + \cdots + n_k[l_k]$ be the cycle structure of n-stage FSR_f. Since there are 2^n states in the cycle structure of an n-stage FSR, we have $n_1 \cdot l_1 + n_2 \cdot l_2 + \cdots + n_k \cdot l_k = 2^n$.

Example 1. *Let $f_1(x) = x_0 + x_1 + x_1x_2 + x_3$ and $f_2(x) = x_0 + x_2 + x_1x_2 + x_3$. It can be verified that, $\Sigma_{f_1} = \Sigma_{f_2} = 2[1] + 1[6]$. The cycle structures of the two FSRs are shown below.*



Let $\mathcal{D}$ and $\mathcal{R}$ be two operations on Boolean functions such that:

$$\mathcal{D}(f(x_0, x_1, \ldots, x_n)) = f(x_0 + 1, x_1 + 1, \ldots, x_n + 1),$$

$$\mathcal{R}(f(x_0, x_1, \ldots, x_n)) = f(x_n, x_{n-1}, \ldots, x_0),$$

then for any Boolean function f, we have

$$\Sigma_f = \Sigma_{\mathcal{D}(f)} = \Sigma_{\mathcal{R}(f)}.$$

It can be verified, the two Boolean functions f_1 and f_2 in Example 1 are related by: $f_1 = \mathcal{D}(f_2) = \mathcal{R}(f_2)$.

The FSR with characteristic function $f = x_0 + x_n$ is called the n-stage pure circulating register (PCR). For any cycle C in the n-stage PCR, the length of C is a divisor of n. Let d be a divisor of n, then there are $M(d) = \frac{1}{d}\sum_{d'|d} \mu(d') 2^{d/d'}$ cycles with length d in the n-stage PCR, therefore the cycle structure of the n-stage PCR is given by

$$\Sigma_{(x_0+x_n)} = \sum_{d|n} M(d)[d].$$

The FSR with characteristic function $f = x_0 + x_1 + \cdots + x_n$ is called the n-stage pure summing register (PSR). For the cycle structures of PSRs, we have

Theorem 1. *The cycle structure of the n-stage PSR is* $\sum_{d|n+1} N(d)[d]$*, where*

$$N(d) = \begin{cases} \frac{1}{d}\sum_{d'|d} \mu(d')2^{d/d'} & \text{in the case } \frac{n+1}{d} \text{ is even} \\ \frac{1}{2d}\sum_{\substack{d'|d \\ d'odd}} \mu(d')2^{d/d'} & \text{in the case } \frac{n+1}{d} \text{ is odd} \end{cases}$$

Proof. Let $f = x_0 + x_{n+1}$ and $g = x_0 + x_1 + \cdots + x_n$, then we have $G(g) \subset G(f)$. So the length of any cycle in FSR_g is a divisor of $n+1$. Let C be a cycle in FSR_f and $\mathbf{X}$ be a state in C, then C is a cycle in FSR_g if and only if $g(\mathbf{X}) = 0$. For an $(n+1)$-stage state $\mathbf{X}$, define $p(\mathbf{X})$ be the least positive integer d such that $\mathbf{X}$ can be written as

$$\mathbf{X} = (x_0, x_1, \ldots, x_{d-1}, x_0, x_1, \ldots, x_{d-1}, \cdots, x_0, x_1, \ldots, x_{d-1}).$$

It is easy to see, $p(\mathbf{X})|(n+1)$. Let $A(d)$ be the number of elements in $\{\mathbf{X}|p(\mathbf{X}) = d\}$ and $B(d)$ be the number of elements in $\{\mathbf{X}|p(\mathbf{X}) = d, g(\mathbf{X}) = 0\}$. In the case $\frac{n+1}{d}$ is even, we have $A(d) = B(d)$ because $p(\mathbf{X}) = d$ implies $g(\mathbf{X}) = 0$. For $A(d)$, we have $\sum_{d'|d} A(d') = 2^d$. Using the Möbius transformation, we get $A(d) = \sum_{d'|d} \mu(d')2^{d/d'}$. Next, we calculate $B(d)$. From the discussion above, we just need to consider the case $\frac{n+1}{d}$ is odd. Let $d = 2^k d_1$, where d_1 is odd. Then we have $\sum_{\substack{d'|d \\ d'odd}} B(2^k d') = 2^{d-1}$. Using the Möbius transformation, we get $B(d) = \frac{1}{2}\sum_{\substack{d'|d \\ d'odd}} \mu(d')2^{d/d'}$. Finally, it is easy to see $N(d) = \frac{1}{d}B(d)$. □

