SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

January 2016, Vol. 59 012204:1–012204:12
doi: 10.1007/s11432-015-5311-0

Stability of nonlinear feedback shift registers

Jianghua ZHONG[1,2*] & Dongdai LIN[1]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[2]*Institute of Complexity Science, Qingdao University, Qingdao* 266071*, China*

Received November 27, 2014; accepted January 5, 2015; published online December 21, 2015

Abstract Convolutional codes have been widely used in many applications such as digital video, radio, and mobile communication. Nonlinear feedback shift registers (NFSRs) are the main building blocks in convolutional decoders. A decoding error may result in a succession of further decoding errors. However, a stable NFSR can limit such an error-propagation. This paper studies the stability of NFSRs using a Boolean network approach. A Boolean network is an autonomous system that evolves as an automaton through Boolean functions. An NFSR can be viewed as a Boolean network. Based on its Boolean network representation, some sufficient and necessary conditions are provided for globally (locally) stable NFSRs. To determine the global stability of an NFSR with its stage greater than 1, the Boolean network approach requires lower time complexity of computations than the exhaustive search and the Lyapunov's direct method.

Keywords nonlinear feedback shift register, stability, Boolean function, Boolean network, semi-tensor product

Citation Zhong J H, Lin D D. Stability of nonlinear feedback shift registers. Sci China Inf Sci, 2016, 59(1): 012204, doi: 10.1007/s11432-015-5311-0

1 Introduction

Convolutional codes have been widely used in many applications such as digital video, radio, mobile communication, and satellite communication. Nonlinear feedback shift registers (NFSRs) are the main building blocks in convolutional decoders. However, in the process of decoding, a decoding error tends to induce a succession of further decoding errors. Although some strategies such as periodic re-synchronization have been proposed to control this error-propagation effect, it is at the expense of introducing encoding queues. A stable NFSR is an alternative to limit this error propagation.

Although numerous efforts have been made on NFSRs over the past decades, the theory of NFSRs has not been well-understood due to its complexity and lack of efficient analysis tools. It is still an open problem to find an efficient way to analyze the cycle structure of any given NFSR. It is also an open problem to give some efficient way to design an NFSR satisfying some properties such as large period and stability. Some studies have focused on the stability of NFSRs. Massey and Liu viewed an NFSR as an automaton and used the Lyapunov's direct method to investigate the stability of the NFSR [1]. Lyapunov's direct method [2] is an important and useful technique in system theory for analysis of the stability of systems, whose variables are real numbers. Via a Lyapunov function, it can determine the

* Corresponding author (email: zhongjianghua@iie.ac.cn)

stability of a given system without the knowledge of the system's solution. However, for a nonlinear system, the Lyapunov function is difficult to construct in general, and the construction of Lyapunov functions is a challenging problem in the system theory all the time. Thanks to the finite states of an NFSR, a Lyapunov function was constructed to determine the global stability of the NFSR, by searching all stable states [1]. Such a method is called the *iterated Lyapunov technique*. However, it still has relatively high time-complexity of computations if the NFSR's stage is large. In addition, Mowle proved that the number of n-stage globally stable NFSRs is 2^{2^n-n-1}, and also pointed out that all these NFSR are binomially distributed [3]. He further gave an algorithm to generate all of them in [4]. However, to the best knowledge of the authors, from then on the stability of NFSRs has not been further studied, due to lack of efficient tools.

An NFSR was viewed as a finite-state automaton in [5] and as a finite-state machine in [6]. In particular, it was viewed as a Boolean network in [7–9]. A Boolean network is an autonomous system that evolves as an automaton through Boolean functions. It is different to any autonomous systems studied in the conventional system theory, where the system variables take infinite number of reals. Boolean network was first introduced by Kauffman in 1969 to model a genetic network whose describing variables take only two values, "on" and "off" (or equivalently, 1 and 0, respectively) [10]. Over the last decades Boolean networks have attracted much attention in many communities, ranging from biology [11–13] and physics [14–16] to system science ([17–20], and their resulting monography [21] and [22,23]).

In the community of system science, Cheng and his co-workers developed an algebraic framework for Boolean networks, using a semi-tensor product approach [21]. 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. Thanks to their algebraic set-up, problems related to Boolean functions can be converted into algebraic problems. In particular, based on the linear system description of a Boolean network, its global stability was investigated in [24] via a Lyapunov function, and in [25] via an incident matrix. It was also studied in [26] via a state transition matrix. Some sufficient and necessary conditions were given in the references therein. Local stability of Boolean networks was addressed in the latter reference. In addition, via a state transition matrix, global stability of Boolean network with impulsive effects was studied in [27], and the time-delay effects on Boolean networks were also investigated in some work, for example, [28,29].

This paper addresses the stability problem of NFSRs using a Boolean network approach. The NFSR is viewed as a Boolean network. Based on its Boolean network representation developed by the authors in [8], some sufficient and necessary conditions are presented for both globally stable NFSRs and locally stable NFSRs via a state transition matrix. Compared to the previous work on the stability of NFSRs, we consider globally stable NFSRs as well as locally stable NFSRs, while the previous work only focused on the globally stable NFSRs. Moreover, the Boolean network approach requires lower time complexity of computations to determine the global stability of an NFSR. On the other hand, compared to the work on stability of *general* Boolean networks in system theory, we focus on the stability of a *particular* type of Boolean networks, namely, NFSRs, which will lead to some deeper and more concise results.

The contribution of this paper is: a novel approach, called Boolean network approach, is used to facilitate the study of the stability of NFSRs. The Boolean network approach requires lower time complexity of computations than the Lyapunov direct method and the exhaustive search to determine the global stability of an NFSR with its stage greater than 1. It is also helpful to analyze the state diagram of a given NFSR and to design stable NFSRs.

We now introduce some notations used in this paper. $\mathbb{F}_2$ denotes the binary Galois field, and $\mathbb{F}_2^n$ denotes the set of all n-dimensional vectors over $\mathbb{F}_2$. $\mathbb{N}$ is the set of nonnegative integers. For a real number r, $\lceil r\rceil$ denotes the smallest integer no less than r. δ_n^i represents the ith column of the identity matrix I_n of dimension n. The set of all δ_n^i, $i=1,2,\ldots,n$, is denoted by Δ_n, that is, $\Delta_n=\{\delta_n^i|i=1,2,\ldots,n\}$. The set of all m-dimensional vectors over Δ_n is denoted as Δ_n^m. $\mathcal{L}_{n\times m}$ stands for the set of all $n\times m$ matrices whose columns belong to Δ_n. For any matrix $A\in\mathcal{L}_{n\times m}$, $A=\left[\delta_n^{i_1}\ \delta_n^{i_2}\ \cdots\ \delta_n^{i_m}\right]$, $i_1,i_2,\ldots,i_m\in\{1,2,\ldots,n\}$. For the sake of simplicity, we write A in a compact form, as $A=\delta_n[i_1\ i_2\ \cdots\ i_m]$. The operators $+$, $-$ and $\times$, respectively, denote the ordinary addition, subtraction, and multiplication in the complex field,

while the operations $\oplus$ and $\odot$, respectively, denote the addition and multiplication modulo 2 in the binary Galois field $\mathbb{F}_2$. Again, for the sake of simplicity, we denote the multiplication of any two complex numbers a and b as ab, namely, $ab = a \times b$.

