Stability and Linearization of Multi-valued Nonlinear Feedback Shift Registers

Haiyan Wang, Dongdai Lin

State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093, China.
{wanghaiyan, ddlin}@iie.ac.cn

Abstract. In this paper, we study stability and linearization of multi-valued nonlinear feedback shift registers which are considered as logic networks. First, the linearization of multi-valued nonlinear feedback shift registers (NFSRs) is discussed, which is to find their state transition matrices by considering it as a logical network via a semi-tensor product approach. For a multi-valued NFSR, the new state transition matrix which can be simply computed from the truth table of its feedback function is more explicit. Second, based on the linearization theory of multi-valued NFSRs, we investigate the stability of multi-valued NFSRs, and some sufficient and necessary conditions are provided for globally (locally) stable multi-valued NFSRs. Finally, some examples are presented to show the effectiveness of the proposed results.

Keywords: Nonlinear feedback shift register, Semi-tensor product, State transition matrix, Stability, Boolean network.

1 Introduction

It is known that nonlinear feedback shift registers (NFSRs) are the main building blocks in many fields. For example, the eSTREAM Stream Cipher Project hardware finalists, Grain [1], Mickey [2] and ,Trivium [3]. In addition, many convolutional decoders use NFSRs as their main building blocks [4]. In the process of decoding, an error tends to induce a successive of further decoding errors. There are some strategies such as periodic re-synchronization have been proposed to control this error-propagation. The stability of an NFSR is an alternative to limit this error propagation.

The theory of NFSRs which is different from LFSRs is not well-understood due to its complexity and lack of efficient analysis tools, though numerous efforts have been made over the past decades. It is known that an n-stage LFSR can use an n-dimensional matrix to describe its state transition. Such a matrix is called a state transition matrix of the LFSR. For an NFSR, does there also exist a state transition matrix? The linearization of NFSRs answers this questions.

The Linearization of NFSRs is to find their state transition matrices. This paper uses a linearization method for NFSRs, namely, the Boolean network approach (preliminary work was given in [5]). An NFSR was viewed as a finite-state automaton in [6] and as a finite-state machine in [7]. In particular, it was viewed as a Boolean network in [8]. A Boolean network is an autonomous system that evolves as an automaton through Boolean functions. However, it is different to any autonomous systems studied in the conventional system theory, where the system variables take infinite number of reals. Over the last decades Boolean network have attracted much attention in many communities, ranging from biology [9] and physics [10] to system science [11], and their resulting monography [12], and [13, 14].

The semi-tensor product of matrices [11] has been successfully used in the study of Boolean networks [15, 16], multi-valued and mix-valued logical networks [17, 18], and some other related fields [19, 20]. In their work, 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. In [16], a matrix expression of a Boolean network was investigated. Multi-valued logical networks were studied, and the controllability of multi-valued logical control networks was revealed in [17]. In particular, based on the linear system description of a Boolean network, its global stability was investigated in [21] via an incident matrix, and it was also studied in [22] via the state transition matrix. Some sufficient and necessary conditions were given in both references. In addition, local stability of Boolean networks was addressed in the latter reference.

This paper investigates the multi-valued NFSR. First, the linearization of multi-valued NFSRs is discussed which is to find their state transition matrices by considering it as a logical network via a semi-tensor product approach. Then, based on the Linearization theory of multi-valued NFSRs (logic network representation), we investigate the stability of multi-valued NFSRs, and some sufficient and necessary conditions are provided for globally (locally) stable multi-valued NFSRs.

The rest of this paper is organized as follows. Section 2 gives some notations and necessary preliminaries on the semi-tensor product of matrices in the study of Boolean networks. In Section 3, we present the linearization of multi-valued NFSRs, and in Section 4, we give the stability of multi-valued NFSRs, and some sufficient and necessary conditions are provided for globally (locally) stable multi-valued NFSRs, which is followed by the conclusion in section 5.

2 Preliminaries

This section presents some notations and necessary preliminaries on the semi-tensor product in the study of logic networks.

Semi-tensor product (STP) of matrices is an extension of conventional matrix product to any two arbitrary matrices. 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 [12, 15, 16] and the references therein for details.

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.
- $\mathcal{D}_k = \{0, 1, 2, \cdots, k-1\}, \Delta_n = \{\delta_n^i | i = 1, 2, \cdots, n\}$.
- 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 in the study of logic networks.

Definition 1 [23] *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 [12] *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 3 [24] *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 $A_i, B_i, i = 1, 2, \ldots, n$ 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.

