Stability of (n,k) Nonlinear feedback shift registers

Meilin Li, Jianquan Lu, Tingwen Huang, Jinde Cao *Fellow, IEEE*

***Abstract*—In this paper, the (n,k) nonlinear feedback shift registers (NFSRs) are regarded as a Boolean network (BN). Semi-tensor product (STP) of matrices is used to convert (n,k) NFSRs into an equivalent algebraic equation. Based on STP of matrices, a novel way is proposed to study stability of (n,k) NFSRs and the period of (n,k) NFSRs. Firstly,**

***Index Terms*—(n,k) NFSRs, stability, semi-tensor product, Boolean network**

I. INTRODUCTION

Information security is very important for our society. There are many confidential information about financial status, research, products for different organizations. In order to protect the confidential information from leakage, the stream cipher has been widely used in encryption. The main building blocks of stream cipher is nonlinear shift registers (NFSR). NFSR can produce pseudo-random sequences.

There are two types of NFSR: (1) Fibonacci NFSR; (2) Galois NFSR. Fibonacci NFSR is shown in Fig.1. Fibonacci NFSR consists n binary storage elements from left to right as $n-1,n-2,...,1,0$. Every i-th $0 \le i \le n-2$ bit is update their values by the value of $(i+1)$-th bit, and the value of $(n-1)$-th bit is updated by feedback function f depending on values of bits of $0,1,...,n-1$.While the Galois NFSR shown in Fig.2 is different from Fibonacci NFSR. In Galois NFSR, the value of every bit is updated by it's own feedback function which at most relate to every bit.

In order to improve the speed of output sequence generation, E. Dubrova proposed a new type of NFSR named (n,k) NFSR in [1]. An (n,k) NFSR can be considered as a generalization of the Galois NFSR. In an (n,k) NFSR, every bit is updated by a feedback function, which is a nonlinear function relating to value of $(i+1)mod\ n$-th bit and up to values of $k-1$ other bits.

II. PRELIMINARIES

In this section, we first review the STP of matrices briefly. Then the multi-linear form of nonlinear Boolean function

This work was supported by the National Natural Science Foundation of China under Grant No. 61573102, and China Postdoctoral Science Foundation under Grant No. 2014M560377 and 2015T80483, and Jiangsu Province Six Talent Peaks Project under Grant 2015-ZNDW-002.

Meilin Li is is with the Department of Mathematics, Southeast University, Nanjing 210096, China 220151318@seu.edu.cn

Jianquan Lu is with the Department of Mathematics, Southeast University, Nanjing 210096, China, and also with the Potsdam Institute for Climate Impact Research, Telegraphenberg, D-14415 Potsdam, Germany jqluma@seu.edu.cn; jqluma@gmail.com

Tingwen Huang is with Texas AM University at Qatar, Dc/o Qatar Foundation, PO Box 5825, Doha, Qatar

Jinde Cao is with the Department of Mathematics, Southeast University, Nanjing 210096, China jdcao@seu.edu.cn

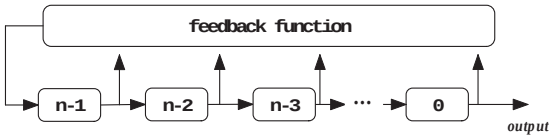

Fig. 1: The Fibonacci NLFSR

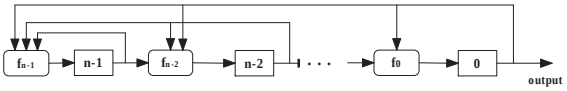

Fig. 2: The Fibonacci NLFSRs

that is obtained by using the semi-tensor product is recalled. Finally, we regard (n,k) NFSRs as a BN. Based on STP, (n,k) NFSRs are converted into a multi-linear forms. We first give some notations used in this paper.

- $\mathscr{D} = \{0,1\}$.
- I_n : the identity matrix of dimension n.
- $\delta^i_{2^n}$: the i-th column of identity matrix I_n.
- $\Delta_{2^n} = \{\delta^i_{2^n} | i = 1,2,3,...,2^n\}$.
- $\mathscr{L}_{n\times m}$: the set of $n\times m$ matrices, whose column belong to Δ_n. For a matrix $L \in (L)_{n\times m}$, and $L = [\delta^{i_1}_n\ \delta^{i_2}_n\ ...\ \delta^{i_m}_n]$, we write $L = \delta_{2^n}[i_1\ i_2\ ...\ i_m]$ for simplicity.
- $col_i(L)$: the i-th column of matrix L.
- $col(L)$: the set of all column of matrix L.
- $\mathbb{R}$: the set of all real number.
- N : the set of all integers.

A. Semi-tensor product of matrices

In this subsection, the definition of STP is given. The the multi-linear form of nonlinear Boolean function is obtained by using the semi-tensor product.

Definition 1: [2] Let $A \in \mathbb{R}^{n\times m}$, $B \in \mathbb{R}^{p\times q}$. The *semi-tensor product* of A and B is defined as:

$$A \ltimes B = (A \otimes I_{\frac{l}{m}})(B \otimes I_{\frac{l}{p}}) \tag{1}$$

where l is the least common multiple of m and p.