The remainder of this paper is organized as follows. Section 2 briefly reviews some related work on Boolean networks. Section 3 is our main results. Some sufficient and necessary conditions are given for globally (locally) stable NFSRs. The paper is concluded in Section 4.

2 Boolean network

In this section, we first briefly review the semi-tensor product of matrices. We then recall the multi-linear form of nonlinear Boolean function that is obtained by the semi-tensor product. Finally, we revisit the Boolean network representation of an NFSR, which is very useful to investigate the stability of NFSRs.

2.1 Semi-tensor product

Semi-tensor product of matrices was introduced by Cheng [21]. It is a generalization of the conventional matrix product. For two matrices A and B, the conventional matrix product of A and B, denoted by AB, requires that the column number of the former matrix A is equal to the row number of the latter matrix B. However, the semi-tensor product relaxes this constraint. It works for any two matrices regardless of their sizes, while it retains all major properties of the conventional matrix product, such as the associative law and the distributive law [21][1)]. Before reviewing the semi-tensor product, we first recall what the Kronecker product is.

Definition 1 ([30]). 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

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

Definition 2 ([21]). 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

$$A \ltimes B = \left(A \otimes I_{\frac{\alpha}{m}}\right)\left(B \otimes I_{\frac{\alpha}{p}}\right). \tag{2}$$

Remark 1. The semi-tensor product is originally defined for any two matrices with entries in the real field. However, it still works for any two matrices with entries in the binary Galois field $\mathbb{F}_2$ under its binary operations, the addition $\oplus$ and the multiplication $\odot$.

2.2 Multi-linear form of Boolean function

A Boolean function f with n variables is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, that is, $f : \mathbb{F}_2^n \to \mathbb{F}_2$. A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is *linear* (*resp. nonlinear*) if f is a *linear* (*resp. nonlinear*) mapping with respect to its variables in $\mathbb{F}_2$. Let i be the decimal number corresponding to the binary $(i_1, i_2, \ldots, i_n)$ via the mapping $i = i_1 2^{n-1} + i_2 2^{n-2} + \cdots + i_n$. Then i ranges from 0 to $2^n - 1$. For the sake of simplicity, we denote $f(i) = f(i_1, i_2, \ldots, i_n)$. Then the truth table of f can be written as $[f(0), f(1), \ldots, f(2^n - 1)]$ that is arranged in the alphabet order, or be written as $[f(2^n - 1), f(2^n - 2), \ldots, f(0)]$ that is arranged in the reverse alphabet order.

Identify 1 and 0, respectively, as $[1 \ \ 0]^{\mathrm{T}}$ and $[0 \ \ 1]^{\mathrm{T}}$. Accordingly, identify a variable $X \in \mathbb{F}_2$ as $[X \ \ X \oplus 1]^{\mathrm{T}}$. In the sequel, we say 1, 0 and X are, respectively, the scalar forms of their vector forms,

1) A toolbox written in Matlab for the related computations of semi-tensor product of matrices are available at the website of http://lsc.amss.ac.cn/~dcheng/stp/STP.zip.

$[1\ 0]^{\mathrm{T}}$, $[0\ 1]^{\mathrm{T}}$ and $[X\ \ X\oplus 1]^{\mathrm{T}}$. To distinguish the scalar form and the vector form of a variable, in the sequel we use the notation X for a variable in $\mathbb{F}_2$, while we use the notation x for its vector variable in Δ_2, that is, $X\in\mathbb{F}_2$, but $x\in\Delta_2$. Using the above vector forms, a Boolean function f is changed to $f:\Delta_2^n\to\Delta_2$, and for any $x_1,x_2\in\Delta_2$, the two operations, addition $\boxplus$ and multiplication $\boxdot$, can be expressed as

$$x_1\boxplus x_2=\begin{bmatrix}0&1&1&0\\1&0&0&1\end{bmatrix}\ltimes x_1\ltimes x_2,\quad x_1\boxdot x_2=\begin{bmatrix}1&0&0&0\\0&1&1&1\end{bmatrix}\ltimes x_1\ltimes x_2.$$

Let $x_1=[X_1\ \ X_1\oplus 1]^{\mathrm{T}}$ and $x_2=[X_2\ \ X_2\oplus 1]^{\mathrm{T}}$. Then straightforward computations show that

$$x_1\boxplus x_2=[X_1\oplus X_2\quad X_1\oplus X_2\oplus 1]^{\mathrm{T}},\quad x_1\boxdot x_2=[X_1\otimes X_2\quad (X_1\otimes X_2)\oplus 1]^{\mathrm{T}}.$$

The above two equations imply that for any two vectors over Δ_2, their addition (multiplication) is formed as follows: the first entry results from the addition (multiplication) over $\mathbb{F}_2$ operating on the first entries of both vectors, while the second entry is the complement of the first one. For example, let $x_1=[1\ \ 0]^{\mathrm{T}}$ and $x_2=[0\ \ 1]^{\mathrm{T}}$, then

$$x_1\boxplus x_2=[1\ \ 0]^{\mathrm{T}},\quad x_1\boxdot x_2=[0\ \ 1]^{\mathrm{T}}.$$

Lemma 1 ([21,31]). Any Boolean function $f(x_1,x_2,\ldots,x_n)$ with $x_1,x_2,\ldots,x_n\in\Delta_2$ can be expressed as a multi-linear form:

$$f(x_1,x_2,\ldots,x_n)=F\ltimes x_1\ltimes x_2\ltimes\cdots\ltimes x_n,\tag{3}$$

where F is called the *structure matrix* of f, and is uniquely expressed as

$$F=\begin{bmatrix}s_1&s_2&\cdots&s_{2^n}\\1-s_1&1-s_2&\cdots&1-s_{2^n}\end{bmatrix}\tag{4}$$

with $[s_1,s_2,\ldots,s_{2^n}]$ being the truth table of f, arranged in the reverse alphabet order.

Note that the number of ones in the truth table $[s_1,s_2,\ldots,s_{2^n}]$ of a Boolean function f is called the *weight* of f. In addition, it is notable to point out that Lemma 1 shows that for any Boolean function, after its variables in $\mathbb{F}_2$ are identified as the vector variables in Δ_2, it is multi-linear with respect to its variables in Δ_2 in the sense of semi-tensor product, but not with respect to its variables in $\mathbb{F}_2$.