Example 1 shows that, there exist $g \neq f$ such that $\Sigma_g = \Sigma_f$. In particular, all the n-stage FSRs that output de Bruijn sequences have the same cycle structure, i.e., $1 \cdot [2^n]$. But for the cycle structure of PCR, we have

Theorem 2. *If* $\Sigma_f = \Sigma_{(x_0+x_n)}$*, then* $f = x_0 + x_n$*.*

Proof. Suppose $f \neq x_0 + x_n$. Then there exists a state $\mathbf{X} = (x_0, x_1, \ldots, x_{n-1})$ whose successor is $\mathbf{Y} = (x_1, x_2, \ldots, x_{n-1}, \overline{x}_0)$. Let C be the cycle in FSR_f that contains $\mathbf{X}$ and $\mathbf{Y}$. Since $\theta_f^n(x_0, x_1, \ldots, x_{n-1}) = (\overline{x}_0, *, \ldots, *)$ and $(x_0, x_1, \ldots, x_{n-1}) \neq (\overline{x}_0, *, \ldots, *)$, the length of C cannot be a divisor of n. Since the lengths of any cycle in the pure circulating shift register is a divisor of n, the cycle structure of FSR_f is not the same as that of the pure circulating shift register. □

Similarly, for the cycle structure of PSR, we have

Theorem 3. *For odd n, if* $\Sigma_f = \Sigma_{(x_0+x_1+\cdots+x_n)}$*, then* $f = x_0 + x_1 + \cdots + x_n$*. For even n, if* $\Sigma_f = \Sigma_{(x_0+x_1+\cdots+x_n)}$*, then* $f = x_0 + x_1 + \cdots + x_n$ *or* $f = x_0 + x_1 + \cdots + x_n + 1$*.*

Proof. Suppose $\Sigma_f = \Sigma_{(x_0+x_1+\cdots+x_n)}$. From the theory of LFSRs we know, the length of any cycle in $\mathrm{FSR}_{(x_0+x_1+\cdots+x_n)}$ is a divisor of $n+1$, therefore, the length of any cycle in FSR_f is a divisor of $n+1$. That implies $G(f) \subset G(x_0 + x_{n+1})$. So $f = x_0 + x_1 + \cdots + x_n$

or $f = x_0 + x_1 + \cdots + x_n + 1$. In the case n is odd, the two cycles $\mathbf{0}$ and $\mathbf{1}$ belong to $\mathrm{FSR}_{(x_0+x_1+\cdots+x_n)}$ but not $\mathrm{FSR}_{(x_0+x_1+\cdots+x_n+1)}$, therefore $\Sigma_{(x_0+x_1+\cdots+x_n)} \neq \Sigma_{(x_0+x_1+\cdots+x_n+1)}$. So we get $f = x_0 + x_1 + \cdots + x_n$. In the case n is even, $\Sigma_{(x_0+x_1+\cdots+x_n)} = \Sigma_{(x_0+x_1+\cdots+x_n+1)}$. So we get $f = x_0 + x_1 + \cdots + x_n$ or $f = x_0 + x_1 + \cdots + x_n + 1$. □

4 Transition Mappings between FSRs

Let $S(2^n)$ denote the symmetric group of $\mathbb{F}_2^n$, i.e., $S(2^n) = \{\sigma | \sigma \text{ is a permutation of } \mathbb{F}_2^n\}$. It is well known that there are $(2^n)!$ elements in $S(2^n)$. For two elements σ and τ in $S(2^n)$, the product $\sigma\tau$ is defined to be: $\sigma\tau(\mathbf{X}) = \sigma(\tau(\mathbf{X}))$. The order of σ, denoted by $ord(\sigma)$, is the least integer k such that $\sigma^k = I$, where I is the identity in group $S(2^n)$. We call σ_1 is conjugate with σ_2 if there exists an element σ such that, $\sigma^{-1}\sigma_1\sigma = \sigma_2$, and the element σ is called a transition mapping from σ_1 to σ_2.

Let FSR_f be an n-stage FSR with characteristic function f, then θ_f is a permutation of $\mathbb{F}_2^n$, i.e., an element in $S(2^n)$. But we should note that, not every element in $S(2^n)$ correspond to an n-stage FSR. There are exactly $2^{2^{n-1}}$ elements in $S(2^n)$ that can be treated as FSRs. If $\sigma = \theta_f$ for some f, then σ is called an FSR for simplicity.