Obviously, if $m = p$ in Definition **??**, then the STP of A and B is reduced to their conventional matrix product AB.

We identify $\Delta_2 \sim \mathscr{D}$ i.e $(\delta^1_2 \sim 1, \delta^2_2 \sim 0)$, and $\delta^1_2(\delta^2_2)$ is called the vector form of logical value $1(0)$.

Lemma 1: [2] Any Boolean function $f(x_1,x_2,...,x_n)$ with variables $x_1,x_2,...,x_n \in \Delta_2$ can be expressed as a multi-linear form:

$$f(x_1,x_2,...,x_n) = Fx_1 \ltimes x_2 \ltimes ... \ltimes x_n. \tag{2}$$

where $F \in \mathscr{L}_{2\times 2^n}$ is called the *structure matrix* of f, and F can be uniquely expressed as

$$F = \begin{bmatrix} s_1 & s_2 & ... & s_{2^n} \\ 1-s_1 & 1-s_2 & ... & 1-s_{2^n} \end{bmatrix} \tag{3}$$

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

In the following, we omit the symbol $\ltimes$ for simplicity.

B. (n,k) NFSRs

A (n,k) NFSRs consist of n binary memory device called bits. The output of a (n,k) NFSRs is the value of the 0-th bit. A (n,k) NFSRs is defined as follows. Let $x_i(t)$ be state variables representing the states at time t of the i-th bit. Let $f_i : \mathscr{D}^k \to \mathscr{D}$, $1 \le k \le n$, be the next state function of the i-th bit. The boolean function f_i depends on the bit $(i+1) mod\ n$ and up to $k-1$ other bits. Assume the indexes of other $k-1$ bits relating to function f_i are $i_1, i_2, ..., i_{k-1}$, $i_j \in \{0,1,...,n-1\}$, $j \in 1,2,...,k-1$, then the next state function of i-th bit can be expressed as follows:

$$x_i(t+1) = f_i(x_{(i+1)mod\ n}(t), x_{i_1}(t), ..., x_{i_{k-1}}(t)). \tag{4}$$

So a (n,k) NFSRs can be described as a BN shown as follows:

$$\begin{cases} x_0(t+1) = f_0(x_1, x_{0_1}, x_{0_2}, ..., x_{0_{k-1}}), \\ x_1(t+1) = f_1(x_2, x_{1_1}, x_{1_2}, ..., x_{1_{k-1}}), \\ \vdots \\ x_{n-1} = f_{n-1}(x_0, x_{n-1_1}, x_{n-1_2}, ..., x_{n-1_{k-1}}) \end{cases} \tag{5}$$

By using Lemma 1, we can obtain that $x_i(t+1) = F_i \ltimes_{i=0}^{n-1} x_i(t)$, where $F_i \in \mathscr{L}_{2\times 2^n}$, then the BN (5) can be converted into following system:

$$x(t+1) = Lx(t), t \in N, \tag{6}$$

where $x(t) = x_0(t) \ltimes x_1 t \ltimes ... \ltimes x_{n-1}(t) \in \Delta_{2^n}$ is the state at time t, and $L \in \mathscr{L}_{2^n \times 2^n}$, $col_i\{L\} = \ltimes_{i=0}^{n-1} col_i\{F_i\}$.

Definition 2: 1) A state $x_0 \in \Delta_{2^n}$ is a *equilibrium state* of (n,k) NFSRs (6), if $Lx_0 = x_0$.

2) $x_0, Lx_0, ..., L^p x_0$ is called a cycle of (n,k) NFSRs (6) with length p, if $L^p x_0 = x_0$, and the elements in set $x_0, Lx_0, ..., L^p x_0$ are distinct.

Let $R(x)$ denote the set of states which can reach state x. Let $R^k(x)$ denote the set of states which can reach state after k steps.

Next, we give the definition of *globally stable* and *locally stable*.

Definition 3: An (n,k) NFSR (6) is *globally stable* to the equilibrium state $\delta_{2^n}^i \sim (i_0, i_1, ..., i_{n-1})$, if for any state $x \in \Delta_{2^n}$, there exist a positive integer N such that $L^N x = \delta_{2^n}^i$.

Definition 4: An (n,k) NFSR (6) is *locally stable* to the equilibrium state $\delta_{2^n}^i \sim (i_0, i_1, ..., i_{n-1})$, if there exist some states $x \in \Delta_{2^n} \setminus \delta_{2^n}^i$, such that $L^N x = \delta_{2^n}^i$ for some positive integer N.

III. MAIN RESULTS

In this section, the stability of system (6) is firstly investigated. Then the period of output sequence of system (6) is studied.