We consider a map φ is defined by

$$\varphi : \quad x \in \mathcal{D}_k \longmapsto X = \delta_k^{k-x} \in \Delta_k.$$

Obviously, φ is a bijection. We denote: $\mathcal{D}_k \sim \Delta_k$.

Lemma 1 [12] *Suppose*

$$\mathbf{x} = X_1 X_2 \cdots X_n$$

with $X_i \in \Delta_k, i = 1, 2, \ldots, n$. Then $\mathbf{x} \in \Delta_{k^n}$ and each X_i is uniquely determined by $\mathbf{x}$. Moreover, For any $j \in \{1, 2, \ldots, k^n\}$, the state $\mathbf{x} = \delta_{k^n}^j \in \Delta_{k^n}$ and the state $[x_1\ x_2\ \cdots\ x_n]^T \in \mathcal{D}_k^n$ satisfying $k^{n-1}x_1 + k^{n-2}x_2 + \cdots + x_n = k^n - j$ are one-to-one correspondent.

Lemma 2 [12] *For any k-valued function $f(x_1, x_2, \ldots, x_n)$ with $x_i \in \mathcal{D}_k, i = 1, 2, \ldots, n$, let $[s_1, s_2, \ldots, s_{k^n}]$ be he truth table of f, arranged in the reverse alphabet order. Then f can be expressed as a multi-linear form:*

$$f(X_1, X_2, \ldots, X_n) = M X_1 X_2 \cdots X_n,$$

where $X_i \in \Delta_k, i = 1, 2, \ldots, n$, and $M = \delta_k[k - s_1\ \ k - s_2\ \ \cdots\ \ k - s_{k^n}]$ is called the structure matrix of f.

A k-valued logic network with n nodes can be described as the following system:

$$\begin{cases} x_1(t+1) = g_1(x_1(t), x_2(t), \ldots, x_n(t)), \\ x_2(t+1) = g_2(x_1(t), x_2(t), \ldots, x_n(t)), \\ \quad \vdots \\ x_{n-1}(t+1) = g_{n-1}(x_1(t), x_2(t), \ldots, x_n(t)), \\ x_n(t+1) = g_n(x_1(t), x_2(t), \ldots, x_n(t)). \end{cases} \tag{1}$$

where $g_i : \mathcal{D}_k^n \to \mathcal{D}_k, x_i \in \mathcal{D}_k$. Let G_i be the structure matrix of the function g_i. Then according to Lemma 1 and Lemma 2, the k-valued logic network can be equivalently described as a linear system:

$$\mathbf{x}(t+1) = L\mathbf{x}(t), \tag{2}$$

where the state $\mathbf{x} \in \Delta_{k^n}$ and the state transition matrix $L = G_1 * G_2 * \cdots * G_n \in \mathcal{L}_{k^n \times k^n}$.

3 Linearization of Multi-valued Nonlinear Feedback Shift Register

The following Fig.1 denotes an n-stage NFSR with a feedback functionin $f(x_1(t), x_2(t), \ldots, x_n(t))$. View the n-stage k-valued NSFR (In the following discussion, we call it NSFR simply.) as a k-valued logic network, then it can be expressed as:

$$\begin{cases} x_1(t+1) = x_2(t), \\ x_2(t+1) = x_3(t), \\ \quad \vdots \\ x_{n-1}(t+1) = x_n(t), \\ x_n(t+1) = f(x_1(t), x_2(t), \ldots, x_n(t)). \end{cases} \tag{3}$$

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

Therefore it has a linear representation (1). We have the following results.

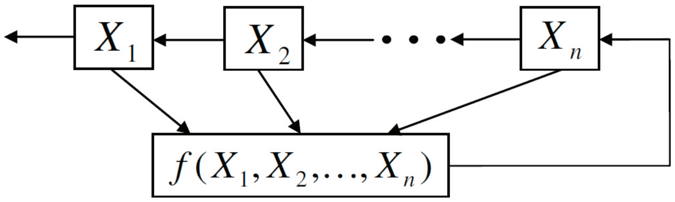

Fig. 1. Nonlinear Feedback Shift Register

Lemma 3 *Consider an n-stage NFSR with a feedback function f. Let $M = [M_1\ M_2\ \cdots\ M_{k^{n-1}}]$ be the structural matrix of NFSR 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 $L \in \mathcal{L}_{k^n \times k}, M \in \mathcal{L}_{k \times k}, j = 1, 2, \ldots, k, i = 1, 2, \ldots, k^{n-1}$.*

