Linearization of Multi-valued Nonlinear Feedback Shift Registers

Haiyan Wang, Jianghua Zhong, Dongdai Lin
State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China.
E-mail: {wanghaiyan, zhongjianghua, ddlin}@iie.ac.cn

Abstract: The Linearization of Nonlinear feedback shift registers (NFSRs) is to find their state transition matrices. In this paper, we investigate the linearization multi-valued NFSRs by considering it as a logical network via a semi-tensor product approach. A new state transition matrix is found for an multi-valued NFSR, which can be simply computed from the truth table of its feedback function, and the new state transition matrix is easier to compute and is more explicit. First, a linear representation of a multi-valued NFSR is given, based on which several necessary and sufficient conditions for the nonsingularity are given. Then, some properties of the state transition matrice are provided, which are helpful to theoretically analyze NFSRs. Finally, we give properties of a maximum length multi-valued NFSR and the linear representation of the general structure of an n-bit shift register with updating functions.

Key Words: Shift register, Semi-tensor product, state transition matrix, Boolean network, Nonsingularity.

1 Introduction

Due to inherent linearity of linear feedback shift registers (LFSRs) makes their generated sequences cryptographically insecure, nonlinear feedback shift registers (NFSRs) have been used as the main building blocks in many stream ciphers. For example, the eSTREAM Stream Cipher Project hardware finalists, Grain [1], Mickey [2] and Trivium [3]. Unlike the well-developed theory of LFSRs, the theory of NFSRs is not well-understood due to its complexity and lack of efficient analysis tools, though numerous efforts have been made over the past decades. For example, given a feedback function, it is hard to predict the periods of NFSR sequences. Golomb pointed out that all sequences generated by an NFSR are periodic if and only if its feedback function is nonsingular [4]. These NFSRs are called nonsingular NFSRs. In particular, those NFSRs generating de Bruijn sequences are called maximum length NFSRs. There are numerous efforts in [5, 6, 7] about the maximum length NFSRs. In addition, other work about NFSRs is in [8, 9, 10, 11].

It is known that an n-stage LFSR is relatively simple, the sequence generated by it can be easily forecasted, then does there exist a linearization method of NFSRs? We use a new linearization method for an NFSR by considering it as a logical network via semi-tensor product approach, namely, the Boolean network approach (preliminary work was given in [12]), because a Boolean network can be equivalently expressed as a linear system by its state transition matrix. In short, the Linearization of Nonlinear feedback shift registers (NFSRs) is to find their state transition matrices. A Boolean network is an autonomous system that evolves as a finite state automaton through Boolean functions. It was first introduced by Kauffman in 1969 [13]. Over the last decades Boolean networks have attracted much attention in many communities, such as biology [14], physics [15] and control theory [16, 17]. In particular, Cheng and his coworkers developed an algebraic framework for Boolean networks, using a semi-tensor product approach [18], i.e., a Boolean function can be expressed as a multi-linear mapping with respect to its variables, and a Boolean network is therefore converted into a conventional discrete-time linear system. It is worth noting that the semi-tensor product of matrices [19] has been successfully used in the study of Boolean (control) networks [20,21,22], multi-valued and mix-valued logical networks [23, 24], and some other related fields. In [21], Cheng and Qi investigated a matrix expression of a Boolean network, and presented some results about the number of cycles of different lengths, transient period and basin of each attractor. Multi-valued logical networks were studied, and the controllability of multi-valued logical control networks was revealed in [23]. Thanks to their algebraic set-up, problems related to Boolean functions can be converted into algebraic problems. Recently, some works about analysis of periods of NFSR sequences used their algebraic set-up to investigate NFSRs [24, 25]. Compared to the work in [24, 25], more explicit results of NFSR are given[12, 28].

This paper investigates multi-valued nonlinear feedback shift register by considering it as a logical network via semi-tensor product approach. A Fibonacci NFSR can be described as in Fig. 1. Assume an n-stage NFSR is a collection of n storage devices $x_1, x_2, \cdots, x_n$ each of which is capable of holding a set of values, $\{0, 1, \cdots, k-1\}$. First, a linear representation of a multi-valued NFSR is given, based on which the explicit form of the state transition matrix is given, some new properties of the state transition matrix are provided as well, and several conditions are given for the nonsingularity. Then, we give some properties of maximum length NFSR and the linear representation of the general structure of an n-bit shift register with updating functions. The rest of this paper is organized as follows. Section 2 gives some necessary preliminaries on the semi-tensor product of matrices. In Section 3, we present the main results of this paper, and in Section 4, we give multi-valued general structure of an n-bit shift register with updating functions by considering it as a logical network via semi-tensor product approach , which is followed by the conclusion in Section 5.

2 Notations and Preliminaries

Semi-tensor product (STP) of matrices is an extension of conventional matrix product to any two arbitrary matri-

This work is supported by National Natural Science Foundation (NNSF) of China under Grant 00000000.

ces. Using it, we can give the logic a vector expression, any logical function can be identified by its structure matrix (or canonical form), and furthermore a finite-valued or mixed-valued logical network can be converted to its algebraic form, which is very useful for the structure analysis and synthesis of such networks. We refer to [18, 20, 21] and the references therein for details. This section presents some notations and necessary preliminaries on the semi-tensor product and matrix expression of logical functions.