Lemma 2 ([21,32]). Suppose

$$\boldsymbol{x}=x_1\ltimes x_2\ltimes\cdots\ltimes x_n\tag{5}$$

with $x_i\in\Delta_2$, $i=1,2,\ldots,n$. Then $\boldsymbol{x}\in\Delta_{2^n}$. Moreover, the vector $\boldsymbol{x}=\delta_{2^n}^j\in\Delta_{2^n}$ with $j\in\{1,2,\ldots,2^n\}$ and the vector $\boldsymbol{X}=[X_1\ \ X_2\ \cdots\ X_n]^{\mathrm{T}}\in\mathbb{F}_2^n$ satisfying $2^{n-1}X_1+2^{n-2}X_2+\cdots+X_n=2^n-j$ are a one-to-one correspondence.

2.3 Boolean network representation of nonlinear feedback shift register

Consider an n-stage nonlinear feedback shift register with a Boolean function $f:\mathbb{F}_2^n\to\mathbb{F}_2$, usually called *feedback function*, see Figure 1, where each small square in the upper row is a binary storage device. The contents of the n storage devices are denoted by the variables $X_1,X_2,\ldots,X_n$, which form a state of the NFSR, $[X_1\ \ X_2\ \cdots\ X_n]^{\mathrm{T}}$. At each periodic interval determined by a master clock, the NFSR's state $[X_1\ \cdots\ X_{n-1}\ \ X_n]^{\mathrm{T}}$ is shifted to the state $[X_2\ \cdots\ X_n\ \ f(X_1,X_2,\ldots,X_n)]^{\mathrm{T}}$. Let $S_0,S_1,S_2,\ldots$ be an output sequence of the NFSR. Then it satisfies the nonlinear recurrence relation:

$$S_{t+n}=f(S_t,S_{t+1},\ldots,S_{t+n-1}),\quad t\in\mathbb{N},\tag{6}$$

where f is a nonlinear Boolean function with respect to the variables $S_t,S_{t+1},\ldots,S_{t+n-1}$ in $\mathbb{F}_2$. In particular, if f is linear with respect to these variables, say,

$$f(S_t,S_{t+1},\ldots,S_{t+n-1})=a_0S_t\oplus a_1S_{t+1}\oplus\cdots\oplus a_{n-1}S_{t+n-1},$$

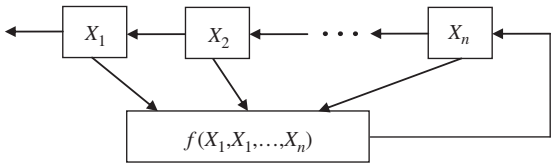

Figure 1 An n-stage nonlinear feedback shift register.

where $a_i \in \mathbb{F}_2$, $i = 0, 1, \ldots, n-1$, then the NFSR is reduced to a linear feedback shift register (LFSR).

View the NSFR as a Boolean network. Then the *Boolean network representation in a nonlinear system* of the NFSR is [8]

$$\boldsymbol{X}(t+1) = \boldsymbol{g}(\boldsymbol{X}(t)), \tag{7}$$

where $\boldsymbol{X} = [X_1 \ \ X_2 \ \cdots \ X_n]^{\mathrm{T}} \in \mathbb{F}_2^n$ is the state, and the vectorial function $\boldsymbol{g} = [g_1 \ \ g_2 \ \cdots \ g_n]^{\mathrm{T}}$ is the *state transition function*, expressed as

$$\begin{cases} g_1(\boldsymbol{X}(t)) = X_2(t), \\ g_2(\boldsymbol{X}(t)) = X_3(t), \\ \quad \cdots \\ g_{n-1}(\boldsymbol{X}(t)) = X_n(t), \\ g_n(\boldsymbol{X}(t)) = f(\boldsymbol{X}(t)). \end{cases} \tag{8}$$

For any positive integer N, let $\boldsymbol{g}^{N+1}(\boldsymbol{X}) = \boldsymbol{g}\left(\boldsymbol{g}^N(\boldsymbol{X})\right)$, which indicates that the state $\boldsymbol{g}^N(\boldsymbol{X})$ is shifted N times from $\boldsymbol{X}$.

Lemma 3 ([8])**.** Let the structure matrix of the feedback function f be

$$G_n = \delta_2[\omega_1 \ \omega_2 \ \cdots \ \omega_{2^n}], \tag{9}$$

where $\omega_i \in \{1, 2\}$, $i = 1, 2, \ldots, 2^n$. Then the Boolean network (7) can be equivalently expressed as a linear system:

$$\boldsymbol{x}(t+1) = L\boldsymbol{x}(t), \quad t \in \mathbb{N}, \tag{10}$$

where $\boldsymbol{x} \in \Delta_{2^n}$ is the state, and $L \in \mathcal{L}_{2^n \times 2^n}$ is the *state transition matrix*, expressed as

$$L = \delta_{2^n}[\eta_1 \ \cdots \ \eta_{2^{n-1}} \ \eta_{2^{n-1}+1} \ \cdots \ \eta_{2^n}], \tag{11}$$

with

$$\begin{cases} \eta_i = \omega_i + 2(i-1), \quad i = 1, 2, \ldots, 2^{n-1}, \\ \eta_{2^{n-1}+i} = \omega_{2^{n-1}+i} + 2(i-1). \end{cases} \tag{12}$$

To distinguish the Boolean network representation (7) in a nonlinear system of the NFSR, we call its equivalent expression (10) the *Boolean network representation in a linear system* of the NFSR.

Remark 2 ([8])**.** The state transition matrix L in (11) and the NFSR are a one-to-one correspondence.

3 Stability of nonlinear feedback shift registers

In this section, we first briefly review some existing basic concepts and properties about the stability of nonlinear feedback shift registers. We then present our main results. It includes twofold work. One is the properties of feedback functions and state diagrams, and the other is the properties of state transition matrices.

3.1 Basic concepts and properties

The *state diagram* of an n-stage NFSR is a directed graph consisting of 2^n nodes and 2^n directed edges. Each node corresponds to a state of the NFSR, and an edge from state $\boldsymbol{X}$ to state $\boldsymbol{Y}$ means that $\boldsymbol{X}$ is shifted to the state $\boldsymbol{Y}$. $\boldsymbol{X}$ is called a *predecessor* of $\boldsymbol{Y}$, and $\boldsymbol{Y}$ is called the *successor* of $\boldsymbol{X}$. Every state of an NFSR has a unique successor, but may have no predecessors or have only one predecessor or have 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, $\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_p$, is called a *cycle of length* p if $\boldsymbol{X}_1$ is the successor of $\boldsymbol{X}_p$, and $\boldsymbol{X}_{i+1}$ is a successor of $\boldsymbol{X}_i$ for any $i \in \{1, 2, \ldots, p-1\}$. Similarly, a sequence of p distinct states, $\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_p$, is called a *transient of length* p, if the following conditions are satisfied: (1) none of them lies on a cycle; (2) $\boldsymbol{X}_1$ is a starting state; (3) $\boldsymbol{X}_{i+1}$ is a successor of $\boldsymbol{X}_i$ for any $i \in \{1, 2, \ldots, p-1\}$; (4) the successor of $\boldsymbol{X}_p$ lies on a cycle.