For $\sigma \in S(2^n)$, we can define the cycle structure of σ just like what we have done for feedback shift register θ_f. $C = (\mathbf{X}_0, \mathbf{X}_1, \ldots, \mathbf{X}_{l-1})$ is called a cycle of σ if $\mathbf{X}_{i+1} = \sigma(\mathbf{X}_i)$ for $i = 0, 1, \ldots, l-2$ and $\mathbf{X}_0 = \sigma(\mathbf{X}_{l-1})$. The cycle structure of σ is a set of cycles such that these cycles form a partition of $\mathbb{F}_2^n$. Suppose σ contains n_1 cycles with length l_1, n_2 cycles with length l_2, $\cdots$, and n_k cycles with length l_k. Then the cycle structure of σ is denoted by $\Sigma_\sigma = n_1[l_1] + n_2[l_2] + \cdots + n_k[l_k]$. In the case σ is an FSR, say FSR_f, the cycle structure of σ is the same as Σ_f. For the cycle structure of Σ_σ we have the following conclusions, which can be found in a book that introduce the basic knowledge of symmetric group.

Lemma 2. *Denote the cycle structure of σ by Σ_σ.*

1. *Let $\Sigma_\sigma = n_1[l_1] + n_2[l_2] + \cdots + n_k[l_k]$, then $ord(\sigma) = lcm(l_1, l_2, \ldots, l_k)$.*
2. *$\Sigma_{\sigma_1} = \Sigma_{\sigma_2}$ if and only if σ_1 is conjugate with σ_2.*
3. *Let $\Sigma_{\sigma_1} = \Sigma_{\sigma_2} = n_1[l_1] + n_2[l_2] + \cdots + n_k[l_k]$, then there are $n_1!(l_1)^{n_1} n_2!(l_2)^{n_2} \cdots n_k!(l_k)^{n_k}$ transition mappings from σ_1 to σ_2.*

Let FSR_f be an FSR that generates de Bruijn sequences, then $\Sigma_f = 1 \cdot [2^n]$. From Case 1 of Lemma 2 we know, $ord(\theta_f) = 2^n$. Conversely, if $ord(\theta_f) = 2^n$, it is not hard to see that $\Sigma_f = 1 \cdot [2^n]$. Therefore, FSR_f generates de Bruijn sequences if and only if $ord(\theta_f) = 2^n$.

Let FSR_f and FSR_g be two FSRs. From Case 2 of Lemma 2 we know, $\Sigma_f = \Sigma_g$ if and only if θ_f is conjugate with θ_g. For any $\sigma \in S(2^n)$, the cycle structure of $\sigma^{-1}\theta_f\sigma$ is the same

as that of θ_f. If furthermore $\sigma^{-1}\theta_f\sigma$ is an FSR, we get an FSR whose cycle structure is the same as that of FSR_f. So it is important to investigate the transition mappings between FSRs, especially the mappings that transfer any FSR to an FSR.

Example 2. *Let FSR_f be an n-stage LFSR with $f = x_0 + c_1x_1 + \cdots + c_{n-1}x_{n-1} + x_n$. The companion matrix of f is*

$$A_f = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & c_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix}$$

Let σ be a nonsingular linear transformation on $\mathbb{F}_2^n$ defined by $\sigma(\mathbf{X}) = \mathbf{X}B_\sigma$, where B_σ is the matrix of σ. Then $\sigma^{-1}\theta_f\sigma(\mathbf{X}) = \mathbf{X}B_\sigma A_f B_\sigma^{-1}$. If $\sigma^{-1}\theta_f\sigma$ is an FSR, then $B_\sigma A_f B_\sigma^{-1}$ will be of rational canonical form. It can be seen, A_f is in rational canonical form. From the uniqueness of rational canonical form, we know $B_\sigma A_f B_\sigma^{-1} = A_f$.

Let D be a permutation of $\mathbb{F}_2^n$ defined by

$$D(x_0, x_1, \ldots, x_{n-1}) = (x_0 + 1, x_1 + 1, \ldots, x_{n-1} + 1).$$

Let θ_f be an n-stage FSR and $\mathbf{X} = (x_0, x_1, \ldots, x_{n-1})$ be a state, then

$$\begin{aligned} D^{-1}\theta_f D(\mathbf{X}) &= D^{-1}\theta_f D(x_0, x_1, \ldots, x_{n-1}) \\ &= D^{-1}\theta_f(x_0 + 1, x_1 + 1, \ldots, x_{n-1} + 1) \\ &= D^{-1}(x_1 + 1, x_2 + 1, \ldots, x_n + 1) \\ &= (x_1, x_2, \ldots, x_n), \end{aligned}$$

where x_n is an element in $\mathbb{F}_2$ satisfying $f(x_0 + 1, x_1 + 1, \cdots, x_n + 1) = 0$. Therefore, we have $D^{-1}\theta_f D = \theta_{\mathcal{D}(f)}$, where $\mathcal{D}(f) = f(x_0 + 1, x_1 + 1, \ldots, x_n + 1)$. The permutation D has the property that: for any FSR θ_f, $D^{-1}\theta_f D$ is also an FSR. The identity I in $S(2^n)$ is another permutation with such property, i.e., $I^{-1}\theta_f I = \theta_f$. In the following we will show that, they are the only two permutations with such property. Firstly, we need a lemma.