First, we give some notations used in this paper.

- I_n : identity matrix.
- δ_n^i: the i-th column of the identity matrix I_n.
- $Col_j(B)$: the j-th column of a matrix B.
- $\mathcal{L}_{m\times n}$: the set of $m\times n$ logical matrices, if $A \in \mathcal{L}_{m\times n}$, and columns of A are of the form of δ_m^i.
- $\mathcal{D}_k = \{0, 1, 2, \cdots, k-1\}, \Delta_n = \{\delta_n^i | i = 1, 2, \cdots, n\}$. By identifying $i \sim \delta_k^{k-i}$, we have $\mathcal{D}_k \sim \Delta_k$. where $i \sim j$ means they are equivalent.
- If $L \in \mathcal{L}_{m\times n}$, it can be expressed as $L = [\delta_m^{i_1}\ \delta_m^{i_2}\ \cdots\ \delta_m^{i_n}]$, For the sake of compactness, it is briefly denoted by $L = \delta_m[i_1\ i_2\ \cdots\ i_n]$.

Next, we give some definitions and results about the semi-tensor product.

Definition 2.1 [27] *Let $A = (a_{ij})$ and B be matrices of dimensions $n \times m$ and $p \times q$, respectively. The Kronecker product of A and B is defined as an $np \times mq$ matrix, given by*

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nm}B \end{pmatrix}.$$

Definition 2.2 [18] *Let A and B be matrices of dimensions $n\times m$ and $p\times q$, respectively, and let α be the least common multiple of m and p. The (left) semi-tensor product of A and B is defined as an $\frac{n\alpha}{m} \times \frac{q\alpha}{p}$ matrix, given by*

$$A \ltimes B = (A \otimes I_{\frac{\alpha}{m}})(B \otimes I_{\frac{\alpha}{p}}).$$

Throughout this paper the default matrix product is the semi-tensor product. The semi-tensor product is a generalization of the conventional matrix product. Thus, we can simply call it product and omit the symbol $\ltimes$ without confusion.

Definition 2.3 [29] *Let $A = [A_1\ A_2\ \cdots\ A_n]$ and $B = [B_1\ B_2\ \cdots\ B_n]$ be matrices of dimensions $m\times n$ and $p\times n$, respectively, where $A_i, B_i, i = 1, 2, \cdots, n$ are the i-th column of matrices A and B respectively. The Khatri-Rao product of A and B is defined as an $mp \times n$ matrix, given by*

$$A * B = [A_1 \otimes B_1\ A_2 \otimes B_2\ \cdots\ A_n \otimes B_n].$$

where $\otimes$ represents the Kronecker product.

Lemma 2.4 [18] *Any Boolean function $f(x_1, x_2, \cdots, x_n)$ with $x_i \in \mathcal{D}_k, i = 1, 2, \cdots, n$, can be expressed as a multilinear form: $f(x_1, x_2, \cdots, x_n) = Mx_1x_2\cdots x_n$, where M is called the structure matrix of f, and is uniquely expressed by the truth table of f, arranged in the reverse alphabet order.*

3 Main Result

A Fibonacci NFSR can be described as in Fig.1, and can be expressed as

$$\begin{cases} x_1(t+1) = x_2(t), \\ x_2(t+1) = x_3(t), \\ \quad\vdots \\ x_{n-1}(t+1) = x_n(t), \\ x_n(t+1) = f(x_1(t), x_2(t), \dots, x_n(t)). \end{cases}$$

where $x_i \in \mathcal{D}_k, i = 1, 2, \cdots, n$, and $f : \mathcal{D}_k^n \to \mathcal{D}_k$.

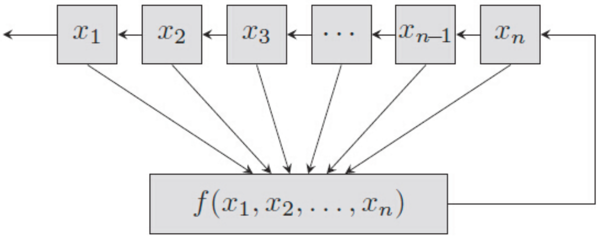

Fig. 1: Shift register

3.1 STP Representation of Nonlinear Feedback Shift Register

Lemma 3.1 [18] *Suppose*

$$\mathbf{x} = X_1X_2\cdots X_n$$

with $X_i \in \Delta_k, i = 1, 2, \cdots, n$. Then $\mathbf{x} \in \Delta_{k^n}$ and and each X_i is uniquely determined by $\mathbf{x}$.

Lemma 3.2 [18] *For any $j \in \{1, 2, \cdots, k^n\}$, the state $\mathbf{x} = \delta_{k^n}^j \in \Delta_{k^n}$ and the state $x = [x_1, x_2 \cdots, x_n]^T \in \mathcal{D}_k^n$ satisfying $k^{n-1}x_1 + k^{n-2}x_2 + \cdots + x_n = k^n - j$ are one-to-one correspondent.*

A Boolean network with n nodes can be described as the following system:

$$x(t+1) = g(x(t)), t \in \mathbb{N},$$

where $x = [x_1, x_2, \cdots, x_n]^T \in \mathcal{D}_k^n$ is the state, t represents the time instant, and $g : \mathcal{D}_k^n \to \mathcal{D}_k^n$ is a vectorial function.