A. Stability of (n,k) NFSRs

Clearly, in a (n,k) NFSRs, the equilibrium state can be any state, assume the equilibrium state of (n,k) NFSRs is $\delta_{2^n}^i \sim (i_0, i_1, ..., i_{n-1})$. If the value of j-th bit of equilibrium state is 1, we can make a coordinate transformation

$$[\mathbf{?}]y_j = \neg x_j, \tag{7}$$

The system (6) is converted into a system with equilibrium state $\delta_{2^n}^{2^n} \sim (0,0,...,0)$ as follows:

$$y(t+1) = \bar{L} y(t), \tag{8}$$

where $y(t) = \ltimes_{i=0}^{n-1} y_i(t)$. Then equilibrium state of system (8) is $\delta_{2^n}^{2^n} \sim (0,0,...,0)$.

Since the form of system (6) is similar to the form of system in [3], we can obtain the same result about the global stability of system (6).

Theorem 1: (n,k) NFSR (8) is globally stable to state $\delta_{2^n}^{2^n}$ if and only if there exist a positive integer $1 \le N \le 2^n - 1$ such that $col(L^N) = \delta_{2^n}^{2^n}$.

From Theorem 1, we can obtain the following corollary.

Corollary 1: (n,k) NFSR (8) is globally stable to $\delta_{2^n}^{2^n}$, if and only if $R(\delta_{2^n}^{2^n}) = \Delta_{2^n}$.

Remark 1: (n,k) NFSR is globally stable to $\delta_{2^n}^{2^n}$, then for any state, it can reach state $\delta_{2^n}^{2^n}$ at most 2^n steps.

In the following, we will give an algorithm to decide if an (n,k) NFSR is globally stable.

B. The period of output sequence of (n,k) NFSRs

In this subsection, the period of output sequence of (n,k) NFSRs is investigated.

In [1], E.Dubrova *et al.* proposed that the

Theorem 2: If the period of a cycle $\mathscr{C} = \{e_0, e_1, ..., e_{p-1}\}$ of (n,k) NFSRs is p, then the period of output sequence of e_i, $0 \le i \le p-1$ is one of the divisors of p.

Proof:

■

Now, we give a algorithm to compute the period of output sequence of a initial state of (n,k) NFSRs.

C. The period of synthesis of (n,k)-NFSRs by composition

In this subsection, in order to increase the period of (n,k) NFSR, a method is provided in [1]. In [1], they construct an (n,k) NFSR with guaranteed long period by composing several smaller NFSRs working in parallel and combining their output using operator $\oplus$.

let $N_1, N_2, ...N_m$ be $(n_1,k_1), (n_2,k_2), ..., (n_m,k_m)$ NFSR respectively. Let R be an (n,k) NFSR composed by $N_1, N_2, ...N_m$, where $n = n_1 + n_2 + ... + n_m$, and $k = max\{k_1, k_2, ..., k_m\}$. Let C_i denote the number of N_i's cycles. Let L_{ij} denote period of the j-th cycle l_{ij} of states in N_i, $i \in \{1,2,...,m\}$, $j \in \{1,2,...,C_i\}$. The new composed (n,k) NFSR can be expressed as a BN as

following:

$$\begin{cases} x_i(t+1) = f_i(x_{(i+1)mod\ n}, x_{i_1}, ..., x_{i_{k_1-1}}), 0 \le i \le n_1, \\ x_i(t+1) = f_i(x_{(i+1)mod\ n}, x_{i_1}, ..., x_{i_{k_2-1}}), n_1 \le i \le n_1+n_2-1, \\ \vdots \\ x_i(t+1) = f_i(x_{(i+1)mod\ n}, x_{i_1}, ..., x_{i_{k_m-1}}), \sum_{j=1}^{m-1} n_j \le i \le \sum_{j=1}^{m} n_j - 1, \end{cases} \tag{9}$$

Let $y(t)$ denote the output of (n,k) NFSR at time t, it can be expressed as follows:

$$y(t) = x_0(t) \oplus x_{k_1}(t) \oplus x_{k_1+k_2} \oplus ... \oplus x_{\sum_{j=1}^{m-1} k_j}. \tag{10}$$

By using Lemma 1, equation (10) can be expressed as follows:

$$y(t) = Hx(t), \tag{11}$$

where $x(t) = \ltimes_{i=0}^{n-1} x_i(t) \in \Delta_{2^n}$, $H \in \mathscr{L}_{2\times 2^n}$.

Lemma 2: The new composed (n,k) NFSR, the cycle of states can be composed by $l_{1i_1}, l_{2i_2}, ..., l_{mi_m}$, and the period of composed cycle is $lcm\{L_{1i_1}, L_{2i_2}, ..., L_{mi_m}\}$.

IV. EXAMPLES

V. CONCLUSION

REFERENCES

[1] E. Dubrova, M. Teslenko, and H. Tenhunen, "On analysis and synthesis of (n,k)-non-linear feedback shift registers," *Design Automation & Test in Europe*, pp. 1286–1291, 2008.

[2] D. Cheng, H. Qi, and Z. Li, *Analysis and Control of Boolean Networks*. Springer London, 2011.

[3] J. Zhong and D. Lin, "Stability of nonlinear feedback shift registers," in *IEEE International Conference on Information and Automation*, pp. 671–676, 2014.