Definition 3. A state $\boldsymbol{X}$ is called an *equilibrium state* of the Boolean network (7) if $\boldsymbol{g}(\boldsymbol{X}) = \boldsymbol{X}$. If the Boolean network (7) is a representation of an NFSR, then its equilibrium state is also called an equilibrium state of the NFSR.

Clearly, an equilibrium state of an NFSR is a cycle of length 1 in its state diagram. On the other hand, it is easy to see that the Boolean network (7) has two possible equilibrium states, $\mathbf{0} = [0\ \ 0\ \cdots\ 0]^{\mathrm{T}}$ and $\mathbf{1} = [1\ \ 1\ \cdots\ 1]^{\mathrm{T}}$. For the equilibrium state $\mathbf{1}$, through a coordinate transformation

$$\bar{\boldsymbol{X}} = \boldsymbol{X} \oplus \mathbf{1}, \tag{13}$$

the Boolean network (7) becomes

$$\bar{\boldsymbol{X}}(t+1) = \boldsymbol{g}\left(\bar{\boldsymbol{X}}(t) \oplus \mathbf{1}\right) \oplus \mathbf{1}. \tag{14}$$

Obviously, $\mathbf{0}$ is the equilibrium state of the Boolean network (14). It means that the equilibrium state $\mathbf{1}$ can be transferred to the equilibrium state $\mathbf{0}$ after a coordinate transformation (13). Without loss of generality, throughout this paper, we assume that $\mathbf{0}$ is an equilibrium state of the Boolean network representation (7) of an NFSR, or equivalently, the feedback function f of the NFSR satisfies $f(\mathbf{0}) = 0$.

Definition 4. An n-stage NFSR is *globally stable* to the equilibrium state $\mathbf{0}$, if for any state $\boldsymbol{X} \in \mathbb{F}_2^n$, there exists a positive integer N such that the state transition function of its Boolean network representation (7) satisfies $\boldsymbol{g}^N(\boldsymbol{X}) = \mathbf{0}$, that is, $\mathbf{0}$ is the unique equilibrium state and there are no other cycles in the state diagram of the NFSR.

Definition 5. An n-stage NFSR is *locally stable* to the equilibrium state $\mathbf{0}$, if there exists some state $\boldsymbol{X}_0 \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ such that for some positive integer N the state transition function of its Boolean network representation (7) satisfies $\boldsymbol{g}^N(\boldsymbol{X}_0) = \mathbf{0}$.

Since an n-stage NFSR has an equivalent Boolean network representation in a linear system, accordingly, an equivalent definition of globally (locally) stable NFSR can be given as follows.

Definition 6. An n-stage NFSR is *globally stable* to the equilibrium state $\mathbf{0}$, if for any state $\boldsymbol{x} \in \Delta_{2^n}$, there exists a positive integer N such that the state transition matrix L of its Boolean network representation (10) satisfies $L^N \boldsymbol{x} = \delta_{2^n}^{2^n}$.

Definition 7. An n-stage NFSR is *locally stable* to the equilibrium state $\mathbf{0}$, if there exists some state $\boldsymbol{x}_0 \in \Delta_{2^n} \setminus \{\delta_{2^n}^{2^n}\}$ such that for some positive integer N the state transition matrix L of its Boolean network representation (10) satisfies $L^N \boldsymbol{x}_0 = \delta_{2^n}^{2^n}$.

If there is no ambiguity with respect to the equilibrium state, we just simply say an NFSR is globally (or locally) stable. In the sequel, that 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 8. An NFSR is called a *globally stable maximum transient NFSR* if it is globally stable and has only one starting state.

Lemma 4 ([3])**.** The starting state of a globally stable maximum transient NFSR is $[0\ \ 0\ \cdots\ 0\ \ 1]^{\mathrm{T}}$.

Lemma 5 ([3]). The feedback function f of a globally stable NFSR satisfies $f(1,1,\ldots,1)=0$ and $f(1,0,\ldots,0)=0$.

Lemma 6 ([26]). A Boolean network $\boldsymbol{x}(t+1)=L\boldsymbol{x}(t)$ with $\boldsymbol{x}\in\Delta_{2^n}$ and $L\in\mathcal{L}_{2^n\times 2^n}$, is globally stable to $\delta_{2^n}^i$ for some $i\in\{1,2,\ldots,2^n\}$, if and only if there exists a positive integer N such that each column of L^N is equal to $\delta_{2^n}^i$.

Lemma 7 ([4]). The number of branch states of an NFSR is equal to the number of starting states.

Lemma 8 ([3]). Given a stage n, the number of globally stable maximum transient NFSRs is $2^{2^{n-1}-n}$.

3.2 Properties of feedback function and state diagram

Proposition 1. Suppose the Boolean network (10) with a state transition matrix $L=\delta_{2^n}[\eta_1\ \eta_1\ \cdots\ \eta_{2^n}]$ is a representation of an n-stage NFSR with a feedback function f. Then the truth table of the feedback function, $[s_1\ s_2\ \cdots\ s_{2^n}]$, arranged in the reverse alphabet order, satisfies: (1) $s_i=1$ if η_i is odd for $i\in\{1,2,\ldots,2^n\}$; (2) $s_i=0$ if η_i is even for $i\in\{1,2,\ldots,2^n\}$.

Proof. Note that $\omega_i=1$ (resp. $\omega_i=2$) in (9) uniquely corresponds to $s_i=1$ (resp. $s_i=0$) for any $i\in\{1,2,\ldots,2^n\}$. Then the result directly follows from (9) and (12).

Theorem 1. An NFSR is locally stable if and only if the feedback function f satisfies $f(0,0,\ldots,0)=f(1,0,\ldots,0)=0$.

Proof. *Necessity:* Clearly, according to Definition 5, $f(0,0,\ldots,0)=0$ is a necessary condition for a locally stable NFSR. For any NFSR whose feedback function f satisfies $f(0,0,\ldots,0)=0$, the state $\mathbf{0}$ has only two possible predecessors: itself and $[1\ \ 0\ \cdots\ 0]^{\mathrm{T}}$. If the NFSR is locally stable, then there exists some state $\boldsymbol{X}_0\in\mathbb{F}_2^n\setminus\{\mathbf{0}\}$ such that for some integer N, $\boldsymbol{g}^N(\boldsymbol{X}_0)=0$. Thus, $\mathbf{0}$ has a predecessor different to itself. Hence, $[1\ \ 0\ \cdots\ 0]^{\mathrm{T}}$ must be a predecessor of $\mathbf{0}$, which means $f(1,0,\cdots,0)=0$.