Lemma 3.3 [16] *The Boolean network can be equivalently described as a linear system:*

$$\mathbf{x}(t+1) = L\mathbf{x}(t), t \in \mathbb{N},$$

where Let G_i be the structure matrix of the i-th component of the vectorial function g, the state $\mathbf{x} \in \Delta_{k^n}$ and the state transition matrix $L \in \mathcal{L}_{k^n\times k^n}$, and $L = G_1 * G_2 * \cdots * G_n$, here $*$ denotes the Khatri-Rao Product.

Lemma 3.4 *Consider an n-stage FSR with a feedback function f. Let $M = [M_1\ M_2\ \cdots\ M_{k^{n-1}}]$ be the structural matrix of FSR which can be got the truth table of f, arranged in the reverse alphabet order, and $L = [L_1\ L_2\ \cdots\ L_{k^{n-1}}]$ be the state transition matrix. Then we have $Col_j(L_i) = \delta_{k^{n-1}}^{(i-1)k+j} Col_j(M_i)$, where $L \in \mathcal{L}_{k^n\times k}, M \in \mathcal{L}_{k\times k}, j = 1, 2, \cdots, k, i = 1, 2, \dots, k^{n-1}$.*

Proof. View the NFSR as a Boolean network. Then the NFSR can be expressed as the following nonlinear system:

$$\begin{cases} x_1(t+1) = x_2(t), \\ x_2(t+1) = x_3(t), \\ \quad \vdots \\ x_{n-1}(t+1) = x_n(t), \\ x_n(t+1) = f(x_1(t), x_2(t), \dots, x_n(t)), \end{cases}$$

where $x_i \in \mathcal{D}_k, i = 1, 2, \cdots, n$, and $f : \mathcal{D}_k^n \to \mathcal{D}_k$. Let T_i be the structure matrix of $x_i(t+1) = x_{i+1}(t), i \in 1, 2, \cdots, n-1$, and M be the structure matrix of $x_n(t+1) = f(x_1(t), x_2(t), \dots, x_n(t))$. Then it is easy to see that

$$T_1 = [\underbrace{G_1 \cdots G_1}_{k^1}], G_1 = [\underbrace{\delta_k^1 \cdots \delta_k^1}_{k^{n-2}} \underbrace{\delta_k^2 \cdots \delta_k^2}_{k^{n-2}} \cdots \underbrace{\delta_k^k \cdots \delta_k^k}_{k^{n-2}}],$$

$$T_2 = [\underbrace{G_2 \cdots G_2}_{k^2}], G_2 = [\underbrace{\delta_k^1 \cdots \delta_k^1}_{k^{n-3}} \underbrace{\delta_k^2 \cdots \delta_k^2}_{k^{n-3}} \cdots \underbrace{\delta_k^k \cdots \delta_k^k}_{k^{n-3}}],$$

$$\vdots$$

$$T_{n-1} = [\underbrace{G_{n-1} \cdots G_{n-1}}_{k^{n-1}}], G_{n-1} = [\delta_k^1 \cdots \delta_k^k],$$

$$M = [M_1 \ \cdots \ M_{k^{n-1}}].$$

Then Lemma 3.3 shows that the unique state transition matrix L satisfying $L = T_1 * T_1 * \cdots T_{n-1} * M$, where "*" is the Khatri-Rao product. Straightforward computations yield the columns of L satisfying

$$Col_j(L_i) = \delta_{k^n-1}^{(i-1)k+j} Col_j(M_i),$$

where $j = 1, 2, \cdots, k, i = 1, 2, \dots, k^{n-1}$. ■

Remark 3.5 *According to the method of Lemma 3.4, the proof of Theorem 4[28] is very simple.*

$$f(x_1, x_2, \cdots, x_n) = Mx_n x_{n-1} \cdots x_1.$$

Let T_i be the structure matrix of $x_i(t+1) = x_{i+1}(t), i \in 1, 2, \cdots, n-1$, and M be the structure matrix of $x_n(t+1) = f(x_n(t), x_{n-1}(t), \dots, x_1(t))$. Then it is easy to see that

$$T_1 = G_1, G_1 = [\underbrace{\delta_k^1 \cdots \delta_k^1}_{k^{n-1}} \underbrace{\delta_k^2 \cdots \delta_k^2}_{k^{n-1}} \cdots \underbrace{\delta_k^k \cdots \delta_k^k}_{k^{n-1}}],$$

$$T_2 = [\underbrace{G_2 \cdots G_2}_{k}], G_2 = [\underbrace{\delta_k^1 \cdots \delta_k^1}_{k^{n-2}} \underbrace{\delta_k^2 \cdots \delta_k^2}_{k^{n-2}} \cdots \underbrace{\delta_k^k \cdots \delta_k^k}_{k^{n-2}}],$$

$$\vdots$$

$$T_{n-1} = [\underbrace{G_{n-1} \cdots G_{n-1}}_{k^{n-2}}],$$

$$G_{n-1} = [\underbrace{\delta_k^1 \cdots \delta_k^1}_{k} \underbrace{\delta_k^2 \cdots \delta_k^2}_{k} \cdots \underbrace{\delta_k^k \cdots \delta_k^k}_{k}],$$

$$M = [M_1 \ \dots \ M_{k^{n-1}}].$$

Then Lemma 3.3 shows that the unique state transition matrix L satisfying $L = M*T_1*T_1*\cdots*T_{n-1}$. Straightforward computations yield the columns of L satisfying

$$Col_j(L_i) = Col_j(M_i)\delta_{k^{n-1}}^i$$

Theorem 3.6 *Let the state transition matrix of FSR be $L = \delta_{k^n}[\eta_1 \ \eta_2 \ \cdots \ \eta_{k^n}]$, the structural matrix be $M = \delta_k[p_1 \ p_2 \ \cdots \ p_{k^n}]$, and $[s_1 \ s_2 \ \cdots \ s_{k^n}]$ be the truth table of the feedback function f. Then $\eta_i = (i \pmod{k^{n-1}} - 1)k + p_i = i(mod\, k^{n-1})k - s_i$.*