Lemma 3. *Let C be a cycle in the n-stage de Bruijn graph, then there exists an FSR that contains C. Let $|C| = s$ and $|\{\mathbf{X}|\mathbf{X} \notin C, \widehat{\mathbf{X}} \in C\}| = t$, then there are $2^{\frac{2^n-(s+t)}{2}}$ such FSRs.*

Proof. A mapping $\theta : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an n-stage FSR if and only if θ is a permutation and $\theta(*, x_1, \ldots, x_{n-1}) = (x_1, \ldots, x_{n-1}, *)$ for any $(x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^{n-1}$. In the following, we will construct such a mapping.

For every state $\mathbf{X}$ in C, define $\theta(\mathbf{X}) = \mathbf{Y}$, where $\mathbf{Y}$ is the successor of $\mathbf{X}$ in C. Let $B = \{\mathbf{X}|\mathbf{X} \notin C, \widehat{\mathbf{X}} \in C\}$. For every state $\mathbf{X}$ in B, define $\theta(\mathbf{X}) = \widetilde{\mathbf{Y}}$, where $\mathbf{Y}$ is the successor of $\widehat{\mathbf{X}}$ in C. Let $A = \mathbb{F}_2^n \setminus (B \cup C)$. It is easy to see, there are $2^n - (s+t)$ elements in A. Since the states in A take the form of conjugate pairs, there are $\frac{2^n-(s+t)}{2}$ conjugate pairs in A. For a conjugate pair $(\mathbf{X}, \widehat{\mathbf{X}})$ in A, let $\mathbf{Y}$ and $\widetilde{\mathbf{Y}}$ be the two possible successor of $\mathbf{X}$ and $\widehat{\mathbf{X}}$. Define $\theta(\mathbf{X}) = \mathbf{Y}$ and $\theta(\widehat{\mathbf{X}}) = \widetilde{\mathbf{Y}}$ (or $\theta(\mathbf{X}) = \widetilde{\mathbf{Y}}$ and $\theta(\widehat{\mathbf{X}}) = \mathbf{Y}$). It is obvious that, θ is a bijection and $\theta(*, x_1, \ldots, x_{n-1}) = (x_1, \ldots, x_{n-1}, *)$ for any $(x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^{n-1}$. So the first assertion is proved. Since for any conjugate pair $(\mathbf{X}, \widehat{\mathbf{X}})$ in A there are exactly two ways to define its' image under θ, there are $2^{\frac{2^n-(s+t)}{2}}$ such FSRs. □

Generally, for any set of non-intersecting cycles $C_1, C_2, \cdots, C_k$ in the n-stage de Bruijn graph, there exists an FSR contains these cycles. Let $|A| = s$ and $|\{\mathbf{X}|\mathbf{X} \notin A, \widehat{\mathbf{X}} \in A\}| = t$ where $A = C_1 \cup C_2 \cup \cdots \cup C_k$, then there are $2^{\frac{2^n-(s+t)}{2}}$ such FSRs.

Theorem 4. *Let σ be a permutation of $\mathbb{F}_2^n$ such that, $\sigma^{-1}\theta_f\sigma$ is an n-stage FSR for any n-stage FSR θ_f. Then $\sigma = I$ or D.*

Proof. Let σ be such a permutation that, $\sigma^{-1}\theta_f\sigma$ is an n-stage FSR for any n-stage FSR θ_f. According to Lemma 1, it is sufficient to show that σ is an automorphism of the n-th order de Bruijn graph G_n, that is, $\mathbf{X} \to \mathbf{Y}$ in G_n implies $\sigma(\mathbf{X}) \to \sigma(\mathbf{Y})$ in G_n for any $\mathbf{X}$ and $\mathbf{Y}$.