Proof. View the NFSR as a k-valued logic network. Then the NFSR can be expressed as the following logic network:

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

where $x_i \in \mathcal{D}_k, i = 1, 2, \ldots, n$, and $f : \mathcal{D}_k^n \to \mathcal{D}_k$. Let T_i be the structure matrix of $x_i(t+1) = x_{i+1}(t), i \in 1, 2, \ldots, n-1$, and M be the structure matrix of $x_n(t+1) = f(x_1(t), x_2(t), \ldots, x_n(t))$. 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 (1) 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 $j = 1, 2, \ldots, k, i = 1, 2, \ldots, k^{n-1}$.

Theorem 4 *Let the state transition matrix of NFSR 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 $j = 1, 2, \ldots, k, i = 1, 2, \ldots, k^{n-1}$.
Let $(i-1)k + j = m$, then straightforward computations show that

$$\begin{cases} \eta_i = (i-1)k + p_i, \\ \eta_{i+k^{n-1}} = (i-1)k + p_{i+k^{n-1}}, \\ \eta_{i+2k^{n-1}} = (i-1)k + p_{i+2k^{n-1}}, \\ \quad \vdots \\ \eta_{i+(k-1)k^{n-1}} = (i-1)k + p_{i+(k-1)k^{n-1}}. \end{cases} \tag{4}$$

where $i = 1, 2, \ldots, k^{n-1}$.
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 $i = 1, 2, \ldots, k^n$.

4 Stability of Multi-valued Nonlinear Feedback Shift Registers

In the beginning of this section, we first briefly review some existing basic definitions and properties about the stability of NFSRs.

The state diagram of an n-stage, k-valued NFSR is a directed graph consisting of k^n nodes and k^n directed edges. Each node corresponds to a state of the NFSR, and an edge from state $\mathbf{X}$ to state $\mathbf{Y}$ means that $\mathbf{X}$ is shifted to the state $\mathbf{Y}$. $\mathbf{X}$ is called a predecessor of $\mathbf{Y}$, and $\mathbf{Y}$ is called the successor of $\mathbf{X}$. Every state of an NFSR has a unique successor, but may have no predecessor or a single predecessor or two predecessors. The state with two predecessors is called a branch state, while the state without predecessors is called a starting state. A sequence of p distinct states, $\mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_p$, is called a cycle of length p if $\mathbf{X}_1$ is the successor of $\mathbf{X}_p$, and $\mathbf{X}_{i+1}$ is a successor of $\mathbf{X}_i$ for any $i \in \{1, 2, \cdots, p-1\}$. Similarly, a sequence of p distinct states, $\mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_p$ is called a transient of length p, if the following conditions are satisfied: (1) none of them lies on a cycle; (2) $\mathbf{X}_1$ is a starting state; (3) $\mathbf{X}_{i+1}$ is a successor of $\mathbf{X}_i$ for any $i \in \{1, 2, \cdots, p-1\}$; (4) the successor of $\mathbf{X}_p$ lies on a cycle.

We consider $\mathbf{g} = [g_1\ g_2\ \cdots\ g_n], \mathbf{x} = [x_1\ x_2\ \cdots\ x_n] \in \mathcal{D}_k^n$, (1) can be expressed as:

$$\mathbf{X}(t+1) = \mathbf{g}(\mathbf{X}(t)). \tag{5}$$

View the n-stage k-valued NSFR as a k-valued logic network, then it can be expressed as (5). For any positive integer N, let $\mathbf{g}^{N+1}(\mathbf{X}(t)) = \mathbf{g}(\mathbf{g}^{N}(\mathbf{X}(t)))$, which indicates that the state $\mathbf{g}(\mathbf{X}(t))$ is shifted $N+1$ times from $\mathbf{X}(t)$.

Definition 4 *A state $\mathbf{X}(t)$ is called an equilibrium state of the logic network (5), if $\mathbf{g}(\mathbf{X}(t)) = \mathbf{X}(t)$. If the logic network (5) is a representation of an k-valued NFSR, then its equilibrium state is also called an equilibrium state of the NFSR.*

Obviously, the logic network (5) has k possible equilibrium states, $\mathbf{i} = [i\, i\, \cdots\, i], i = 0, 1, \cdots, k-1$. Without loss of generality, throughout this paper, we assume $\mathbf{0}$ is an equilibrium state of the logic network representation (5) of an NFSR, or equivalently, the feedback function f of the NFSR satisfies $f(\mathbf{0}) = 0$. For the equilibrium state $\mathbf{i}$, through a coordinate transformation

$$\bar{\mathbf{X}}(t) = \mathbf{X}(t) \oplus k - i,$$

the logic network (5) becomes

$$\bar{\mathbf{X}}(t+1) = \mathbf{g}(\bar{\mathbf{X}}(t) + k - i) + k - i. \tag{6}$$

It is easy to see that $\mathbf{0}$ is the equilibrium state of the logic network (6).