Proof. We simplify the representation

$$Col_j(L_i) = \delta_{k^n-1}^{(i-1)k+j} Col_j(M_i),$$

where $j = 1, 2, \cdots, k, i = 1, 2, \dots, k^{n-1}$.
Let $(i-1)k + j = m$, then straightforward computations show that

$$\begin{cases} \eta_i = (i-1)k + p_i, \\ \eta_{i+k^{n-1}} = (i-1)k + p_{i+k^{n-1}}, \\ \eta_{i+2k^{n-1}} = (i-1)k + p_{i+2k^{n-1}}, \\ \quad \vdots \\ \eta_{i+(k-1)k^{n-1}} = (i-1)k + p_{i+(k-1)k^{n-1}}. \end{cases} \tag{1}$$

where $i = 1, 2, \dots, k^{n-1}$.
Therefore $\eta_i = (i \pmod{k^{n-1}} - 1)k + p_i, i = 1, 2, \cdots, k^n$. Moreover, since $s_i = k - p_i$, we have $\eta_i = (i \pmod{k^{n-1}} - 1)k + p_i = (i \pmod{k^{n-1}} - 1)k - s_i$, where $i = 1, 2, \cdots, k^n$. ■

Remark 3.7 *when $k = 2$, the result of Theorem 3.6 is the same as the result of Theorem 1 in [4].*

Theorem 3.8 *Consider the linearization of an n-stage NFSR. Let $M = \delta_k[p_1 \ p_2 \ \cdots \ p_{k^n}]$ be the structure matrix, and $L = \delta_{k^n}[\eta_1 \ \eta_2 \ \cdots \ \eta_{k^n}]$ be the state transition matrix. We define $A_i = \delta_k[p_i, p_{i+k^{n-1}}, \cdots, p_{i+(k-1)k^{n-1}}], i = 1, 2, \cdots, k^{n-1}$. Then the NFSR is nonsingular if and only if $\det(A_i) \neq 0, i = 1, 2, \cdots, k^{n-1}$.*

Proof. (Necessity) Since the NFSR is nonsingular, each state of a nonlinear FSR has only one successor and one predecessor, that is, for any two states $\delta_{k^n}^j, \delta_{k^n}^j, i \neq j$, we have $L\delta_{k^n}^j \neq L\delta_{k^n}^j$, which is equivalent to $\delta_{k^n}^{\eta_i} \neq \delta_{k^n}^{\eta_j}$, i.e., for all $i \neq j$, $Col_i(L) \neq Col_j(L)$, it shows $\eta_1, \eta_{1+k^{n-1}}, \cdots, \eta_{1+(k-1)k^{n-1}}$ are distinct. According to Formulation (1), we have $p_1, p_{1+k^{n-1}}, \cdots, p_{1+(k-1)k^{n-1}}$ are distinct, i.e., $\det(A_1) \neq 0$. The same reasoning holds for $\det(A_i) \neq 0, i = 2, 3, \cdots, k^{n-1}$.
(Sufficiency) Since $\det(A_1) \neq 0$, that is, $p_1, p_{1+k^{n-1}}, \cdots, p_{1+(k-1)k^{n-1}}$ are distinct, we hve $\eta_1, \eta_{1+k^{n-1}}, \cdots, \eta_{1+(k-1)k^{n-1}}$ are distinct. Moreover, $p_1, p_{1+k^{n-1}}, \cdots, p_{1+(k-1)k^{n-1}} \in \{1, 2, \cdots, k\}$, we have $\eta_1, \eta_{1+k^{n-1}}, \cdots, \eta_{1+(k-1)k^{n-1}} \in \{1, 2, \cdots, k\}$.
The same reasoning holds for

$$\begin{cases} \eta_{2+ik^{n-1}} \in \{k+1, k+2, \cdots, 2k\}, \\ \quad \vdots \\ \eta_{k^{n-1}+ik^{n-1}} \in \{k^n - k, k^n - k + 1, \cdots, k^n\}. \end{cases}$$

therefore L is nonsingular, i,e., the NFSR is nonsingular. ■

3.2 The properties of state transition matrix

Theorem 3.9 *Consider the linearization of an n-stage NFSR. Let $L = \delta_{k^n}[\eta_1 \ \eta_2 \ \cdots \ \eta_{k^n}]$ be the state transition matrix.*
(1) $\eta_{\frac{i(k^n-1)}{k-1}+1} = \frac{i(k^n-1)}{k-1} + 1$ if and only if the state diagram of the NFSR has a unit cycle containing the state

$[k-i-1, k-i-1, \ldots, k-i-1]^T$.
(2) Specially, $\eta_{k^n} = k^n$ if and only if the state diagram of the NFSR has a unit cycle containing the state $[0, 0, \ldots, 0]^T$, and $\eta_1 = 1$ if and only if the state diagram of the NFSR has a unit cycle containing the state $[k-1, k-1, \ldots, k-1]^T$.