Let $C = (\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_l)$ be a cycle in G_n. According to Lemma 2, there exists an FSR_f that contains C. By the definition of σ, we know $\sigma^{-1}\theta_f\sigma$ is also an FSR, denoted by FSR_g. It is easy to see, $E = (\sigma(\mathbf{X}_1), \sigma(\mathbf{X}_2), \ldots, \sigma(\mathbf{X}_l))$ is a cycle in FSR_g, therefore, E is a cycle in G_n. Let $\mathbf{X}$ and $\mathbf{Y}$ be two states such that $\mathbf{X}$ is a predecessor of $\mathbf{Y}$ in G_n. Then there exist a cycle C_1 in G_n such that $C_1 = (\mathbf{X}, \mathbf{Y}, *, \ldots, *)$. Since $(\sigma(\mathbf{X}), \sigma(\mathbf{Y}), *, \ldots, *)$ is also a cycle in G_n, we know $\sigma(\mathbf{X})$ is a predecessor of $\sigma(\mathbf{Y})$ in G_n. Considering that σ is a bijection, we get the conclusion that σ is an automorphism of G_n. □

In the following, we consider the case θ_f is a maximum-length FSR. Let M_n be the set of n-stage maximum-length FSRs and define

$$A(M_n) = \{\sigma|\sigma^{-1}\theta_f\sigma \text{ is an FSR for any } \theta_f \in M_n\}.$$

It is obvious that, both I and D belong to $A(M_n)$. An interesting question is: whether $A(M_n)$ contains some other elements except I and D? The answer to this question is no, and some lemmas are needed before the proof.

Lemma 4. *Let $(x_0, x_1, \ldots, x_{n-1})$ be an n-stage state such that $(x_1, x_2, \ldots, x_{n-1}) \neq (0, 0, \ldots, 0)$ or $(1, 1, \ldots, 1)$, then both $(x_0, x_1, \ldots, x_{n-1}) \to (x_1, \ldots, x_{n-1}, 0)$ and $(x_0, x_1, \ldots, x_{n-1}) \to (x_1, \ldots, x_{n-1}, 1)$ can be extended to full cycles.*

Proof. Let f be a linear Boolean function that correspond to a primitive polynomial $p(x)$ of degree n. FSR_f contains two cycles, i.e., the cycle C_0 contains only the all zero state $(0,0,\ldots,0)$ and the cycle C_1 contains all the states except the all zero state. Without lose of generality, suppose $(x_0,x_1,\ldots,x_{n-1}) \to (x_1,\ldots,x_{n-1},0)$ is in C_1. Then FSR_{f+1} contains two cycles, i.e., the cycle C_2 that contains only the all one state $(1,1,\ldots,1)$ and the cycle C_3 that contains all the state except the all one state. It can be verified, $(x_0,x_1,\ldots,x_{n-1}) \to (x_1,\ldots,x_{n-1},1)$ is in C_3. So $(x_0,x_1,\ldots,x_{n-1}) \to (x_1,\ldots,x_{n-1},0)$ can be extended to the full cycle generated by FSR with characteristic function $f+x_1^0x_2^0\cdots x_{n-1}^0$, and $(x_0,x_1,\ldots,x_{n-1}) \to (x_1,\ldots,x_{n-1},1)$ can be extended to the full cycle generated by FSR with characteristic function $f+1+x_1^1x_2^1\cdots x_{n-1}^1$, where $x_1^{a_1}x_2^{a_2}\cdots x_{n-1}^{a_{n-1}}$ denote the Boolean function that takes value 1 on the point $(a_1,a_2,\ldots,a_{n-1})$ and takes value 0 on the other points. □

Lemma 5. *Let σ be a bijection of $\mathbb{F}_2^n$ such that, $\sigma^{-1}\theta_f\sigma$ is an n-stage FSR for any n-stage maximum length FSR θ_f, then we have*

1. *$\sigma(\mathbf{X}) = (0,0,\ldots,0)$ implies $\mathbf{X} = (0,0,\ldots,0)$ or $(1,1,\ldots,1)$;*
2. *$\sigma(\mathbf{X}) = (1,1,\ldots,1)$ implies $\mathbf{X} = (0,0,\ldots,0)$ or $(1,1,\ldots,1)$.*

Proof. We just consider the case $\sigma(\mathbf{X}) = (0,0,\ldots,0)$, and the other case can be proved similarly. Assume $\mathbf{X} = (x_0,x_1,\ldots,x_{n-1})$. The proof is divided into three cases.