Definition 5 *An n-stage NFSR is globally stable to the equilibrium state $\mathbf{0}$, if for any state $\mathbf{X}(t)$, there exists a positive integer N such that the state transition function of its logic network representation (5) satisfies $\mathbf{g}^{N}(\mathbf{X}(t)) = 0$, that is, $\mathbf{0}$ is the unique equilibrium state and there are no cycles in the state diagram of the NFSR.*

Definition 6 *An n-stage NFSR is locally stable to the equilibrium state $\mathbf{0}$, if there exists some state $\mathbf{X}(t) \neq \mathbf{0}$ such that for some positive integer N the state transition function of its Boolean network representation (1) satisfies $\mathbf{g}^{N}(\mathbf{X}(t)) = \mathbf{0}$.*

Since an n-stage NFSR has an equivalent logic network representation in a linear system (2), accordingly, we give an equivalent definition of globally (locally) stable NFSR as follows.

Definition 7 *An n-stage NFSR is globally stable to the equilibrium state $\mathbf{0}$, if for any state $\mathbf{x}(t)$, there exists a positive integer N such that the state transition matrix L of its logic network representation (2) satisfies $L^{N}\mathbf{x}(t) = \delta_{k^n}^{k^n}$.*

Definition 8 *An n-stage NFSR is locally stable to the equilibrium state $\mathbf{0}$, if there exists some state $\mathbf{x}(t) \neq \delta_{k^n}^{k^n}$ such that for some positive integer N the state transition matrix L of its logic network representation (2) satisfies $L^{N}\mathbf{x}(t) = \delta_{k^n}^{k^n}$.*

In the sequel, an NFSR is globally (resp. locally) stable means an NFSR is globally (resp. locally) stable to the equilibrium state $\mathbf{0}$. From their definitions, it is easy to see that a globally stable NFSR must be locally stable, but not the vice versa.

Definition 9 *An NFSR is called a globally stable maximum transient NFSR if it is globally stable and has a single starting state.*

Some properties of local stability are next given.

Theorem 5 *An NFSR is locally stable if and only if the feedback function satisfies $f(0,\cdots,0)=0$, and there are at least $i\in\{1,2,\cdots,k-1\}$ such that $f(i,0,\cdots,0)=0$.*

Proof. Necessity: Clearly, according to Definition 6, $f(0,\cdots,0)=0$ is a necessary condition for a locally stable NFSR. For any NFSR whose feedback function f satisfies $f(0,\cdots,0)=0$, the state 0 has only two possible predecessors: itself and $[i\ 0\ \cdots\ 0], i\in\{1,2,\cdots,k-1\}$. If the NFSR is locally stable, then there exists some state $X(t)\neq\mathbf{0}$ such that for some integer N, $\mathbf{g}^N(x(t))=0$. Thus, $\mathbf{0}$ has a predecessor different to itself. Hence, here there are at least $i\in\{1,2,\cdots,k-1\}$ such that $f(i,0,\cdots,0)=0$.

Sufficiency: $f(0,\cdots,0)=0$ implies that $\mathbf{0}$ is an equilibrium state of the NFSR. If there are at least $i\in\{1,2,\cdots,k-1\}$ such that $f(i,0,\cdots,0)=0$, then $[i\ 0\ \cdots\ 0]$ is a predecessor of $\mathbf{0}$. In other words, there exists a state $x(t)=[i,0,\cdots,0]$ such that $g(x(t))=0$, which implies that the NFSR is locally stable.

Theorem 6 *Let $L=\delta_{k^n}[\eta_1\ \eta_2\ \ldots\ \eta_{k^n}]$ be the state transition matrix of the logic network representation (2) in a linear system of an n-stage NFSR. Then the NFSR is locally stable, then $\eta_{k^n}=k^n$ and there are at least $i\in\{1,2,\cdots,k-1\}$ such that $\eta_{(k-i)k^{n-1}}=k^n$.*

Proof. The result follows from (4) in Theorem 4 and Theorem 5.