Sufficiency: $f(0,0,\ldots,0)=0$ implies that $\mathbf{0}$ is an equilibrium state of the NFSR. If $f(1,0,\ldots,0)=0$, then $[1\ \ 0\ \cdots\ 0]^{\mathrm{T}}$ is a predecessor of $\mathbf{0}$. In other words, there exists a state $\boldsymbol{X}_0=[1\ \ 0\ \cdots\ 0]^{\mathrm{T}}$ such that $\boldsymbol{g}(\boldsymbol{X}_0)=0$, which implies that the NFSR is locally stable.

Ref. [3] showed that the starting state of a globally stable maximum transient NFSR is $[0\ \ 0\ \cdots\ 0\ 1]^{\mathrm{T}}$. In fact, it is also a starting state of a locally stable NFSR.

Proposition 2. $[0\ \ 0\ \cdots\ 0\ \ 1]^{\mathrm{T}}$ is a starting state of an n-stage locally stable NFSR.

Proof. Since the NFSR is locally stable, according to Theorem 1, we have $f(0,0,\ldots,0)=f(1,0,\ldots,0)=0$, and thereby $[1\ \ 0\ \cdots\ 0]^{\mathrm{T}}$ is a predecessor of $[0\ \ 0\ \cdots\ 0]^{\mathrm{T}}$. The two possible predecessors of the state $[0\ \ 0\ \cdots\ 0\ \ 1]^{\mathrm{T}}$ are $[0\ \ 0\ \cdots\ 0]^{\mathrm{T}}$ and $[1\ \ 0\ \cdots\ 0]^{\mathrm{T}}$. If $[0\ \ 0\ \cdots\ 0]^{\mathrm{T}}$ is a predecessor of $[0\ \ 0\ \cdots\ 0\ \ 1]^{\mathrm{T}}$, then $f(0,0,\ldots,0)=1$, which is a contradiction. If $[1\ \ 0\ \cdots\ 0]^{\mathrm{T}}$ is a predecessor of $[0\ \ 0\ \cdots\ 0\ \ 1]^{\mathrm{T}}$, then $[1\ \ 0\ \cdots\ 0]^{\mathrm{T}}$ has two successors, $[0\ \ 0\ \cdots\ 1]^{\mathrm{T}}$ and $[0\ \ 0\ \cdots\ 0]^{\mathrm{T}}$, which is contrary to the uniqueness of the successor of any state of an NFSR.

From [4], it can be seen that the weight of the feedback function of an n-stage globally stable NFSR is no greater than 2^n-n-1 and all these n-stage globally stable NFSR are binomially distributed. We will further show that the weight of the feedback function of an n-stage globally stable maximum transient NFSR is $2^{n-1}-1$. Moreover, except that the 2^{n-1}th and 2^nth components of the truth table of the feedback function are 0, the first half truth table of the feedback function is complement of the second half.

Theorem 2. If an n-stage NFSR with a feedback function f is globally stable maximum transient, then

(1) the weight of f is $2^{n-1}-1$;

(2) moreover, the truth table $[s_1\ \ s_2\ \ \cdots\ \ s_{2^n}]$ of f, arranged in the reverse alphabet order, satisfies (i) $s_1=s_{2^{n-1}}=s_{2^n}=0$; (ii) $s_i=s_{2^{n-1}+i}\oplus 1$ for any $i\in\{1,2,3,\ldots,2^{n-1}-1\}$ and any $n\geqslant 2$.

Proof. Let $L=\delta_{2^n}[\eta_1\ \ \eta_2\ \ \cdots\ \ \eta_{2^n}]$ be the state transition matrix of Boolean network representation in a linear system of the NFSR. Then from Lemma 3, $\eta_i,\eta_{2^{n-1}+i}\in\{2i-1,2i\}$ for any $i\in\{1,2,\ldots,2^{n-1}\}$. According to Proposition 5 in the next subsection, for the globally stable maximum transient NFSR, we have $\eta_1=2$, and $\eta_{2^{n-1}}=\eta_{2^n}=2^n$. Moreover, if $n\geqslant 2$, then all η_is are distinct for $i=1,2,3,\ldots,2^{n-1}-1,2^{n-1}+1,\ldots,2^n-1$. Then the result follows from Proposition 1.

3.3 Properties of state transition matrix

Proposition 3. Let $L = \delta_{2^n}[\eta_1 \ \ \eta_2 \ \cdots \ \eta_{2^n}]$ be the state transition matrix of the Boolean network representation in a linear system of an n-stage NFSR. Then the NFSR is locally stable if and only if $\eta_{2^{n-1}} = \eta_{2^n} = 2^n$.

Proof. The result follows from Theorem 1 and Lemma 3.

Theorem 3. An n-stage NFSR is globally stable if and only if there exists a positive integer $N \leqslant 2^n - 1$ such that each column of the matrix L^N is equal to $\delta_{2^n}^{2^n}$, where L is the state transition matrix of the Boolean network representation (10) in a linear system of the NFSR. In particular, an n-stage NFSR is globally stable maximum transient if and only if $N = 2^n - 1$ is the least power such that each column of the matrix L^N is equal to $\delta_{2^n}^{2^n}$.

Proof. As the equilibrium state $\mathbf{0} \in \mathbb{F}_2^n$ is uniquely corresponding to the state $\delta_{2^n}^{2^n} \in \Delta_{2^n}$, that an n-stage NFSR is globally stable to the equilibrium state $\mathbf{0}$ is equivalent to that the n-stage NFSR is globally stable to the state $\delta_{2^n}^{2^n}$. 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 $\delta_{2^n}^{2^n-1}$ (or equivalently, the state $[0 \ \cdots \ 0 \ \ 1]^{\mathrm{T}}$) must shift $2^n - 1$ times to go through all other states and finally reaches the state $\delta_{2^n}^{2^n}$ (or equivalently, the state $\mathbf{0}$) and keeps staying at this state. Therefore, $N = 2^n - 1$ is the smallest power such that each column of L^N is equal to $\delta_{2^n}^{2^n}$. Then the results follow from Lemma 6.

Assume the truth table of the feedback function f of an n-stage NFSR to be $[s_1, s_2, \ldots, s_{2^n}]$, arranged in the reverse alphabet order. Denote the structure matrix of f as $G_n = \delta_2[\omega_1 \ \ \omega_2 \ \cdots \ \omega_{2^n}]$. Then $\omega_i = 2 - s_i$ for all $i = 1, 2, \ldots, 2^n$. Thus, according to Lemma 3, the columns of the state transition matrix $L = \delta_{2^n}[\eta_1 \ \cdots \ \eta_{2^{n-1}} \ \ \eta_{2^{n-1}+1} \ \cdots \ \eta_{2^n}]$ satisfies

$$\begin{cases} \eta_i = 2i - s_i, \ i = 1, 2, \ldots, 2^{n-1}, \\ \eta_{2^{n_1}+i} = 2i - s_{2^{n_1}+i}. \end{cases} \tag{15}$$

Define a mapping

$$\rho(i) = \eta_i, \quad i = 1, 2, \ldots, 2^n. \tag{16}$$

Then the state transition matrix L and the mapping ρ are a one-to-one correspondence. Moreover, for any positive integer k, the computations of L^k from a known L are reduced to the computations of ρ^k from a known ρ.