Suppose $(x_1,x_2,\ldots,x_{n-1}) \neq (0,0,\ldots,0)$ or $(1,1,\ldots,1)$. According to Lemma 4, both $(x_0,x_1,\ldots,x_{n-1}) \to (x_1,\ldots,x_{n-1},0)$ and $(x_0,x_1,\ldots,x_{n-1}) \to (x_1,\ldots,x_{n-1},1)$ can be extended to full cycles, say M_1 and M_2 respectively. Let $\sigma(M)$ be the full cycle derived from the image of the full cycle M under σ. From the definition of σ, both $\sigma(M_1)$ and $\sigma(M_2)$ are full cycles that contain $\sigma((x_0,x_1,\ldots,x_{n-1})) \to \sigma((x_1,\ldots,x_{n-1},0))$ and $\sigma((x_0,x_1,\ldots,x_{n-1})) \to \sigma((x_1,\ldots,x_{n-1},1))$ respectively. Since

$$\sigma((x_0,x_1,\ldots,x_{n-1})) = (0,0,\ldots,0),$$

one of

$$\sigma((x_0,x_1,\ldots,x_{n-1})) \to \sigma((x_1,\ldots,x_{n-1},0))$$

and

$$\sigma((x_0,x_1,\ldots,x_{n-1})) \to \sigma((x_1,\ldots,x_{n-1},1))$$

will be $(0,0,\ldots,0) \to (0,0,\ldots,0)$ which is impossible.

Suppose $(x_1,x_2,\ldots,x_{n-1}) = (0,0,\ldots,0)$. We need to show $x_0 = 0$. Suppose the opposite, i.e., $x_0 = 1$, then the two predecessor of $\mathbf{X} = (1,0,\ldots,0)$ in the n-th order de Bruijn graph G_n are $(0,1,0,\ldots,0)$ and $(1,1,0,\ldots,0)$. According to Lemma 4, both $(0,1,0,\ldots,0) \to$

$(1,0,\ldots,0)$ and $(1,1,0,\ldots,0) \to (1,0,\ldots,0)$ can be extended to full cycles, say M_1 and M_2 respectively. From the definition of σ, both $\sigma(M_1)$ and $\sigma(M_2)$ are full cycles that contain $\sigma((0,1,0,\ldots,0)) \to \sigma((1,0,\ldots,0))$ and $\sigma((1,1,0,\ldots,0)) \to \sigma((1,0,\ldots,0))$ respectively. Since

$$\sigma((1,0,\ldots,0)) = (0,0,\ldots,0),$$

one of

$$\sigma((0,1,0,\ldots,0)) \to \sigma((1,0,\ldots,0))$$

and

$$\sigma((1,1,0,\ldots,0)) \to \sigma((1,0,\ldots,0))$$

will be $(0,0,\ldots,0) \to (0,0,\ldots,0)$ which is impossible.

The proof for the case $(x_1,x_2,\ldots,x_{n-1}) = (1,1,\ldots,1)$ is similar. □

Lemma 6. *Let σ be a permutation of $\mathbb{F}_2^n$ such that, $\sigma^{-1}\theta_f\sigma$ is an n-stage FSR for any n-stage maximum length FSR θ_f, then there are two cases may happen:*

1. $\sigma((0,0,\ldots,0)) = (0,0,\ldots,0)$, $\sigma((1,1,\ldots,1)) = (1,1,\ldots,1)$,
   $\sigma((0,\ldots,0,1)) = (0,\ldots,0,1)$, $\sigma((1,0,\ldots,0)) = (1,0,\ldots,0)$,
   $\sigma((0,1,\ldots,1)) = (0,1,\ldots,1)$, $\sigma((1,\ldots,1,0)) = (1,\ldots,1,0)$

2. $\sigma((0,0,\ldots,0)) = (1,1,\ldots,1)$, $\sigma((1,1,\ldots,1)) = (0,0,\ldots,0)$,
   $\sigma((0,\ldots,0,1)) = (1,\ldots,1,0)$, $\sigma((1,0,\ldots,0)) = (0,1,\ldots,1)$,
   $\sigma((0,1,\ldots,1)) = (1,0,\ldots,0)$, $\sigma((1,\ldots,1,0)) = (0,\ldots,0,1)$

Proof. According to Lemma 5, there are two cases may happen:

1. $\sigma((0,0,\ldots,0)) = (0,0,\ldots,0)$, $\sigma((1,1,\ldots,1)) = (1,1,\ldots,1)$,

2. $\sigma((0,0,\ldots,0)) = (1,1,\ldots,1)$, $\sigma((1,1,\ldots,1)) = (0,0,\ldots,0)$,

We just consider Case 1, and the other case can be proved similarly.