Theorem 7 *Let $L=\delta_{k^n}[\eta_1\ \eta_2\ \ldots\ \eta_{k^n}]$ be the state transition matrix of the logic network representation (2) in a linear system of an n-stage locally stable NFSR. Assume the initial state of system (2) be $\mathbf{x}_0=\delta_{k^n}^r$, if*
(1)$col_{k^n}(L)=\delta_{k^n}^{k^n}$;
(2)there exists an integer l, such that $col_r(L^l)=\delta_{k^n}^{k^n}$.

Proof. Clearly, according to Definition 8, $f(0,\cdots,0)=0$ is a necessary condition for a locally stable NFSR, i.e., $s_{k^n}=0$, according to (4) in Theorem 4, we have $\eta_{k^n}=k^n$, i.e., $col_{k^n}(L)=\delta_{k^n}^{k^n}$,
There exists an integer l, such that $col_r(L^l)=\delta_{k^n}^{k^n}$. thus $L^l\delta_{k^n}^r=\delta_{k^n}^{k^n}$.
This completes the proof.

Next, some properties of global stability are next given.

Theorem 8 *If the NFSR is globally stable maximum transient, then there exists a unique $i\in\{1,2,\cdots,k-1\}$ such that $f(i,0,\cdots,0)=0$.*

Proof. If the NFSR is globally stable maximum transient, then other states have unique predecessor and successor, except the starting state and the state $\mathbf{0}$. the state $\mathbf{0}$ has only two types of possible predecessors: itself and $[i,0,\cdots,0], i\in\{1,2,\cdots,k-1\}$, moreover the NFSR is globally stable maximum transient, thus $\mathbf{0}$ has a unique predecessor different to itself.

Theorem 9 *Let $L = \delta_{k^n}[\eta_1\ \eta_2\ \ldots\ \eta_{k^n}]$ be the state transition matrix of the logic network representation (2) in a linear system of an n-stage NFSR. If the NFSR is globally stable maximum transient, then there exists a unique $i \in \{1, 2, \cdots, k-1\}$ such that $\eta_{k^n} = \eta_{(k-i)k^{n-1}} = 0$.*

Proof. As the NFSR is globally stable maximum transient, then there exists a unique $i \in \{1, 2, \cdots, k-1\}$ such that $f(i, 0, \cdots, 0) = f(0, 0, \cdots, 0) = 0$, thus $s_{k^n} = s_{(k-i)k^{n-1}} = 0$. The result follows from Theorem 4.

Theorem 10 *Let L be the state transition matrix of the logic network representation (2) in a linear system of an n-stage NFSR. If the NFSR is globally stable, then there exists an integer N such that each columns of L^N are equal to $\delta_{k^n}^{k^n}$.*

Proof. As the equilibrium state $\mathbf{0} \in \mathcal{D}_k^n$ is uniquely corresponding to the state $\delta_{k^n}^{k^n} \in \Delta_{k^n}$, that an n-stage NFSR is globally stale to the equilibrium state $\mathbf{0}$ is equivalent to that the n-stage NFSR is globally stable to the state $\delta_{k^n}^{k^n}$. Clearly, any state of an n-stage globally stable NFSR with one more starting states must be shifted fewer times to reach the equilibrium state $\mathbf{0}$ than the n-stage globally stable maximum transient NFSR. For an n-stage globally stable maximum transient NFSR, the starting state $\mathbf{x}_0 = \delta_{k^n}^i$, must shift $k^n - 1$ times to go through all other states and finally reaches the state $\delta_{k^n}^{k^n}$. (or equivalently, the state $\mathbf{0}$) and keeps staying at this state. Therefore, $N = k^n - 1$ is the largest power such that each column of L^N is equal to $\delta_{k^n}^{k^n}$.

Theorem 11 *Let $L = \delta_{k^n}[\eta_1\ \eta_2\ \ldots\ \eta_{k^n}]$ be the state transition matrix of the logic network representation in a linear system of an n-stage NFSR. Then, $\delta_{k^n}^j, j \in \{1, 2, \cdots, k^n\}$ is a branch state if and only if there exist at least two different elements a_1, a_2 in the set $\{0, 1, \cdots, k-1\}$ such that $\eta_{a_1 k^{n-1}+i} = \eta_{a_2 k^{n-1}+i} = j$ and $i = \lceil \frac{j}{k} \rceil$.*