Remark 3. Theorem 3 implies that the Boolean network approach requires lower time complexity of computations than the exhaustive search and Lyapunov direct method in [1] to determine the global stability of an NFSR with its stage greater than 1. The reason is as follows. Assume the algebraic normal form of the feedback function is known, denoted by $f(X_1, X_2, \ldots, X_n) = \sum_{i=0}^{2^n-1} a_i X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$, where $a_i \in \mathbb{F}_2$ and i is the decimal number corresponding to the binary $(i_1, i_2, \ldots, i_n)$. Then the time complexity of computing the truth table of the feedback function from its algebraic normal form is $2^n[1 + \sum_{i=1}^{d} (i+1)\binom{n}{i}]$ operations with the degree d of the feedback function. Eq. (15) shows that the time complexity of computing the state transition matrix L from the known truth table of the feedback function is 2^{n+1} operations. For any positive integer k, L^k is just a permutation of L^{k-1}, which is reduced to the computation of ρ^k from ρ^{k-1}, where ρ is in (16). Clearly, such a computation only requires some substitutions, but does not require any operations such as addition and multiplication. Moreover, at most $2^n - 1$ iterations are required to do on ρ. Therefore, totally the time complexity of computations for the Boolean network approach to determine the global stability of an n-stage NFSR is

$$C_{\mathrm{bn}} = 2^{n+1} + 2^n \left[1 + \sum_{i=1}^{d} (i+1) \binom{n}{i}\right] \tag{17}$$

operations. However, the time complexity of computations for the exhaustive search is

$$C_{\rm es} = \frac{n}{2}\,2^{2n} + n2^{n-1} + 2^n\left[1 + \sum_{i=1}^{d}(i+1)\begin{pmatrix} n \\ i \end{pmatrix}\right] \tag{18}$$

operations and the time complexity of computations for the Lyapunov direct method in [1] is

$$C_{\rm ld} = 2^{2n} + n2^{2n-1} + \sum_{j=1}^{M} 2^n|\mathcal{S}_j| + M\left[n + \sum_{i=1}^{d}(i+1)\begin{pmatrix} n \\ i \end{pmatrix}\right] \tag{19}$$

operations, where the positive integer M satisfies $1 \leqslant M \leqslant 2^n$, and $|\mathcal{S}_j|$ denotes the cardinality of the set $\mathcal{S}_j$ that is determined by the Lyapunov function constructed therein. It is seen that $C_{\rm bn}$ is smaller than $C_{\rm es}$ in the case of $n > 1$, and it is smaller than $C_{\rm ld}$ for any positive integer n.

Proposition 4. Let $L = \delta_{2^n}[\eta_1 \ \ \eta_2 \ \cdots \ \eta_{2^n}]$ be the state transition matrix of the Boolean network representation in a linear system of an n-stage NFSR. Then $\delta_{2^n}^j$, $j \in \{1, 2, \ldots, 2^n\}$, is a branch state if and only if $\eta_i = \eta_{2^{n-1}+i} = j$ with $i = \lceil \frac{j}{2} \rceil$.

Proof. *Sufficiency:* If $\eta_i = \eta_{2^{n-1}+i} = j$ with $i = \lceil \frac{j}{2} \rceil$, then $L\delta_{2^n}^i = L\delta_{2^n}^{2^{n-1}+i} = \delta_{2^n}^j$, which indicates that $\delta_{2^n}^j$ has two predecessors, $\delta_{2^n}^i$ and $\delta_{2^n}^{2^{n-1}+i}$. Hence, $\delta_{2^n}^j$ is a branch state.

Necessity: Assume $\delta_{2^n}^j$ is a branch state. According to Lemma 2, the state $\delta_{2^n}^j$ is uniquely corresponding to the state $\boldsymbol{X} = [X_1 \ \ X_2 \ \cdots \ X_n]^{\rm T} \in \mathbb{F}_2^n$ satisfying $2^{n-1}X_1 + 2^{n-2}X_2 + \cdots + X_n = 2^n - j$. The state $\boldsymbol{X}$ has two possible predecessors, $[1 \ \ X_1 \ \ X_2 \ \cdots \ X_{n-1}]^{\rm T}$ and $[0 \ \ X_1 \ \ X_2 \ \cdots \ X_{n-1}]^{\rm T}$. Suppose $\delta_{2^n}^i$ corresponds to the state $[1 \ \ X_1 \ \ X_2 \ \cdots \ X_{n-1}]^{\rm T}$. Then $\delta_{2^n}^{2^{n-1}+i}$ corresponds to the state $[0 \ \ X_1 \ \ X_2 \ \cdots \ X_{n-1}]^{\rm T}$. In other words, $\delta_{2^n}^i$ and $\delta_{2^n}^{2^{n-1}+i}$ are the two predecessors of $\delta_{2^n}^j$, which means $L\delta_{2^n}^i = \delta_{2^n}^j$ and $L\delta_{2^n}^{2^{n-1}+i} = \delta_{2^n}^j$. Hence, we deduce that the ith column and the $(2^{n-1}+i)$th column of L are equal to $\delta_{2^n}^j$, which yields $\eta_i = \eta_{2^{n-1}+i} = j$. On the other hand, according to Lemma 2, we have

$$\begin{aligned} 2^n - j &= 2^{n-1}X_1 + 2^{n-2}X_2 + \cdots + 2X_{n-1} + X_n = 2\left(2^{n-2}X_1 + 2^{n-3}X_2 + \cdots + X_{n-1}\right) + X_n \\ &= 2\left(2^n - 2^{n-1} - i\right) + X_n. \end{aligned}$$

It yields $2i = j + X_n$. Since $X_n \in \mathbb{F}_2$, we conclude that $i = \lceil \frac{j}{2} \rceil$.

Example 1. Consider two 3-stage NFSRs. The feedback functions are respectively as follows.

(a) $f(X_1, X_2, X_3) = X_1X_2 \oplus X_2X_3 \oplus X_2 \oplus X_3$;

(b) $f(X_1, X_2, X_3) = X_1X_2X_3 \oplus X_1X_2 \oplus X_1X_3 \oplus X_3$.

Computations show that the state transition matrices of the Boolean network representations of both NFSRs, respectively, are:

(a) $L = \delta_8[2\ 4\ 5\ 8\ 1\ 3\ 5\ 8]$;

(b) $L = \delta_8[2\ 4\ 5\ 8\ 1\ 3\ 6\ 8]$.

From Proposition 4, the first NFSR has two branch states, δ_8^5 and δ_8^8, while the second NFSR only has one branch state, δ_8^8. Thus, according to Lemma 7, the first has two starting states, but the second has only one starting state. It is easy to check that for the first case $N = 6$ is the least power such that each column of L^N is δ_8^8, while for the second case $N = 7$. According to Theorem 3, both NFSRs are globally stale and the second is globally stable maximum transient. All those features are consistent with their state diagrams, shown in Figure 2.