Proof. Suppose f is the feedback function of the NFSR. The state diagram of the NFSR has a unit cycle containing the state $[k-i-1, k-i-1, \ldots, k-i-1]^T$, if and only if $f(k-i-1, k-i-1, \ldots, k-i-1) = k-i-1$. Since the truth table of f is arranged in the reverse alphabet order, $s_m = k-i-1$, then

$$m = ik^{n-1} + ik^{n-2} + \cdots + ik + i + 1 = \frac{i(k^n-1)}{k-1} + 1.$$

According to Theorem 3.6,
$\eta_{\frac{i(k^n-1)}{k-1}+1} = ((\frac{i(k^n-1)}{k-1} + 1) \pmod{k^{n-1}})k - s_{\frac{i(k^n-1)}{k-1}+1}$
$= \frac{i(k^n-1)}{k-1} + 1$. Specially, theorem 3.6 shows that $\eta_1 = 1$ if and only if $f(k-1, k-1, \cdots, k-1) = k-1$, which is equivalent to that the successor of $[k-1, k-1, \cdots, k-1]T$ is itself. Thus, the result follows. The same reasoning holds for $\eta_{k^n} = k^n$. ■

Theorem 3.10 *Consider the linearization of an n-stage NFSR. $\delta_{k^n}^i$ is a starting state if and only if $\delta_{k^n}^i$ is not a column of the state transition matrix L, where $i \in 1, 2, \ldots, k^n$.*

Proof. (Necessity) Assume $\delta_{k^n}^i$ is a column of L. Without loss of generality, suppose $\delta_{k^n}^i$ is the j-th column of L for some $j \in 1, 2, \cdots, k^n$. Then $L\delta_{k^n}^j = \delta_{k^n}^i$, which implies that $\delta_{k^n}^j$ is a predecessor of $\delta_{k^n}^i$. It is in contradiction with the assumption that $\delta_{k^n}^i$ is a starting state.
(Sufficiency) Assume $\delta_{k^n}^i$ is not a starting state. Then $\delta_{k^n}^i$ has at least one predecessor. Without loss of generality, we assume $\delta_{k^n}^j$ is a predecessor of $\delta_{k^n}^i$ for some $j \in 1, 2, \cdots, k^n$. Then we conclude that $L\delta_{k^n}^j = \delta_{k^n}^i$, which means that $\delta_{k^n}^i$ is the j-th column of L. It is contrary to the assumption. ■

Theorem 3.11 *Consider the linearization of an n-stage NFSR. The state transition matrix $L = \delta_{k^n}[\eta_1\ \eta_2\ \cdots\ \eta_{k^n}]$ is singular if and only if there exist some $i \in \{1, 2, \ldots, k^{n-1}\}$ such that $\eta_{i+a_1k^{n-1}} = \eta_{i+a_2k^{n-1}}, a_1, a_2 \in \{0, 1, \ldots, k-1\}$ and $a_1 \neq a_2$. Moreover, if $\eta_{i+a_1k^{n-1}} = \eta_{i+a_2k^{n-1}} = j$ then $\delta_{k^n}^j$ is a branch state.*

Proof. According to Theorem 3.6, it is easy to see that the necessity and sufficiency of the result hold. On the other hand, if $\eta_{i+a_1k^{n-1}} = \eta_{i+a_2k^{n-1}} = j$, we have $L\delta_{k^n}^{i+a_1k^{n-1}} = L\delta_{k^n}^{i+a_2k^{n-1}} = \delta_{k^n}^j$, which implies that the state $\delta_{k^n}^j$ has two predecessors, $\delta_{k^n}^{i+a_1k^{n-1}}$ and $\delta_{k^n}^{i+a_1k^{n-1}}$. Thus $\delta_{k^n}^j$ is a branch state. ■

Corollary 3.12 *If a matrix*

$$L = \delta_{k^n}[\eta_1\ \eta_2\ \cdots\ \eta_{k^n}] \in \mathcal{L}_{k^n \times k^n},$$

satisfies

$$\eta_i, \eta_{i+k^{n-1}}, \cdots, \eta_{i+(k-1)k^{n-1}} \in \{ki-k+1, ki-k, \cdots, ki\},$$

where $i = 1, 2, \cdots, k^{n-1}$, then there exists an n-stage NFSR such that L is a state transition matrix of the NFSR. Moreover, if the matrix L is nonsingular, then the NFSR is also nonsingular.