It is easy to see, $(0,0,\ldots,0) \to (0,0,\ldots,1)$ can be extended to a full cycle, say M_1. From the definition of σ, $\sigma(M_1)$ is a full cycle that contains $\sigma((0,0,0,\ldots,0)) \to \sigma((0,0,\ldots,1))$. Since $\sigma((0,0,\ldots,0)) = (0,0,\ldots,0)$, we have: $\sigma((0,0,0,\ldots,0)) \to \sigma((0,0,\ldots,1))$ is just $(0,0,0,\ldots,0) \to (0,0,\ldots,1)$, therefore, $\sigma((0,\ldots,0,1)) = (0,\ldots,0,1)$. Similarly we can show that $\sigma((1,0,\ldots,0)) = (1,0,\ldots,0)$, $\sigma((0,1,\ldots,1)) = (0,1,\ldots,1)$ and $\sigma((1,\ldots,1,0)) = (1,\ldots,1,0)$. □

Theorem 5. *Let σ be a bijection of $\mathbb{F}_2^n$ such that, $\sigma^{-1}\theta_f\sigma$ is an n-stage FSR for any n-stage maximum length FSR θ_f, then $\sigma = I$ or D.*

Proof. Let σ be such a bijection that, $\sigma^{-1}\theta_f\sigma$ is an n-stage FSR for any n-stage maximum length FSR θ_f. According to Lemma 6, there are two cases may happen. In the rest of this proof, we always assume Case 1 of Lemma 6.

According to Lemma 1, it is sufficient to show σ is an automorphism of the n-th order de Bruijn graph G_n, that is, $\mathbf{X} \to \mathbf{Y}$ in G_n implies $\sigma(\mathbf{X}) \to \sigma(\mathbf{Y})$ in G_n for any $\mathbf{X}$ and $\mathbf{Y}$. Let A be a set that contains the following eight edges in the n-stage de Bruijn graph

$$(0,0,\ldots,0) \to (0,0,\ldots,0), (0,0,\ldots,0) \to (0,\ldots,0,1),$$

$$(1,0,\ldots,0) \to (0,0,\ldots,0), (1,0,\ldots,0) \to (0,\ldots,0,1),$$

$$(1,1,\ldots,1) \to (1,1,\ldots,1), (1,1,\ldots,1) \to (1,\ldots,1,0),$$

$$(0,1,\ldots,1) \to (1,\ldots,1,1), (0,1,\ldots,1) \to (1,\ldots,1,0).$$

Let $\mathbf{X} \to \mathbf{Y}$ be an edge in G_n. If $\mathbf{X} \to \mathbf{Y} \in A$, then we have

$$\sigma(\mathbf{X}) = \mathbf{X} \text{ and } \sigma(\mathbf{Y}) = \mathbf{Y},$$

therefore, $\sigma(\mathbf{X}) \to \sigma(\mathbf{Y})$ is in G_n. If $\mathbf{X} \to \mathbf{Y} \notin A$, then $\mathbf{X} \to \mathbf{Y}$ can be extended to a full cycle, say M. From the definition of σ, $\sigma(M)$ is a full cycle that contains $\sigma(\mathbf{X}) \to \sigma(\mathbf{Y})$. Therefore, $\sigma(\mathbf{X}) \to \sigma(\mathbf{Y})$ is in G_n. □

At the end of this paper, we present an example supporting Theorem 5.

Example 3. *There are two de Bruijn cycles of order* 3*:*

$$C_1 = (000, 001, 011, 111, 110, 101, 010, 100),$$

$$C_2 = (000, 001, 010, 101, 011, 111, 110, 100).$$

Denote the corresponding FSRs by FSR_f *and* FSR_g *respectively. Define*

$$A(f) = \{\sigma | \sigma^{-1}\theta_f\sigma \text{ is an FSR}\}.$$

Then we have

$$A(f) = \{I, D, \theta_f, \theta_f^2, \ldots, \theta_f^7, D\theta_f, D\theta_f^2, \ldots, D\theta_f^7\},$$
$$A(g) = \{I, D, \theta_g, \theta_g^2, \ldots, \theta_g^7, D\theta_g, D\theta_g^2, \ldots, D\theta_g^7\}.$$

For simplicity of presentation, we denote a state $(x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^n$ *by a decimal number between* 0 *and* $2^n - 1$*:* $x_0 2^{n-1} + x_1 2^{n-2} + \cdots + x_{n-1}$*. A bijection of* $\mathbb{F}_2^3$

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ i_0 & i_1 & i_2 & i_3 & i_4 & i_5 & i_6 & i_7 \end{pmatrix}$$

is denoted by $\sigma = (i_0, i_1, i_2, i_3, i_4, i_5, i_6, i_7)$*. The table below shows the elements in* $A(f)$ *and* $A(g)$*, from which we know* $A(M_3) = A(f) \cap A(g) = \{I, D\}$*.*