Proposition 5. Let $L = \delta_{2^n}[\eta_1 \ \ \eta_2 \ \cdots \ \eta_{2^n}]$ be the state transition matrix of Boolean network representation in a linear system of an n-stage NFSR. If the NFSR is globally stable maximum transient, then

(1) $\eta_1 = 2$ and $\eta_{2^{n-1}} = \eta_{2^n} = 2^n$;

(2) moreover, if $n \geqslant 2$, then η_i and $\eta_{2^{n-1}+i}$ are distinct and belong to the set $\{2i-1, 2i\}$ for all $i = 1, 2, 3, \ldots, 2^{n-1} - 1$.

Proof. According to Lemma 3, $\eta_i, \eta_{2^{n-1}+i} \in \{2i-1, 2i\}$ for any $i = 1, 2, \ldots, 2^{n-1}$. As a globally stable NFSR must be a locally stable NFSR, according to Theorem 1 and Lemma 3, we have $\eta_{2^{n-1}} = \eta_{2^n} = 2^n$.

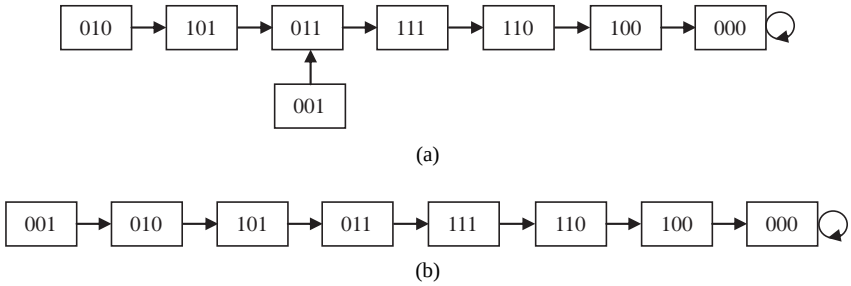

Figure 2 State diagrams of two 3-stage NFSRs in Example 1. (a) The NFSR with a feedback function in case (a); (b) the NFSR with a feedback function in case (b).

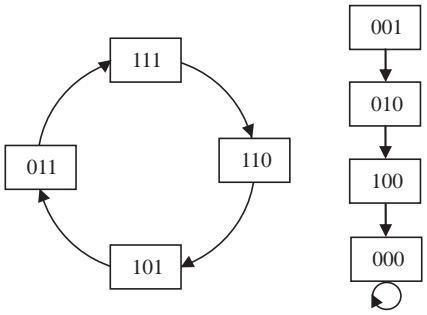

Figure 3 State diagram of a 3-stage NFSR in Example 2.

Lemmas 3 and 5 yield $\eta_1 = 2$. Then we can claim that the other η_is, $i = 1, 2, \ldots, 2^{n-1} - 1, 2^{n-1} + 1, \ldots, 2^n - 1$, are distinct in the case of $n \geqslant 2$. Otherwise, if there exist some η_is, $i \in \{1, 2, \ldots, 2^{n-1} - 1, 2^{n-1} + 1, \ldots, 2^n - 1\}$, are equal in the case of $n \geqslant 2$, then without loss of generality, we can assume $\eta_i = \eta_{2^{n-1}+i} = 2i$ for some $i \in \{1, 2, \ldots, 2^{n-1} - 1, 2^{n-1} + 1, \ldots, 2^n - 1\}$. Thus, for the two states $\delta_{2^n}^i$ and $\delta_{2^n}^{2^{n-1}+i}$, we have $L\delta_{2^n}^i = L\delta_{2^n}^{2^{n-1}+i} = \delta_{2^n}^{2i}$, which implies that the state $\delta_{2^n}^{2i}$ has two predecessors, $\delta_{2^n}^i$ and $\delta_{2^n}^{2^{n-1}+i}$. Therefore, the NFSR has a branch state $\delta_{2^n}^{2i}$ that is different to $\delta_{2^n}^{2^n}$, and it is not globally stable maximum transient, which is in contradiction with the assumption.

The inverse of Proposition 5 is not true. It can be shown by the following example.

Example 2. Consider a 3-stage NFSR with a feedback function $f = X_1X_2X_3 \oplus X_1X_2 \oplus X_1X_3 \oplus X_2X_3$. Direct computations show that the truth table of f is [0 1 1 0 1 0 0 0]. According to Lemma 3, the state transition matrix of its Boolean network representation in a linear system is $L = \delta_8[2\ 3\ 5\ 8\ 1\ 4\ 6\ 8]$. It is easy to compute that $L^7 = \delta_8[5\ 1\ 2\ 8\ 3\ 8\ 8\ 8]$. From Theorem 3, the NFSR is not globally stable maximum transient. In fact, the state diagram of the NFSR is as in Figure 3, which consists of a cycle of length 4 and a transient of length 3.

In general, we have the following result.

Proposition 6. Let $L = \delta_{2^n}[\eta_1\ \eta_2\ \cdots\ \eta_{2^n}]$ be the transition matrix of the Boolean network representation in a linear system of an n-stage NFSR. Assume

(1) $\eta_1 = 2$ and $\eta_{2^{n-1}} = \eta_{2^n} = 2^n$;

(2) moreover, if $n \geqslant 2$, then η_i and $\eta_{2^{n-1}+i}$ are distinct and belong to the set of $\{2i - 1, 2i\}$ for all $i = 1, 2, 3, \ldots, 2^{n-1} - 1$.

Then the state diagram of the NFSR must be either of the types: (1) a transient of length $2^n - 1$; (2) a transient and cycles without branch states. Moreover, the number of the possible NFSRs whose state diagrams belong to the second type is $2^{2^{n-1}-2} - 2^{2^{n-1}-n}$ in the case of $n \geqslant 2$.

Proof. Clearly, if $n = 1$, then $\eta_1 = \eta_2 = 2$, and the state diagram of the NFSR is a transient of length 1. As $\eta_1 = 2$ and $\eta_{2^{n-1}} = \eta_{2^n} = 2^n$, we conclude that $\delta_{2^n}^{2^n}$ (or equivalently, the state $\mathbf{0}$) is the only equilibrium state. Since except $\eta_{2^{n-1}} = \eta_{2^n} = 2^n$, the other η_is are distinct in the case of $n \geqslant 2$, we deduce that the NFSR is locally stable and $\eta_{2^n}^{2^{n-1}}$ is the predecessor of $\delta_{2^n}^{2^n}$. Moreover, according to Proposition 4

and Lemma 2, $\delta_{2^n}^{2^n}$ is the only branch state. From Proposition 2 and Lemma 2, $\delta_{2^n}^{2^n-1}$ is a starting state. Together considering Lemma 7, we deduce that $\delta_{2^n}^{2^n-1}$ is the only starting state. In addition, it is easy to see that such an L satisfying above conditions totally has $2^{2^{n-1}-2}$ possible forms in the case of $n \geqslant 2$. It implies that the number of possible NFSRs is $2^{2^{n-1}-2}$ for any $n \geqslant 2$, which is greater than $2^{2^{n-1}-n}$, the number of the globally stable maximum transient NFSRs in Lemma 8. Thus, in the case of $n \geqslant 2$, besides the $2^{2^{n-1}-n}$ globally maximum transient NFSRs, there must be $2^{2^{n-1}-2} - 2^{2^{n-1}-n}$ NFSRs whose state diagrams include both transient and cycles without branch states. Hence, the result follows.