Proof. (Sufficiency) $\eta_{a_1 k^{n-1}+i} = \eta_{a_2 k^{n-1}+i} = j$, then $L\delta_{a_1 k^{n-1}+i} = L\delta_{a_2 k^{n-1}+i} = \delta_{k^n}^j$, thus $\delta_{k^n}^j, j \in \{1, 2, \cdots, k^n\}$ is a branch state.
(Necessity) If $\delta_{k^n}^j$ is a branch state. According to Lemma 1, the state $\delta_{k^n}^j$ is uniquely corresponding to the state $\mathbf{X} = [X_1\ X_2\ \cdots\ X_n]^T \in \mathcal{D}_k^n$ satisfying $k^{n-1}X_1 + k^{n-2}X_2 + \cdots + X_n = k^n - j$. The state $\mathbf{X}$ is a branch state, then it has at least two possible predecessor: $[k-1-a_1, X_1, \cdots, X_{n-1}]^T$ and $[k-1-a_2, X_1, \cdots, X_{n-1}]^T$, where $a_1, a_2 \in \{0, 1, \cdots, k-1\}$ and $a_1 \neq a_2$. Since the matrix L uniquely corresponds to the truth table of the feedback function that is arranged in the reverse alphabet order, accordingly we arrange all k^n states in $\mathcal{D}_k^n$ of the NFSR in the reverse decimal order as well. Thus, it is easy to see that if we denote as $\mathbf{X}_{a_1 k^{n-1}+i} = [k-1-a_1, X_1, \cdots, X_{n-1}]^T$, and then $\mathbf{X}_{a_2 k^{n-1}+i} = [k-1-a_2, X_1, \cdots, X_{n-1}]^T$. According to Lemma 1, we have

$$k^n - a_1 k^{n-1} + i = (k-1-a_1)k^{n-1} + X_1 k^{n-2} + \cdots + X_{n-1}. \tag{7}$$

$$k^n - j = X_1 k^{n-1} + X_2 k^{n-2} + \cdots + X_n. \tag{8}$$

According to (7) and (8), we have

$$k^n - j = k(X_1k^{n-2}+X_1k^{n-2}+\cdots+X_{n-1})+X_n = k(k^{n-1}-i)+X_n = k^n-ki+X_n.$$

It yields $ki = j + X_n$, Since $X_n \in \{0, 1, \cdots, k-1\}$, we conclude that $i = \lceil \frac{j}{k} \rceil$.

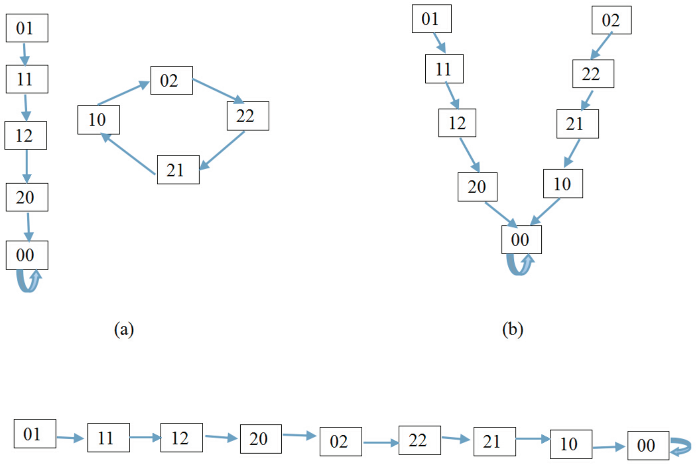

Fig. 2. The State Diagram of The Example

In the end of this section, an example is given to show the effectiveness of the results obtained in this paper.

Example Consider the following three 2-stage 3-valued NFSRs. The state $\mathbf{0}$ is their equilibrium state.

Consider a nonlinear feedback shift register with a feedback function:

$$f_1(x_1, x_2) = x_1 + x_2 + x_1^2 + 2x_1^2x_2^2. \tag{9}$$

Using the vector form, $0 \sim \delta_3^3, 1 \sim \delta_3^2, 0 \sim \delta_3^1$, we obtain from (9):

$$f_1(x_1, x_2) = \delta_3[1\ 0\ 0\ 0\ 2\ 2\ 2\ 1\ 0]x_1x_2 = M_1x_1x_2.$$

The state diagram in Fig.2 (a) shows it is locally stable. According to (4) in Theorem 4, we have:

$$\mathbf{x}(t+1) = \delta_9[2\ 6\ 9\ 3\ 4\ 7\ 1\ 5\ 9]\mathbf{x}(t) = L_1\mathbf{x}(t).$$