Table 1: The elements in $A(f)$ and $A(g)$

elements in $A(f)$	elements in $A(g)$
$I=(0,1,2,3,4,5,6,7)$	$I=(0,1,2,3,4,5,6,7)$
$D=(7,6,5,4,3,2,1,0)$	$D=(7,6,5,4,3,2,1,0)$
$\theta_f=(1,3,4,7,0,2,5,6)$	$\theta_g=(1,2,5,7,0,3,4,6)$
$\theta_f^2=(3,7,0,6,1,4,2,5)$	$\theta_g^2=(2,5,3,6,1,7,0,4)$
$\theta_f^3=(7,6,1,5,3,0,4,2)$	$\theta_g^3=(5,3,7,4,2,6,1,0)$
$\theta_f^4=(6,5,3,2,7,1,0,4)$	$\theta_g^4=(3,7,6,0,5,4,2,1)$
$\theta_f^5=(5,2,7,4,6,3,1,0)$	$\theta_g^5=(7,6,4,1,3,0,5,2)$
$\theta_f^6=(2,4,6,0,5,7,3,1)$	$\theta_g^6=(6,4,0,2,7,1,3,5)$
$\theta_f^7=(4,0,5,1,2,6,7,3)$	$\theta_g^7=(4,0,1,5,6,2,7,3)$
$D\theta_g=(6,5,2,0,7,4,3,1)$	$D\theta_f=(6,4,3,0,7,5,2,1)$
$D\theta_g^2=(5,2,4,1,6,0,7,3)$	$D\theta_f^2=(4,0,7,1,6,3,5,2)$
$D\theta_g^3=(2,4,0,3,5,1,6,7)$	$D\theta_f^3=(0,1,6,2,4,7,3,5)$
$D\theta_g^4=(4,0,1,7,2,3,5,6)$	$D\theta_f^4=(1,2,4,5,0,6,7,3)$
$D\theta_g^5=(0,1,3,6,4,7,2,5)$	$D\theta_f^5=(2,5,0,3,1,4,6,7)$
$D\theta_g^6=(1,3,7,5,0,6,4,2)$	$D\theta_f^6=(5,3,1,7,2,0,4,6)$
$D\theta_g^7=(3,7,6,2,1,5,0,4)$	$D\theta_f^7=(3,7,2,6,5,1,0,4)$

5 Conclusion

In this paper, the conditions for two feedback shift registers (FSRs) with the same cycle structure are considered. We determine the cycle structures of PSRs and prove the uniqueness of the cycle structures of PCRs and PSRs. In the view of group theory, two FSRs have the same cycle structure if and only if they are conjugate with each other. Since a conjugate of an FSR may no longer an FSR, it is interesting to consider the permutations that always transfer an FSR to an FSR, and it is showed that there are exactly two such permutations, i.e., I and D. Furthermore, we show that they are just the two bijections that transfer any maximum length FSR to an maximum length FSR.

References

[1] De Caniere C, Preneel B. Trivium. New Stream Cipher Designs: the eSTREAM Finalists. Springer Berlin Heidelberg, 2008.

[2] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," EUROCRYPT 2003, Warsaw, Poland, pp. 346-359, 2003.

[3] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback," CRYPTO 2003, Santa Barbara, California, USA, pp. 176-194, 2003.

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

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

[6] M. Hell and T. Johansson, "The Grain family of stream ciphers," LNCS, Spring-Verlag, Berlin, Germany, vol. 4986, pp. 179-190, 2008. Springer Berlin Heidelberg, 2008.

[7] K. Kjeldsen, "On the cycle structure of a set of nonlinear shift registers with symmetric feedback functions," J. Combinatorial Theory, vol. A, no. 20, pp. 154-169, 1976.

[8] E. J. Van Lantschoot, "Double adjacencies between cycles of a circulating shift register," IEEE Trans. computers, vol. 22, no. 10, pp. 944-955, Oct. 1973.

[9] 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.

[10] J. Mykkeltveit, "Generating and counting the double adjacencies in a pure circulating shift register," IEEE Trans. computers, vol. 24, no. 3, pp. 299-304, Mar. 1975.

[11] 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.

[12] J. Søreng, "The periods of the sequences generated by some symmetric shift registers," J. Combinatorial Theory, vol. A, no. 21, pp. 164-187, 1976.

[13] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," IEEE Trans. computers, vol. 34, no. 1, pp. 81-85, Jan. 1985.

[14] Z.X. Wan and M.L. Liu, "The automorphisms and homomorphisms of de Bruijn-Good graphs," Acta Math. Sinica (in Chinese), vol. 22, no. 2, pp. 170-177, Mar. 1979.