Proof. According to Equations (1), we have

$$\begin{cases} \eta_i = ik - s_i, \\ \eta_{i+k^{n-1}} = ik - s_{i+k^{n-1}}, \\ \eta_{i+2k^{n-1}} = ik - s_{i+2k^{n-1}}, \\ \quad\vdots \\ \eta_{i+(k-1)k^{n-1}} = (ik - s_{i+(k-1)k^{n-1}}. \end{cases} \tag{2}$$

Equations (1) and (2) show that for a matrix L satisfying $\eta_i, \eta_{i+k^{n-1}}, \cdots, \eta_{i+(k-1)k^{n-1}} \in \{ki-k+1, ki-k, \cdots, ki\}, i = 1, 2, \cdots, k^{n-1}$ there exists an NFSR whose state transition matrix is L. Moreover, Theorem 3.6 implies the truth table of the feedback function, $[s_1, s_2, \cdots, s_{k^n}]$ is the truth table of the feedback function, arranged in the reverse alphabet order, satisfies: $s_i, s_{i+k^{n-1}}, \cdots, s_{i+(k-1)k^{n-1}} \in \{0, 1, \cdots, k-1\}$ if $\eta_i, \eta_{i+k^{n-1}}, \cdots, \eta_{i+(k-1)k^{n-1}} \in \{ki-k+1, ki-k, \cdots, ki\}$. Moreover, if L is nonsingular, then the feedback function is nonsingular as well. Thus, the NFSR is nonsingular. ■

In the end of this section, an example is given to show the effectiveness of the results obtained in this paper.
Example Consider a nonlinear feedback shift register with a feedback function

$$f(x_1, x_2) = x_2 + x_1(x_2^2 + 1)(\text{mod}3).$$

Through computation, the structure matrix and the state transition matrixis are $M = \delta_3[3\ 1\ 1\ 2\ 3\ 2\ 1\ 2\ 3]$ and $L = \delta_9[3\ 4\ 7\ 2\ 6\ 8\ 1\ 5\ 9]$ respectively. Then according to theorem 3.6, it is nonsingular.

3.3 Properties of Maximum Length NFSR

In this subsection, we survey some of the necessary conditions of the feedback function $f(x_1, \ldots, x_n) \in \mathcal{D}_k$ to generate de Bruijin sequences.

Proposition 3.13 *To avoid all i cycle $i = 0, 1, \ldots, k-1$, $f(i, \ldots, i) \neq i$.*

Proof. It is proved obviously.

Proposition 3.14 *To avoid all $(0, 0, \ldots, 0, i)$ of length $n+1$, the coefficients of all the linear terms of f are not $k-1$ simultaneously, and $c_0 \neq i$.*

Proof. If all linear coefficient of f are $k-1$, then $f = c_0 + (k-1)(x_1 + x_2 + \cdots x_n) + \cdots + c_{12\ldots n}x_1x_2\cdots x_n$.

$$\begin{cases} f(0, 0, \cdots, 0, i) = i + (k-1)i = 0, \\ f(0, 0, \cdots, i, 0) = i + (k-1)i = 0, \\ \quad\vdots \\ f(i, 0, \cdots, 0, 0) = i + (k-1)i = 0. \end{cases}$$

There must be $(0, 0, \ldots, 0, i)$ of length $n+1$. ■

Lemma 3.15 [22] *Consider a k-valued n-stage NFSR with the structural matrix L. The number of fixed points and the number of cycles which have length s of the NFSR, are de-*

noted by N_1, N_s respectively, then

$$N_1 = tr(L), N_s = \frac{tr(L^s) - \sum_{t \in P(s)} tN_t}{s}.$$

where $2 \leq s \leq k^n$, and $P(s)$ is a set of proper factors of s, tr is the sum of the diagonal elements of a matrix.

Proposition 3.16 *An n-stage NFSR is a maximum length NFSR if and only if the state transition matrix L of its linearization satisfies $L^{k^n} = I_{k^n}$ and $tr(L^m) = 0$ for any positive integer $m < k^n$.*

Proof. The result follows from Lemma 3.15.
(Sufficiency) $ord(L) = k^n$, i.e., $L^{k^n} = I_k$, then $N_{k^n} = \frac{tr(L^{k^n}) - \sum_{t \in P(s)} tN_t}{k^n} = 1$, which shows that NFSR is a maximum length.
(Necessity) If $ord(L) = m < k^n$, i.e., $tr(L^m) = k^n$, then $N_{k^n} = \frac{tr(L^{k^n}) - \sum_{t \in P(s)} tN_t}{k^n} < 1$, which is contradictory with the condition. ■

Lemma 3.17 [12] *Let $A = \delta_m[\zeta_1 \; \zeta_2 \; \cdots \; \zeta_m] \in \mathcal{L}_{m \times m}$ be a cyclic permutation matrix. If $\zeta_{i_0} = m$ for some $i_0 \in 1, 2, \cdots, m-1$, then $ord(A) = \frac{m}{gcd(m, i_0)}$ and $tr(A^l) = 0$ for any positive integer $l < ord(A)$.*

Proposition 3.18 *For an n-stage NFSR, the state transition matrix $L \in \mathcal{L}_{k^n \times k^n}$ satisfies $ord(L) = k^n$, then $tr(L^l) = 0$ for any positive integer $l < k^n$. Moreover $det(L) = (-1)^{k^n - 1}$.*

Proof. $ord(L) = k^n$ implies $L \neq I_{k^n}$ and L is nonsingular. Thus L is a permutation matrix. We have L is similar to the cyclic permutation matrix B_{k^n}, where

$$B_{k^n} = \delta_{k^n}[k^n \; 1 \; 2 \; 3 \cdots \; k^n - 1].$$

We deduce that L^l is similar to $B^l_{k^n}$ for any positive integer l. Hence $\det(L) = \det(B_{k^n}) = (-1)^{k^n - 1} \times 1 = (-1)^{k^n - 1}$. Moreover, from lemma 3.16, we see $ord(B_{k^n}) = k^n$, while lemma 3.16 shows that $tr(B_{k^n}) = 0$ for any positive integer $l < ord(A)$. Therefore $tr(L^l) = 0$ for any positive integer $l < k^n$. ■

Theorem 3.19 *An n-stage NFSR is a maximum length NFSR if and only if the state transition matrix L satisfies $ord(L) = k^n$.*

Proof. The result yields from proposition 3.16 and proposition 3.18.