$L_1^2 = \delta_9[6\ 7\ 9\ 9\ 3\ 1\ 2\ 4\ 9], L_1^3 = \delta_9[7\ 1\ 9\ 9\ 9\ 2\ 6\ 3\ 9], L_1^4 = \delta_9[1\ 2\ 9\ 9\ 9\ 6\ 7\ 9\ 9]$. $f(0,0) = 0$, $\mathbf{0}$ is a unique equilibrium state. According to Theorem 5, Theorem 6, $f(2,0) = f(2,1) = 0$, and $\eta_3 = \eta_9 = 9$. According Theorem 7, the initial state $\mathbf{x}_0 = \delta_9^8$, therefore $Col_8(L^4) = \delta_9^9$.

Consider a nonlinear feedback shift register with a feedback function:

$$f_2(x_1, x_2) = x_1 + x_2 + 2x_1x_2^2 + 2x_1^2x_2^2. \tag{10}$$

Using the vector form, $0 \sim \delta_3^3, 1 \sim \delta_3^2, 0 \sim \delta_3^1$, we obtain from (10):

$$f_2(x_1, x_2) = \delta_3[2\ 3\ 3\ 3\ 1\ 3\ 1\ 2\ 3]x_1x_2 = M_2x_1x_2.$$

The state diagram in Fig.2 (b) shows it is locally stable. According to (4) in Theorem 4, we have:

$$\mathbf{x}(t+1) = \delta_9[2\ 6\ 9\ 3\ 4\ 9\ 1\ 5\ 9]\mathbf{x}(t) = L_2\mathbf{x}(t).$$

$L_2^2 = \delta_9[6\ 9\ 9\ 9\ 3\ 9\ 2\ 4\ 9], L_2^3 = \delta_9[9\ 9\ 9\ 9\ 9\ 9\ 6\ 3\ 9], L_2^4 = \delta_9[9\ 9\ 9\ 9\ 9\ 9\ 9\ 9\ 9]$. δ_9^9 is a branch state, according to Theorem 11, there exist at least two different elements η_3, η_6 such that $\eta_3 = \eta_6 = 9$. According Theorem 10, there exists an integer $N = 4$ such that each columns of L_2^4 are equal to δ_9^9.

Consider a nonlinear feedback shift register with a feedback function:

$$f_3(x_1, x_2) = 2x_1 + x_2 + x_1^2 + x_1x_2^2 + x_1^2x_2^2. \tag{11}$$

Using the vector form, $0 \sim \delta_3^3, 1 \sim \delta_3^2, 0 \sim \delta_3^1$, we obtain from (11):

$$f_3(x_1, x_2) = \delta_3[2\ 3\ 1\ 3\ 1\ 3\ 1\ 2\ 3]x_1x_2 = M_3x_1x_2.$$

The state diagram in the last picture of Fig.2 shows it is globally stable maximum transient. According to (4) in Theorem 4, we have:

$$\mathbf{x}(t+1) = \delta_9[2\ 6\ 7\ 3\ 4\ 9\ 1\ 5\ 9]\mathbf{x}(t) = L_3\mathbf{x}(t).$$

$L_3^2 = \delta_9[6\ 9\ 1\ 7\ 3\ 9\ 2\ 4\ 9], L_3^3 = \delta_9[9\ 9\ 2\ 1\ 7\ 9\ 6\ 3\ 9], L_3^4 = \delta_9[9\ 9\ 6\ 2\ 1\ 9\ 9\ 7\ 9], L_3^2 = \delta_9[9\ 9\ 9\ 6\ 2\ 9\ 9\ 1\ 9], L_3^3 = \delta_9[9\ 9\ 9\ 9\ 6\ 9\ 9\ 2\ 9], L_3^4 = \delta_9[9\ 9\ 9\ 9\ 9\ 9\ 9\ 6\ 9], L_3^4 = \delta_9[9\ 9\ 9\ 9\ 9\ 9\ 9\ 9\ 9]$. According Theorem 8, there exists a unique state $[1\ 0]$ such that $f(1,0) = 0$. there exists an integer 8 such that each columns of L_3^8 are equal to δ_9^9.