Remark 4. Proposition 6 provides a method to construct all globally stable maximum transient NFSRs. We can first design all possible state transition matrices satisfying the assumptions in Proposition 6, and then use Theorem 3 to select the desired ones.

4 Conclusion

This paper considered the stability of nonlinear feedback shift registers, by viewing them as Boolean networks. Globally stable nonlinear feedback shift registers as well as locally stable nonlinear feedback shift registers were investigated. Some sufficient and necessary conditions were given for both types of nonlinear feedback shift registers. They provide a method to construct globally (locally) stable nonlinear feedback shift registers. They are also helpful to analyze the state diagram of a nonlinear feedback shift register. As Boolean networks, nonlinear feedback shift registers are subject to impulsive effects and time-delay effects, which might be interesting to be considered in the future work.

Acknowledgements

This work was supported in part by Strategic Priority Research Program of CAS (Grant No. XDA06010701), National Basic Research Program of China (973 Program) (Grant No. 2011CB302400), and National Natural Science Foundation of China (Grant Nos. 61379139, 61104075), and in part by China Postdoctoral Science Foundation Funded Project (Grant No. 2014M550100) and Department of Science and Technology of Shandong Province in China (Grant No. BS2012DX008).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Massey J L, Liu R W. Application of Lyapnunov's direct method to the error-propagation effect in convolutional codes. IEEE Trans Inf Theory, 1964, 10: 248–250
2 Laselle J, Lefschetz S. Stability by Liapunov's Direct method with Applications. New York: Academic Press, 1961
3 Mowle F J. Relations between P_n cycles and stable feedback shift registers. IEEE Trans Electron Comput, 1996, EC-15: 375–378
4 Mowle F J. An algorithm for generating stable feedback shift registers of order n. J ACM, 1967, 14: 529–542
5 Fontaine C. Nonlinear feedback shift register. In: van Tilborg H C A, Jajodia S, eds., Encryclopedia of Cryptography and Security. New York: Springer, 2011. 846–848
6 Golomb S W. Shift Register Sequences. Laguna Hills: Holden-Day, 1967
7 Qi H. On shift register via semi-tensor product approach. In: Proceedings of the 32nd Chinese Control Conference. Piscataway: IEEE Conference Publication Operations, 2013. 208–212
8 Zhong J, Lin D. On maximum length nonlinear feedback shift registers using a Boolean network approach. In: Proceedings of the 33rd Chinese Control Conference. Piscataway: IEEE Conference Publication Operations, 2014. 2502–2507
9 Zhao D, Peng H, Li L, et al. Novel way to research nonlinear feedback shift register. Sci China Inf Sci, 2014, 9: 092114
10 Kauffman S A. Metabolic stability and epigenesis in randomly constructed genetic nets. J Theor Biol, 1969, 22: 437–467
11 Harris S E, Sawhill B K, Wuensche A, et al. A model of transcriptional regulatory networks based on biases in the observed regulation rules. Complexity, 2002, 7: 23–40
12 Huang S, Ingber I. Shape-dependent control of cell growth, differentiation, and apotosis: switching between attractors in cell regulatory networks. Exp Cell Res, 2000, 261: 91–103

13 Shmulevich I, Dougherty R, Kim S, et al. Probabilistic Boolean neworks: a rule-based uncertainty model for gene regulatory networks. Bioinformatics, 2002, 2: 261–274
14 Albert R, Barabasi A L. Dynamics of complex systems: scaling laws or the period of Boolean networks. Phys Rev Lett, 2000, 84: 5660–5663
15 Aldana M. Boolean dynamics of networks with scale-free topology. Phys D, 2003, 185: 45–66
16 Samuelsson B, Troein C. Superpolynomial growth in the number of attractots in Kauffman networks. Phys Rev Lett, 20003, 90: 098701
17 Cheng D. Input-state approach to Boolean networks. IEEE Trans Neural Netw, 2009, 20: 512–521
18 Cheng D. Disturbance decoupling of Boolean control networks. IEEE Trans Automat Control, 2011, 56: 2–10
19 Cheng D, Qi H. Linear representation of dynamics of Boolean networks. IEEE Trans Automat Control, 2010, 55: 2251–2258
20 Cheng D, Qi H. State-space analysis of Boolean networks. IEEE Trans Neural Netw, 2010, 21: 584–594
21 Cheng D, Qi H, Li Z. Analysis and Control of Boolean networks. London: Springer-Verlag, 2011
22 Zhong J, Lu J, Huang T, et al. Synchronization of master-slave Booleannet works with impulsive effects: necessaryand-sufficient criteria. Neurocomputing, 2014, 143: 269–274
23 Chen H, Sun J. A new approach for global controllability of higher order Boolean control network. Neural Netw, 2013, 39: 12–17
24 Wang Y, Li H. On definition and construction of Lyapunov functions for Boolean networks. In: Proceeding of the 10th World Congress on Intelligent Control and Automation. Piscataway: IEEE Conference Publication Operations, 2012. 1247–1252
25 Cheng D, Qi H, Li Z, et al. Stability and stabilization of Boolean networks. Int J Robust Nonlinear Contr, 2011, 21: 134–156
26 Li F, Sun J. Stability and stabilization of multivalued logical network. Nonlinear Anal-Real World App, 2011, 12: 3701–3712
27 Li F, Sun J. Stability and stabilization of Boolean networks with impulsive effects. Syst Control Lett, 2012, 61: 1–5
28 Liu Y, Lu J, Wu B. Some necessary and sufficient conditions for the output controllability of temporal Boolean control networks. ESAIM Control Optim Calc Var, 2014, 20: 158–173
29 Zhong J, Lu J, Liu Y, et al. Synchronization in an array of output-coupled Boolean networks with time delay. IEEE Trans Neural Netw Learn Syst, 2014, 25: 2288–2294
30 Roger A H, Johnson C R. Topics in Matrix Analysis. Cambridge: Cambridge University Press, 1991
31 Qi H, Cheng D. Logic and logic-based control. J Contr Theory Appl, 2008, 6: 123–133
32 Cheng D, Qi H, Zhao Y. An Introduction to Semi-tensor Product of Matrices and its Applications. Singapore: World Scientific Publishing Company, 2012