Theorem 3.20 *For an n-stage maximum length NFSR, the state transition matrix L of its linearization is denoted by*

$$L = \delta_{k^n}[\eta_1 \; \eta_2 \; \ldots \; \eta_{k^n}].$$

Then
(1) $\eta_{\frac{i(k^{n-1})}{k-1}} \neq \frac{i(k^{n-1})}{k-1}, i = 0, 1, \cdots, k-1$.
(2) There exists unique $i \in 1, 2, \cdots, k-1$ such that $\eta_{ik^{n-1}} = k^n$.

Proof. (1) One hand,

$$\eta_{\frac{i(k^{n-1})}{k-1}+1} = \frac{i(k^{n-1})}{k-1} + 1 = i(k^{n-1} + \cdots + k + 1) + 1,$$

the other hand,
$\eta_{\frac{i(k^{n-1})}{k-1}+1} = ((\frac{i(k^{n-1})}{k-1} + 1)(\bmod (k^{n-1}))k + k - f(k-i-1, \cdots, k-i-1) = i(k^{n-1} + \cdots + k) + k - f(k-i-1, \cdots, k-i-1)$.

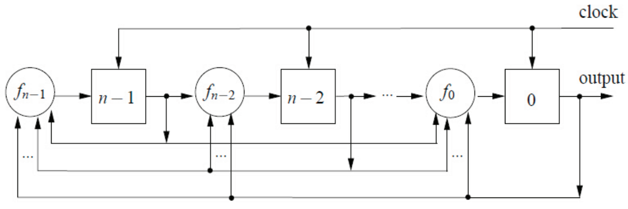

Fig. 2. The general structure of an n-bit shift register with updating functions.

Then we have $f(k-i-1, \cdots, k-i-1) = k-i-1$, i.e., the state diagram of the NFSR has a unit cycle containing the state $[k-i-1, \cdots, k-i-1]^T$, which is a contradiction with the maximum length NFSR.
(2) According to theorem 3.6, we have
$\eta_{ik^{n-1}} = (k^{n-1} - 1)k + k - s_{k^{n-1}+(i-1)k^{n-1}}$
$= k^n - f(k-i, 0, \cdots, 0)$.
Because of the NFSR is maximum length, there exists unique $i \in 1, 2, \cdots, k-1$ such that $(k-i, 0, \cdots, 0)$ is the predecessor of the state $(0, 0, \cdots, 0)$. Then $\eta_{ik^{n-1}} = k^n - f(k-i, 0, \cdots, 0) = k^n$. ■

4 The generalized NFSR

The general structure of an n-bit shift register with updating functions can be described as in Fig.2, and can be expressed as

$$\begin{cases} x_1(t+1) = x_2(t) \oplus f_1(x_1(t), x_3(t), \cdots, x_n(t)), \\ x_2(t+1) = x_3(t) \oplus f_2(x_1(t), x_2(t), x_4(t), \cdots, x_n(t)), \\ \quad \vdots \\ x_i(t+1) = x_{i+1}(t) \oplus f_i(x_1(t), \cdots, x_i(t), x_{i+2}(t), \cdots, x_n(t)), \\ x_n(t+1) = x_1 \oplus f_n(x_2(t), \ldots, x_n(t)). \end{cases}$$

where $x_i \in \mathcal{D}_k$, and $f_i : \mathcal{D}^n_k \to \mathcal{D}_k, i = 1, 2, \cdots, n$. Now in vector form above formulation becomes

$$\begin{cases} x_1(t+1) = T_1 x(t), \\ x_2(t+1) = T_2 x(t), \\ \quad \vdots \\ x_n(t+1) = T_n x(t). \end{cases} \tag{3}$$

Let $T_i, i \in 1, 2, \cdots, n-1$ be the structure matrix of $x_i(t+1) = x_{i+1}(t) \oplus f_i(x_1(t), \cdots, x_i(t), x_{i+2}(t), \cdots, x_n(t))$, and $T_i = \delta_k[p^i_1, \cdots, p^i_{k^n}]$, which can be got the truth table of $x_i(t+1) = x_{i+1}(t) \oplus f_i(x_1(t), \cdots, x_i(t), x_{i+2}(t), \cdots, x_n(t))$, and $L = \delta_{k^n}[\eta_1 \; \eta_2 \; \cdots \; \eta_{k^n}]$ be the state transition matrix of shift register. Then it is easy to see that

$$\eta_i = k^n - (p^1_i k^{n-1} + p^2_i k^{n-2} + \cdots + p^n_i).$$

5 Conclusion

This paper used Boolean network approach to facilitate the linearization of multi-valued NFSRs. Therefore we study an NFSR by the new state transition matrix, which is actually a linearization of the NFSR. The new state transition matrix can be simply computed from the truth table of the feedback function of the multi-valued NFSRs. We give some properties of the new state transition matrix, properties of a maximum length multi-valued NFSR and the linear representation of general structureof an n-bit shift register with updating functions as well.