Remark 1 *In [25], we know the starting state of a globally stable maximum transient NFSR is* $[0\ 0\ \cdots\ 1]$ *when* $k = 2$. *While* $k > 2$, *the starting state of a globally stable maximum transient NFSR is not unique. For example, when* $k = 3, n = 2$, *we consider two nonlinear feedback shift registers with feedback functions* $f(x_1, x_2) = 2x_1 + x_2 + x_1^2 + x_1x_2^2 + x_1^2x_2^2$ *and* $f(x_1, x_2) = 2x_1 + x_2 + 2x_1^2 + 2x_1x_2^2 + x_1^2x_2^2$ *respectively. They are both globally stable maximum transient, but their starting states are* $[0\ 1]$ *and* $[0\ 2]$ *respectively.*

5 Conclusion

In this paper, we considered the stability and linearization of multi-valued NFSRs. the linearization of multi-valued NFSRs is to find their state transition matrices by considering it as a logical network via a semi-tensor product approach. The new state transition matrix which can be simply computed from the truth table of its feedback function is easier to compute and is more explicit. Then, based on the linearization theory of multi-valued NFSRs, globally (locally) stable multi-valued NFSRs were investigated. Some sufficient and necessary conditions were given. These results provide a method to construct globally or locally stable NFSRs, and are also helpful to analyze the state diagram of a NFSRs.

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. J. L. Massy, R. W. Liu, Application of Lyapnunovs direct method to the error-propagation effect in convolutional codes. IEEE Trans. Information Theory 10 (1964) 248-250.
5. 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.
6. C. Fontaine, Nonlinear feedback shift register, Encryclopedia of Cryptography and Security, pp. 846-848, 2011.
7. S. W. Golomb, Shift Register Sequences, Holden-Day, Laguna Hills, CA, USA, 1967.
8. J. Zhong and D. Lin, Stability of Nonlinear Feedback Shift Registers, Proceeding of the IEEE International Conference on Information and Automation , Hailar, China, July, 2014, in press.
9. S. Huang and I. Ingber, Shape-dependent control of cell growth, differentiation, and apotosis: switching between attractors in cell regulatory networks, Exper. Cell Res., vol. 261, no. 1, pp. 91-103, 2000.
10. M. Aldana, Boolean dynamics of networks with scale-free topology, Physica D, vol. 185, no.1, pp. 45-66, 2003.
11. D. Cheng, Disturbance decoupling of Boolean control networks, IEEE Trans. Autom. Control, vol. 56, no. 1, pp. 2-10, 2011.
12. D. Cheng, H. Qi, and Z. Li, Analysis and Control of Boolean Networks, London, U. K.: Springer-Verlag, 2011.
13. D. Laschov and M. Margaliot, A maximum principle for single-input Boolean control networks, IEEE Trans. Automatic Control, vol. 56, no. 4, pp. 913-917, 2011.
14. G. Hochma, M. Margaliot, E. Fornasini, and M. E. Valcher, Symbolic dynamics of Boolean control networks, Automatica, vol. 49, no. 8, pp. 2525-2530, 2013.
15. D. Cheng and H. Qi. Controllability and observability of Boolean control networks. Automatica, 45(7): 1659-1667, 2009.
16. D. Cheng and H. Qi. A linear representation of dynamics of Boolean networks. IEEE Trans. Aut. Contr., 55(10): 2251- 2258, 2010.

17. Z. Li and D. Cheng. Algebraic approach to dynamics of multi-valued networks. Int. J. Bifurcat. Chaos, 20(3): 561- 582, 2010.
18. Z. Liu and Y. Wang. Disturbance decoupling of mix-valued logical networks via the semi-tensor product. Automatica, 48(8): 1839-1844, 2012.
19. D. Laschov and M. Margaliot. Controllability of Boolean control networks via the Perron-Frobenius theory. Automatica, 48(6): 1218-1223, 2012.
20. Y. Wang, C. Zhang and Z. Liu. A matrix approach to graph maximum stable set and coloring problems with application to multi-agent systems. Automatica, 48(7): 1227-1236, 2012.
21. D. Cheng, H. Qi, Z. Li, and J. B. Liu, Stability and stabilization of Boolean networks, Int. J. Robust and Nonlinear Control, vo. 21, no. 2, pp. 134-156, 2011.
22. F. Li and J. Sun, Stability and stabilization of multivalued logical network, Nonlinear Analysis: Real Word Applications, vol. 12, no. 6, pp. 3701-3712, 2011.
23. A. H. Roger and C. R. Johnson. Topics in Matrix Analysis. U.K.: Cambridge University Press, 1991.
24. 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.
25. F. J. Mowler, Relations between P_n cycles and stable feedback shift registers, IEEE Trans. Electronic Computers, vol. EC-15, no. 3, pp. 375-378, 1966.