References

[1] M. Hell, T. Johansson and W. Meier. Grain-A Stream Cipher for Constrained Environments, eSTREAM, ECRYPT Stream Cipher Project, Report 2005/010, 2005.

[2] S. Babbage and M. Dodd. The Stream CipherMICKEY (version 1), eSTREAM, ECRYPT Stream Cipher Project, Report 2005/015, 2005.

[3] C. De Cannière and B. Preneel, Trivium Specifications. eSTREAM, ECRYPT Stream Cipher Project, Report 2005/030, 2005.

[4] S. W. Golomb. Shift Register Sequences. Holden-Day, Laguna Hills, CA, USA, 1967.

[5] P. Dąbrowski, G. Labuzek, T. Rachwalik, and J. Szmidt. Searching for nonlinear feedback shift registers with parallel computing. Information Processing Letters 114 (5): 268-272, 2014

[6] H. Fredricksen. A survey of full length nonlinear shift register cycle algorithms. SIAM Review 24(2): 195-221, 1982 .

[7] H. Hu and G. Guang. Periods on two kinds of nonlinear feedback shift registers with time varying feedback functions. Int. J. Foundations of Computer Science 22 (6): 1317-1329, 2011.

[8] E. Dubrova. A transformation from the Fibonacci to the Galois NLFSRs. IEEE Trans. Information Theory 55(11): 5263-5271, 2009.

[9] T. Tian and W.F. Qi. On the largest affine sub-families of a family of NFSR sequences. Des. Codes Cryptogr. 71: 163-181, 2014.

[10] Z. Ma, W.-F. Qi, and T. Tian. On the decomposition of an NFSR into the cascade connection of an NFSR into an LFSR. J. Complexity 29(2): 173-181, 2013.

[11] E. Dubrova. Scalable method for constructing Galois NLFRs with period $2^n - 1$ using cross-join pairs. IEEE Trans. Information Theory 59(1): 703-709, 2013.

[12] J. Zhong and D. Lin. On maximum length nonlinear feedback shift registers using a Boolean network approach. In: Proceedings of the 33rd Chinese Control Conference, Nanjing, China, July 28-30, 2014, pp. 2502-2507.

[13] S. A. Kauffman. Metabolic stability and epigenesis in randomly constructed genetic nets. J. Theoretical Biol. 22: 437-467, 1969.

[14] S. E. Harris, B. K. Sawhill, A. Wuensche, and S. Kauffman. A model of transcriptional regulatory networks based on biases in the observed regulation rules. Complexity 7: 23-40, 2002.

[15] M. Aldana. Boolean dynamics of networks with scale-free topology. Physica D, 185: 45-66, 2003.

[16] D. Cheng. Disturbance decoupling of Boolean control networks. IEEE Trans. Autom. Control, 56(1): 2-10, 2011.

[17] G. Hochma, M. Margaliot, E. Fornasini, and M. E. Valcher. Symbolic dynamics of Boolean control networks. Automatica, 49(8): 2525-2530, 2013.

[18] D. Cheng, H. Qi, and Z. Li. Analysis and Control of Boolean Networks. London, U. K.: Springer-Verlag, 2011.

[19] P. Dabrowski, G. Labuzek, T. Rachwalik, and J. Szmidt. Searching for nonlinear feedback shift registers with parallel computing. Information Processing Letters 114 (5): 268-272, 2014.

[20] D. Cheng and H. Qi. Controllability and observability of Boolean control networks. Automatica, 45(7): 1659-1667, 2009.

[21] D. Cheng and H. Qi. A linear representation of dynamics of Boolean networks. IEEE Trans. Aut. Contr., 55(10): 2251-2258, 2010.

[22] D. Cheng, Z. Li and H. Qi. Realization of Boolean control networks. Automatica, 46(1): 62-69, 2010.

[23] Z. Li and D. Cheng. Algebraic approach to dynamics of multivalued networks. Int. J. Bifurcat. Chaos, 20(3): 561- 582, 2010.

[24] Z. Liu and Y. Wang. Disturbance decoupling of mix-valued logical networks via the semi-tensor product. Automatica, 48(8): 1839-1844, 2012.

[25] H. Qi. On shift register via semi-tensor product approach, In: Proceedings of the 32th Chinese Control Conference, Xian, China, July, 2013, pp. 208-212.

[26] D. Zhao, H. Peng, L. Li, S. Hui, and Y. Yang. Novel way to research nonlinear feedback shift register. SCIENCE CHINA Information Sciences, 57, 092114(14) doi: 10.1007/s11432-013-5058-4.

[27] A. H. Roger and C. R. Johnson. Topics in Matrix Analysis. U.K.: Cambridge University Press, 1991.

[28] Z. Liu, Y. Wang, Y.Zhao. Nonsingularity of nonlinear feedback shift registers, Proceedings of the 32th Chinese Control Conference, 2014, pp. 2438-2443.

[29] X. Zhang, Z. Yang, and C. Cao. Inequalities involving Khatri-Rao products of positive semi-definite matrices. Applied Mathematics E-notes 2: 117-124, 2002.